SEGURANÇA DA INFORMAÇÃO: elaboração projeto para empresa Telmaster

Rafael Ramos[1]
Ricardo Bernardes de Mello[2]

RESUMO

Este trabalho tem como objetivo principal analisar a segurança da informação de uma empresa do ramo de telecomunicações. Tal abordagem se faz necessária devido à vulnerabilidade em processos internos e também da interconexão da rede de comunicação. Este propósito será conseguido a partir de estudo de caso realizado em uma empresa do Sul de Minas, localizada na cidade de Botelhos, chamada TELMASTER (nome fictício), no setor de tecnologia da informação. A pesquisa evidenciou a melhora nos processos internos, garantia da segurança da informação e confiabilidade.

Palavras-chave: Segurança da informação. Vulnerabilidade. Confiabilidade.

1 INTRODUÇÃO

Vê-se em um tempo no qual a informação está se disseminando em uma velocidade nunca antes vista, principalmente no meio corporativo e empresarial. Muitas destas informações são confidenciais e de suma importância para o desenvolvimento e segurança dos colaboradores que a manipulam e também para a empresa e corporações.

A empresa TELMASTER até o presente momento não possui um documento, uma política, onde se assegure e também a seus colaboradores, em caso de vazamento de informações e/ou infrações nas quais não foram explicitas ou acordadas.

Vendo esta deficiência, este trabalho irá propor uma política de segurança da informação na qual se adequará ao ambiente de uma fábrica de software e também dará o passo inicial para se romper com a cultura organizacional que não se adéqua as normas.

1 Tecnólogo em Redes de Computadores Cesep, MBA em Gestão de Projetos Unis. rafaelramoscp@hotmail.com.

2 Mestre em Sistemas de Produção na Agropecuária Unifenas. rmello@unis.edu.br.

Este será de forma ainda simplista, pois, após análise da empresa e reuniões com coordenadores e gerentes, vimos que, uma política inicial, será mais bem aceita pela empresa e colaboradores caso não afete a produção e não engesse processos, mas também, que seja estruturada o suficiente para dar o passo inicial para se propor a política que deverá ser (caso implantada) continuamente revista, atualizada e aprimorada, adicionando novos processos e métodos para abranger toda empresa em uma etapa posterior.

Alguns dados serão ocultos e/ou substituído neste trabalho, vendo que seu sigilo foi solicitado. Deste modo, será trabalhado em cima do ambiente atual da empresa, contudo, respeitando esta questão.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a prevenção que inibe ou dificulta ataques e intrusos de alcançarem seus objetivos de forma indevida, sendo realizados por meio de acessos não autorizados ou até mesmo do uso inapropriado de computadores e redes.

Segundo CARUSO (1999), o bem de maior valor para uma empresa não é sempre originado na linha de produção, mas sim, o que faz surgir o produto final, o segredo no tempero da massa, um protocolo diferenciado, os clientes são alguns exemplos nos quais segredos são extremamente guardados e assegurados.

De acordo com a NBR 17999 (2003), deste modo também se acata a proteção dos sistemas de informação contra a negação de serviços, como a modificação não autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento.

Observando a norma brasileira ISO/IEC 27001 (2006), ela destaca aspectos estruturais e fundamentais, como a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas na segurança da informação.

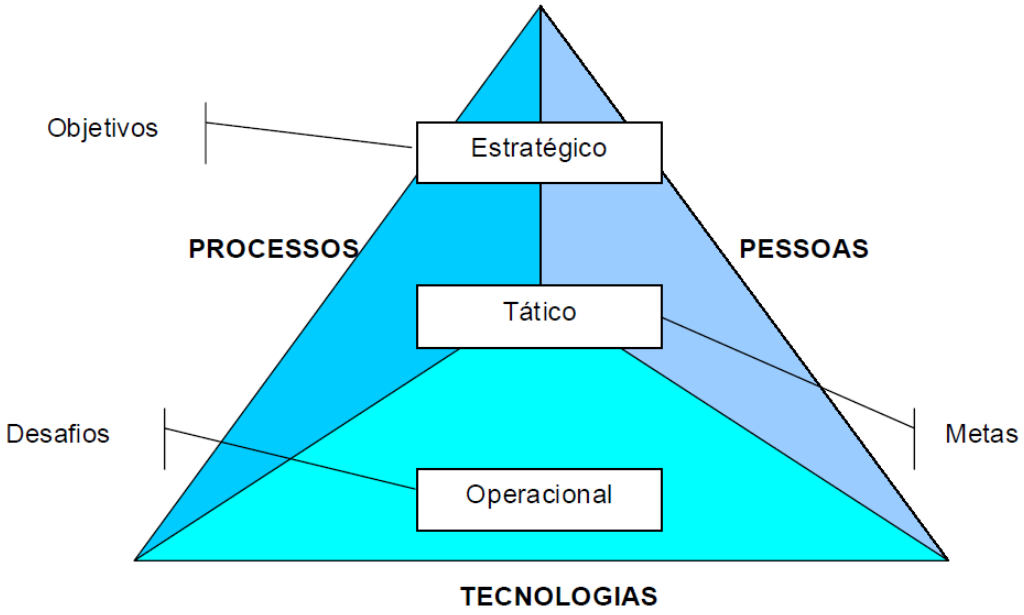
Deve se atentar que, nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja ainda será menor que o custo de não dispor dela adequadamente.

2.1 A importância da informação

A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. Contém valor, pois está integrada com as pessoas (o elo mais fraco de toda cadeia

da segurança da informação), processos e tecnologias. A figura 1 demonstra do ponto de vista estratégico, o relacionamento dos processos, tecnologias e pessoas.

Figura 1 – Relacionamento dos processos (Laureano, 2005, pag. 4).



Fonte: Laureano, 2005.

Hoje vivemos em uma sociedade que se baseia em informações e que exibe uma crescente para coletar e armazenar todas estas informações e o uso efetivo destas informações permitem que uma organização aumente significativamente a eficiência de suas operações (Katzam, 1977).

Este ativo (a informação), como qualquer outro ativo é importante para os negócios, tem um valor para a organização e consequentemente necessita ser protegida (NBR 17999, 2003). A informação representa a inteligência competitiva dos negócios e é reconhecido como ativo crítico para a continuidade operacional e saúde da empresa (Sêmola, 2003). Na sociedade da informação, ela é o principal patrimônio da empresa e está sob constante risco (Dias, 2000). A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade (Rezende e Abreu, 2000).

Como expressou o autor Edison Fontes em seu pequeno artigo publicado na internet:

Todos esses anos de experiência na gestão da segurança da informação me fez confirmar cada vez mais que a pessoa humana é um fator crítico para o sucesso do processo de proteção da informação. A tecnologia existente possibilita a empresa ter uma boa proteção, mas, quem vai garantir que ela tira proveito dessa tecnologia e implementa de forma efetiva os controles adequados é o usuário (FONTES, Segurança da Informação: o usuário faz a diferença!).

Isto ressalta a importância de lidar com a pessoa, com o ser humano e a sociedade como um todo, pois, mesmo que toda informação esteja armazenada em meios eletrônicos, pois ao manipular toda estas informações, quem o fará será uma pessoa, um ser humano.

2.2 Classificação

Assegurar que a informação receba um nível adequado de proteção é de suma importância, mas para isto, deve-se filtrar e classificar estas informações para que cada uma receba exatamente o nível de segurança necessário, para que não haja aumento de custo nas implementações e "engessamento" dos processos em questão. Conforme a Norma Brasileira ISO/IEC 17799 de 2005, convém que a informação seja classificada de acordo com o perfil e a necessidade de cada empresa, para indicar as prioridades e o nível esperado de proteção se referindo informação.

A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento, para que toda informação receba o nível exato de atenção e criteriosidade.

Conforme (NBR 17999, 2003; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002), os princípios básicos se resumem em três pontos para garantir a segurança da informação aos quais são eles:

Primeiro ponto: Confidencialidade, a informação somente pode ser acessada por pessoas explicitamente autorizadas; É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

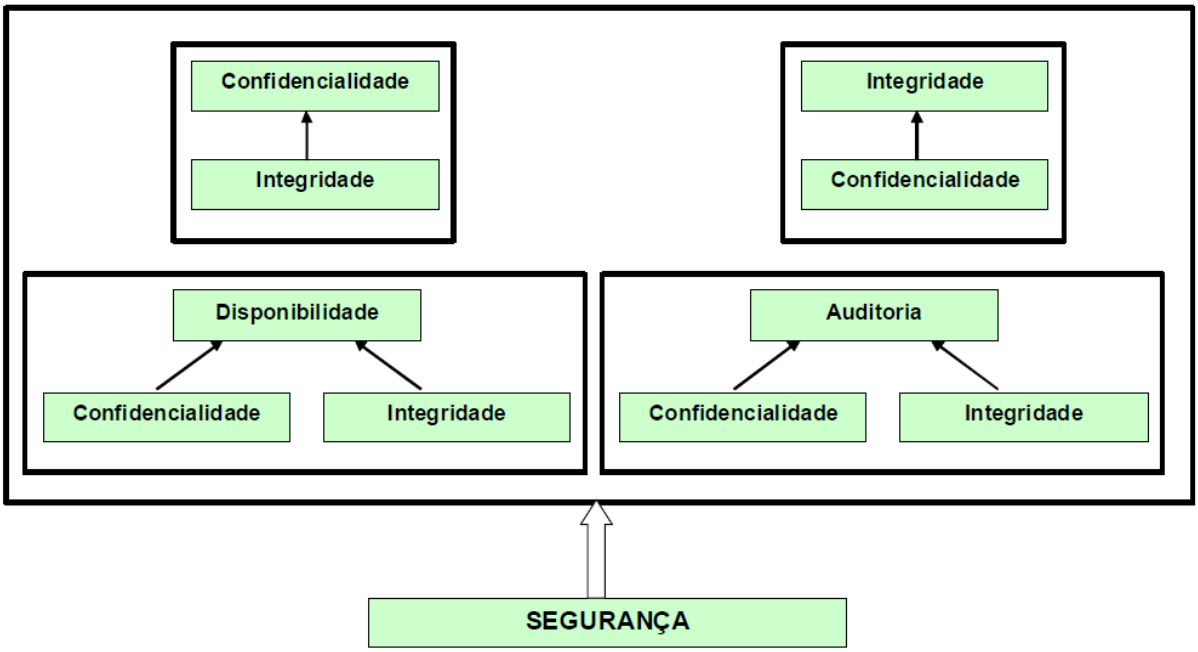
Segundo ponto: Disponibilidade, a informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;

Terceiro ponto: Integridade, a informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas.

A segurança não visa somente o lado da empresa, mas também a dos usuários, aumentando a produtividade através de um ambiente mais organizado, proporcionando maior controle sobre os recursos. A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem os seus objetivos, pois seus sistemas de informação serão mais confiáveis, juntamente com todos colaboradores.

Conforme citado (Laureano, 2005 apud Stoneburner, 2001) em seu artigo são sugerido que a segurança somente é obtida através da relação e correta implementação de quatro princípios da segurança: confidencialidade, integridade, disponibilidade e auditoria. A figura 2 ilustra a relação dos princípios para a obtenção da segurança da informação.

Figura 2 – Relação dos princípios da Segurança da Informação



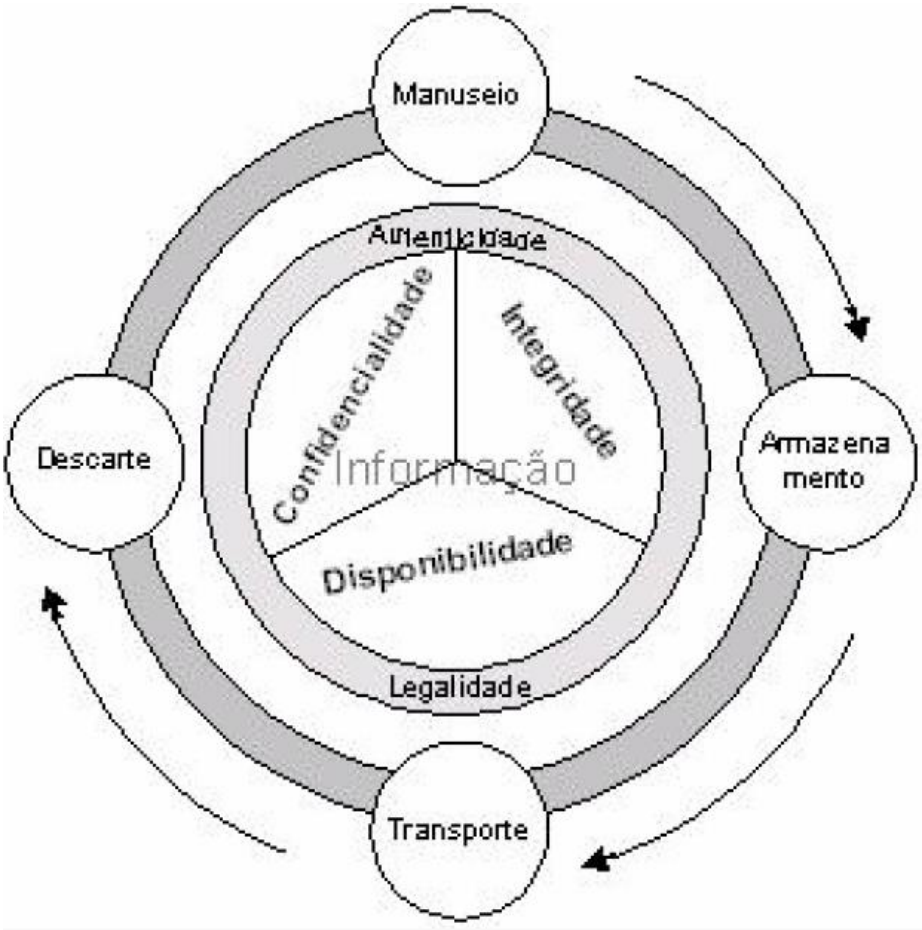
Fonte: Laureano, 2005.

2.3 Ciclo de vida

De acordo com (Sêmola, 2003) o ciclo de vida da informação é composto e identificado pelos momentos vividos que a colocam em risco. Estes são vivenciados justamente quando os ativos fazem uso da informação, sejam eles físicos, tecnológicos e/ou humanos.

Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a figura 3 revela todos os quatro momentos do ciclo de vida que são merecedores de atenção.

Figura 3 – Situações em que a informação se torna exposta (Laureano, 2005, pag. 10).



Fonte: Laureano, 2005.

LAUREANO (2005), explica que existem os seguintes momentos do ciclo de vida da informação:

2.3.1 Manuseio

Este é o momento em que a informação é criada e manipulada, por exemplo, ao folhear um maço de papéis, digitando informações recém geradas em uma aplicação ou ao utilizar a senha de acesso para autenticação.

2.3.2 Armazenamento

Nesta etapa a informação é armazenada, seja ela em uma anotação de papel posteriormente postada em um arquivo, em um banco de dados onde será compartilhada, ou, mesmo em um dispositivo móvel, como um pen drive, celular, que será guardado no fundo da gaveta por exemplo.

2.3.3 Transporte

Será nesta fase em que a informação será transportada, seja, por exemplo, ao encaminhar informações por correio eletrônico, ao enviar um documento via fax, ou, ainda, ao falar ao telefone uma informação confidencial.

2.3.4 Descarte

Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar algum dispositivo usado que apresentou falha na leitura.

2.4 Dado, informação e conhecimento

Em primeiro momento se torna difícil diferencia as três palavras descritas no título acima, pois as mesmas foram de algum modo generalizado pelo único termo "informação", contudo, são três coisas distintas.

2.4.1 Dado

É qualquer indício ou registro que permita identificar alguma característica de uma entidade ou evento.

"Indício ou registro": por que um dado não é, necessariamente, resultado de uma intenção de registrar alguma coisa – um som qualquer, uma pegada, a sombra de um objeto, o aspecto de uma rocha, podem ser dados; o dado não precisa ser um registro físico (uma imagem ou um valor), guardado na memória de uma pessoa, ou transmitido verbalmente, podem ser dados (Hashimoto, 2009).

Dados devem ser trabalhados, analisados por pessoas para se tornarem úteis como informação.

2.4.2 Informação

É o significado que um conjunto de dados tem para alguém. Um conjunto de dados representa uma Informação, para uma pessoa, quando ela consegue perceber as relações entre os elementos do conjunto, que lhe definem um contexto, e suas relações com outros dados e informações que já lhe são familiares, lembranças, impressões, experiências, etc., estabelecendo assim seu significado para ela (Hashimoto, 2009).

A informação na verdade são dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto. Ela deve informar, enquanto dados não têm essa missão.

2.4.3 Conhecimento

Ao conceituar "informação", mencionamos a necessidade de seu detentor possuir uma capacidade de estabelecer relações dentro de um conjunto de dados e desse conjunto com outros conjuntos de dados e informações já existentes em sua memória, para estabelecer seu significado. É a essa capacidade, desenvolvida por alguém, que chamamos de conhecimento (Hashimoto, 2009).

3 METODOLOGIA

Utilizando a técnica de "Brainstorm", (que na tradução literal para o português é algo como "tempestade de idéias"), na qual se é utilizada para gerar idéias (Minicucci, 2001), obtivemos uma grande quantidade informações, atingindo assim seu objetivo, onde após expor

todas estas ideias, pode-se selecionar o que é realmente importante, viável e útil para o desenvolvimento da política.

A técnica de Brainstorming pode ser utilizada para identificação de problemas, de causas ou de soluções (Rocha, Scheinkman, Souza e Azevedo, 2000). Deste modo, foi exposto o problema da ausência da política de segurança da informação, a sugestão de proposta dela e da cultura de toda empresa, visando à melhor pratica de acordo com as características da empresa.

Foi observado que a empresa TELMASTER, por se tratar de uma fábrica de software e que como citado anteriormente, ainda não possui uma política de segurança da informação, de se propor algo simples e inicial, abordando pontos chaves e específicos da área de tecnologia da informação, para que possa ser aderida pelos diretores e gerentes, juntamente a algo que possa ser facilmente localizado, lido e compreendido por todos colaboradores da empresa, para que assim, além de da política documental, possa também haver uma mudança inicial em sua cultura.

Conforme a Norma Brasileira ISO/IEC 17799 de 2005 os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.

Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos. Convém que a análise/avaliação de riscos seja repetida periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados desta análise/avaliação.

Deste modo, em conjunto com a política é elaborada uma análise de risco de pontos cruciais dos quais será abordado na política, tais como: Usuário e senha, e-mail corporativo, acesso à internet, uso de software, hardware e equipamentos móveis, compartilhamento de dados.

Ainda com referência a Norma Brasileira ISO/IEC 17799 de 2005 é laborado uma política de segurança que será proposta a empresa TELMASTER, que tem como objetivo prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Está será clara, alinhada com os objetivos do negócio e demonstrando apoio e comprometimento com a segurança da informação por meio da publicação e manutenção desta política para toda a organização.

4 POLÍTICA DE SEGURANÇA

Nesta etapa será exposta a proposta de uma política de segurança da informação e uma análise de risco referente ao ambiente e a proposta oferecia a empresa.

Ressaltando novamente que as informações foram alteradas por sigilo da empresa real.

O objetivo desta proposta é expor os riscos ao qual uma empresa sem uma política de segurança da informação está exposta, mesmo que esta seja simplista inicialmente para que possa ser aderida e apoiada, dando início a uma nova cultura organizacional.

4.1 Usuário e Senha

Neste tópico serão abordados os procedimentos, critérios e orientações referentes para a utilização das contas de usuários e senhas no ambiente da empresa TELMASTER.

A identificação do colaborador (por meio de crachá, login/senha ou outro meio) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso dos recursos dispostos pela empresa, sendo assim de caráter pessoal e intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.

Caso o usuário desconfie que sua senha não seja mais segura, ou de seu domínio exclusivo, deve solicitar ao Departamento de Tecnologia da Informação (TI) a alteração desta;

As senhas deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras e números. Sugere-se a utilização de maiúsculas, minúsculas e caracteres especiais (“$”, “%”, “&”,...); Deve ser evitada a composição de senhas com sequencias numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento...);

Para o primeiro acesso a conta, é enviada através de um documento lacrado, o usuário e senha de acesso à rede. As contas e aplicativos que se vinculam a ela, recomenda-se que troque a senha primaria no primeiro acesso. Todas as informações para o primeiro acesso estarão neste documento;

Serão atribuídos apenas os privilégios necessários a uma conta, que deverá permitir a realização das tarefas pertinentes ao seu usuário;

O bloqueio da conta do usuário será realizado automaticamente após 3 (três) tentativas com a senha incorreta, para desbloqueio desta é necessário entrar em contato com o Departamento de TI da empresa TELMASTER para que o usuário seja devidamente desbloqueado. O Usuário desvinculado da empresa terá sua conta desabilitada por 30 (trinta) dias, após este período a mesma será excluída;

As senhas só poderão ser reinicializadas por solicitação formal do seu detentor ao Departamento de TI; Para casos considerados críticos, a solicitação de reinicialização de conta deverá ser feita através do contato do superior direto do detentor, salvo, situações específicas.

4.2 Email corporativo

Neste tópico serão abordados os procedimentos, critérios e orientações referentes à utilização do serviço de correio eletrônico (Email Corporativo) da empresa TELMASTER.

Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização, com direitos de envio/recebimento de mensagens, via Intranet e Internet, contas com inatividade por um período igual ou superior a 30 (trinta) dias serão bloqueadas, a fim de evitar o recebimento e o envio de novas mensagens. O tamanho das caixas postais será de acordo com o os perfis pré-estabelecidos pela equipe de TI;

O envio e recebimento de e-mails terão um tamanho limite de 10MB, incluindo anexo, cabeçalho e corpo do mesmo. O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente; O mesmo é responsável direto pelas mensagens manuseadas por intermédio do seu endereço de correio eletrônico, ao qual é autenticado pelo seu usuário e senha de acesso, deste modo, destacam-se pontos críticos que se deve abster, tais como:

Envio de mensagens não autorizadas divulgando informações sigilosas; Acesso não autorizado à caixa postal de outro usuário; O Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes; Promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno;

Prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso; Distribuição de qualquer material que caracterize violação de direito autoral; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados; mensagens do tipo “corrente” e “spam”;

Material que caracterize a divulgação, incentivo ou a prática que possa causar atos ilícitos, ou que, de qualquer forma, possam danificar e/ou inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

Todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa a empresa e/ou seus colaboradores.

4.3 Acesso à Internet

Neste tópico serão abordados os procedimentos, critérios e orientações referentes para a utilização da internet dentro da empresa TELMASTER.

A TELMASTER possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à Internet feitos por seus usuários;

A Internet, no âmbito da empresa TELMASTER, é uma concessão e não um direito. Portanto, sua utilização, deve ser para atividades ligadas ao trabalho;

É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão, bate-papo, sites sem a autorização previa de superiores responsáveis pelo colaborador;

Colaboradores com acesso à Internet não podem efetuar upload de qualquer software licenciado, de dados e/ou de seus clientes referente à empresa TELMASTER sem a autorização expressa da Diretoria ou do responsável pelo software/dado;

Os downloads se restringem ao tamanho de 30MB, salvo cargos nos quais não se encaixam nesta regra, caso haja a necessidade do download ao qual possui um arquivo de volume maior, este deverá ser solicitado ao Departamento de TI;

Os colaboradores devem utilizar a Internet de forma adequada e diligente; observando a conformidade com a lei, a moral e os bons costumes; Sendo ele o detentor do login de rede ao qual permite o acesso à internet, se torna o único responsável pela utilização da internet através deste.

Deve-se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, ou que, de qualquer forma, possa danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

O uso de softwares de comunicação instantânea, tais como Skype, Gtalk, Microsoft Messenger (MSN) e afins são restritos, utilizados exclusivamente para fins de trabalho;

Não é permitida a utilização de software de peer-to-peer (P2P), tais como Kazaa, Emule e afins;

O Acesso a sites, tais como Facebook, You Tube... Sendo de redes sociais, relacionamento, streaming de vídeo e/ou áudio e afins são restritos, sendo utilizados exclusivamente para fins de trabalho;

Não se faz permitido acesso a sites e utilização de softwares de Proxy;

A TELMASTER monitora e bloqueia automaticamente sites de pornografia, pedofilia e outros contrários à lei e/ou em desconformidades com a política da empresa. O acesso a esses sites é terminantemente proibido, mesmo que estes não estejam bloqueados no sistema de segurança;

Devido ao bloqueio de sites ser baseado em um sistema automatizado, algumas páginas poderão ser bloqueadas inadvertidamente. Caso seja bloqueado um site cujo conteúdo esteja de acordo com esta norma, o usuário pode solicitar o desbloqueio através de solicitações ao Departamento de TI, bastando informar qual a URL bloqueada; O fato de um site não estar

bloqueado não significa que o mesmo possa ser acessado pelos usuários. Deverão ser observados todos os preceitos desta norma, desde a proibição de acesso a sites contrários à lei ao uso excessivo da Internet para assuntos não relativos a trabalho no horário do expediente, por exemplo.

4.4 Telefonia e Impressão

Neste tópico serão abordados os procedimentos, critérios e orientações referentes à utilização da Telefonia e Impressão no âmbito da empresa TELMASTER.

A telefonia e impressão no âmbito da empresa TELMASTER são monitoramentos, podendo, quando necessário, recorrer ao colaborador que solicitou a ligação ou realizou as impressões;

Impressões são restritas para fins de trabalho, evite desperdícios, quando possível realize impressões frente e verso. Caso haja necessidade de manutenção, troca de toner e/ou tinta, deverá ser informado ao Departamento de TI. Havendo falta de folha, comunicar ao departamento Administrativo da empresa TELMASTER;

Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso. Evite imprimir e-mails desnecessários, encaminhe a mensagem ao destinatário e para arquivamento, use o computador;

Se a impressora emitir alguma folha em branco recoloque-a na bandeja;

A telefonia se faz restrita a fins de trabalho, havendo assim uma senha para colaboradores específicos para realizações de ligações externas. Havendo a necessidade de entrar em contato com algum fornecedor ou contato da empresa TELMASTER haverá uma lista de códigos abreviados pra este fim na intranet;

Havendo a necessidade de ligações externas nas quais não se encontra na lista abreviada, deve-se contatar a telefonista para efetuar esta ligação, informando o nome do colaborador, nome do contato, número do telefone e o motivo.

4.5 Uso de Software

Neste tópico serão abordados os procedimentos, critérios e orientações referentes aos softwares da empresa TELMASTER.

Todo software executado nos equipamentos da rede corporativa da TELMASTER deverá ser licenciado, sendo vetada a utilização de qualquer software sem licença; O Departamento de TI poderá desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso;

Os sistemas ou qualquer outro tipo de software, desenvolvidos ou adquiridos pela TELMASTER, são de sua exclusiva propriedade e a sua utilização se restringe a apoiar os seus

negócios sendo expressamente proibido seu compartilhamento em qualquer meio sem autorização dos Diretores e/ou dos superiores direto do colaborador;

A instalação de softwares pode ser de forma autônoma, dês de que, tenha conhecimento para tal e esteja dentro da conformidade com direitos autorais, sejam eles softwares freewares ou sem necessidade de chaves (licenças) para instalação, caso contrário, se faz necessária a solicitação da instalação do mesmo pelo Departamento de TI;

É realizado o controle da distribuição/instalação destes softwares, sendo verificado o número de licenças disponível e qual sua real necessidade.

4.6 Hardware e equipamentos móveis

Neste tópico serão abordados os procedimentos, critérios e orientações referentes aos hardwares e equipamentos móveis dentro do âmbito da empresa TELMASTER.

A TELMASTER fornece todo equipamento (hardware) necessário para desempenhar a função determinada do colaborador, deste modo, não se faz necessário a utilização de equipamentos (computadores, impressoras, PDA´s, Netbooks, Tablets e demais dispositivos móveis) pessoais na rede da Empresa TELMASTER, salvo mediante concessão e autorização do uso pela diretoria e/ou gerência responsável pelo cliente/fornecedor/parceiro;

Em casos onde houver necessidade da utilização de equipamentos de terceiros na rede da TELMASTER, os equipamentos deverão ser encaminhados ao departamento de TI para devidas verificações e permissões, não sendo autorizada a utilização destes antes que possam ser verificados e devidamente autorizados;

Solicite suporte técnico sempre que verificado o mau funcionamento dos equipamentos ou do sistema de rede corporativa; Em caso de quebra, roubo, defeito... Entre em contato imediatamente com o Departamento de TI;

Os equipamentos, principalmente os considerados críticos, devem estar dispostos em áreas protegidas e devidamente equipadas;

A troca ou manutenção dos equipamentos de propriedade da TELMASTER deve ser realizada apenas pela equipe do Departamento de TI, suporte técnico do equipamento caso o mesmo esteja na garantia ou caso seja expressamente autorizado pelo Departamento responsável.

4.7 Conteúdo pessoal e direito autoral

Neste tópico serão abordados os procedimentos, critérios e orientações referentes ao conteúdo pessoal e de direito autoral no âmbito da empresa TELMASTER.

Faz necessário evitar manusear o conteúdo pessoal com o conteúdo do trabalho (profissional), salvando/arquivando fotos pessoais, musica, arquivos... Em computadores

fornecidos pela TELMASTER, podendo colocar em risco informações ou imagem pessoal ou comprometedora. A empresa TELMASTER não se responsabiliza por divulgação e ou exclusão destes arquivos que não condiz com o ambiente de trabalho;

O colaborador se faz responsável por todo arquivo que não condiz com o ambiente de trabalho, assumindo assim a responsabilidade por arquivos (fotos, músicas, documentos...) que possuem de algum modo direitos autorais e ou são de propriedade de terceiros.

4.8 Compartilhamento de dados

Neste tópico serão abordados os procedimentos, critérios e orientações referentes ao compartilhamento de dados no âmbito da empresa TELMASTER.

Caso seja necessário o compartilhamento de algum arquivo/pasta deve-se comunicar ao Departamento de TI da empresa TELMASTER, evitando assim pastas e arquivos locais nos equipamentos compartilhados, nos quais aumentam relativamente o trafego na rede e a disseminação de vírus;

Torna-se restrito os acessos e permissões necessárias exatamente para a realização das atividades funcionais, impedindo assim as permissões e acessos a conteúdo indevido ou não autorizado, caso o usuário verifique permissões excedentes as necessárias o mesmo se faz responsável em informar o Departamento de TI para que se possa averiguar;

O bloqueio do dispositivo USB das estações de trabalho é automático, caso necessário o desbloqueio do mesmo, o colaborador deve encaminhada uma solicitação para o Departamento de TI;

Toda e qualquer informação que chegue ao conhecimento do colaborador por força da natureza dos serviços prestados, que se relacionem propriedades intelectuais privadas e comunicações sigilosas, constituem informações confidenciais, sendo assim não sendo permitido seu compartilhamento e/ou disseminação de qualquer forma, para qualquer meio e /ou pessoa.

4.9 Validade

A presente política passa a vigorar a partir da data de sua homologação e publicação na empresa TELMASTER, sendo válida por tempo indeterminado.

4.10 Termo individual de conformidade e responsabilidade

Pelo presente instrumento, eu, _____, que possuo o CPF de nº _____, declaro estar ciente das minhas responsabilidades e concordar com a Política de Segurança da Informação composta por suas diretrizes gerais, normas, procedimentos e instruções, que estão disponíveis na intranet, na seção Política de Segurança (http://segurancadainformacao.telmaster.com.br).

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo e os equipamentos por mim utilizados estão sujeitos à monitoração sem aviso prévio.

Cidade, estado, dia, mês e ano.

_____

Assinatura do Colaborador.

5 CONSIDERAÇÕES FINAIS

Após o levantamento e ajuntamento de toda informação, filtra-la e organiza-la, o projeto para a política de segurança da informação a empresa TELMASTER se torna uma referência para a aplicação e adequação desta.

Será apresentada aos diretores da empresa, ao gerente e coordenador de TI expondo que a mesma foi elaborada para se adequar ao ambiente e característica desta, evitando engessamento de processos e assegurando o colaborador e também a empresa, cumprindo assim, seus objetivos iniciais.

Conclui-se que, a elaboração deste documento foi totalmente voltada para o perfil da empresa TELMASTER, podendo servir como orientação para outras empresas, dês que, se encaixe no mesmo perfil, cultura e abrangência, mas nunca como cópia idêntica, vendo que cada empresa possui suas características únicas.

Destaca-se a importância desta proposta vendo que se trata inicialmente de uma “quebra” de cultura organizacional, a onde serão oferecidos documentação e levantamento de informações para que se possa embasar todos os argumentos, orientações e restrições, devendo ser devidamente atualizada e revisada sempre que se achar necessário pela equipe que ficará responsável pela mesma.

Information security: development project for company Telmaster

ABSTRACT

This work aims to analyze the information security of a company in the telecommunications industry. Such an approach is necessary because of the vulnerability in internal processes and also the interconnection of the communication network. This purpose will be achieved from conducted case study in a South Mining company, located in Botelhos called TELMASTER (not her real name), in the information technology sector. The research showed the improvement in internal processes, security of information assurance and reliability.

Keywords: Information Security. Vulnerability. Reliability.

REFERÊNCIAS

LAUREANO M. A. P. **Gestão de segurança da informação**. Disponível em <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> em Setembro de 2015.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva 3. Ed**. Rio de Janeiro: Elsevier, 2003. 160p

CARUSO, Carlos A. A., STEFFEN, Flavio D. **Segurança em Informática e de Informações**. São Paulo: Senac, 1999.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença!** Disponível em <http://www.viaseg.com.br/artigos/artigo_edison_051125.htm> em Setembro de 2015.

NBR ISO/IEC 17799 – Tecnologia da Informação. **Código de Prática para Gestão da Segurança da Informação.** Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

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

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Axcel Books. Rio de Janeiro, 2000.

KRAUSE, Micki e TIPTON, Harold F. **Handbook of Information Security Management**. Auerbach Publications, 1999.

HASHIMOTO, A. N. **Dado, Informação e Conhecimento**. Disponível em <http://kmol.online.pt/artigos/2009/09/25/dado-informacao-conhecimento> em Setembro de 2015.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo, 2000.

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. **Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408**. Editora Campus. Rio de Janeiro, 2002

KATZAM JR, Harry. **Segurança de em Computação**. Editora LTC. Rio de Janeiro, 1977.

MINICUCCI, Agostinho. **Técnicas do trabalho de grupo – 3.ed**. – São Paulo: Atlas, 2001.

ROCHA, J.F; SCHEINKMAN, J; SOUZA, R. L; AZEVEDO, S. S. **Planejamento para a gestão do centro cirúrgico do hospital geral de bonsucesso ministério da saúde / RJ**. Disponível em <http://www.hgb.rj.saude.gov.br/ciencia/centrocirurgico/> em Outubro de 2015.