colloquium exactarum

GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DO SETOR DE SAÚDE: UM ESTUDO DE CASO

INFORMATION SECURITY MANAGEMENT IN A COMPANY OF HEALTH SECTOR: A CASE STUDY

Kellen da Silva Ramos1, Helton Molina Sapia2, Haroldo Cesar Alessi, Rogerio Marcus Alessi, Glauco Antonio Ruiz, Dione Jonathan Ferrari, Danillo Roberto Pereira.

Universidade do Oeste Paulista - UNOESTE, Especialização em MBA em TI, Presidente Prudente/SP.
e-mail: khirbet.qumran@gmail1, helton@unoeste.br2

RESUMO – A Segurança da Informação é a proteção de um complexo de dados disponíveis no interior de uma organização. Cada vez mais, ela tem se tornado importante para a sobrevivência de empresas no mercado, devido ao aumento do uso da internet e do surgimento de novas tecnologias. Este trabalho apresenta um estudo de caso sobre a gestão da Segurança da Informação em uma empresa privada. Foram apontadas as vulnerabilidades e ameaças da empresa com base nos parâmetros propostos pela Gestão da Segurança da Informação. As informações foram coletadas por meio de visitas ao local, as quais propiciaram o registro das falhas de segurança e justificaram a necessidade de realização deste estudo. Ao final, é apresentada uma visão geral dos resultados obtidos pelo desenvolvimento do estudo de caso, pontuando as falhas encontradas e sugerindo soluções que podem possibilitar a melhora dos resultados se forem implantadas de forma gradual.
Palavras-chave: Segurança da Informação; Gestão de Segurança da Informação; política de Segurança da Informação.

ABSTRACT – The Information Security is the protection of a data complex available within a company. Increasingly, it has become important for the survival of companies on the market, due to the increased of the use of the internet and the emergence of new technologies. This paper presents a case study on the Management of Information Security in a private company. It were pointed out the vulnerabilities and threats of the company on the basis of the parameters proposed for the Management of Information Security. The information was collected through on-site visits, which led to the registration of the security flaws and justified the need of this study. In the end, it is presented an overview of the results achieved by the development of the case study, punctuating the flaws encountered and suggesting solutions that can enable the improvement of the results if they were deployed gradually.
Keywords: Information Security; Management of Information Security, Information Security policy.

Recebido em: 15/08/2017
Revisado em: 15/09/2017
Aprovado em: 22/09/2017

1. INTRODUÇÃO

A Segurança da Informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio. A norma ABNT NBR ISO/IEC 27001:2013 define a Segurança da Informação como: "Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.".

Com o avanço da tecnologia a Segurança da Informação se tornou alvo de discussões em todo mundo. Nas pequenas e médias empresas a segurança ainda é menor por falta de pessoal qualificado e falta de medidas preventivas. A tecnologia está presente em todas as atividades hoje em dia, e o diferencial das empresas é poder dar ao usuário (cliente) um nível adequado de segurança.

A palavra informação pode ser entendida como todo o conteúdo ou dado valioso para uma empresa ou indivíduo, que consiste em qualquer conteúdo com capacidade de armazenamento ou transferência, servindo assim para as utilidades do ser humano.

É importante que as empresas se conscientizem que a tecnologia sozinha não pode, por si só, resolver o problema da Segurança da Informação. É preciso estruturar os processos e qualificar os profissionais.

A empresa em que se realizou o estudo de caso preferiu não ser identificada, mantendo sigilo de algumas informações. A justificativa para a realização deste estudo é a importância e a avaliação da Segurança da Informação como mecanismo para assegurar a execução das atividades da empresa. A empresa em que ele foi realizado está atuando há 20 anos no mercado. Para preservar o nome dela adotamos como pseudônimo Sweet Care. A empresa é uma prestadora de serviço na área de planos de saúde, com abrangência de atendimento em Presidente Prudente/SP e região. A matriz fica situada em Presidente Prudente/SP com mais quatro filiais em cidades vizinhas. Inicialmente, foi realizado um estudo dos negócios e dos processos da empresa e suas relações com partes interessadas internas e externas e a partir daí foi desenvolvida uma gestão de riscos.

O objetivo deste estudo foi apresentar um estudo de caso sobre a gestão de Segurança da Informação no setor da TI (Tecnologia da Informação) em uma empresa privada. Sendo assim, este estudo será realizado com auxílio das normas da família

ABNT NBR ISO/IEC 27000 e o COBIT. Como resultado, foi apresentado um relatório à empresa com melhorias nas boas práticas da Segurança da Informação. Foram considerados alguns objetivos para realização deste estudo de caso:

- Avaliar como está estabelecida a gestão de Segurança da Informação no setor de TI da empresa Sweet Care;
- Apresentar a Segurança da Informação e sua importância dentro do ambiente empresarial, principalmente do setor da TI;
- Certificar os responsáveis da empresa quanto à importância da gestão da informação;
- Apresentar as características das normas da ABNT NBR ISO/IEC 27000 e do COBIT.

2. METODOLOGIA

De acordo com Dantas (2011), a política de Segurança da Informação pode ser considerada como um documento que estabelece princípios, compromissos, valores, orientações, requisitos e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações. A política de segurança tende a estabelecer normas e regras de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes, como a indisponibilidade do serviço, a perda de informações, furtos, entre outros.

A Segurança da Informação é a proteção de determinados dados, onde podemos entender que a informação é todo o conteúdo ou dado valioso para uma empresa ou indivíduo. Já as ameaças à Segurança da Informação são agentes ou condições que causam incidentes que comprometem os ativos de informação por meio de exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e/ou disponibilidade, consequentemente causando impactos aos negócios da empresa.

Como citado acima, este estudo foi realizado com auxílio da família de normas ISO/IEC 27000 e do COBIT. As normas da família ISO/IEC 27000 orientam acerca do Sistema de Gestão de Segurança da Informação (SGSI). O SGSI é uma forma de segurança para todos os tipos de dados e informações e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade. Seus principais benefícios são:

- Estabelecimento de uma metodologia clara de gestão da segurança;
- Reduzir o risco de perda, roubo ou alteração da informação;
- O acesso à informação feito através de medidas de segurança;

- Confiança e regras claras para todos os envolvidos de uma empresa;
- Os riscos e seus controles são continuamente verificados.

COBIT é a sigla para Control Objectives for Information and Related Techonology. Na prática, significa uma estrutura capaz de fornecer a governança de TI na empresa. O COBIT funciona por meio da aplicação de diversas práticas de controle da informação que vão desde o planejamento até o monitoramento de resultados. Sendo assim, de modo geral, o COBIT estabelece as melhores práticas de governança de TI (COBIT5, 2012).

O COBIT tem um conjunto de ferramentas eficazes no controle dos processos, dando o diagnóstico do que fazer, mas não como fazer, questão que terá que ser resolvida com a ajuda das melhores práticas de outras metodologias (FERNANDES e ABREU, 2014).

É um modelo abrangente, independente da plataforma de TI utilizada no ramo da empresa. Atualmente, ele está em sua quinta versão, contando com uma arquitetura formada por quatro domínios fundamentais: planejar e organizar, adquirir e implementar, entregar e suportar, monitorar e avaliar.

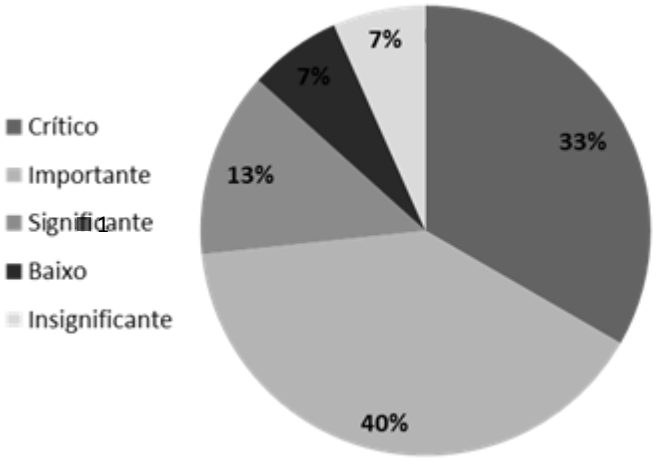
Essa organização é extremamente eficiente e funcional, possuindo ainda possui 34 processos e 210 pontos de controle.

Na análise dos resultados, os treinamentos em segurança da informação devem alcançar todos os funcionários e serem graduados mediante a criticidade das atividades para a empresa. Devem incluir palestras, workshops e seminários. A conscientização da cultura da Segurança da Informação deve ser o objetivo principal dos treinamentos. Regularmente, devem ser organizados encontros com funcionários falando sobre a segurança da informação.

3. RESULTADOS

De acordo com as informações obtidas das ferramentas do COBIT, ABNT ISO/IEC 27002:2013 e estudos sobre Segurança da Informação dentro da empresa Sweet Care, foi possível alcançar conclusões muito importantes. Uma análise da Gráfico 1 auxiliará na compreensão dos resultados.

Gráfico 1. Gestão de riscos.



Fonte: Elaborada pelos autores.

O Gráfico 1 - Gestão de Riscos foi elaborada com base nas informações sobre relevância do ativo, conforme critérios de riscos, obtidas através da aplicação da norma ABNT NBR ISO/IEC 27002:2013 na empresa objeto de estudo. No Quadro 1 estão dispostos os critérios utilizados para compreender a gestão de riscos.

Quadro 1. Critérios de riscos

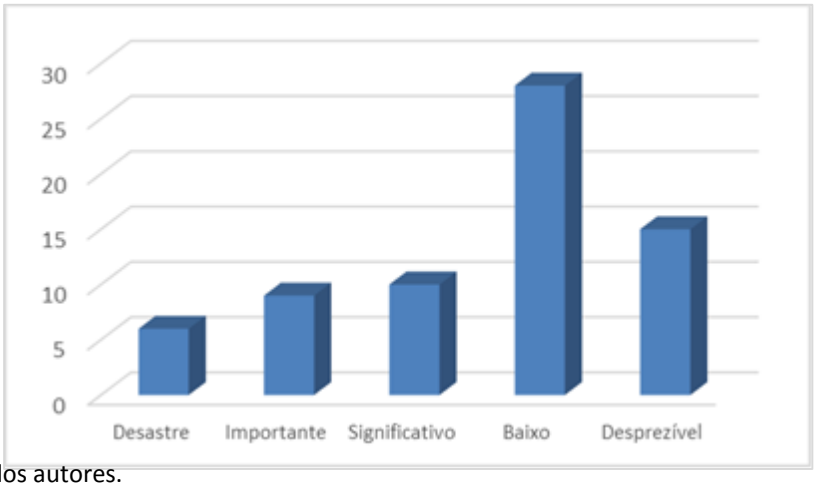
Critério	**Descrição**
Crítico	Sem esse ativo a empresa tem prejuízos financeiros e não executa suas atividades.
Importante	É um ativo que afeta nos custos da empresa e nas suas atividades.
Significante	É decisivo para o negócio da empresa.
Baixo	Pouco afeta o andamento da rotina da empresa.
Insignificante	Não afeta o bom andamento da rotina da empresa.

Fonte: elaborado pelos autores.

Observando o Gráfico 1, é possível verificar que existe em média 33% de ativos considerados como nível crítico. São eles: segurança de rede, sistema operacional, infraestrutura, investimento na TI e organização do backup. Em média 40% de ativos considerados de nível importante, os quais são: Segurança da Informação, treinamentos, controle de acesso, organização de contratos para terceiros, documentação e contratação de funcionários na área da TI. Em média 13% de ativos foram considerados nível significante, sendo eles: teste e recursos críticos da TI. Em média 7%

de ativos considerados nível baixo, que é: registro de chamada e também 7% de ativos considerados nível insignificante, que podemos citar: cotação de equipamentos da TI.

Gráfico 2. Impacto.



Fonte: Elaborada pelos autores.

No Gráfico 2 “Impacto” é possível observar o resultado obtido através dos controles do COBIT aplicado na empresa. Sendo classificados com os seguintes termos:

Quadro 2. Classificação do impacto

Termo	**Descrição**
Desastre	A empresa deixa de funcionar por no mínimo 12 horas e tem altíssimos prejuízos.
Importante	Atinge a imagem da empresa e assim causando a interrupção dos negócios por algumas horas. A empresa deixa de funcionar/produzir por até 12 horas.
Significativo	Afeta a empresa e causa interrupção por no mínimo 3 horas.
Baixo	Pouco afeta a empresa, podendo ser controlado rapidamente voltando aos negócios.
Desprezível	Não afeta a empresa, mas deve ser tratado.

Fonte: Elaborado pelos autores.

Com a Figura 2 é possível verificar que existem 68 vulnerabilidades encontradas na empresa Sweet Care. Elas podem ser classificadas como: 6 - Desastres, 9 - Importantes, 10 - Significativos, 28 - Baixos e 15 – Desprezível.

Esses gráficos apresentados comprovam a necessidade de mudança na empresa no setor da TI. Mostrando também que se forem aplicadas e seguidas as orientações demonstradas nesse estudo de caso, através do uso de normas e procedimentos, os riscos podem ser diminuídos consideravelmente.

4. DISCUSSÃO

A empresa ainda não gerencia os riscos de Segurança da Informação aos quais está exposto, o que pode ser decorrente da ausência de uma política de Segurança da Informação e também pelo fato dela não ser tratada ainda como uma estratégia. Hoje existem apenas medidas emergenciais que são usadas para tratar esses riscos que, e na maioria das vezes, acontecem de forma intuitiva, não chegando a ser um processo formal definido.

De modo geral, este estudo de caso contribuiu para que houvesse uma empresa uma conscientização da importância do setor de TI naquela empresa, que antes era considerado um setor técnico e não como uma estratégia de negócios.

O estudo de caso será utilizado pela empresa para projetos internos, buscando a melhoria não só no setor da TI, mas na empresa e suas filiais como um todo.

A finalidade da utilização do COBIT é utilizá-lo como instrumento de apoio, pois essa ferramenta permite boas práticas para controles de TI em toda a empresa. Os controles do COBIT foram selecionados através das deficiências mais urgentes percebidas na empresa. Ainda assim, dificilmente poderão aplicar todos os processos do COBIT, pois seus controles serão um auxílio para mapear os processos de forma mais detalhadas.

Os controles da norma ISO/IEC 27001 (2013) que foram selecionadas para que possam colaborar no auxílio de boas práticas de gestão da empresa. Essa norma aborda pontos importantes como o gerenciamento de acesso ao usuário, mostrando sempre a melhor forma a ser utilizada ao realizar que pode ser feita uma atividade. Os controles da norma foram selecionados através das deficiências nas atividades diárias da empresa. Esses controles que vão ajudar a empresa a melhorar a gestão de Segurança da Informação.

5. CONCLUSÃO

Foi elaborada uma Política de Segurança da Informação da empresa, especificando as responsabilidades dentro do setor de TI, responsabilidades dos gerentes da empresa, responsabilidades dos funcionários da empresa, mecanismos de proteção contra softwares maliciosos, regras e orientação de acesso à internet - além de destacar as infrações puníveis de acordo com as normas em caso de violação. A política de segurança da informação foi baseada da norma ISO/IEC 27001 (2013). Buscou ser de uma linguagem simples, clara e objetiva. Ela deverá posteriormente ser atualizada e a cada atualização deve ser aprovada pela administração da empresa e ser inserida em seu regimento.

Vários problemas foram considerados durante a elaboração deste estudo de caso. Por isso, a sugestão é que os apontamentos reflitam em mudanças aplicadas de maneira gradual para que sejam obtidos os resultados esperados. Os funcionários do setor da TI discutirão as mudanças que precisam ser feitas junto com os gerentes e a diretoria. Colocar em prática os procedimentos que foram alcançados neste estudo de caso com máxima urgência é de suma importância para não expor a empresa e suas filias a tantos riscos desnecessários.

Para a gerência da empresa foi possível constatar que o setor da TI é o centro dos principais processos de negócio, e sem o perfeito funcionamento desse setor toda a empresa enfrenta situações caóticas – além de reduzir suas possibilidades de crescimento. Tem-se agora um quadro bem definido sobre a situação da empresa nesse campo, o que possibilita para a instituição uma evolução coordenada. O passo dado com este trabalho foi inicial, mas esperamos que possa marcar o início de uma nova fase na saúde da Segurança da Informação da empresa Sweet Care.

REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 27001. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013.

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

COBIT5 - A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA, 2012.

DANTAS, M. Segurança da Informação: uma abordagem focada em gestão de riscos. Olinda, 2011.

FERNANDES, AGUINALDO ARAGON; ABREU, VLADIMIR FERRAZ DE. Implantando a Governança de TI – da estratégia a gestão de processos e serviços. 4ª ed. Rio de Janeiro: Brasport, 2014.