SEGURANÇA DA INFORMAÇÃO VERSUS PRONTUÁRIO ELETRÔNICO: HOSPITAL GERAL DE FORTALEZA - CE

1° Ten Med Angela Cristina Figueiredo Lopes
Graduada em Medicina.

Resumo: Nos dias de hoje, as empresas, principalmente da área da saúde, dependem cada vez mais dos sistemas de informação e da Internet para fazer negócios, não podendo se dar ao luxo de sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores. Este trabalho teve como objetivo analisar como o PEP (prontuário eletrônico do paciente) garante a segurança da informação no âmbito organizacional, do Hospital Geral de Fortaleza, no sentido de identificar a sua contribuição no processo produtivo da Organização.

Palavras-chave: Segurança. Informação. Prontuário eletrônico do paciente.

INTRODUÇÃO

A Segurança da Informação para o ambiente médico atual é vital para manter não só a visão como também a missão da mesma, pois no ramo de atividade médica toda e qualquer informação pertencente a um associado, deve manter um alto nível de segurança, não só os dados cadastrais como também informações relativas aos gastos, transações e etc., dos mesmos.

A questão da segurança da informação tornou-se nos dias de hoje um tema importante, principalmente na área da saúde, pois a informação é um ativo, e como qualquer outro ativo tem um valor e necessita ser protegido, não somente aquelas empresas de médio e grande porte, mas também aquele comércio pequeno que possua somente um computador e utilize a internet, também aquele usuário doméstico que usa o computador para trocar correspondências eletrônicas de caráter pessoal, todos têm o direito que os dados que estão gravados na máquina se mantenham intactos e acessíveis somente às pessoas autorizadas.

Assim sendo, temos como problema básico de pesquisa: Como o PEP (prontuário eletrônico do paciente) garante a segurança da informação no âmbito organizacional, do Hospital Geral de Fortaleza, no sentido de identificar a sua contribuição no processo produtivo da organização.

2 PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)

O Conselho Federal de Medicina, através das resoluções 1638/2002 e 1639/2002 aprovou em julho de 2002 a utilização do PEP. A visão de prontuário médico permanece, contudo seu conceito passa a incluir não somente o documento tradicional em papel, mas também o registro em suporte eletrônico.

O Prontuário Médico é definido pelo CFM como:

Documento único, constituído por informações, sinais e imagens registrados a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, com caráter legal, sigiloso e científico, utilizado para possibilitar tanto a comunicação entre os membros de uma equipe multiprofissional como a continuidade da assistência prestada ao indivíduo.

3 METODOLOGIA

O universo considerado para a realização da pesquisa foi o ambiente em que se realiza a tecnologia da informação dentro do Hospital Geral de Fortaleza (HGeF) , o setor de Suporte de Tecnologia e Telecomunicações. Dentre os informantes estão o coordenador do setor, mais 39 (trinta e nove) colaboradores também vinculados ao referido setor, totalizando 40 (quarenta) informantes.

Nesta pesquisa, foi utilizado um questionário com perguntas fechadas, semi-fechadas. Esta flexibilidade que foi utilizada para as perguntas visou dar maior mobilidade para que pudesse ser obtida a informação com o maior grau de detalhe possível, sem, entretanto cansar o respondente.

Por outro lado, o uso da entrevista não seria o adequado já que "uma entrevista que se prolongue muito além de trinta minutos se torna repetitiva e se empobrece consideravelmente" (GIL, 1991), justificando assim a utilização do referido questionário.

Então o instrumento da coleta de dados foi o questionário (anexo) respondido pelos funcionários com vista à obtenção das seguintes informações:

- Elementos essenciais de estratégia de segurança utilizadas no Hospital; e
- Sobre os conhecimentos e responsabilidades dos funcionários referentes ao assunto da segurança da informação e a utilização do PEP.

4 RESULTADOS

Conforme dados coletados na pesquisa através do questionário com perguntas fechadas e semi-fechadas, teve-se o seguinte resultado:

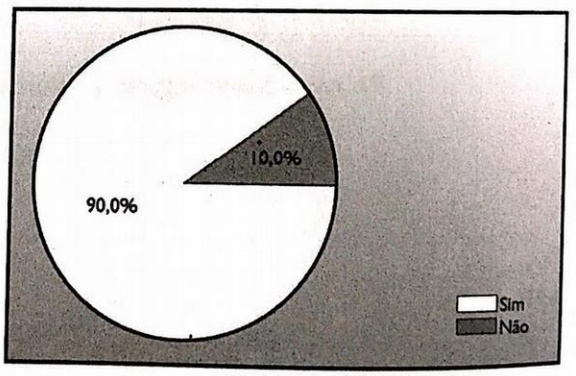

Gráfico 1 – Se o funcionário utiliza ou consulta freqüência o PEP. Fonte: Dados da pesquisa/Jan 2009.

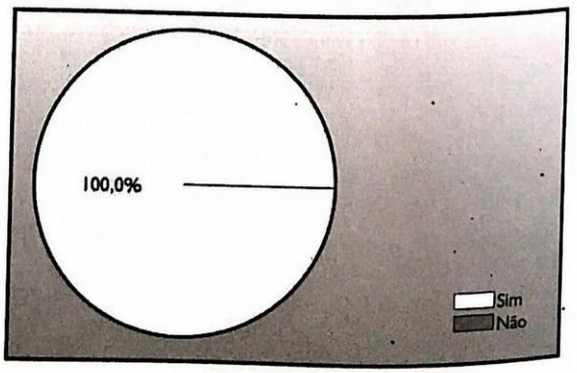

Gráfico 2 – Se o PEP possibilita um registro mais completo que o prontuário em papel. Fonte: Dados da pesquisa/Jan 2009.

Dos 40 (quarenta) funcionários entrevistados 10% (dez por cento) responderam que não utilizam o PEP com frequencia e 90% (noventa por cento) utiliza e consulta o PEP com frequencia.

Através dos dados obtidos nesta pergunta, pode-se dizer que os funcionários deste hospital estão cada vez mais utilizando o prontuário eletrônico do paciente (PEP) e que vem mudando a concepção de um repositório de informações médicas para um documento dinâmico capaz de subsidiar e nortear as atividades dos profissionais que dele fazem uso.

Perguntou-se aos entrevistados, se eles consideram que o PEP possibilita um registro mais completo de informações que o prontuário em papel, 100% (cem por cento) dos entrevistados deu respostas positivas a respeito desse assunto.

Uma das questões levantadas na pesquisa foi se os funcionários sentiam alguma dificuldade na interpretação das informações registradas no PEP, 30% (trinta por cento) responderam que não e 70% (setenta por cento) responderam que sim.

Dos entrevistados, 20% (vinte por cento) disseram não ter conhecimento à existência de política de segurança da informação ou algum documento que trate alguns aspectos de segurança, e 80% (oitenta por cento) disseram ter conhecimento.

Desses 80% (oitenta por cento) que representa 32 (trinta e duas) pessoas, pediu-se que se especificasse o documento que trata do assunto. 15,63% (quinze vírgula sessenta e três por cento) deram como repostas o documento manual prevenção de incidentes de segurança, 53,12% (cinquenta e três vírgula doze por cento) especificou o documento políticas e diretrizes da segurança da informação, 18,75% (dezoito vírgula setenta e cinco por cento) o manual de segurança: A Internet e o novo Outlook e 12,5% (doze e meio por cento) a classificação de documentos internos.

Dos funcionários entrevistados que totalizam 100% (cem por cento), 65% (sessenta e cinco por cento) disseram que esses documentos não foram divulgados e 35% (trinta e cinco por cento) disseram que esses documentos foram divulgados no setor.

Desses 35% (trinta e cinco por cento), pediu-se que os entrevistados dissessem a forma que esses documentos foram divulgados. 42,85% (quarenta e dois vírgula oitenta e cinco por cento) disseram que esses documentos foram divulgados em palestra no Hospital Geral de Fortaleza (HGeF) e 57,15% (cinquenta e sete vírgula quinze por cento) disseram que

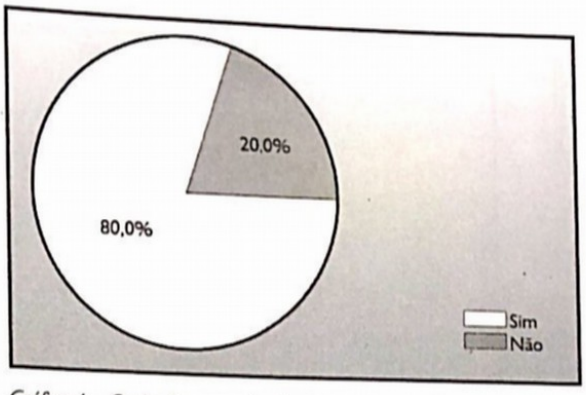

Gráfico 4 – Conhecimentos dos funcionários com relação a documentos de políticas de seguranças. Fonte: Dados da pesquisa/Jan 2009.

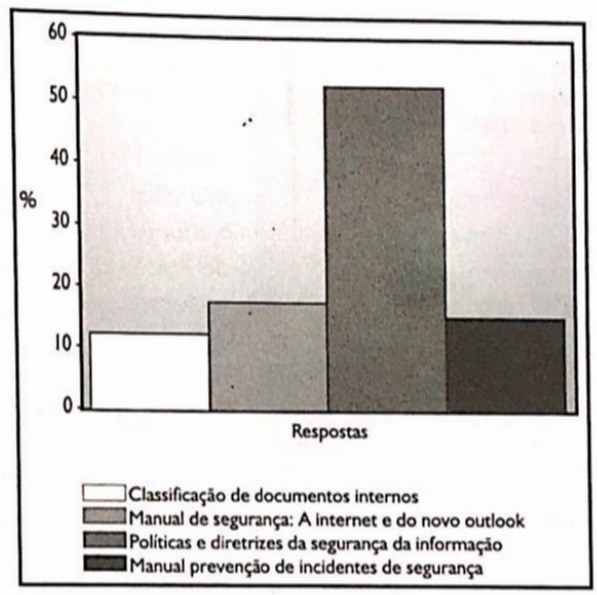

Gráfico 5 – Documentos de segurança existentes no Hospital Geral de Fortaleza (HGeF). Fonte: Dados da pesquisa/Jan 2009.

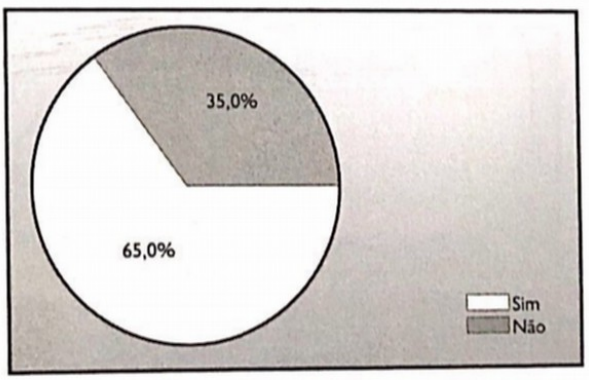

Gráfico 6 – Com relação a divulgação dos documentos de segurança da informação. Fonte: Dados da pesquisa/Jan 2009.

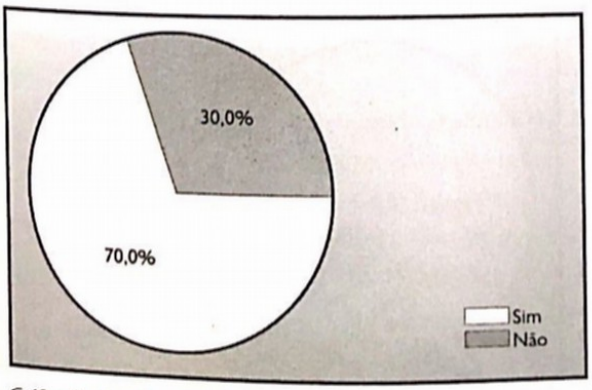

Gráfico 3 – Se o funcionário sente alguma dificuldade na interpretação das informações registradas no PEP. Fonte: Dados da pesquisa/ Jan 2009.

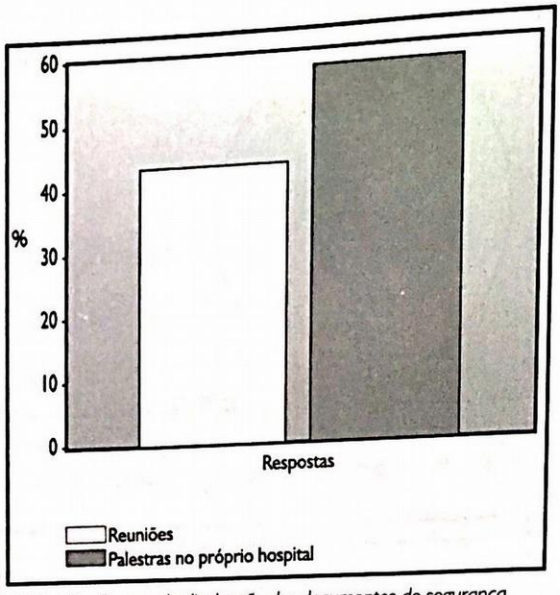

Gráfico 7 – Formas de divulgação dos documentos de segurança. Fonte: Dados da pesquisa/Jan 2009.

foi através de reuniões no próprio setor.

Uma das questões abordadas foi se a política de segurança do Hospital Geral de Fortaleza (HGeF) define que cada funcionário é responsável direto ou indireto pela segurança das informações na empresa. Dos 40 (quarenta) funcionários entrevistados, 100% (cem por cento) disseram que sim, que o hospital possui essa política.

Dos entrevistados, 75% (setenta e cinco por cento) disseram que sim, receberam treinamento e 25% (vinte e cinco por cento) disseram não ter recebido treinamento.

Desses 75% (setenta e cinco por cento) que representa 30 (trinta) pessoas perguntou-se qual o nome do treinamento que eles receberam. 33,4% (trinta e três vírgula quatro por cento) deram como repostas o curso Melhores práticas da segurança da informação do PEP, 13,3% (treze vírgula três por cento) disseram que foi o curso de Sistema de organização, segurança e planejamento da informação, 23,3% (vinte e três vírgula três por cento) palestra Segurança de tecnologia da informação, 10% (dez por cento) o curso Segurança em rede e internet e 20% (vinte por cento) o curso Controle e monitoramento da rede.

Nessa pesquisa foi analisado o ponto referente aos atos de comer, beber e fumar nas instalações de processamento de informação, locais restritos ou próximos a materiais inflamáveis. Dos entrevistados, 100% (cem por cento) disseram que no Hospital Geral de Fortaleza (HGeF) possui uma política referente a esses atos.

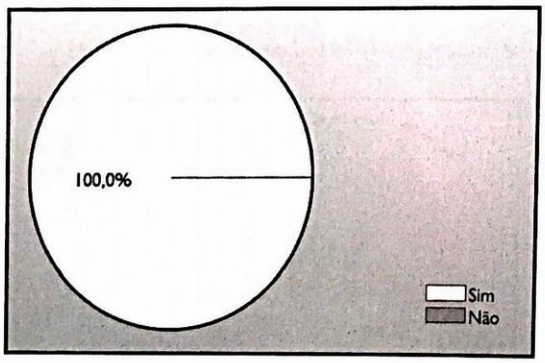

Gráfico 8 – Responsabilidade direta ou indireta do funcionário pela segurança das informações. Fonte: Dados da pesquisa/Jan 2009.

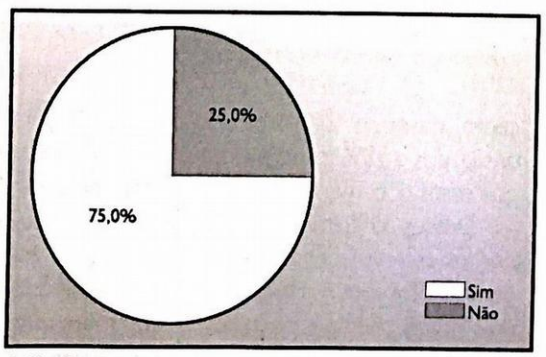

Gráfico 9 – O funcionário já recebeu algum treinamento sobre confiabilidade de usuário e senha nos sistemas. Fonte: Dados da pesquisa/Jan 2009.

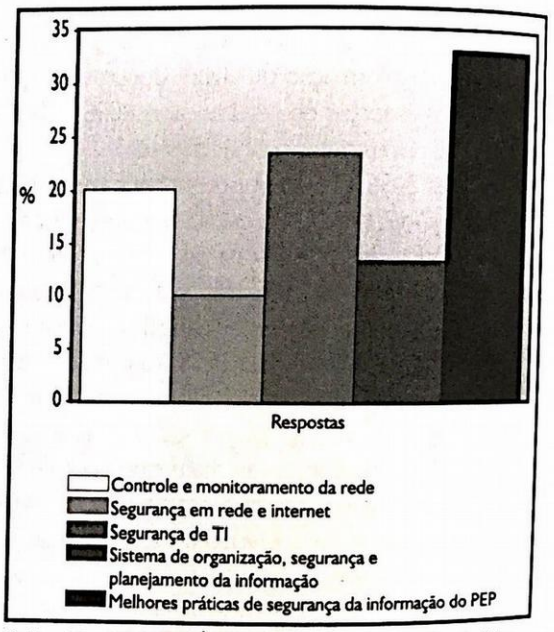

Gráfico 10 – Os tipos de treinamentos recebidos pelos funcionários. Fonte: Dados da pesquisa/Jan 2009.

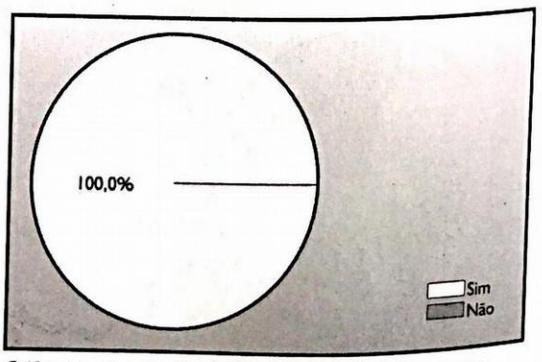

Gráfico 11 – Possui políticas referentes a atos de beber, comer e fumar nas instalações do Hospital Geral de Fortaleza (HGeF)/Jan 2009. Fonte: Dados da pesquisa/Jan 2009

Dos entrevistados, 90% (noventa por cento) responderam que o Hospital Geral de Fortaleza (HGeF) estabelece uma classificação dos documentos e 10% (dez por cento) responderam que não existe uma classificação das informações.

Desses 90% (noventa por cento), que representa 36 pessoas, perguntou-se como é feita essa classificação, obteve como respostas: 2,8% (dois vírgula oito por cento) disseram que a classificação é feita como: confidencial, restrito, aberto ao público, 55,5% (cinquenta e cinco e meio por cento) disse que a classificação é feita por assunto e 41,7% (quarenta e um vírgula sete por cento) deixaram esta pergunta em branco, ou seja, não responderam nada.

Outra questão levantada foi se o Hospital Geral de Fortaleza (HGeF) faz o controle de envio e saída de informações confidenciais. Dos entrevistados 90% (noventa por cento responderam que sim e 10% (dez por cento) responderam que não.

Pode-se observar que o Hospital Geral de Fortaleza (HGeF) nesse requisito, controla bem a saída de documentos. As informações confidenciais são caracterizadas pelo seu caráter sigiloso e de divulgação restrita a poucos, merecem maior atenção da empresa.

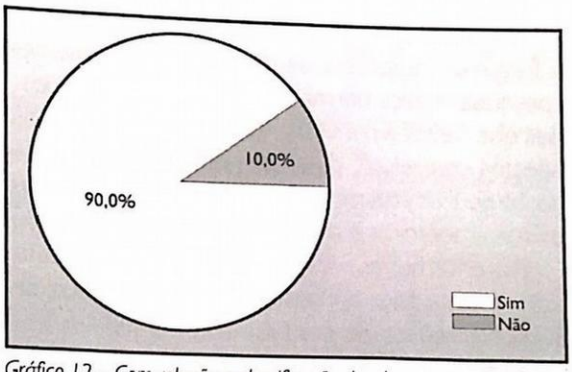

Gráfico 12 – Com relação a classificação dos documentos. Fonte: Dados da pesquisa/Jan 2009.

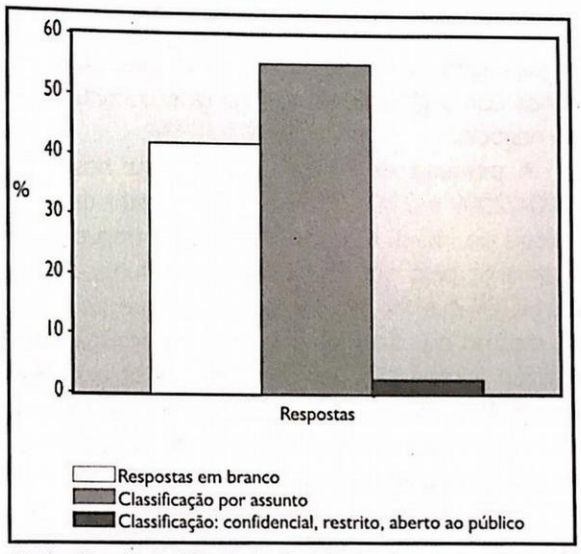

Gráfico 13 – Como é feita a classificação dos documentos. Fonte: Dados da pesquisa/Jan 2009.

5 CONCLUSÃO

Pode-se interpretar que a opinião dos respondentes em que os problemas de segurança em 2009 irão diminuir no HGeF, é em função das novas ferramentas de proteção que são disponibilizadas pelo Hospital através do plano de continuidade de negócios que este possui, ou seja, um conjunto de softwares e hardware, somados a consultoria que podem apoiar os funcionários de tecnologia da informação em uma arquitetura de tecnologia da informação mais segura.

Verifica-se que grande parte dos funcionários de tecnologia da informação, afirmam que a segurança da informação é muito importante e consequentemente que o HGeF possui uma política de segurança. Isso mostra que o HGeF pensa em segurança como um processo estruturado.

Entende-se que uma política estabelecida é uma evidência de que a empresa discutiu, inclusive entre a alta direção, os aspectos das ameaças e vulnerabilidades de seus ativos, e repensou em como deve ser uma conduta apropriada de seus funcionários para a proteção da informação.

Já obstáculos, pode-se verificar que o principal é a conscientização do funcionário. Isso fortalece a idéia que focar investimentos em novas tecnologias de proteção, além de serem caras, não trazem o mesmo resultado do que um trabalho direcionado na conscientização e treinamento dos funcionários. As ameaças como vazamento de informações, acessos não autorizados e funcionários insatisfeitos, surgem de dentro da organização.

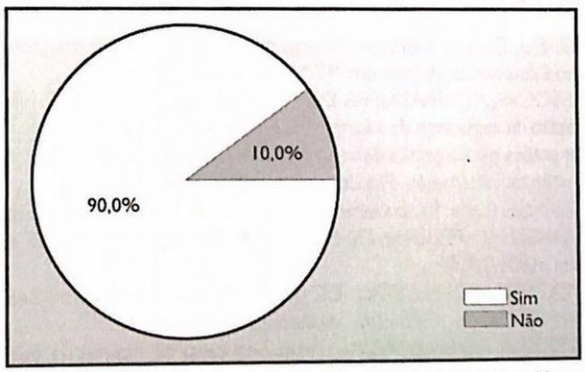

Gráfico 14 – Com relação a existência de controle de envio e saída de informações confidenciais. Fonte: Dados da pesquisa/Jan 2009.

Divulgar e orientar os funcionários sobre as suas responsabilidades e procedimentos em relação à segurança da informação, somados aos processos de controle, podem reduzir os incidentes de segurança e consequentemente melhorar o nível da segurança da organização.

Os objetivos específicos elencados nesta pesquisa foram decompostos de modo que, inicialmente, a pesquisa técnica normativa, por se tratar de questões que merecem investigação teórica, abarcou os aspectos conceituais da gestão estratégica da informação do PEP, através da pesquisa em livros, artigos, revistas acadêmicas e pesquisa eletrônica (internet).

Posteriormente, houve a passagem da investigação teórica para a investigação empírica, que se utilizou da técnica de pesquisa-ação na medida em que após a coleta de dados através do questionário com perguntas fechadas e semi-fechadas procurou identificar se o HGeF aplica os princípios de gestão de segurança da informação do PEP e verificar quais os procedimentos que são percebidos pelos funcionários como garantia de segurança e continuidade do negócio.

A pesquisa de campo foi realizada nos dias 06/01/2009 e 07/01/2009 dentro do setor de tecnologia do HGeF. O questionário foi entregue pessoalmente pelo entrevistador para os funcionários do HGeF que foi respondido e entregue de volta no mesmo dia. Com os questionários em mãos se realizou a tabulação dos dados coletados e se fez uma análise confrontando com as informações do contidas no referencial teórico e com as normas e diretrizes de Segurança do HGeF.

Este trabalho possibilitou entender, que independente do tamanho ou segmento da empresa, a informação é um dos ativos mais importantes e conseqüentemente a segurança deste ativo também. Conhecer o ambiente de tecnologia é imprescindível, mas também, o ambiente de negócio composto pelos seus processos e o nível de entendimento dos funcionários a respeito da importância da informação é necessário.

Pensar em pessoas, processos e tecnologia, ajudam a empresa como HGeF que tem a obrigação de possuir políticas de segurança, a arquitetar um plano de trabalho que possa abranger os três pilares em um equilíbrio razoável.

O domínio da informação sempre teve fundamental importância para as corporações, sendo indispensável arma, do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa ter um suporte imbatível para a tomada ágil e eficiente de decisão.

Obviamente, da forma como hoje é manipulada e armazenada, quando se faz extensivo uso dos meios e equipamentos eletrônicos, a informação passou a ser objeto de preocupação dos profissionais de tecnologia da informação, responsáveis pelos métodos de tratamento e pela sistematização dos dados, de modo a formar a referida base confiável para processos decisórios.

Contudo, defende-se que o direcionamento de atividades no sentido de melhorar a conscientização do funcionário sobre o assunto segurança da informação pode trazer grandes resultados, sem grandes investimentos.

REFERÊNCIAS

ABREU, Dimitri. Melhores Práticas para Classificar as Informações.São Paulo: Módulo e-Security Magazine, 2001. Disponível em www.modulo.com.br. Acesso em: 17 NOV 08.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS-ABNT. NBR ISO/IEC 17799: tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001._____ NBR ISO/IEC 17799:2005: Tecnologia da informação: código de prática para a gestão da segurança da informação, 2005._____ NBR ISO/IEC 17799: Tecnologia da informação: Código de pratica para gestão da informação. Rio de Janeiro: ABNT, 2003.

BAIENSE, Carla. Risco Gerenciado. E - Manager nº39, p.14-17. São Paulo: TB Editora, mai 2003.

CONSELHO FEDERAL DE MEDICINA. Resoluções 1638/2002 e 1639/2002. Disponível em: http://www.portalmedico.org.br/. Acesso em: 10/01/2009.

CONSELHO FEDERAL DE MEDICINA. Resolução 1.246/1988. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/1988/1246_1988.htm. . Acesso em: 10/01/2009.

FERREIRA, Fernando Nicolau Freitas. Segurança da Informação. Rio de Janeiro:Ed. Moderna LTDA., 2003.

FONTES, Edison. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva,2006.

GABBAY, M. S. Fatores influenciadores na implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte. Tese (mestrado) – Universidade Federal do Rio Grande do Norte, 2003. Disponível em: < artigocientifico.uol.com.br/uploads/artc_1173362630_58.pdf>. Acesso em 15 SET 08.

GIL, Antonio Carlos. Como elaborar projeto de pesquisa. São Paulo: Atlas,1991.

IOM, Institute O. M., The Computer-Based Patient Record; 2ª ed. Washington, USA, National Academy Press, 1997.

LAUDON, K.C.; LAUDON, J. P. Sistemas de informação: organizando as informações: arquivos e bancos de dados. 4. ed. Rio de Janeiro: J.C. Editora, 1999.

LE, Y., Computer-based Patient Record Systems. Healthcare Informatics. Maio de 2001. Spotlight. Disponível em: < http://www.healthcareinformatics.com/issues/2002/05_01/cpr.pdf>. Acesso em10 JAN 09.

MARCONI, M. de A. e LAKATOS, E. M. Técnicas de pesquisa. 6 ed. São Paulo: Atlas, 2006.

MARTINS, José Carlos Cordeiro. Gestão de projetos de segurança da informação. Rio de Janeiro: Brasport, 2003.

MASSAD, E. et al. – O prontuário eletrônico do paciente na assistencia, informação e conhecimento médico. São Paulo: H. de f. Marin, 2003.Disponível em < http://www.med.fm.usp.br/dim/livrosdim/prontuário.pdf > Acesso em 12 JAN 09

MEYLAN,Franck. Evolução da Segurança da Informação e perspectivas para 2008. Disponível em: < www.itweb.com.br/noticias/index.asp?cod=45280>. Acesso no dia 30 OUT 08.

MOREIRA, Stringasci Nilton. Segurança mínima : uma visão corporativa da segurança da informação.Rio de Janeiro: Axcel Books, 2001.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR- NIC. Pesquisa sobre o uso da tecnologia da informação e da comunicação no Brasil 2007. Comitê Gestor da Internet no Brasil: São Paulo, 2008. Disponível em: <www.cetic.br/pesquisa2008.pdf >. Acesso no dia 30 OUT 08

OLIVEIRA, S. de. As tríplices da segurança da informação, 14 mar. 2005. Disponível em:<http://www.modulo.com.br/index.jsp> . Acesso em: 30 JUL 08.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da informação: aplicada a sistemas de informação empresariais. São Paulo: Atlas,2000.

RUDIO, Franz Victor. Introdução ao projeto de pesquisa científica. 25. ed. Petrópolis: Vozes, 1999.

RUIZ, Miguel. Artigo Segurança da Informação cresce no Brasil. São Paulo,: MR Consultoria, 2006. Disponível em:<www.novomilenio.info.br/ano06/0609d004.html>. Acesso no dia 30 OUT 08.

SALVADOR, V. F. M.; ALMEIDA FILHO, F. G. V. – Aspectos éticos e de segurança do prontuário eletrônico do paciente – II Jornada do conhecimento e da tecnologia, 22 e 26 ag. 2005. UNIVEM; Marília, SP. Disponível em < http://galileu.fundanet.br/jornada/artigos/computacao/Valeria_Farinazzo.pdf> . Acesso em 12 JAN 09.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva Segunda Edição, Rio de Janeiro: Campus, 2003.