PROPOSTA DE IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO COM BASE EM ITIL PARA UMA REDE DE COMPUTADORES ORGANIZACIONAL

Pedro Medeiros Vargas Chaves[1]
Helmuth Grossmann Jr.[2]

RESUMO

A implementação de Políticas de Segurança da Informação (PSI) é essencial para auxiliar as organizações a protegerem-se contra perda de dados e ameaças externas. Assim, este artigo tem como tema a proposta de implementação de Políticas de Segurança da Informação com base em ITIL (*Information Technology Infrastructure Library*) para a rede de computadores da empresa Biotecno, desenvolvedora de câmaras refrigeradoras para medicamentos, de Santa Rosa – RS, buscando responder a questão problema: como a implantação de PSI com base em ITIL poderá contribuir para prover à segurança dos dados e informações da organização? Para elaborar o estudo foi preciso desenvolver alguns tópicos como: políticas de segurança da Informação e ITIL baseados em autores como Ferreira e Araújo, Fontes e Dawel. Referente à categorização da pesquisa, foi teórico-empírica, qualitativa, exploratória e estudo de caso. Utilizou-se a pesquisa bibliográfica que forneceu o embasamento em termos de conceitos e teorias sobre a segurança da informação e seus aspectos, bem como, aplicou-se um questionário ao gestor da empresa para verificar quais suas percepções em termos de PSI. Com base nessas informações, realizou-se a análise e discussão dos resultados. Com base nesse artigo conclui-se que, com as novas ameaças à segurança da informação que surgem constantemente, e por ela ser um importante ativo da organização, é importante para a empresa implementar uma Política de Segurança da Informação. Diante disso, os resultados e considerações trazem a importância da organização estabelecer os níveis de segurança que pretende seguir garantindo sua segurança sem esquecer do bem-estar dos funcionários que precisam estar bem informados.

Palavras-chave: Segurança da Informação – Políticas de Segurança – ITIL

ABSTRACT

The Implementation of Information Security Policies (ISPs) is essential to help organizations protect themselves against data loss and external threats. Thus, this work has as its theme the proposal to implement Information Security Policies based on Information Technology Infrastructure Library (ITIL) for the Biotecno's computers network, developer of medical refrigeration chambers in Santa Rosa - RS, seeking answer the problem question: how can ITIL-based ISP deployment contribute to providing the security of the organization's data and information? To elaborate the study it was necessary to develop some topics such as: Information security policies and ITIL based on authors like Ferreira and Araújo, Fontes and Dawel. Regarding

[1] Acadêmico do Curso de Gestão da Tecnologia da Informação - 6º Semestre. Faculdades Integradas Machado de Assis. pedrochaves.gti@gmail.com
[2] Mestre em Ciências da Computação. Orientador. Professor do Curso de Gestão da Tecnologia da Informação. Faculdades Integradas Machado de Assis. helmuth.jr@gmail.com

the categorization of the research, it was theoretical-empirical, qualitative, exploratory and case study. It was used used the bibliographic research that provided the baseline in terms of concepts and theories about information security and its aspects, as well as, a questionnaire was applied to the company manager to verify what their perceptions in terms of ISP. Based on this information, the analysis and discussion of the results was made. It is concluded that with the new information security threats that constantly arise, and because it is an important asset of the organization, it is important for the company to implement an Information Security Policy. Therefore, the results and considerations make it important for the organization to establish the levels of security that it intends to continue guaranteeing its safety without forgetting the well-being of the employees who need to be well informed.

Keywords: Information Security - Security Policies - ITIL

INTRODUÇÃO

Atualmente, um dos bens mais preciosos e ativos mais valiosos de uma organização é a informação. Ela é utilizada em todos os níveis hierárquicos e é uma vantagem competitiva para as empresas que sabem fazer um correto uso dela, o que torna necessário uma proteção adequada.

O desenvolvimento de PSI permite que a empresa implemente controles, práticas e procedimentos que garantam a segurança da informação e a continuidade dos negócios, protegendo-a de ameaças. Ela deve ser baseada em uma das melhores práticas de segurança e nesse estudo utilizou-se a ITIL por permitir a implementação em empresas independente do porte e auxiliar na qualidade dos serviços e segurança dos ativos e processos estratégicos de TI (Tecnologia da Informação).

Diante disso, elaborou-se este artigo, o qual aborda o tema: proposta de Implementação de Políticas de Segurança da Informação com Base em ITIL para uma Rede de Computadores da Biotecno, desenvolvedora de câmaras refrigeradoras para conservação de medicamentos, localizada em Santa Rosa – RS.

Com este estudo busca-se responder a questão problema: como a implantação de Políticas de Segurança da Informação com base em ITIL poderá contribuir para prover a segurança dos dados e informações da organização Biotecno? Para tanto partiu-se da hipótese de que o implemento de PSI contribui para manter as informações mais seguras de acessos lógicos e físicos, diminuindo a perda ou exposição das informações a terceiros.

Este estudo teve como objetivo geral propor um plano de implementação de políticas de segurança com base ITIL em uma organização desenvolvedora de

produtos para a área médica. Especificamente, buscou-se estudar as melhores práticas de TI baseadas em ITIL; mapear e analisar a estrutura e os processos de TI para identificar os possíveis problemas e necessidades de melhorias relacionados à segurança da informação; identificar os requisitos necessários para a elaboração das políticas de segurança, e por fim, elaborar, a partir das melhores práticas de TI baseadas em ITIL, a proposta de implementação de Políticas de Segurança da Informação que se adeque à empresa.

Com relação a metodologia empregada na realização deste estudo, quanto a natureza, trata-se de uma pesquisa teórico-empírica e com relação ao tratamento dos dados esta pesquisa é considerada qualitativa. Considerando os objetivos traçados para este estudo a pesquisa foi exploratória. Com relação à forma de pesquisa técnica, foram realizadas pesquisas bibliográficas, documental e estudo de caso.

Para o desenvolvimento deste estudo foram utilizadas documentações diretas e indiretas. No caso da documentação direta, explorou-se a observação direta extensiva, através da aplicação de um questionário ao gestor. Com base nos dados coletados fez-se o plano de análise e interpretação, sendo que a abordagem foi feita através do método hipotético-dedutivo; e a pesquisa qualitativa foi analisada de maneira comparativa, histórica e monográfica.

As informações obtidas foram comparadas com o embasamento teórico de modo a estabelecer um melhor entendimento e enriquecimento da discussão do problema proposto. No embasamento teórico, utilizou-se bibliografias de autores como: Ferreira e Araújo, Fontes e Dawel, entre outros.

Como primeira etapa fez-se uma breve introdução ao tema e, dando continuidade, foi desenvolvido o referencial teórico, abordando assuntos relacionados a Segurança da Informação, Políticas de Segurança da Informação e ITIL. Na segunda etapa deste trabalho, estão os métodos e técnicas, categorização da pesquisa, coleta e tratamento de dados. Na terceira etapa, as informações para a análise dos resultados foram obtidas através de um questionário aplicado ao gestor da empresa em estudo. Por fim, foi apresentada a conclusão, contendo os resultados e discussões ressaltando a importância da organização estabelecer os níveis de segurança através da implementação de uma Política de Segurança da Informação adequada a ela, garantindo sua proteção sem esquecer de que seus funcionários devem ser seus aliados nesse processo, mantendo-os bem informados.

1 REFERENCIAL TEÓRICO

No referencial teórico são abordados os seguintes tópicos: Gestão da Tecnologia da Informação, Segurança da Informação, Políticas de Segurança e Modelo ITIL.

1.1 TECNOLOGIA DA INFORMAÇÃO

A Tecnologia da Informação vem, de forma gradativa, tornando-se cada vez mais importante, trazendo benefícios e qualidade para as organizações e para os usuários. Tendo como principal finalidade a eficiência e a velocidade na realização dos processos e tarefas segundo Foina, “a Tecnologia da Informação é um conjunto de métodos e ferramentas, mecanizadas ou não, que se propõe a garantir a qualidade e pontualidade das informações dentro da malha empresarial.” (FOINA, 2009, p. 32).

O uso da TI nas empresas e organizações como ferramenta de gestão ocorre devido a sua capacidade de proporcionar o crescimento e competitividade necessários a elas. Conforme Castells, a administração dos recursos de materiais humanos e financeiros, pode ser realizada com mais rapidez e precisão com a utilização da tecnologia da informação (CASTELLS, 2000).

A crescente evolução da TI e a facilidade com a qual as empresas podem lidar com essa ferramenta fez com que as organizações passassem a dispor de uma infraestrutura de TI cada vez maior, não apenas para armazenar informações, mas também para ajudar no controle, no processamento de dados e informações e nos processos de trabalho.

Segundo Laudon e Laudon a TI permite que as diversas áreas e processos das empresas sejam interligados e coordenados (LAUDON; LAUDON, 2007). Para os administradores da empresa a Tecnologia da Informação auxilia no alcance das metas estabelecidas e, as informações geradas com o seu auxilio, servem de base para a maioria das decisões tomadas.

A TI trouxe para as empresas muitos benefícios, como automação nos processos, controle, redução de custo, a possibilidade de coletar, armazenar e processar informação e conectar pessoas. Ela mudou a forma de fazer negócios, pois além de ser uma ferramenta que manipula dados e processa informações, é

considerada como uma estratégia de negócio que viabiliza o relacionamento com clientes e traz vantagens competitivas.

No mundo globalizado, o produto mais valioso de uma empresa é a informação na hora certa, no formato certo. Las Casas afirma que “a tecnologia permite que a informação flua bilateralmente entre cliente e empresa. Cria um relacionamento que integra cliente e empresa, permite que a empresa detenha o mercado, estabelece um diálogo, permite customização e transforma o produto em serviço e o serviço em produto.” (LAS CASAS, 2010, p. 29).

Em decorrência da evolução das tecnologias surge a Gestão da Tecnologia da Informação. Esta passou a ser difundida em escala mundial, tendo como atribuição básica realizar a gestão de toda a estrutura tecnológica existente mantendo, organizando e planejando formas de torná-la mais rentável e vantajosa aos negócios. Uma vez que as informações são um dos bens mais importantes no meio organizacional, a Gestão da Tecnologia da Informação precisa abranger um aspecto muito importante para as empresas: a segurança da informação.

1.2 SEGURANÇA DA INFORMAÇÃO

A informação é um dos maiores patrimônios de uma organização pois ajuda a mantê-la competitiva no mercado e auxilia os gestores na tomada de decisão. Sendo assim, sua segurança é fundamental para as empresas.

Conforme Baltzan e Phillips a informação organizacional é seu capital intelectual e assim como as empresas protegem seus ativos, o capital intelectual também deve ser protegido. Para os autores “a segurança da informação é um termo amplo que abrange a proteção da informação contra mau uso acidental ou intencional por pessoas dentro e fora da empresa.” (BALTZAN; PHILLIPS, 2012, p. 104).

Os dirigentes das empresas perceberam a importância da aplicação de tecnologia nas estratégias de negócios pois está permite diferenciar uma empresa de seus concorrentes. Entretanto, somente a tecnologia não será suficiente para obter sucesso. É preciso informações que permitam a correta tomada de decisão e investimento em métodos que garantam a segurança dessas informações. Segundo Ferreira e Araújo uma solução de segurança adequada deve satisfazer os seguintes requerimentos fundamentais de segurança:

- Confidencialidade: garante de que a informação será acessada somente por pessoas autorizadas a terem acesso;

- Integridade: garante a exatidão da informação e dos métodos de processamento. Uma informação integra vai estar do mesmo jeito que ela foi enviada;

- Disponibilidade: garante que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

- Auditabilidade: o acesso e o uso da informação devem ser registrados, permitindo a identificação de quem fez o acesso e o que foi feito ou alterado na informação;

- Não repúdio: o usuário que gerou ou alterou a informação não pode negar o fato, pois a empresa faz uso de mecanismos que garantem a verificação da autoria (FERREIRA; ARAÚJO, 2008).

Quanto a confiabilidade da informação, para Ferreira e Araújo ela pode ser classificada em três classes. A primeira delas é a informação pública que são aquelas divulgadas fora da organização pois não causam impactos para os negócios como cartazes de divulgação. A segunda classe é a de informações internas as quais todos os empregados da empresa tem acesso mas que não podem tornar-se públicas. E a terceira abrange as informações confidenciais que podem ser acessadas apenas por um grupo de pessoas autorizadas (FERREIRA; ARAÚJO, 2008).

Quanto ao quesito integridade existem duas maneiras pelas quais pode ocorrer violação: violação lógica e violação física. Para Dawel, a lógica ocorre quando a informação sofre alterações, é apagada ou acessada por uma pessoa não autorizada, como ocorre em um roubo de senha. A física quando a informação sofre alterações nos ativos físicos onde é armazenada e compartilhada como por exemplo quando o servidor é danificado causando falha no banco de dados (DAWEL, 2005).

Esses cinco requisitos fundamentais são essenciais para manter as informações protegidas e devem estar interligados para que assim, a organização possa desenvolver um plano de segurança de acordo com as suas necessidades.

De uma forma simples, para Fontes, um plano de segurança da informação deve possibilitar que os controles de proteção sejam implementados de forma estruturada; ser padronizada para todas as plataformas de tecnologia; considerar todos os tipos de usuários; atender de forma corporativa os requisitos legais; garantir

que o acesso à informação utilize autenticação (confirme a identidade dos usuários) e autorização (permite que um usuário tenha acesso a uma determinada informação) semelhantes em todos os ambientes; considerar a necessidade da disponibilidade dos recursos de informação para a realização do negócio corporativo; ter flexibilidade para manter a efetividade da proteção; estar comprometida com os requisitos do negócio (FONTES, 2008).

Uma organização é formada por pessoas, equipamentos e estrutura física. A informação passa por equipamentos de tecnologia da informação e é acessada por pessoas dos mais diferentes níveis organizacionais. Assim, para Ferreira e Araújo a segurança pode ser desmembrada em quatro grandes aspectos:

- Segurança computacional: conceitos e técnicas utilizados para proteger o ambiente informatizado contra eventos inesperados que possam causar qualquer prejuízo;

- Segurança lógica: prevenção contra acesso não autorizado;

- Segurança física: procedimentos e recursos para prevenir acesso não autorizado, dano e interferência nas informações e instalações físicas da organização;

- Continuidade de negócios: estrutura de procedimentos para reduzir, a um nível aceitável, o risco de interrupção ocasionada por desastres ou falhas por meio da combinação de ações de prevenção e recuperação (FERREIRA; ARAÚJO, 2008).

Segundo Baltzan e Phillips, para que a segurança da informação abranja todos esses aspectos é preciso trabalhar duas linhas de defesa: pessoas e tecnologia (BALTZAN; PHILLIPS, 2012).

A primeira linha de segurança que uma empresa deve seguir é criar um plano de segurança da informação detalhado baseado em cinco passos, definidos por Baltzan e Phillips: desenvolver as políticas de segurança da informação; comunicar as políticas de segurança da informação; identificar os principais ativos e riscos associados a informação; testar e reavaliar esses riscos; obter apoio das partes interessadas (BALTZAN; PHILLIPS, 2012).

A segunda linha de defesa das empresas é a Tecnologia. As organizações podem implementar várias tecnologias para evitar violações de segurança da informação. Determinar em quais tipos de tecnologia investir ajuda a atender as três principais áreas de segurança da informação. A primeira, segundo Baltzan e Phillips

é autenticação e autorização (a autenticação é um método para confirmar as identidades dos usuários); e a segunda prevenção e resistência, ouse seja, sistemas de detecção de intrusos permitem controlar toda a atividade na rede, incluindo possíveis violações de segurança (BALTZAN; PHILLIPS, 2012).

Conforme Baltzan e Phillips para essas duas áreas de segurança é possível realizar os seguintes procedimentos: filtragem de conteúdo que é feita pelas empresas utilizando um software que filtra conteúdo para evitar a transmissão de informações não autorizadas; criptografia que codifica a informação de uma forma alternativa, que requer uma chave ou uma senha para descriptografar as informações; e firewalls que é um hardware e/ou software que protege uma rede privada por meio da análise das informações que entram e saem da rede (BALTZAN; PHILLIPS, 2012).

A terceira área de segurança da informação, conforme Baltzan e Phillips é detecção e resposta, que ocorre se as estratégias de prevenção e resistência falham e há uma violação de segurança. Nesse caso uma empresa pode utilizar as tecnologias de detecção e resposta para minimizar os estragos. O tipo mais comum é o uso de um software antivírus (BALTZAN; PHILLIPS, 2012).

Assim, conforme Baltzan e Phillips a segurança da Informação abrange a proteção da informação (BALTZAN; PHILLIPS, 2012). Os controles de segurança devem ser possíveis de serem implementados em todas as plataformas de tecnologia, evidentemente considerando as características e limitações de cada uma. Logo, as políticas da segurança da informação são implantadas para que exista uma solução que seja válida para toda a corporação.

1.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Atualmente, independente do estágio de tecnologia da organização, a proteção da informação deve ser uma das preocupações dos executivos e proprietários das empresas. As políticas de segurança da informação resumem-se em estabelecer regras de segurança física e lógica às informações contidas na organização por meio de sistemas de computação. Segundo Dawel as políticas de segurança podem ser definidas como um conjunto de diretrizes que definem formalmente as regras e os direitos dos funcionários e prestadores de serviços, visando à proteção adequada dos ativos da informação (DAWEL, 2005).

Apesar da importância que a informação tem para as empresas é necessário permitir que funcionários, consumidores e parceiros tenham acesso a elas. Com a existência de uma política de segurança fica explicito o que cada pessoa da organização deve cumprir no que se refere à proteção da informação.

No entanto, a política não deve surgir do nada. Segundo Castro é necessário que a política esteja alinhada aos objetivos da organização e a partir dos objetivos de negócio, são definidos os objetivos da segurança da informação, que possibilitam a realização do negócio no que depende do uso dos recursos de informação. Assim, a política e demais regulamentos definem estratégias, regras, padrões e procedimentos que direcionarão todas as ações para atingir os objetivos da segurança da informação. Essas ações podem ser atividades técnicas ou atividades de usuários (CASTRO, 2012).

As políticas de segurança da informação identificam as regras necessárias para manter a segurança da informação. Segundo Ferreira e Araújo as políticas de segurança da informação deve ser:

> - Simples;
> - Compreensíveis (escritas de maneira clara e concisa);
> - Homologadas e assinadas pela Alta Administração;
> - Estruturadas de forma a permitir a sua implantação por fases;
> - Alinhadas com as estratégias de negócio da empresa, padrões e procedimentos já existentes;
> - Orientadas aos riscos (qualquer medida de proteção das informações deve direcionar para os riscos da empresa);
> - Flexíveis (moldáveis aos novos requerimentos de tecnologia e negócios);
> - Protetores dos ativos de informações, priorizando os de maior valor e de maior importância;
> - Positivas e não apenas concentradas em ações proibitivas ou punitivas (FERREIRA; ARAÚJO, 2008, p. 37-38)

A elaboração da política de segurança da informação deve adequar-se às necessidades da organização. Para isso é necessário fazer um levantamento das informações gerais da empresa, para que se possa esclarecer onde há riscos e vulnerabilidades nos processos lógicos e na infraestrutura física.

As políticas elaboradas servirão como guia prático para a realização dos procedimentos de segurança da informação, ajudando a criar confiança nas atividades organizacionais. Segundo Baltzan e Phillips as políticas de segurança “identificam as regras necessárias para manter a segurança da informação.” (BALTZAN; PHILLIPS, 2012, p. 108). Para que a PSI realmente seja aplicada na

empresa é necessário a sua ampla divulgação e os funcionários devem ser treinados facilitando o processo de conscientização da sua importância.

Do mesmo modo que uma empresa precisa oferecer qualidade nos serviços, ela precisa também se adequar às necessidades de segurança. Para Ferreira e Araújo os principais benefícios de implantar uma política de segurança são a formalização e documentação dos procedimentos de segurança adotados pela organização; implementação de novos procedimentos e controles; prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou desastres e maior segurança nos processos do negócio. A médio prazo ocorre a padronização dos procedimentos de segurança incorporados na rotina da empresa; adaptação segura de novos processos do negócio; qualificação e quantificação dos sistemas de resposta a incidentes; e conformidade com padrões de segurança. A longo prazo ocorre o retorno sobre o investimento realizado, por meio da redução dos problemas e incidentes de segurança da informação e a consolidação da imagem corporativa associada à Segurança da Informação (FERREIRA; ARAÚJO, 2008).

Assim, considerar e analisar estes aspectos possibilita a elaboração de uma política de segurança da informação adequada para a organização. Ferreira e Araújo aponta como fatores comuns entre todas as Políticas de Segurança da Informação:

- Especificação da política: deve ser breve, utilizar palavras simples e formalizar o que é esperado dos funcionários da organização;

- Declaração da Alta Administração: o nome do executivo principal da organização demostra aos colaboradores que este executivo está de acordo com as políticas expostas no documento, bem como mostra seu comprometimento para que elas sejam adequadamente cumpridas;

- Autores / Patrocinadores da Política: os nomes dos profissionais, ou equipes, que desenvolveram as políticas devem estar especificados no documento;

- Referências a outra políticas, normas e procedimentos: em muitas organizações é comum que as políticas em vigor façam referência a outros regulamentos internos já existentes ou em desenvolvimento;

- Procedimentos para requisição de exceções à política: mais importante do que preparar e divulgar a política, também é o processo de requisição de exceções a ela descrevendo os procedimentos de solicitação;

- Procedimentos para mudanças da política: as políticas devem especificar responsáveis, em nível hierárquico e/ou especificação técnica, para seu controle e atualização;

- Datas de publicação, validade e revisão: a política deve possuir a assinatura do principal executivo aprovando-a, a data da última atualização e do início de sua vigência (FERREIRA; ARAÚJO, 2008).

Assim, uma política de segurança deve desenvolver ações alinhadas com as melhores práticas para a proteção e controle da informação. Conforme Dawel, como padrão de mercado aceito e seguido pela grande maioria das organizações e governos encontram-se a ITIL - Information Technology Infrastructure Library (DAWEL, 2005). Essa prática recomenda a existência de processo formal de conscientização em segurança da informação, pode ser agregado à empresas de grande, médio e pequeno porte e auxilia nos primeiros passos da busca da qualidade de serviços e segurança dos ativos e processos estratégicos de TI.

1.4 ITIL

As organizações estão cada vez mais dependentes de Tecnologia da Informação para auxiliar no cumprimento dos objetivos de negócio. Essa dependência constante e crescente necessita fortemente de qualidade dos serviços de Tecnologia alinhados com as exigências do negócio. Segundo Ferreira e Araújo o avanço da tecnologia fez com que os negócios ficassem totalmente dependentes da TI e “é essencial que as áreas de TI reconheçam que isto significa que a qualidade, a quantidade e a disponibilidade da infraestrutura afetam diretamente a qualidade, a quantidade e a disponibilidade que o negócio pode oferecer.” (FERREIRA; ARAÚJO, 2008, p. 65).

Dentre as melhores práticas para a proteção e controle da informação, encontra-se o ITIL (ou Biblioteca para Infraestrutura de serviços de TI, na língua portuguesa) que adota uma estratégia orientada a processos para atender qualquer tipo de organização e, conforme Ferreira e Araújo, "considera o Gerenciamento de Serviços em TI como um conjunto de processos estreitamente relacionados e altamente integrados. Para atingir os objetivos chaves do Gerenciamento de Serviços em TI, devem ser utilizadas: as pessoas, processos e tecnologias." (FERREIRA; ARAÚJO, 2008, p. 65).

Isso garante que as organizações possam estar seguras da entrega de serviços de TI de qualidade alinhados com os processos de negócios, atendendo as necessidades dos clientes. Assim, para Abreu e Fernandes "ITIL é um agrupamento das melhores práticas utilizadas para o gerenciamento de serviços de tecnologia da informação de alta qualidade, obtidas em consenso após décadas de observação prática, pesquisa e trabalho de profissionais de TI e processamento de dados em todo o mundo." (ABREU; FERNANDES, 2012, p. 256).

A ITIL surgiu em 1980 com objetivo de melhorar os processos dos departamentos de TI do Governo Britânico e foi desenvolvida pela CCTA (*Central Computing and Telecommunications Agency*), atual OGC (*Office of Government Commerce*), órgão do Governo Britânico responsável por desenvolver padrões de melhorias de processos internos. A segunda versão ITIL V2 surgiu em 1999 e teve o propósito de abordar a eficiência e eficácia dos serviços. Em 2007 foi lançado o ITIL V3 que foca o Gerenciamento de serviços para negócio e tecnologia, tendo em vista os ciclos de vida das boas práticas de serviço, ou seja, conforme afirma Abreu e Fernandes “permite que se tenha uma visão do gerenciamento de serviços pela perspectiva do próprio serviço, em vez de focar em cada processo ou prática por vez.” (ABREU; FERNANDES, 2012, p. 257).

A biblioteca ITIL contempla os seguintes assuntos: estratégia de serviços, desenho de serviços, transição de serviços, operação de serviços e melhoria contínua de serviços. Cada um deles é relacionado a um estágio do ciclo de vida do serviço.

O primeiro assunto abordado pela biblioteca trata da estratégia de serviços. Nessa etapa são definidos quais serviços de TI a empresa oferece e para quem (definição de mercado), são desenvolvidas ofertas, ativos estratégicos e ocorre a preparação e determinação da execução dos serviços.

O segundo assunto abordado é o desenho de serviços que, segundo Freitas, “busca orientar a concepção dos Serviços de TI para garantir a qualidade do serviço, a satisfação do cliente e a relação custo e benefício na prestação de serviços.” (FREITAS, 2010, p. 92). Este estágio do ciclo de vida do serviço estabelece o uso de práticas, processos e políticas de TI na produção do serviço e está diretamente ligado a segurança da informação.

O estágio de desenho dos serviços abrange um conjunto de processos-chaves de gerenciamento de serviços, que segundo Abreu e Fernandes englobam:

- Catálogo de Serviços: trata de todos os serviços que estão operacionais e aqueles que estão sendo preparados para entrar em operação;

- Nível de Serviço: busca manter e melhorar a qualidade dos serviços de TI através de um ciclo contínuo de atividades envolvendo um planejamento, coordenação, elaboração, estabelecimento de acordo de metas de desempenho e responsabilidades mútuas, monitoramento e divulgação de níveis de serviço, operacionais e de contratos de apoio (fornecedores);

- Capacidade: assegura que a capacidade da infraestrutura de TI absorva as demandas do negócio;

- Disponibilidade: visa assegurar que os serviços de TI não sejam interrompidos preservando os níveis de disponibilidade e confiabilidade requeridos;

- Continuidade do Serviço de TI: visa assegurar que todos os recursos técnicos e serviços de TI possam ser recuperados dentro de um prazo preestabelecido;

- Segurança da Informação: relaciona-se a garantia de confiabilidade, integridade e disponibilidade de dados, segurança dos componentes de TI, documentação e procedimentos;

- Fornecedores: gerencia fornecedores e os contratos necessários para suportar os serviços por eles prestados (ABREU; FERNANDES, 2012).

Assim, a biblioteca ITIL refere-se a efetividade da segurança da informação através do detalhamento do planejamento e gerenciamento. É preciso analisar o impacto que cada processo realizado tem sobre o negócio, definir os requisitos necessários para o seu desenvolvimento, analisar os riscos envolvidos e verificar os resultados. Abreu e Fernandes afirmam que “há a necessidade de aquisição ou desenvolvimento de ferramentas para automatizar atividades de desenho de serviços (processos, infraestrutura, software, etc.) e para aumentar a eficácia, a eficiência, a segurança e a qualidade do gerenciamento do serviço durante a sua operação contínua.” (ABREU; FERNANDES, 2012, p. 271).

O terceiro assunto abordado pela ITIL é a transição de serviços, que segundo Freitas, tem como objetivo colocar no ambiente de produção um serviço que saiu do estágio de desenho garantindo o cumprimento dos requisitos de custo, qualidade e prazo de entrega (FREITAS, 2010).

Similar a ITIL V2, a V3 contempla ainda a fase de Operação de Serviços que trata sobre o gerenciamento de incidentes e problemas. Esta fase inclui as

atividades necessárias para entregar e suportar os serviços e, conforme Abreu e Fernandes, tem o objetivo de coordenar e executar essas atividades dentro dos níveis de serviços estabelecidos com os clientes (ABREU; FERNANDES, 2012).

No estágio de operação de serviço, segundo Abreu e Fernandes, está o Gerenciamento de Eventos que monitora todos os eventos que ocorrem na infraestrutura de TI para garantir a normalidade da operação. Pode ser dos tipos: exceção (incidentes, problemas ou mudança), advertências ou pedidos de informação. Cada um dos tipos terá tratamento distinto (ABREU; FERNANDES, 2012).

Por último a biblioteca ITIL trata sobre a melhoria contínua de serviços que visa garantir que os serviços de TI estejam constantemente alinhados e integrados às necessidades do negócio. Conforme Abreu e Fernandes essa etapa contem em seu escopo todas às atividades que suportam o planejamento contínuo da melhoria de processos (ABREU; FERNANDES, 2012).

Assim, a ITIL busca o alinhamento dos serviços de TI aos serviços do negócio em todas as etapas dos processos desenvolvidos garantindo que a segurança da informação seja gerenciada de forma correta em todos os serviços e atividades de TI. Ela também garante o controle dos riscos de segurança e que os recursos da empresa sejam utilizados de maneira responsável.

2 METODOLOGIA

Esta etapa está organizada em três tópicos com o objetivo de ajudar na compreensão e análise das informações: categorização da pesquisa, geração de dados e análise e interpretação dos dados.

2.1 CATEGORIZAÇÃO DA PESQUISA

Quanto à natureza o estudo caracteriza-se como uma pesquisa teórico-empírica uma vez que teve tanto pesquisas em bibliografia quanto observação do ambiente e coleta de dados na empresa em estudo. Gil classifica o estudo teórico-empírica como “pesquisa aplicada voltada à aquisição de conhecimentos com vistas à aplicação numa situação específica. ” (GIL, 2010, p.27).

Quanto ao tratamento dos dados, o projeto caracteriza-se como uma pesquisa qualitativa, uma vez que buscou avaliar o contexto da organização e seus

processos através de observação do ambiente e questionário aberto aplicado ao gestor. É classificada por Vianna como uma pesquisa na qual o pesquisador “analisará cada situação a partir de dados descritivos, buscando identificar relações necessárias à compreensão da realidade estudada. ” (VIANNA, 2001, p.122).

Quanto aos fins, este estudo trata-se de uma pesquisa exploratória a fim de que a informações coletadas na empresa sobre como ocorre a proteção das informações atualmente sejam compreendidas mais facilmente. Segundo Gil as pesquisas exploratórias “têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. ” (GIL, 2010, p.27).

Quanto aos procedimentos técnicos, pode-se qualificar essa pesquisa como pesquisa bibliográfica e estudo de caso. Pesquisa bibliográfica segundo Gil é realizada “com propósito de fornecer fundamentação teórica ao trabalho bem como a identificação do estágio atual do conhecimento referente ao tema” (GIL, 2010, p. 29). Buscou-se conhecimentos sobre o assunto tratado neste estudo, desenvolvidos por diferentes pesquisadores a fim de solucionar o problema da pesquisa e foi feita a análise da empresa para que a teoria pudesse ser utilizada para desenvolver uma política de informação para a Biotecno.

Por fim, a pesquisa qualifica-se com estudo de caso, definida por Vianna como “um estudo detalhado de um objeto ou situação de forma a permitir o entendimento da sua totalidade. ” (VIANNA, 2001, p.140).

Esclarecendo o tipo de pesquisa é o momento de trazer o plano de coleta de dados.

2.2 GERAÇÃO DE DADOS

Para a coleta de dados foram utilizados dois tipos de fontes: primárias (questionários e entrevistas com as pessoas na empresa em estudo) e secundárias (levantamento de relatórios e documentos que descrevam informações importantes para o estudo).

Cervo, Bervian e Silva afirmam que o questionário “é a forma mais usada para coletar dados, pois possibilita medir com mais exatidão o que se deseja” (CERVO; BERVIAN; SILVA, 2007, p. 53). Assim, em um primeiro momento, foi aplicado um questionário ao gestor da empresa com a finalidade de verificar o interesse da

organização na elaboração de políticas de segurança da informação e quais aspectos ela deve prever, objetivando verificar e descobrir as atuais lacunas existentes na empresa e tornando possível a elaboração de um projeto mais específico. O questionário abrange vinte e seis questões abertas, detalhando, baseando em Ferreira e Araújo, as áreas de segurança física e backup[3] (FERREIRA, ARAÚJO, 2008) e baseado em Fontes as áreas de política de segurança de informação, gestão da segurança da informação e controle de acesso aos sistemas de informação da empresa (FONTES, 2008).

O questionário foi aplicado pelo pesquisador ao gestor da empresa, de forma eletrônica (as perguntas foram enviadas por e-mail) no dia 28 de agosto de 2017 e a resposta foi recebida no mesmo dia.

Em um segundo momento, foi realizada coleta de dados por meio de documentação indireta através de pesquisa bibliográfica de autores como Ferreira e Araújo, Freitas, Fontes, entre outros, e documentação direta por meio de observação simples tendo em vista que é necessário analisar o ambiente da empresa, seus processos e infraestrutura para propor uma política de segurança da informação que auxilie a empresa na proteção das informações, o que foi feito durante o horário de expediente na empresa pelo próprio pesquisador, nos meses de setembro e outubro de 2017.

Com a coleta de dados permite-se a análise e interpretação dos seus resultados, levando ao alcance do objetivo do estudo.

2.3 ANÁLISE E INTERPRETAÇÃO DOS DADOS

O método de abordagem que foi utilizado neste estudo é o hipotético-dedutivo porque se partiu de um problema para construir as possíveis respostas, que foi definido como sendo: como a implantação de Políticas de Segurança da Informação com base em ITIL pode contribuir para prover a segurança dos dados e informações da organização Biotecno? Como possível solução, após a geração de dados foi desenvolvida uma Política de Segurança de Segurança da Informação com base em ITIL adequando a linguagem da norma para a empresa por ser tratar de uma

[3] Backup é um termo inglês que significa cópia de segurança. É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento, garantindo que, se por algum motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos.

organização de pequeno porte, e foi definido como a PSI pode ser implementada, seus custos e tempo de implantação

Além do método de abordagem tem-se os métodos de procedimentos. Neste estudo foram utilizados o histórico, o comparativo e o monográfico.

O método de procedimento histórico foi utilizado para auxiliar na fundamentação bibliográfica utilizando autores que tratam sobre assuntos relevantes para este estudo em específico. Segundo Markoni e Lakatos esse método “consiste em investigar os acontecimentos, processos e instituições do passado para verificar sua influência na sociedade de hoje” (MARCONI; LAKATOS, 2010, p.172).

O método de procedimento comparativo foi utilizado para realizar a comparação entre teoria e prática. Segundo Vianna o método comparativo “consiste no confronto entre elementos, levando em consideração seus atributos” (VIANNA, 2001, p.152). Assim, após pesquisa bibliográfica foi realizada uma adaptação das normas ITIL para construção de uma política de segurança de informação que se adequasse a empresa Biotecno.

Por fim, foi empregado o método de procedimento monográfico que conforme Marconi e Lakatos “consiste na observação de determinados indivíduos, profissões, condições, instituições, grupos ou comunidades, com a finalidade de se obter generalizações” (MARCONI; LAKATOS, 2010, p.173). O método de procedimento monográfico foi utilizado por se tratar de um estudo de caso aplicado à Empresa Biotecno, desenvolvedora de câmaras refrigeradoras para conservação de medicamentos, referente a implementação de Políticas de Segurança da Informação com Base em ITIL.

Os dados obtidos na técnica de coleta, por meio da observação e da aplicação de questionário ao gestor, foram estudados e confrontados com a teoria já existente sobre o tema analisado, para que se tivesse clareza da atual situação da empresa e dos passos a serem seguidos para elaboração de uma política de segurança da informação.

3 ANÁLISE DOS RESULTADOS

O propósito da segurança da informação é alinhar a segurança de TI com a segurança do negócio, garantindo integridade, disponibilidade e confiabilidade nos termos acordados através da especificação de uma PSI. Para Cestari Filho, segundo

as orientações da ITIL, o objetivo da segurança é cumprido quando se seguem os princípios: confidencialidade (somente quem tem direito de acesso, vê ou observa a informação; integridade (a informação está completa, precisa e protegida contra modificações não autorizadas); disponibilidade (a informação está disponível e utilizável quando necessário e os sistemas podem resistir a ataques, prevenir ou recuperar-se de falhas); autenticidade (transações comerciais, bem como o intercâmbio de informações entre empresas ou com parceiros são confiáveis) (CESTARI FILHO, 2011).

Considerando esses princípios, para conhecer a organização, a infraestrutura de TI, os processos e as necessidades para a elaboração de uma PSI, foi aplicado um questionário estruturado ao gestor da organização, composto de vinte e seis questões abertas focando a obtenção de informações sobre a política de segurança da informação a ser elaborada para a empresa.

A Biotecno é uma empresa de pequeno porte, que atualmente conta com 25 funcionários trabalhando divididos em 15 estações de trabalho, que atua na área de refrigeração médico-científica, fundada em 2002, na cidade de Santa Rosa - RS. Através dos esforços de seus idealizadores, um casal que sonhava desenvolver um produto inovador e inédito no Brasil, capaz de revolucionar a atual maneira de conservar vacinas no país, a Biotecno despontou no mercado nacional. Aliando o conhecimento de sua equipe de desenvolvimento de projetos às necessidades dos postos de saúde, clínicas e hospitais, a Biotecno desenvolveu uma linha de câmaras para conservação imunobiológicos, termolábeis e hemoderivados capaz de manter-se em funcionamento em períodos de ausência de energia elétrica comercial, evitando perdas de material por estas eventualidades. A empresa atende atualmente todo pais.

Na primeira etapa do questionário, baseado em Fontes as questões foram voltadas as áreas de política de segurança de informação, gestão da segurança da informação e controle de acesso aos sistemas de informação da empresa (FONTES, 2008).

Quanto as políticas de segurança da informação, a primeira questão buscou avaliar a existência de um documento principal de política de segurança de informação definindo as diretrizes e filosofia da organização em relação ao uso e proteção da informação, ao que o gestor afirmou existir um documento contendo as normas da empresa no qual está incluído a especificação de que as informações da

Biotecno são sigilosas e não podem ser repassadas a terceiros. Este é repassado ao funcionário no momento da contratação e assinado por ele, garantindo a ciência de que as informações da empresa são sigilosas.

Não existe um documento formal especificando a PSI, nem outros regulamentos que complementam e detalham como os objetivos descritos da política principal de segurança da informação podem e devem ser alcançados.

Segundo Fontes quando um funcionário começa a trabalhar em uma organização, ele recebe um Termo de Compromisso onde são descritas suas principais responsabilidades em relação à informação e garante que ele esteja ciente sobre a necessidade de manter o sigilo das informações da organização as quais terá acesso, seguir as normas de segurança da informação e seguir o padrão ético da organização (FONTES, 2008). Assim, a elaboração de PSI permite prevenir problemas legais e garantir a proteção dos ativos da organização contra acesso indevido. Nesse processo é essencial o envolvimento da administração da empresa.

O gestor afirmou ainda não existir um processo de conscientização e treinamento de usuários em segurança da informação. Segundo Ferreira e Araújo o ideal é que a empresa forme um Comitê de Segurança da Informação constituído por profissionais dos diversos departamentos da empresa que deverá catalogar as informações da organização e agrupá-las por categorias ressaltando sempre que as PSI devem ser simples, escritas de maneira clara e concisa, estruturada de forma a permitir sua implantação por fases, orientadas com as estratégias de negócios e aos riscos, flexíveis e protetoras dos ativos de informação, priorizando os de maior importância (FERREIRA; ARAÚJO, 2008).

Quanto a gestão da segurança da informação, segundo o gestor, não existe uma política de classificação da informação que define os níveis de sigilo e indica para cada um deles como deve ser tratada a informação.

Segundo Ferreira e Araújo, ao elaborar uma PSI, deve-se determinar a classificação que será utilizada e os controles de segurança adequados. Cada classificação deve ser de fácil compreensão e claramente descrita para demostrar a diferenciação entre elas, devendo-se evitar níveis excessivos. Os níveis sugeridos são: informação pública, informação interna, informação confidencial e informação confidencial restrita (FERREIRA; ARAÚJO, 2008).

Quanto ao controle de acesso aos sistemas de informação da empresa os usuários não são orientados que são responsáveis pelo acesso realizado com a sua

autenticação. O sistema usado atualmente pela empresa é o Sistema Gestor, desenvolvido pela Abase Sistemas, localizada em Três de Maio – RS, que permite o cadastro de clientes, gestão financeira, gestão contábil, controle de materiais e vendas. O armazenamento das senhas no Banco de Dados do Sistema Abase, segundo informa o desenvolvedor, é feito de modo criptografado. Além disso, utiliza nas estações de trabalho, o Windows Server 12, que faz autenticação de acesso nos terminais. A GPO[4] (*Group Policy* ou Diretiva de Grupo) do Windows Server 2012 não está ativa o que não garante o armazenamento de senhas com criptografia reversível.

Na empresa, tanto para o site quanto para os e-mails é utilizado a KingHost, uma empresa especializada em segurança, suporte técnico e servidores, localizada em Porto Alegre - RS, que realiza a hospedagem do site (www.biotecno.com.br) e o serviço de e-mails coorporativo. A empresa trabalha com criptografia em seu serviço de e-mail. A gestora afirmou ainda que armazena uma lista com usuários e senhas dos e-mails para controle da empresa.

Além disso, o gestor afirma que, em alguns casos, existe mais de um colaborador utilizando o mesmo usuário e senha, para acesso aos computadores da Biotecno. Está não é secreta e de conhecimento exclusivamente do usuário, o armazenamento das senhas não é feito de modo criptografado e não existe uma política de troca periódica das senhas.

Fontes afirma que a proteção dos recursos está baseada na importância das informações e na necessidade de acesso de casa usuário, enquanto a identificação e autenticação são feitas normalmente por um usuário e senha. Esse controle de acesso lógico deve assegurar que apenas usuários autorizados tenham acesso aos recursos e que esse acesso seja apenas aos recursos necessários a execução de suas atividades, garantindo ainda que o acesso aos recursos críticos seja monitorado e restrito (FONTES, 2008).

O acesso a informação, no caso da Biotecno, é autorizado pelo gestor da empresa e liberado para o usuário somente após essa autorização, sendo que no momento, não existe um processo de revalidação periódica pelo gestor, dos usuários que estão autorizados a acessar a informação que o gestor autoriza.

---

[4] Conjunto de regras que controlam o ambiente de trabalho de contas de usuário e contas de computador. É capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede.

Para Ferreira e Araújo, o processo adequado para manutenção de um controle efetivo sobre os acessos aos Sistemas de Informação requer revisão periódica das contas de usuários e seus respectivos privilégios. Além disso, os autores afirmam que a identificação do usuário deve ser única e cada usuário deve ter uma identificação própria. Os usuários que forem demitidos devem ter seus acessos bloqueados (FERREIRA; ARAÚJO, 2008).

O gestor afirmou ainda, quando questionado, que não existe uma política para a definição de uso (ou não) de criptografia quando do armazenamento, apresentação ou transmissão de dados. Quanto a isso, conforme Ferreira e Araújo, durante o processo de avaliação de riscos e classificação da informação, deve-se determinar o nível de proteção a ser dado a determinada informação, e conforme o nível torna-se adequado o uso de criptografia para proteger a confidencialidade e integridade das informações (FERREIRA; ARAÚJO, 2008).

Na segunda etapa do questionário, baseando em Ferreira e Araújo as questões foram voltadas as áreas de segurança física e backup (FERREIRA; ARAÚJO, 2008).

Quanto ao Backup, o gestor informou que existe um funcionário responsável por sua realização. Isso não ocorre de forma automatizada e o processo é realizado manualmente. Para isso é utilizado o backup automático do Windows Server 2012 e é armazenado em um HD externo, que é guardado pelo gestor da empresa em um local seguro. O processo ocorre uma vez por semana (podendo variar o dia), levando em torno de uma hora e meia (normalmente ocorre das 17h15min as 18h45min).

Segundo Fontes, a disponibilidade do ambiente de processamento de dados é fundamental em qualquer organização. Para manter as informações disponíveis é necessário possuir procedimentos de backup (FONTES, 2008).

Não existem procedimentos formalizados de restauração de backups em caso de sinistros e não são realizados testes periódicos de restauração para validar o backup.

Nesse sentindo Ferreira e Araújo orientam que a organização deve elaborar seus procedimentos de backup visando diminuir riscos de continuidade seguindo as premissas: manter os backups distante fisicamente do locar de armazenamento dos dados originais; realizar testes nas mídias de armazenamento para assegurar que os dados estejam seguros e em perfeito estado para serem utilizados; desenvolver e

manter uma documentação dos procedimentos de backup sempre atualizada; assegurar que seja mantido um inventário sobre as mídias que armazenam os backups (FERREIRA; ARAÚJO, 2008).

Quanto a Segurança Física, não existem dispositivos de monitoramento, controle e combate a incêndio ou sistemas de ar-condicionado, ventilação e acústica.

Conforme Ferreira e Araújo, quanto mais críticos forem os equipamentos para a continuidade dos negócios, mais investimentos em recursos devem ser efetuados, com um técnico de segurança avaliando a necessidade de uso de equipamentos para extinção de incêndio automáticos, uso de portas corta-fogo e uso de alarmes de incêndio e detectores de fumaça. Para os autores a utilização de equipamentos de ar-condicionado, ventilação e acústica exige planejamento e em muitas ocasiões a realização de obras envolvendo especialistas em TI e engenharia (FERREIRA; ARAÚJO, 2008).

Quando ao abastecimento de energia elétrica de forma alternativa a empresa conta com um gerador para a rede inteira e o servidor está ligado a um nobreak, o que vai em conformidade com Ferreira e Araújo que afirmam que, para cada ativo considerado crítico, principalmente os de processamento de dados, deve haver fornecimento de energia de forma alternativa, independente das empresas fornecedoras de energia elétrica (FERREIRA; ARAÚJO, 2008). Quando um equipamento precisa de manutenção é chamada uma empresa terceirizada, mas não existe um procedimento formalizado para isso.

Para Castro, uma PSI deve ser implementada na empresa de forma que deixe claro para o funcionário como agir em relação aos recursos da empresa e deve incluir:

- Política de senhas: define as regras sobre o uso de senhas nos recursos computacionais (tamanho mínimo e máximo, regra de formação e periodicidade de troca);

- Política de backup: define as regras sobre a realização de cópias de segurança (tipo de mídia utilizada, período de retenção e frequência de execução);

- Política de privacidade: define como são tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários;

- Política de confidencialidade: define como são tratadas as informações institucionais e quem pode ter acesso;

- Política de uso aceitável: define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações em que não devem ser usados (CASTRO, 2012).

Assim, diante do levantamento dos dados na organização, torna-se evidente que a implementação de PSI é imprescindível para auxiliar a empresa a proteger-se de invasões e perda de dados. A proposta desenvolvida nesse estudo foi estruturada em 5 seções e 7 subseções, baseadas nas recomendações da ITIL, e adaptadas às necessidades da Biotecno. As seções são:

1) Especificação da política (dentro dela foi definida as aplicações da política);

2) Confidencialidade;

3) Integridade (especificando detalhadamente os critérios identificação, autorização de acesso, políticas de senha e cancelamento de acesso);

4) Disponibilidade (trazendo duas áreas: computadores e recursos tecnológicos e, política de backups);

5) Continuidade de negócios.

Em um primeiro momento, na especificação da política é ressaltado que o propósito da segurança da informação é alinhar a segurança de TI com a segurança do negócio, garantindo integridade e confiabilidade nos termos acordados através da especificação de uma PSI. Segundo a ITIL, o objetivo da segurança é cumprido quando se seguem os princípios: confidencialidade; integridade; disponibilidade e autenticidade.

Já as aplicações da política, estabelece que as diretrizes nela estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte dando ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Informa ainda que é obrigação de cada colaborador manter-se atualizado em relação a PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações. É de responsabilidade do gestor formalizar a ciência e o aceite da Política de Segurança da Informação por meio de termo e compromisso de cada colaborador e cabe a todos colaboradores e administradores cumprir com as reponsabilidades voltadas a política de segurança da informação.

A segunda sessão trata sobre a confidencialidade, lembrando que a Informação deve ser acessada e utilizada exclusivamente pelos usuários autorizados que necessitam dela para realização de suas atividades profissionais na empresa. As informações devem ser classificadas em um dos seguintes níveis:

- Confidencial Restrita: informações de interesse estratégico da organização, sujeitas a alto grau de sigilo, devendo ser acessada apenas pela alta administração da organização. Por exemplo: processos jurídicos estratégicos; estratégia de negócio; informações contábeis.

- Confidencial: são informações que se divulgadas de forma indevida podem reduzir vantagens competitivas da empresa, como por exemplo contratos com fornecedores, informações pessoais de funcionários, estratégias de marketing.

- Interna: informações utilizadas de forma rotineira pelos colaboradores na condução das atividades da empresa, não destinado ao público externo. Por exemplo: documentos de rotinas operacionais; políticas corporativas; campanhas internas.

- Pública: informações criadas para fins de publicação por meio de canais autorizados, que não necessitam proteção ou tratamento específico. Por exemplo: campanha de marketing externa; informações geradas para consumo público.

Em cada um dos níveis foram especificados o tratamento da informação quando a documentos eletrônicos, correio eletrônico, armazenamento de arquivos (no computador ou em diretórios de rede) e destruição das informações.

A terceira seção tratou sobre integridade lembrando que qualquer informação que é acessada, transmitida, recebida ou produzida fazendo uso da internet da Biotecno está sujeita a divulgação e auditoria. Portanto, a empresa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela. Suas subseções tratam sobre: identificação (prevendo o uso de senhas, crachás e identificações de acesso aos sistemas); autorização de Acesso (prevendo que cada usuário deve ser identificado individualmente por meio de uma credencial de acesso, através de login e senha); políticas de senha (estabelecendo critérios para escolha e armazenamento de senhas); cancelamento de Acesso (estabelece os critérios de cancelamento de acesso aos sistemas e e-mail).

A quarta seção trata sobre a disponibilidade aos computadores e recursos tecnológicos, lembrando aos colaboradores de suas responsabilidades quando ao uso dos equipamentos e informando ainda sobre a política de backups.

Quanto ao backup, conforme destacado pelo gestor da empresa, este já é realizado uma vez por semana por um funcionário responsável, o que aumenta os riscos de perda de informação. Portanto, a recomendação para a empresa é que o Backup seja feito com duas mídias externa (HD externo) da seguinte forma: uma mídia externa será utilizada para configurar um backup automático do Windows Server 2012 todos os dias úteis, copiando arquivos e pastas necessários as rotinas diárias que totalizam 359,41 Gb. A outra mídia externa é usada uma vez por semana para realizar um backup manual, por um funcionário responsável, que armazena todos os dados da empresa (pastas, arquivos, bancos de dados) totalizando 1,42 TB, e esta fica armazenada fora da empresa sob responsabilidade do gestor.

A longo prazo a empresa pode usar backup em nuvem, sendo o custo de US$66,15 por mês no Microsoft Azure para o armazenamento de 1,42 TB.

Por fim, a última sessão da política é destinada a continuidade de negócios.

A ilustração 1 demostra como a política pode ser implantada na empresa de forma escalonada através da ferramenta 5W2H considerando as necessidades da Biotecno e o custo de implantação.

Pontes et al., define a ferramenta 5W2H como um documento que visa identificar as ações e responsabilidades de quem fará a execução, através de um questionamento, onde após isso será possível fazer orientações das diversas ações que deverão ser implementadas (PONTES ET. AL, 2005).

What (O que)	Who (Quem)	Where (Onde)	When (Quando)	Why (Por que)	How (Como)	How much (quanto vai custar?)
Seção 1 – Especificação da Política	Gestora.	Na empresa.	Copia da PSI: entrega Imediata. Folders informativos: 3 semanas.	Segundo Dawel, a falha na conscientização dos colaboradores em tornar a segurança parte da cultura da empresa está entre os erros mais comuns das organizações. Materiais instrutivos e treinamentos podem ser usados nessa etapa preparando os funcionários para as normas (DAWEL, 2005).	- Entrega de uma cópia da PSI a cada funcionário; - Folders informativos lembrando da importância do cumprimento da política em sua fase inicial.	- Impressão da PSI (R$ 1,00 por cópia): R$25,00. - Folders informativos produzidos na empresa pela gestora e impressos na própria empresa: R$ 20,00. Tempo:
Seção 2 – Confidenciali-dade	Gestora.	Na empresa.	2 semanas.	Segundo Dawel, 95% dos problemas de segurança podem ser resolvidos com gerenciamento (DAWEL, 2005). Isso ocorre quando as empresas não sabem como controlar o trânsito das informações. A empresa precisa realizar a classificação da informação e as permissões de acesso conforme as atribuições dos funcionários.	A gerencia define as autorizações de acesso.	30h do gestor para definir as autorizações.

Seção 3 - Integridade	Funcionário responsável e gestor.	Na empresa.	- Folders informativos: 3 semanas. - Realizar a revisão: 6 meses. - Compra do Windows Server: 1 mês. - Office 365 Enterprise E1: no prazo de 3 meses. - Ativação de armazenamento de senhas usando criptografia reversível: imediato.	Segundo Dawel entre os problemas mais comuns encontrados nas empresas estão: enviar informações por meios não seguros; salvar informações sensíveis e confidenciais em áreas públicas; emprestar credenciais de acesso (física ou lógica); acessar sites proibidos; enviar correntes e email em massa; salvar arquivos pessoais na rede (MP3, vídeos etc) (DAWEL, 2005). Conscientizar e contar com o apoio dos funcionários é essencial para a garantia da segurança das informações.	- Folders informativos lembrando da importância do uso de identificação, da senha ser individual e dos critérios para escolha da senha; - A gerencia deve revisar as autorizações de acesso. - Criação de login e senha próprio para cada usuário. - Email corporativo para a empresa que trabalhe com criptografia na transmissão de mensagens. - Ativação de armazenamento de senhas usando criptografia reversível do Windows Server 2012. Para isso basta entrar no painel do Gerenciador do Servidor do Windows Server 2012, acessar a opção Políticas de Segurança Local e ativar a opção.	- Folders informativos produzidos na empresa pela gestora e impressos na própria empresa: R$ 20,00. - A gerencia realizar a revisão: 30h do gestor para realizar a revisão. - Compra do Windows Server com 25 usuários para que cada funcionário tenha seu próprio login e senha de acesso R$2000,00 e no caso de aumento de funcionários cada pacote com mais 5 acessos em custo aproximando de R$500,00. - Office 365 Enterprise E1: R$31,00 usuário/mês. - Ativação de armazenamento de senhas usando criptografia reversível do Windows Server 2012. Custo: 1 hora de trabalho de um funcionário que ficará responsável pela ativação.
Seção 4 – Disponibilidade	Funcionário responsável.	Na empresa	- Backup em mídias externas: imediato. - Backup em nuvem: no período de um ano.	Para Castro nos procedimentos é backup dizem respeito a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução. Já a politica de uso aceitável, também chamada de "Termo de Uso" ou "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas (CASTRO, 2012).	- Realizar backup semanal de duas mídias externas (HD Externo): uma usada para o backup diário através da configuração automática do Windows Server de pastas e arquivos usados diariamente, totalizando 359,41 Gb; uma usada para realizar o backup de pastas, arquivos e bancos de dados uma vez por semana, totalizando 1,42Tb, que será guardado fora da empresa sob responsabilidade do gestor. - Backup em nuvem.	- Backup em mídia externa: um HD Externo de 1Tb para backup diário. Custo: R$250,00. - Backup em mídia externa: um HD Externo de 2Tb para backup semanal. Custo: a empresa já possui o equipamento. - Backup em nuvem. Custo de US$66,15 por mês no Microsoft Azure para o armazenando de 1,42 Tb.
Seção 5 – Continuidade de Negócios	Coordenador por funcionário responsável e gestor.	Funcionário responsável	- Dentro do período de 1 ano e meio a dois anos.	Conforme Dawel, convém que as informações críticas sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados. Além disso, convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências. Pois além da proteção lógica das informações a segurança física também é algo muito importante, está segurança está relacionada com equipamentos que armazenam as informações utilizadas na organização (DAWEL, 2005).	- Construir uma sala própria para o servidor com: rack de servidores; rack de rede; porta de aço com visor de vidro temperado; fechadura com código eletrônico; gerador; ar condicionado; entradas de energia redundante; sala com proteção antichamas.	- rack de servidores (R$700,00); rack de rede (R$3500,00); porta de aço com visor de vidro temperado (R$1200,00); fechadura com código eletrônico (1550,00); gerador (a empresa já possui); ar condicionado (R$2000,00); entradas de energia redundante (R$2000,00); 1 extintor de incêndio de CO_2 usado para equipamentos elétricos (R$ 370,00 de 6kg). Total aproximado: R$ 8620,00.

Ilustração 1: Necessidade de Implantação da Política
Fonte: produção do pesquisador

Assim, conforme a necessidade da empresa e os custos de implantação as seções podem ser desenvolvidas em sequência e de forma escalonada. Os custos exatos da implantação das Políticas de Segurança da Informação variam muito da forma conforme a organização pretende obter a segurança da informação dentro do seu ambiente. Segundo Dawel há outros custos a serem levados em conta pela organização que são:

a) Materiais especializados e treinamento;

b) Auxilio externo (contratação de uma consultoria especializada, para acompanhar as tomadas de decisões);

c) Tecnologia empregada (obtenção de equipamentos necessários ou a adequação dos já existentes na organização);

d) Tempo dos funcionários: altamente necessário para que os funcionários possam se preparar e aplicar os conhecimentos obtidos, assim possibilitando a realização de melhorias (DAWEL, 2005).

Ainda segundo Dawel, o que será implantado na empresa é selecionado de acordo com as vulnerabilidades, riscos, obrigações contratuais, requisitos legais e de regulação submetidos à empresa (DAWEL, 2005). É importante ressaltar que os responsáveis por esta implantação devem ter visão empresarial pois a generalização da proteção, sem considerar os fatores críticos e sem identificar os processos importantes pode gerar gastos sem retorno efetivo para a empresa e/ou sem estar protegendo o que precisa ser protegido.

Finalizada a elaboração das PSI para a Biotecno e o levantamento de custos, observou-se a necessidade de estabelecer um processo continuo e estruturado para continuidade do programa, que foi desenvolvido utilizando a ferramenta 5W2H. Assim, as ações sugeridas são:

What (O que)	**Who (Quem)**	**Where (Onde)**	**When (Quando)**	**Why (Por que)**	**How (Como)**	**How much (Quanto vai custar)**
Criação de campanha d e conscientização dos colaboradores sobre a importância da PSI.	Funcionário responsável.	Na empresa.	Dois primeiros meses de implantação da PSI.	Para disseminação de conhecimento e conscientização dos colaboradores da empresa sobre a importância do tema e o cumprimento das normas.	Em folhetos informativos criados na própria empresa.	R$ 80,00
Realizar treinamento com todos os colaboradores da empresa.	Funcionário responsável.	Na empresa.	No primeiro mês de implantação da PSI podendo ser repetido a cada dois anos.	Afim de conscientizar, entender mais sobre a importância da segurança da informação na organização e torna-los responsáveis por suas ações.	Funcionário responsável realiza o treinamento.	4h do tempo do funcionário responsável.

Pesquisa de sugestões de melhoria referente a segurança da informação.	Todos os funcionários da empresa.	Na empresa.	No terceiro mês após a realização do treinamento.	Com intuito de atrair o interesse dos colaboradores para este assunto.	A empresa conta com um banco de ideias elaborado pelos funcionários e as sugestões de melhoria da área podem facilmente passar a fazer parte dos temas sugeridos.	1h de cada funcionário para pesquisa.
Criação de um conselho de segurança.	Gestores líderes de todos os setores da organização.	Na empresa.	No primeiro mês de implantação da PSI.	Para decidir, pré-aprovar novas propostas e ações, antes de serem levadas para o conselho diretivo.	Reunindo os membros e explicando a importância do conselho.	1h mensal do tempo dos membros do conselho.

Ilustração 2: Ações sugeridas
Fonte: produção do pesquisador

Espera-se que após a implantação de todas as etapas da PSI, a organização estabeleça um nível de segurança elevado em paralelo ao bem-estar dos colaboradores.

CONCLUSÃO

Através deste artigo foi possível propor a implementação de Políticas de Segurança da Informação voltadas às necessidades da Biotecno, desenvolvedora de câmaras refrigeradoras para conservação de medicamentos, sendo que para tanto, o primeiro objetivo foi estudar as melhores práticas de TI baseadas em ITIL para desenvolvimento do projeto em questão, o qual foi alcançado através do referencial teórico com estudo em autores renomados.

Na sequência, buscou-se atingir o segundo objetivo que era mapear e analisar a estrutura e os processos de TI para identificar os possíveis problemas e necessidades de melhorias, relacionados à segurança da informação, o qual foi atingido por meio da um questionário aplicado ao gestor verificando como a informação é armazenada e utilizada, e seu conhecimento sobre segurança da informação.

Além disso, tinha-se como objetivo, identificar os requisitos necessários para a elaboração das políticas de segurança, o que foi alcançado através de pesquisa bibliográfica, observação do ambiente da empresa e entrevista com o gestor.

Por fim, elaborar, a partir das melhores práticas de TI baseadas em ITIL, a proposta de implementação de Políticas de Segurança da Informação adequada à empresa, a qual foi sugerida do terceiro capítulo deste artigo.

O problema de pesquisa visava identificar: como a implantação de Políticas de Segurança da Informação com base em ITIL poderá contribuir para prover a segurança dos dados e informações da organização Biotecno? E foi solucionado com o desenvolvimento de uma PSI para a empresa além de sugestões que a auxiliem a manter as informações protegidas e os funcionários envolvidos nesse processo.

Considerando o aspecto da contribuição do estudo para o acadêmico, pode-se afirmar que esta pesquisa foi de grande importância no que se refere ao aspecto que relacionado ao aprendizado, pois permitiu que se realizasse a comparação entre a teoria e a prática, observando a realidade da organização frente aos autores da área de segurança da informação. Além disso, proporcionou uma visão mais abrangente acerca do tema estudado, o que resultou em crescimento pessoal e intelectual.

Para a empresa, o presente estudo mostrou-se proveitoso, já que o desenvolvimento de políticas de segurança da informação traz grandes vantagens ao negócio uma vez que com isso é possível garantir os princípios de confiabilidade, disponibilidade e integridade dos dados armazenados na organização.

Independente do porte, as organizações que desejam crescer no mercado competitivo e ter qualidade na gestão da TI precisam manter suas informações em segurança e investir em políticas para que isso seja alcançado. O estudo traz como resultado para a empresa em análise que para se implantar uma eficaz segurança da informação dentro de uma organização é preciso seguir alguns critérios como a análise dos riscos e a definição de Políticas de Segurança. As práticas da ITIL auxiliam as empresas pois podem ser aplicadas na infraestrutura organizacional garantindo a segurança dos ativos nos níveis estratégico, tático e operacional e sua análise e busca por melhorias deve ser contínua.

REFERÊNCIAS

ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: Brasport, 2012.

BALTZAN, Paige; PHILLIPS, Amy. **Sistemas de Informação**. Porto Alegre: AMGH, 2012.

CASTELLS, Manuel. **A sociedade em rede**. 3 ed. São Paulo: Paz e Terra, 2000.

CASTRO, Vander de**. Internet nas empresas**: bloquear ou liberar o uso para atividades pessoais? 2012. Disponível em: <http://corporate.canaltech.com.br/materia/seguranca/Internet-nas-empresas-bloquear-ou-liberar-o-uso-para-atividades-pessoais/>. Acesso em: 12 out. 2017.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia Cientifica**. 6 ed. São Paulo: Person Prentice Hall, 2007.

CESTARI FILHO, Felício. **ITIL V3 Fundamentos**. Rio de Janeiro: RNP/ ESR, 2011.

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

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

FREITAS, Marcos André dos Santos. **Fundamentos do Gerenciamento de serviços de TI**: preparatório para a certificação ITIL V3 Fondation. Rio de Janeiro: Brasport, 2010.

FOINA, Paulo Rogério. **Tecnologia de informação: planejamento e gestão**. São Paulo: Atlas, 2009.

FONTES, Edison Luiz Gonçalves. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5 ed. São Paulo: Atlas, 2010.

LAS CASAS, Alexandre Luzzi. **Técnicas de Vendas – Como vender e obter bons resultados**. São Paulo: Saint Paul, 2010.

LAUDON, Kenneth C.; Jane P. Laudon. **Sistemas de Informações Gerenciais**. Tradução Thelma Guimarães; revisão técnica Belmiro N. João. 7. Ed. São Paulo: Pearson Prentice Hall, 2007.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria**. Fundamentos da Metodologia Científica**. 7. ed. São Paulo: Atlas, 2010.

PONTES, H. L. J; et al. **Melhoria no sistema produtivo de uma fábrica de café: estudo de caso.** São Paulo: SIMPEP, 2005.

VIANNA, Ilca Oliveira de Almeida. **Metodologia do trabalho cientifico:** um enfoque didático da produção cientifica. 1ed. São Paulo: E.P.U, 2001.