Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

LUIZ HENRIQUE SENA E MESQUITA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO PARA UMA EMPRESA DE PLANO DE SAÚDE AMBULATORIAL

Brasília

2015

LUIZ HENRIQUE SENA DE MESQUITA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO PARA UMA EMPRESA DE PLANO DE SAÚDE AMBULATORIAL

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Mestre Gilberto de Oliveira Netto

Brasília
2015

LUIZ HENRIQUE SENA DE MESQUITA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO PARA UMA EMPRESA DE PLANO DE SAÚDE AMBULATORIAL

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu em* Redes de Computadores com Ênfase em Segurança.

Orientador: Mestre Gilberto de Oliveira Netto

Brasília, ___de _____de 2015.

Banca Examinadora

Prof. Dr. Nome completo

Prof. Dr. Nome completo

RESUMO

No cenário atual todas as empresas precisam da tecnologia para poder gerir o negócio, seja, armazenando dados, realizando consultas ou fazendo transações, pode-se dizer que todas estão sujeitas a ataques cibernéticos ou até mesmo ataques por meio de engenharia social. Visando mitigar a perda de ativos e garantir uma maior segurança, as empresas precisam desenvolver uma política de segurança da informação, onde descreve o que deve ser feito e o que não pode ser feito, levando em consideração os pilares da segurança de informação. O trabalho explica os porquês de ter uma política de segurança da informação, e esclarece as etapas de criação e divulgação. Baseando em uma experiência real, onde foi realizado uma análise de uma organização do ramo de plano de saúde ambulatorial, e elaborado uma política de segurança da informação, que por mais que tenha sido desenvolvida para uma empresa especifica, pode ser utilizada como modelo para qualquer outra organização.

ABSTRACT

In Current Scenario All businesses need as Technology to Power Manage Business, BE, storing data, Performing Queries UO Making Transactions, we CAN Say That All are subject to cyber attacks or even attacks through social engineering. To mitigate the loss of assets and ensure greater security, as companies need to develop a Security Policy Information, Where describes what should be done and What CAN NOT be done, taking into account the Pillars of Information Security. The work explains the whys of having a Security Policy Information and clarifies how STAGES Creation and Dissemination. Based on a real experience, Where was Held An Analysis of an Organization of outpatient health plan type, and Prepared An Information Security Policy, que BY More that has been developed paragraph A Specific Company, can be used as paragraph model any another Organization.

SUMÁRIO

INTRODUÇÃO

Nos dias atuais à informação está cada vez mais acessível, já que temos uma vasta variedade de aparatos eletrônicos, que nos possibilitam uma navegação rápida e fácil, e junto com essa facilidade vem o aumento de usuários, que deixam as rotinas manuais de lado para viver no mundo cibernético.

No ramo dos negócios, a tecnologia está mais do que envolvida, passou a ser uma ferramenta fundamental para uma empresa que busca vencer em qualquer área que esteja ingressando, pois precisa de equipamentos para realizar cálculos, organizar agendas, gerar planilhas e entre outras tarefas, sendo que por de traz destas tarefas está uma muito importante, que é o armazenamento de informação. Guardar a informação, ter ela para futuro acesso é o que a tecnologia traz de mais fundamental para uma organização, é essa informação que mantem uma empresa ativa, portanto a informação é um dos ativos mais importantes para uma organização. E já que este item possui tanta relevância, ele precisa ter uma segurança aceitável.

Portanto o presente trabalho visa esclarecer a importância de se desenvolver uma política de segurança da informação para uma empresa, pegando como exemplo uma empresa do distrito federal, do ramo de planos de saúde ambulatorial. Vale citar que esta empresa, conta com alguns departamentos peculiares, como um *CallCenter* e um setor de vendas, portanto certas informações ficarão expostas para consultas, e com isso se faz necessário por parte da alta administração, tomar algumas medidas de prevenção, como mostrar para os colaboradores algumas diretrizes de como se deve comportar no ambiente de trabalho. Além destes setores peculiares, temos a grande taxa de processos que ocorrem diariamente, processos estes que geram transferências de dados.

Com isso este trabalho irá expor a importância da informação para a empresa, e mostrar como desenvolver um documento que guie os usuários de modo que traga segurança às informações e aos recursos de TI, documento este denominado como Política de Segurança da Informação.

Sabendo da importância deste documento, é necessário saber entender como proceder no desenvolvimento e é neste ponto que o trabalho irá focar,

esclarecendo os pontos que precisam ser utilizados como parâmetros, e apresentando um modelo de política da informação, que pode ser utilizado para desenvolver outros para qualquer outro tipo de organização.

O trabalho foi estruturado em 4 sessões, o primeiro relata a importância da informação para uma organização e a mostra que a tecnologia é um ponto essencial que determina onde a empresa pode chegar, o segundo capitulo traz os tópicos relatados no primeiro, mas focando na empresa de exemplo, mostrando algumas peculiaridades, já o terceiro explica o que é uma política de segurança da informação, mostrando o que é necessário conhecer e fazer antes de começar a desenvolver o documento. Na quarta sessão o trabalho toma a forma do modelo de documento, mostrando os tópicos que devem ser citados e possíveis regras e normas que ao serem seguidas, guardam a segurança do ativo informação.

1 INFORMAÇÃO E TECNOLOGIA NO AMBITO ORGANIZACIONAL

Toda empresa, independente do seguimento escolhido, precisa gerir e armazenar informações. E as que almejam um crescimento significativo, precisam dar a devida importância para este item, sendo ele dados de clientes, segredo de produtos produzidos, ou novos conhecimentos adquiridos sobre o mercado atual, e uma das preocupações que se deve ter com a informação é o modo como ela é gerida dentro da organização, já que dependendo do tipo dos dados, o vazamento pode causar prejuízos catastróficos.

1.1 A importância da informação

Há vários tipos de informações que uma organização pode adquirir, podendo ser dados cadastrais de clientes, informações financeiras, atualidades do mercado, entre outros. Mas o que se deve ter como verdade é que “A informação assume atualmente uma importância crescente, sendo um diferencial de sucesso.” (Fernando Brum, 2011).

Dentre os tipos de informação que uma empresa pode conter, existem alguns que não podem ser divulgados, e outros que devem ser consultados por indivíduos devidamente autenticados.

Dentro dos dados que não podem ser divulgados, estão as informações que segundo OLIVEIRA (2012), auxiliam no processo decisório, pois quando devidamente estruturada é de crucial importância para a empresa, determinando o caminho correto a seguir, para alcançar o objetivo em foco. Já os dados que precisam ser consultados, por exemplo, uma conta de um cliente acessada via um portal na web, precisa de uma segurança e disponibilidade adequada, e implantando estes itens, a organização ganha uma boa reputação, podendo ser encarada como um diferencial na escolha dos clientes.

Mas para que seja possível o gerenciamento deste bem tão importante, é indispensável à utilização da tecnologia já que não é viável a utilização de papelada

para armazenar dados e a questão da disponibilidade junto com a comodidade de acesso aos dados não se pode tornar possível sem os meios eletrônicos.

1.2 Utilização da tecnologia

Nos dias atuais, a tecnologia está em todos os lugares, e principalmente para as empresas, se tornou um item crucial, sendo utilizada na produção de seus produtos ou realização de suas tarefas. Mas um dos processos mais importantes que a tecnologia ajuda a entregar é o gerenciamento das informações, sendo que para armazenar, consultar e proteger os dados, é indispensável o uso de sistemas e computadores.

Um dos motivos da tecnologia ter se tornado primordial para uma instituição de negócios é a mudança cultural da sociedade mundial, que está muito mais exigente, querendo mais comodidade e qualidade nos produtos adquiridos. E para entregar estes itens, se faz totalmente necessário à utilização de sistemas, que por sua vez estão se adaptando e atualizando a cada dia, visando o aprimoramento e inovação.

Dada a importância da utilização dos aparatos eletrônicos para a sobrevivência e crescimento da organização, é necessário salientar que os operadores também precisam estar treinados e cientes de como utilizar tais mecanismos. Porque do mesmo modo que a tecnologia entrega comodidade e organização, traz também pontos vulneráveis, que quando não se é tomado os devidos cuidados, podem gerar prejuízos incalculáveis.

2 UTILIZAÇÃO DA INFORMAÇÃO E TECNOLOGIA EM UMA EMPRESA DE PLANO DE SAUDE AMBULATORIAL

A importância da informação e da tecnologia é igual para todas as empresas, mas também cada uma utiliza destes itens de seus modos peculiares.

E dentro de uma organização do âmbito de plano de saúde com cobertura ambulatorial, a informação armazenada contém dados de clientes, utilizações e dados financeiros. Já a tecnologia deve entregar armazenamento confiável e acesso fácil e seguro aos dados.

2.1 Informações gerenciadas

Uma empresa que segue este ramo de negócios precisa armazenar uma série de dados críticos, se tornando extremamente dependente destas informações. Também existe a preocupação com o acesso rápido e fácil internamente e externamente, já que à necessidade de utilização em pontos fora da sede.

O motivo de categorizar a informação como crítica, se deve ao fato dos dados pertencerem a clientes, contendo dados pessoais, como informações bancárias, além disso, existem as informações relacionadas a pagamento de prestadores de serviço, que realização as consultas e exames nos clientes do plano.

Dentre as informações armazenadas estão:

- Dados cadastrais de clientes;
- Dados cadastrais de prestadores de serviço;
- Informação de pagamento de mensalidades;
- Informação de pagamento de prestadores;
- Informação de utilização de clientes;
- Pedidos de autorização;

Além de armazenar estes dados, a empresa deve disponibilizar as informações para os prestadores e clientes, para que sejam acessados externamente. Essa necessidade de acesso é importante porque o prestador precisa consultar os dados do paciente antes de realizar o atendimento.

E além de disponibilizar para acesso, é de extrema importância garantir a segurança dos dados, porque o vazamento de informações dos clientes ou prestadores para pessoas não autenticadas pode causar sérios danos para a organização.

2.2 Tecnologia utilizada

Como informado, os dados devem ser armazenados com segurança e consultados com agilidade, garantindo a integridade e disponibilidade. Para isso é necessário à utilização de sistemas adaptados para este ramo de atividade.

Para entregar o serviço contratado pelo cliente, os sistemas devem garantir:

- Inserção de dados cadastrais;
- Armazenamento dos dados;
- Backup dos dados;
- Portal de acesso para os Prestadores;
- Portal de acesso para os Clientes;
- Gestão financeira integrada;
- Emissão de guias de serviço;
- Geração de relatórios gerenciais;
- Registro de atendimentos SAC;

Além de um sistema para gerenciar estes itens, é necessária uma rede de computadores, com alguns servidores, onde exista uma zona desmilitarizada (*DMZ*) para a hospedagem dos portais.

A rede da sede deve conter alguns itens para entregar o resultado esperado, cada item possui a sua importância, dentre estes itens estão:

a) Microcomputadores

Para que os funcionários realizem as tarefas internas, como: (gestão financeira, atendimento SAC, cadastro de contratos, auditoria de pedidos, checagem de contratos, analise de contas medicas)

b) Servidores

São necessários alguns servidores para gerenciar e armazenar dados, os serviços necessários são: (armazenamento de dados, banco de dados, correio eletrônico, *firewall*, aplicação *web*, aplicação interna, gerenciados de domínio, *backup*)

Mas para que estes itens possam entregar o resultado esperado, é necessária uma utilização adequada dos recursos. Portanto os operadores devem seguir determinadas normas de segurança e zelar pelos recursos disponibilizados para exercerem suas tarefas. Tendo este cenário em mente e compreendendo que o funcionamento adequado, depende de uma boa utilização, se faz necessário estabelecer um conjunto de controles, implantando regras e normas de acesso e utilização dos recursos de TI, um dos primeiros passos a seguir segundo Diana Paula (2013), é elaborar e aprovar uma Política de Segurança da Informação (PSI).

3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para começar a implantar uma gestão de segurança, é necessário desenvolver uma política de segurança da informação, este é um conjunto de regras onde são estabelecidos os processos que devem ser realizados e o enfatizado o que não é recomendado fazer, sempre buscando zelar pelos recursos de tecnologia da informação (TI) e garantir a integridade, disponibilidade, confidencialidade e autenticidade das informações armazenadas.

3.1 Princípios da gestão de segurança

Antes de começar a implantar uma gestão de segurança, é indispensável ter o conhecimento pleno dos princípios da segurança da informação, sendo eles: (autenticidade, confidencialidade, integridade e disponibilidade).

3.1.1 *Autenticidade*

Este pilar da segurança visa garantir que a informação passada é de fato procedente da origem alegada, segundo Spanceski (2004) o controle de autenticidade está associado com a identificação do computador ou utilizador.

Segundo Spanceski (2004), “A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos”.

3.1.2 *Confidencialidade*

A confidencialidade busca proteger a informação contra acessos não autorizados, sendo eles internos ou externos. Os dados não podem ser lidos ou copiados por alguém cujo não possua autorização adequada.

Essa proteção é independente do modo de armazenamento da informação, sendo ela por mídia impressa ou digital. Portanto seguindo a linha de pensamento de Dias (2000) a confidencialidade deve proteger as informações contra o acesso de qualquer pessoa não explicitamente autorizada, isto é, as informações e processos são liberados apenas a pessoas autorizadas.

3.1.3 *Integridade*

A integridade consiste em proteger os dados contra modificações não autorizadas. Estas modificações incluem alteração de status, remoção e alteração de conteúdo. Segundo Carneiro (2002), a integridade é a proteção dos dados com o objetivo de não serem alteradas ou apagadas sem que se tenha a autorização explicita do proprietário.

3.1.4 *Disponibilidade*

Garante que os acessos autorizados a informações e recursos não fiquem indisponíveis. Protegendo os dados e recursos de maneira que o acesso fique com status ativo sempre que for requisitado, sendo chamado também de continuidade de serviço.

3.2 Análise de riscos

Quando uma organização começa a elaborar uma política de segurança da informação, ela vê a necessidade de realizar algumas atividades antes de desenvolver a política propriamente dita.

Alguns destes itens a serem elaborados antes da PSI, é o relatório de análise de riscos. Neste passo é realizada uma verificação geral dos processos da empresa, buscando:

a) Identificar

Analisar e listar as informações, processos, equipamentos, pessoas e os seus riscos existentes dentro da organização, para tentar estimar o impacto que um desastre pode causar, para poder identificar os riscos, pode-se seguir:

- Experiências passadas;
- Boas práticas;
- Consultoria externa;
- Banco de dados;

b) Classificar

Com a identificação de informações e riscos disponível, o próximo passo é classificar as informações existentes dentro da organização, visando priorizar no momento de elaborar as medidas de controle. Os itens identificados são classificados como impacto (alto, médio, baixo) de acordo com a importância de cada ativo.

c) Controlar

Neste item, são criadas as medidas de controle, aceitação e mitigação. Outro ponto desenvolvido neste tópico, é a referência ao responsável pelo controle de cada risco listado, colocando o prazo de resolução e o responsável pela ação.

3.3 Características

Além do embasamento da análise de riscos, e o entendimento dos pilares da segurança, para elaborar uma política de segurança, deve-se ter o conhecimento pleno da organização e de seus processos.

Para isso é necessário ter em mente o objetivo central da empresa e entender o passo a passo de cada processo, compreendendo o funcionamento de cada setor, visando encontrar melhorias para a segurança dos ativos. Mas antes de avaliar e analisar a organização como um todo, é necessário conseguir apoio da diretória, para garantir que a política seja bem vista e aceita.

Garantindo o apoio da diretória, o próximo passo é listar todos os ativos da organização, sendo eles internos e externos, entender os pontos chaves dos processos, e desenvolver regras a serem cumpridas, de modo que estabeleça um padrão dentre os processos realizados, garantindo um alto nível de segurança, zelando pelos recursos de TI e pelas informações contidas dentro da organização.

O documento elaborado deve ser redigido com uma linguagem simples e de fácil entendimento, já que o público alvo abrange toda a organização, passando pelo setor de limpeza chegando até a alta cúpula da administração. A política deve começar esclarecendo o objetivo, deixando claro que todos os usuários devem seguir as regras citadas, estando passiveis a punições, sempre visando garantir a boa utilização dos recursos entregues pelo TI, sendo eles: (microcomputadores, impressoras, diretórios de armazenamento de dados, sistemas, correio eletrônico, entre outros recursos de informática). Portanto os itens citados dentro do documento são tanto sistemas, equipamentos como boas práticas de comportamento.

Após o desenvolvimento do documento, deve-se realizar uma apresentação do mesmo para todo o corpo de funcionários da empresa, porque a divulgação e tão importante quando a própria política de segurança, sendo que para cobrar a adaptação e cumprimento dos itens descritos no documento, o mesmo deve ser conhecido e esclarecido.

Para que a divulgação seja realizada da maneira correta, o departamento de recursos humanos deve estar altamente comprometido com o processo de apresentação, já que todos os funcionários principalmente os novos, devem passar por apresentações e treinamentos de como realizar e de quais cuidados devem tomar em determinadas situações durante a rotina do trabalho. Além do cuidado

com a divulgação o processo de implantação da PSI, não fica estagnado, sendo que a todo o momento os recursos de TI passam por atualizações, e novos processos são incorporados na rotina da organização, e com isso novos meios de ataques são desenvolvidos, com isso o setor de TI deve buscar uma melhoria continua nas rotinas, buscando se prevenir.

4 PROCESSO DE DESENVOLVIMENTO

Compreendendo o que deve ser levado em consideração ao desenvolver uma política de segurança da informação, uma empresa do âmbito de plano de saúde ambulatorial, precisa compreender a importância de manter seguro os dados dos clientes, e garantir a disponibilidade do serviço a todo o momento.

Portanto antes de desenvolver a política em si, a equipe responsável, deve realizar o levantamento de todos os ativos da organização, e os riscos que os mesmos estão passiveis de sofrer. Como dito, deve-se desenvolver a análise de riscos, para após começar a desenvolver as boas práticas a serem seguidas pela organização.

Para esclarecer um pouco melhor as etapas de elaboração de uma PSI, será utilizado um exemplo real onde foi elaborado um documento para a organização exemplo

4.1 Análise da empresa e seus riscos

Para realizar a análise da organização como um todo e os riscos nos quais os ativos estavam expostos, não foi necessário dedicar muitos dias durante a elaboração, sendo que o cargo ocupado (Coordenador do setor de Tecnologia) proporcionou ao funcionário a experiência necessária, tendo em vista que a cada problema ocorrido, o mesmo esteve presente para garantir a correção, e buscar uma solução para evitar novos incidentes.

Dentre os alguns itens que identificados como importantes para utilizar de base na elaboração da política estão:

a) Utilização de ativos / Segurança da rede

Está relacionado com a má utilização dos recursos de rede disponíveis, como o armazenamento inadequado de arquivos nos diretórios de rede compartilhados, onde houve situações em que vários arquivos de músicas foram identificados dentro das pastas alocadas na rede, ou até mesmo

arquivos antigos que não possuem mais serventia, mas estavam ocupando espaço no diretório público, poluindo a lista de arquivos e deixando o disco com pouco espaço.

Outro caso sobre a utilização da rede está na questão da utilização dos LOGIN, já que ocorreu de algumas vezes determinadas ações estarem registradas como uma determinada pessoa, mesmo ela não estando no serviço naquele momento, situação originada porque o usuário passou a senha ou esqueceu o sistema logado na conta dele.

E para tentar mitigar estes casos existe algumas ações que podem ser tomadas, como criar uma regra de manutenção dos diretórios e alertar o usuário sobre a importância de manter a senha em sigilo, deixando claro que se for pego tentando utilizar o login de outra pessoa, ele está sujeito a punições.

b) Controle de acesso

Este tópico tem a visão de esclarecer aos funcionários o direito de possuir uma login e senha, junto com uma conta de e-mail e um diretório pessoal alocado na rede, e mostrar como deve ser realizada a solicitação de conta e permissões. Este item se torna importante, porque houve várias situações onde o acesso ao sistema ou alguma permissão não estava de acordo, e como o setor de TI não tem como monitorar as contratações da empresa, deve-se estabelecer a responsabilidade para o coordenador da equipe onde o funcionário está alocado.

Tendo em vista a importância da senha, o funcionário tem o dever de manter a mesma em sigilo, além de periodicamente altera-las, não utilizando fáceis combinações e além de mostrar o que se deve fazer, é importante documentar a total responsabilidade do usuário com o cuidado com os seus acessos, porque serão utilizados como parâmetro para verificações.

d) Utilizo de ativos

Este item engloba a utilização dos ativos disponibilizados pela empresa, para que os funcionários possam exercer suas funções.

Para a utilização do e-mail, busca-se mostrar a importância de utilizar a ferramenta de modo adequado, apenas para assuntos da empresa, assim como não encaminhar arquivos muito grande em anexo.

Já sobre a utilização da internet, um dos pontos mais críticos é o acesso a determinados sites, burlando o mecanismo do firewall, então foi esclarecido que as utilizações de mecanismos desta natureza são proibidas, e que acesso a sites não autorizados podem gerar punições, além de padronizar a utilização dos navegadores.

Os funcionários também possuem a responsabilidade de manter o equipamento em boas condições, toda e qualquer manutenção deve ser realizada pelo departamento de TI, e as ações executadas indevidamente podem ser rastreadas até a máquina de origem.

A utilização da impressora está ligada tanto com a redução de custos, como a não divulgação de dados críticos, sendo que ao imprimir um relatório com informações sigilosas, o funcionário deve ir buscar a impressão no mesmo instante, evitando que outra pessoa tenha acesso.

h) Mesa limpa

Manter o ambiente onde trabalha organizado é de extrema importância, até porque leva em consideração a mesma questão da impressão com dados confidenciais, sendo que ao deixar o computador desbloqueado com dados importantes e sigilosos na tela, qualquer pessoa pode ter acesso e causar sérios danos para a empresa, já que a empresa lida com dados financeiros de clientes, entre outras informações.

Estes foram os itens analisados e levantados para o desenvolvimento da política de segurança da informação.

Quadro de análise de riscos

Risco	Impacto	Resposta	Responsável
Lotação do servidor de arquivo	Médio/Alto	Limpeza imediata de arquivos não essenciais, com realização de backup	Analista de Redes
Utilização indevida de credenciais de outro funcionário	Baixo	Conscientização e punição de funcionários envolvidos	Gestor de TI Coordenador da área afetada
Não alteração periódica de senha	Baixo/Médio	Conscientização de funcionários	Gestor de TI Coordenador da área afetada
Acesso a sites indevidos	Médio/Alto	Monitoramento recorrente, varredura com antivírus, conscientização e punição de funcionários envolvidos.	Analista de Redes Coordenador da área afetada
Utilização inadequada de ativos físicos	Médio/Baixo	Monitoramento recorrente, conscientização e punição de funcionários envolvidos.	Gestor de TI Coordenador da área afetada
Perca do Banco de Dados	Alto	Restauração de backup recente e análise de causas	Gestor de TI Analista de Sistemas Analista de Redes
Manuseio inadequado de informações	Médio/Alto	Conscientização e punição de funcionários envolvidos	Gestor de TI Coordenador da área afetada
Parada de servidor	Alto	Restauração de backup recente em outro Hardware, análise de causas	Gestor de TI Analista de Sistemas Analista de Redes
Acesso indevido ao CPD	Alto	Monitoramento constante por câmera, varredura com antivírus nos servidores e testes de aplicações	Gestor de TI Analista de Sistemas Analista de Redes

4.2 Elaboração da política

Após realizar a análise dos riscos da organização, obteve-se uma base sólida para desenvolver a política de segurança, porem foi necessário buscar embasamento em normas para mostrar que o documento além de necessário era um item comum nas organizações de médio a grande porte. Para o embasamento foi utilizado a norma ISO/IEC 27002:2005, onde define os controles necessário que uma organização deve implementar para garantir:

- Continuidade do Negócio;
- Mitigar os Riscos;
- Maximizar os Retornos de Investimento;
- Maximizar as Oportunidades de Negócio;
- Proteção sobre ameaças;

Além dos itens citados acima, a norma contribuiu para a elaboração do documento PSI, já que informa todos os passos a seguir para a elaboração, mesmo sendo um padrão orientado nas demais bibliografias, porem com a credibilidade de uma norma.

Junto com a norma ISO/IEC 27002:2005, também utilizei como estrutura e forte aliado na apresentação para aceitação de política alguns itens da constituição federal e Código Penal:

- Constituição Federal, art. 5º, inciso X:

Garante o sigilo das informações pessoais de um indivíduo.

- Art. 154 do Código Penal - Decreto Lei 2848/40:

Diz respeito a violação de equipamentos ou sistemas eletrônicos conectados ou não a internet, com a intenção de destruir ou instalar vulnerabilidade.

A política de segurança desenvolvida foi separada em tópicos, para deixar mais didático, e também para facilitar a busca de determinado item. A elaboração foi realizada apenas por uma pessoa, e iniciada sem uma autorização prévia da diretoria.

A elaboração da PSI durou 1 mês, lembrando que os itens a serem citados, já estavam listados com as ocorrências vividas dentro da empresa, então a etapa de análise de riscos não chegou a demorar muito.

E, Após a conclusão do documento, o mesmo deveria ser avaliado e autorizado pela diretoria e presidência, como a empresa não tinha o conhecimento do que seria uma política de segurança da informação, somente a direção do setor tecnológico, foi realizado uma breve apresentação para o diretor de tecnologia, relatando todos casos listados, onde os funcionários utilizaram da má fé ou mesmo da falta de conhecimento, para realizar ações que geraram prejuízos ou deixaram certas vulnerabilidades que poderiam chegar a causar danos a organização.

Após a apresentação dos casos mostrei o documento, como um método de mitigar todos os riscos, evitar que as situações anteriores voltassem a ocorrer, além de garantir o direito da empresa de se proteger já que os funcionários passariam a estar cientes do que pode ou não ser feito.

Com o decorrer de três dias de análise do documento, o diretor informou a aprovação da política e que a mesma poderia ser implantada, com isso reuni os coordenadores de cada setor, para a divulgação da política, apresentei os mesmos casos apresentados para o diretor, expliquei os pilares da segurança, e entreguei o documento para cada coordenador explicando os principais itens. Ficou acordado que o processo de implantação não tinha chegado ao fim, já que existe a necessidade de atualização da PSI, e ficou agendado de realizarmos reuniões periódicas, para levantar e discutir itens, para acrescentar ou melhorar o documento.

5 MODELO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA UMA EMPRESA DE PLANO DE SAÚDE AMBULATORIAL

Compreendendo o que deve ser levado em consideração ao desenvolver uma política de segurança da informação, a estrutura de uma empresa do âmbito de plano de saúde ambulatorial e que houve uma experiência real de desenvolvimento.

O modelo abaixo descreve os tópicos acrescentados no documento, para constituir a política de segurança da informação. Documento que será seguido por todo o corpo de funcionários, e por isso deve chamar a atenção dos mesmos, tendo no objetivo uma clareza e ênfase na importância de seguir as regras descritas.

5.1 Objetivo

Neste tópico, a política deve esclarecer o que ela visa alcançar, neste caso o objetivo é garantir que os recursos e as informações sejam utilizados da maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a empresa, juntamente com seus funcionários, parceiros e clientes.

A política é desenvolvida para fornecer aos funcionários, informações suficientes para saber se os procedimentos descritos são aplicáveis a ele ou não, em caso de dúvida sobre o que é considerado, de alguma forma, violação, o usuário deve entrar em contato com o setor responsável, buscando esclarecimento.

Outro ponto importante é salientar a importância da implantação de controles para preservar os interesses dos funcionários, clientes e demais parceiros contra danos que possam acontecer devido à falha de segurança. Também mostrar que o documento descrever as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços, e, portanto, considerados proibidos.

Listar os objetos da Política de Segurança, que são os serviços e recursos colocados à disposição dos funcionários e parceiros, tais como: computadores, correio eletrônico, Internet, informações armazenadas em diretórios da rede e sistemas de aplicação.

Deixar claro que normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

E mostrar que nos casos onde os procedimentos ou normas estabelecidas sejam violados, a direção da organização se reserva o direito de aplicar as punições cabíveis aos usuários responsáveis pela violação da política, se resguardando do direito de monitorar todos os processos.

5.2 Tópicos levantados

A PSI pode ser elaborada em tópicos, deixando mais claro o entendimento e facilitando a leitura. Tendo como foco uma empresa com as características mostradas neste trabalho, o documento pode conter os tópicos e regras a seguir.

5.2.1. *Política de segurança da rede*

Esse tópico visa definir as normas de utilização da rede que abrange o LOGIN, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso.

a) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor. Isso inclui acesso aos dados não autorizados para o usuário,

conectar-se a servidor ou descktop cujo acesso não seja expressamente autorizado ou colocar à prova a segurança de outras redes;

b) Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques e tentativas de provocar congestionamento no trafego da rede, tentativas de sobrecarregar um servidor e tentativas de invasão em servidores;

c) Antes de ausentar-se do seu local de trabalho, o usuário deverá efetuar logout/logoff nos programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, e bloquear a estação de trabalho através de senha;

d) O usuário deve fazer manutenção no seu diretório pessoal periodicamente, evitando o acúmulo de informações desnecessárias;

e) Materiais de natureza pornográfica e racista não podem ser armazenados, distribuídos, editados ou gravados através do uso dos recursos de TI;

f) Jogos ou qualquer tipo de software/aplicativo não podem ser gravados ou instalados no computador local ou em qualquer outro diretório da rede;

g) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que possam comprometer o desempenho e funcionamento dos sistemas. Em alguns casos pode haver mais de um compartilhamento referente aos arquivos de usuários de um mesmo departamento;

h) O diretório de compartilhamento público não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza

específica. Ela deve ser utilizada apenas para armazenar informações de interesse geral;

i) Será feita semestralmente a limpeza dos arquivos armazenados na pasta de compartilhamento público ou similar, para que não haja acúmulo desnecessário de informações e degradação do acesso ao ambiente de rede;

j) É proibida a instalação ou remoção de softwares que não sejam devidamente acompanhadas pela equipe técnica da área de TI, autorizada formalmente pelo coordenador responsável pela área do solicitante;

k) Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como demais modificações que não sejam justificadas e efetuadas pela área de TI;

l) Os acessos a sistemas, devem ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados. As senhas compartilhadas devem ser excepcionais e autorizadas pela equipe técnica;

m) Quando da utilização de equipamentos de informática particulares o funcionário deverá comunicar à coordenação do seu setor para que entre em contato com a área de TI.

n) O acesso às informações é feito através da conta criada pela área de TI, através de solicitação do coordenador da área responsável. Caso não seja estritamente necessário, o funcionário não deverá ter conta de acesso à rede interna de computadores;

5.2.2. *Politica de controle de acessos*

Este tópico visa definir as normas de administração das contas que abrange: criação, manutenção, desativação da conta e eficiência na utilização das senhas

a) Todo funcionário poderá ter uma conta para acesso aos recursos da rede de computadores da empresa (Login de acesso ao Windows). Os acessos a demais sistemas incluindo correio eletrônico devem ser informados pelo coordenador da área no momento da solicitação da conta do usuário. Para solicitação de criação de conta para novos funcionários, os coordenadores devem proceder conforme descrito abaixo:

b) O coordenador do departamento a que o funcionário pertence deverá fazer uma solicitação de criação de conta, para o setor de TI, na solicitação, deverá ser informado os dados do funcionário/colaborador;

c) A equipe de segurança retornará para a coordenação do departamento as informações sobre a conta criada, respondendo a solicitação correspondente;

d) Cada funcionário que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos de trabalho;

e) A manutenção dos arquivos é de responsabilidade do usuário, sendo que o mesmo deve evitar acumulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;

f) As contas podem ser monitoradas pela equipe de TI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos;

g) Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. A concessão de senhas deve ser controlada, considerando:

• Senhas temporárias devem ser alteradas imediatamente, não devem ser armazenadas de forma desprotegida.

• As senhas devem ser bloqueadas após 3 a 5 tentativas sem sucesso, sendo que, administrador da rede e o usuário devem ser notificados sobre estas tentativas.

• As senhas devem conter números e caracteres, contendo no mínimo 8 dígitos.

h) As responsabilidades do administrador do sistema incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos, de acordo com a comunicação do coordenador de departamento a que o funcionário pertence;

i) As responsabilidades do usuário incluem, principalmente, os cuidados com a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese;

j) Tudo que for executado com a senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário;

5.2.3. *Política de utilização de e-mail*

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento de contas.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio publico e que não está sob o controle da equipe técnica de TI. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia passa através de e-mails. Mas é importante também lembrar que grande parte das pragas eletrônicas atuais chega por esse meio. Os vírus atuais são enviados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo pode conter vírus.

a) O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens;

b) O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção do envio, esta deve ser acatada e o envio não deverá mais acontecer;

c) É proibido o envio de e-mail mal-intencionado, tais como mail bombing (enviar vários milhares de mensagens idênticas para uma caixa de correio eletrônico) ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou com anexos numerosos/muito grandes;

d) É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;

e) É obrigatória a utilização do software homologado pela área de TI, para ser o cliente de email;

f) Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controles extras para verificar a

chegada da mensagem, deve ser solicitado notificação de “recebimento” e “leitura”;

g) Desconfiar de todos e-mails com assuntos estranhos e/ou em outros idiomas;

h) Evitar anexos muito grandes;

i) Não utilizar o e-mail da empresa para fins pessoais;

j) É obrigatória a utilização de assinatura nos e-mails, seguindo padrão estabelecido pela empresa;

k) Todos os e-mails coorporativos, estão sujeitos a monitoramento. Visando o cumprimento das normas deste documento.

5.2.4. *Política de acesso à internet*

Esse tópico visa definir as normas de utilização da Internet que abrange a navegação em sites, downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários da empresa, não sendo permitido o seu uso para fins recreativos durante o horário de trabalho.

a) Somente navegação de sites é permitida. Casos específicos que exijam outros tipos e serviços como download de arquivos, deverão ser solicitados diretamente à equipe de TI com autorização do coordenador ou diretor do usuário que deseja este acesso;

b) É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida.

c) É obrigatoriedade a utilização dos programas homologados pelo departamento de TI para serem clientes de navegação, exemplo: Google Chrome, Internet Explorer ou Firefox;

d) O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas, serão bloqueados, e as tentativas de acesso serão monitoradas;

e) É proibida a utilização de qualquer mecanismo para burlar o controle de acesso a sites indevidos, a tentativa será monitorada e se necessário haverá punições conforme análise do supervisor imediato;

f) Haverá geração de relatórios dos sites acessados por usuário, se necessário à publicação desse relatório e prestação de contas do usuário dos acessos;

4.2.5. *Politica de uso das estações de trabalho*

Cada estação de trabalho possui códigos internos os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho, o usuário deverá ter certeza que efetuou o logoff ou bloqueou a estação de trabalho.

a) Não utilizar nenhum tipo de software/hardware sem autorização da área de TI;

b) Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe sistema de backup diário e confiável;

c) Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade. Poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação;

d) É vedada a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento de TI;

e) É de responsabilidade do usuário do equipamento zelar pelo mesmo, mantendo a boa aparência;

f) As entradas USB junto com as saídas de áudio, serão bloqueadas, sendo necessário autorização prévia para utilização.

4.2.6. *Política de uso de mídias*

Esse tópico visa definir as normas de utilização de mídias, como: (Impressora, CD/DVD e Pen drive) disponíveis na rede da empresa. Visando segurança das informações críticas, sendo elas:

- Dados de clientes
- Dados de prestadores
- Informações financeiras
- Negociações de procedimentos
- Dados de utilização de clientes

a) Ao enviar o arquivo para impressão, o usuário deverá imediatamente verificar se o que foi solicitado já está disponível na impressora, não deixando documentos nas bandejas das impressoras mais tempo do que o necessário.

b) Em caso de erro na impressão e o papel puder ser reaproveitado na sua próxima tentativa, recolocá-lo na bandeja de impressão. Caso contrário, se o papel servir para rascunho, o usuário deverá levá-lo para sua mesa. Se o papel não puder ser reaproveitado, deve ser picotado ou jogado no lixo.

c) Se a impressora emitir alguma folha em branco, esta deve ser recolocada na bandeja para nova utilização;

d) Manter a impressora sempre abastecida de papel, evitando o acúmulo de trabalhos na fila de impressão, prejudicando as solicitações;

e) Utilizar a impressão colorida somente quando estritamente necessário e sempre na versão final de trabalhos e não para impressões intermediárias ou rascunhos.

f) É proibido a utilização de dispositivos USB assim como mídias de CD/DVD, podendo ser utilizado apenas mediante a autorização prévia.

4.2.7. *Politica de mesa limpa e tela limpa*

A política de tela limpa deve ser considerada para todos os departamentos e seguida por todos os funcionários/colaboradores, de forma a garantir que as informações manipuladas por sistemas aplicativos, planilhas Excel, documentos Word etc., não fiquem expostas, permitindo o seu acesso a pessoas não autorizadas.

a) Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados. Devem ser guardados de maneira adequada, de preferência em gavetas ou armários trancados;

b) As salas devem ser mantidas limpas, sem caixa ou qualquer outro material sobre o chão de modo a facilitar o deslocamento dos funcionários/colaboradores;

c) Sempre que o computador não estiver em uso, não se deve deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no local;

d) Agendas, livros ou qualquer outro material que possa conter informações sobre as empresas ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso de outras pessoas que não as responsáveis pela informação.

4.2.8. *Verificação da utilização da politica*

Para garantir o cumprimento das regras mencionadas acima, a empresa se reserva o direito de:

a) Implantar softwares e sistemas que monitorem e gravem todos os usos de Internet através da rede e das estações de trabalho da empresa;

b) Inspecionar qualquer arquivo armazenado na rede esteja ele no disco local da estação ou nas áreas privadas da rede;

c) Monitorar a utilização dos correios eletrônicos;

d) Monitorar os logs de acessos a servidores e estações de trabalho, se resguardando do direito de utiliza-los com prova de descumprimento das normas;

4.2.9. Violação da política, advertências e punições

A empresa se reserva no direito de aplicar advertências e punições sempre que for provado o não cumprimento desta política de segurança.

a) Sempre que for detectado um violação, a primeira ação a ser tomada, será a determinação da razão, podendo ser por negligencia, acidente ou erro;

b) Após definir a razão, deverá verificar o motivo, podendo ser classificado como:

- Desconhecimento da Politica
- Ação previamente determinada

c) Para evitar o não cumprimento da política por desconhecimento, o documento deverá ser divulgado, para conhecimento de toda empresa;

d) Caso exista a necessidade de advertir algum funcionário, será informado a diretória responsável, e ao coordenador, para que seja analisado o caso, e aplicado a punição cabível;

5.3 Publicação da política de segurança da informação

Para desenvolver uma PSI, pode ser utilizado como base vários modelos disponibilizados por organizações, encontradas pela internet, porem o descrito acima, também serve como uma ótima base para elaborar um documento de segurança. Não só uma empresa voltada para plano de saúde, mas qualquer empresa de porte médio/alto pode utilizar este modelo, já que ele abrange todos os pontos importantes, sendo necessárias apenas algumas modificações, para voltar as regras para a realidade atual da organização.

Redigido o documento, basta prosseguir para a fase de divulgação do mesmo, a princípio a melhor maneira é organizar uma palestra para todo o corpo de funcionário, enfatizando a importância do cumprimento das regras e posteriormente, criar métodos para relembrar, como e-mails e folders.

CONCLUSÃO

O trabalho mostra que é necessário entender e pesquisar para desenvolver uma política de segurança, que por sua vez é a primeira etapa para implantar uma gestão de segurança eficiente dentro de qualquer organização. Mas mesmo buscando um foco especifico em um ramo de empresa, o modelo apresentado traz vários pontos em comum com outras realidades, precisando apenas de algumas adaptações para a realidade de cada empresa.

Toda organização possui informações críticas para o negócio, e as que almejam um crescimento significativo no mercado, precisam se preocupar com esse ativo tão importante, e consequentemente com os demais recursos de TI, já que a disponibilidade da informação passa integralmente pela conservação e continuidade de serviço e dos recursos de TI. Para alcançar um ambiente com segurança e que garanta a continuidade do serviço, a empresa precisa formalizar e alinhar os processos, criando regras e normas que devem ser seguidas por todo corpo de funcionários.

Para desenvolver um documento com o intuito de garantir todos os pontos necessários para uma gestão de segurança eficiente, basta seguir os capítulos deste trabalho, que estampam a importância de entender os pilares da segurança (autenticidade, integridade, disponibilidade e confidencialidade), para buscar um resultado significativo, além de analisar e levantar os riscos existentes internamente e externamente e utilizar o modelo apresentado como base de criação para uma política.

O levantamento de todos os processos e de seus ricos é fundamental para o bom desenvolvimento de uma política de segurança, já que ela vai ser totalmente embasada nessas informações, buscando aperfeiçoar as rotinas e encaixar os processos de forma que fiquem alinhados com os conceitos de segurança, e traga melhores resultados para a organização, deixando claro para os clientes a preocupação com seus dados pessoais. Outro ponto importante que a política entregar é o fato que a informação precisa estar sempre disponível para acesso, evidenciando a preocupação com a autenticação por meio de login e senha, estes pontos que estão diretamente ligados com a disponibilidade e

autenticidade, tornam a empresa bem vista pelos parceiros de negócio e clientes, já que os dados buscados estão sempre disponíveis quando requeridos. O modelo apresentado neste trabalho foi desenvolvido realizando uma análise e verificação dentro de uma empresa do Distrito Federal, que comercializa um plano próprio de saúde ambulatorial. Neste tipo de negócio, a empresa lida com informações confidenciais, como dados pessoais e informações financeiras, precisando entregar uma segurança para o cliente, e garantir a disponibilidade do serviço 24h por dia.

Portanto para desenvolver uma PSI, deve-se seguir os itens levantados neste trabalho e utilizar alguns dos exemplos existentes e disponibilizados na internet. Sempre Utilizando de uma linguagem simples e de fácil compreensão, para que atinja todo o público alvo.

REFERÊNCIAS

BASTOS, FABRICIO. Politica de Segurança da Informação – Como fazer?,disponível em <http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/> [consultado em 08/08/2015]

CAMPOS, A. (s/d), Auditoria em tecnologia da informação, disponível em < http://correio.fdvmg.edu.br/downloads/DET479/apostila%20auditoria.pdf>[consultado em 09/08/15]

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988 disponível em < http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>

Art. 154 do Código Penal - Decreto Lei 2848/40 disponível em < http://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>

FERNANDO, BRUM. A importância da Informação para Empresas de Sucesso, disponível em <http://www.brumconsulting.com.br/2011/08/importancia-informacao-sucesso-empresas.html> [consultado em 10/08/15]

FIPECAFI, POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, disponível em <http://www.fipecafi.org/downloads/ti/psi-politica-seguranca-informacao-fipecafi-ti-v1-01.pdf> [consultado em 09/08/15]

PALME, FERNANDO. Resumo ISO/IEC 27002:2005 disponível em < http://pt.slideshare.net/fernando.palma/resumo-iso-27002-31383032>

PAULA, DIANA. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – INTRODUÇÃO AO DESENVOLVIMENTO, disponível em <http://www.profissionaisti.com.br/2013/03/politica-de-seguranca-da-informacao-introducao-ao-desenvolvimento/> [consultado em 10/08/2015]

PEREIRA, JOÃO LUIZ. Segurança da Informação – Uma Abordagem Social, disponível em <http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf> [consultado em 09/08/2015]

SPANCESKI, R. FRANCINI, (2004), Política de Segurança da Informação – Desenvolvimento de um Modelo voltado para Instituições de ensino monografia de Bacharel, [em linha] disponível em <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf> [consultado em 09/08/15].