Análise e Gestão de Risco, Implementação de Políticas de Segurança em uma Unidade da Polícia Civil do Estado de São Paulo: Manual de Implementação

Edson Henrique Graciano Carriel [1], Eduardo Alves Moraes [2] ,Luiz Carlos Ornaghi [3]

RESUMO

A informação é o ativo mais importante dentro de qualquer organização, e ao longo dos tempos a busca de procedimentos e métodos que garantam a segurança da informação vem aumentando. Paralelo a isso, também cresce a curiosidade da concorrência ou pessoas mal intencionadas em desvendarem segredos que possam trazer vantagens comerciais, pessoais ou financeiras. A utilização de uma Politica de Segurança da Informação se faz necessário em um ambiente corporativo, pois nele estão constituídos os anseios gerais da organização com as regras que padronizam como cada ativo deve ser tratado, controles a serem utilizados, os planos de contingências e também descreve as responsabilidades dos usuários na manipulação das informações. Este trabalho foi desenvolvido a partir da análise do ambiente em uma Unidade da Polícia Civil do Estado de São Paulo. Foram analisados o fator da segurança da informação, a existência de uma politica de segurança da informação já estabelecida, os ativos mais importantes, forma de tratamento das informações e as ameaças e vulnerabilidades que a Unidade Policial está sujeita. Ao final do trabalho é apresentado um manual de implementação de politicas de segurança, contendo as soluções que venham sanar ou mitigar as vulnerabilidades e problemas encontrados, contendo as regras e procedimentos que devem ser realizados para proteção dos ativos da Unidade Policial.

Palavras-Chave: Políticas, Segurança, Análise, Polícia, Risco.

ABSTRACT

Information is the most important asset within any organization, and over time the search for methods and procedures that ensure information security is increasing. Parallel to this, it also increases the curiosity of competition or

---

[1] Aluno do curso de Segurança da Informação – Faculdade de Tecnologia de Ourinhos/SP (FATEC)

E-mail: edycarriel@yahoo.com.br

[2] Professor Orientador: Esp. Eduardo Alves Moraes – (FATEC) – Campus Ourinhos/SP. E-mail: eduardo.moraes@fatec.sp.gov.br

[3] Aluno do curso de Segurança da Informação – Faculdade de Tecnologia de Ourinhos/SP (FATEC)

E-mail: ornaghi@cednet.com.br

malicious people to unravel secrets that can bring business benefits, financial or personal. Using an Information Security Policy is needed in a corporate environment because it is made of the general expectations of the organization with the rules that standardize how each asset should be treated controls to be used, plans for contingencies and also describes responsibilities of users in manipulating the information. This work was developed from the analysis of environment on a Civilian Police Unit of the State of São Paulo. Were analyzed the factor of information security, the existence of a policy of information security already established, the most important assets, form processing of information and the threats and vulnerabilities that the Police Unit is subject. At the end of the work is presented an implementation manual of policies security, containing solutions that will remedy or mitigate vulnerabilities and problems encountered, containing the rules and procedures that must be performed to protect the assets of the Unit Officer.

Keywords: Political, Security, Analysis, Police, Risk.

1 INTRODUÇÃO

A segurança da informação, sempre foi uma preocupação da humanidade ao longo dos séculos, sendo muito utilizada por diversas civilizações, que procuravam manter suas informações e descobertas em sigilo. Inicialmente com o aparecimento do homem na pré-história, em cavernas foram encontradas informações em forma de símbolos, mostrando que já nesse período o homem procurava registrar suas informações de forma singular. Eras mais tarde, também registravam informações, mas de forma escrita, método que era utilizado na comunicação entre grupos específicos.

Segundo Santos (2009), há aproximadamente 3500 (a.C.), os povos sumérios já haviam desenvolvido a escrita cuneiforme, sendo utilizadas placas de argila onde estes povos cunhavam (marcavam com cunhas) este tipo de escrita, se utilizando de sinais onde estes representavam ideias e objetos. Também Aranha (2012), ressalta que segredos e códigos secretos existem desde os primórdios da humanidade. Há registros de escrita codificada já no Egito Antigo, datando de aproximadamente 1900 (a.C.).

Desta maneira, verificam-se ao longo da história que a preocupação em garantir a segurança das informações vem de muito tempo, e ao longo dos anos os esforços em criar regras e políticas mais eficazes vem aumentando.

No atual cenário da segurança da informação, nota-se que grande parte das empresas e seus usuários desconhecem os perigos as quais estão expostos, realizando troca de informações em redes e locais que não oferecem o mínimo de

segurança necessária. Percebe-se que se faz necessário não somente criar regras ou políticas de segurança da informação, mas também fazer com que estas, sejam devidamente cumpridas, monitoradas e atualizadas para poderem estar alinhadas com os objetivos, recursos e cultura da empresa.

Esse trabalho mostra os pontos vulneráveis que existe em uma Unidade da Policia Civil do Estado de São Paulo.

Analisou-se ativos como, Inquéritos Policiais, que são processos onde são registrados todos os delitos cometidos por um indivíduo e guardam informações sigilosas referentes a esses delitos praticados, que tem um grau de importância muito significante para a polícia. Em contrapartida tem-se como elemento principal da própria segurança o fator humano, que de acordo com Frisch (2002) “a segurança tem início e termina com as pessoas.” Toda essa análise visa promover mudanças que tragam maior confiabilidade, integridade e disponibilidade aos processos que compõe o ambiente analisado.

Outros pontos chaves que também se destacaram foram: os problemas encontrados, hipótese e os objetivos o qual irão delinear e fazer parte do Manual de Implementação de Políticas de Segurança na unidade de policia pesquisada.

Partindo-se da idéia que algo que dá proteção, deve ao menos conseguir se proteger investigou-se o funcionamento de uma unidade da Polícia Civil, indagando se o que se pensa é aplicado nesse tipo de ambiente. Será que internamente a policia mantém a mesma excelência de segurança que prestam a todos os cidadãos?

Assim como acontece em qualquer organização, há vários fatores a se pensar no provimento de um ambiente seguro e geralmente passam despercebidos. Talvez o excesso de confiança na execução das tarefas faz com que se deixem de lado certos passos primordiais para um bom funcionamento e segurança dos ativos. Quando não é dada a devida atenção aos processos, vários pontos ficam vulneráveis, deixando a organização exposta e propícia a ataques.

É simples promover mudanças após o surgimento de algum evento negativo, mas ter que visualizar uma ameaça em potencial, é bem mais difícil. Criar métodos e planos alternativos para isso também requer um trabalho árduo, mas de extrema importância para a organização e é isso que será apresentado nesse Manual de Implementação de Políticas de Segurança.

Sabe-se que a Policia Civil possui uma Política de Segurança da Informação, mas que se torna ineficiente por não conseguir por em prática o que rege o Manual de Boas Práticas em todas as unidades policiais do Estado.

Um problema que evidencia isso é a falta de recursos financeiros, que se vê com maior atenuação em cidades do interior. Trabalham com o mínimo de recursos possíveis, o que afeta diretamente o desempenho dos processos. Outros aspectos que afetam diretamente a segurança dos ativos são:

- Falta de treinamento
- Conscientização para importância das informações
- Desvalorização salarial
- Carga horária exaustiva
- Políticas de Segurança Ineficientes
- Falta de padronização de processos

Todos esses pontos somados geram um nível crítico a segurança dos ativos, tornando-se um risco muito grande para a unidade.

Ao final do deste documento, será apresentado um Manual de Implementação de Políticas de Segurança, contendo as melhores práticas a serem seguidas pela unidade, visando fechar as lacunas vulneráveis, destacando aos administradores a importância de sua disseminação e utilização por todos os colaboradores.

A ânsia por analisar algo sobre determinado assunto, muitas vezes começa a partir de uma necessidade apresentada ou simplesmente por uma curiosidade. A partir disso tem-se um aprofundamento no assunto e o surgimento de indagações, que ao decorrer do processo de análise vão sendo respondidas de forma positiva ou negativa.

É a partir da análise do ambiente de pesquisa que se entende o funcionamento de cada setor, o tratamento dado a cada ativo, o nível de importância de cada um, nível de criticidade e qual melhor plano de contingência a ser aplicado.

2 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação atualmente pode ser vista como um dos principais meios através do qual as organizações procuram garantir que seu negócio esteja alicerçado de maneira a impedir que suas informações sejam roubadas, perdidas, ou que ainda possam ser acessadas de forma errada por pessoas não autorizadas, prejudicando seu processo. A implementação da Segurança da Informação dentro de um ambiente corporativo se faz necessário, visto que grande parte dos documentos utilizados atualmente estão em formato digital, no entendimento de Fontes (2006).

De acordo com a norma ABNT NBR ISO/IEC 27002 (2005), o crescente número da interconectividade coloca os ativos das mais diversas organizações expostos a uma grande variedade de ameaças e vulnerabilidades. A necessidade que o homem tem de se relacionar com outras pessoas para conseguir desenvolver suas atividades diárias, faz com que cada vez mais, esforços sejam direcionados para prover proteção as informações, que assim como outros ativos, são de extrema importância para a organização e necessitam ser adequadamente protegidos. Dessa maneira percebe-se que a informação, é importante dentro de um ambiente corporativo, bem como sua proteção, como comenta Menezes (2006, p.15): “Presentemente a informação é o principal bem, consequentemente, a sua proteção é inexorável”.

A informação é um ativo que pode estar em formado físico ou lógico, então não importa a forma que se encontre ou, sejam transmitidos, deve-se sempre dar atenção especial e oferecer proteção adequada.

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio. (ABNT NBR ISO/IEC 27002, 2005).

2.2 – Ambiente Seguro

Segundo Fontes (2008) empresas que colocam todos suas informações nas mãos de pessoas que as gerenciam e não seguem politicas de segurança bem definidas, só se lembram de dar a devida proteção as suas informações em momentos de crise. Segundo ele, esses momentos de crise podem ser causados por:

> vírus, que destruiu vários arquivos do disco rígido dos usuários (sem cópia de segurança), uma fraude que utilizou o acesso às informações via ambiente computacional ou na ocorrência de uma contingência causada pela natureza (FONTES, 2008, p.12).

Para se obter um ambiente seguro é necessário estabelecer os requisitos necessários para tal objetivo, e no caso da Unidade Policial não é diferente. Todos os tipos de organizações sejam públicas ou privadas devem definir que patamar de segurança é compatível com seu negócio. Não existe solução certa ou errada. Existe solução mais adequada ou menos adequada a cada organização (FONTES, 2008, p.13).

> É essencial que uma organização identifique os seus requisitos de segurança da informação.
> Existem três fontes principais de requisitos de segurança da informação.
> 1. Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
> 2. Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.
> 3. A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações (ABNT NBR ISO/IEC 27002, 2005).

3 METODOLOGIA

Segundo Gil (2009) metodologia é a descrição dos “procedimentos a serem seguidos na realização da pesquisa”. Pode-se dizer que é a forma utilizada para se chegar a um resultado ou a padronização dos passos a serem seguidos, facilitando os trabalhos no decorrer da pesquisa.

Será utilizado o método de pesquisa exploratória, visando “proporcionar maior familiaridade com os processos realizados, com vistas a torná-lo mais explícito ou a construir hipóteses.” (GIL, 2009, p. 41).

3.1 Coleta de Informações

A metodologia utilizada será a obtenção de informações através de coleta de dados que será da seguinte forma: Aplicação de questionários, visitas técnicas, integração aos processos e identificação e tratamento dos ativos. Todos esses procedimentos a serem realizados, vão de encontro com o que diz Gil (2009): “Coleta de Dados envolve a descrição das técnicas a serem utilizadas”, é isso que será explanado nos tópicos subsequentes.

3.2 Aplicação de Questionário

Através de um documento impresso com perguntas simples e objetivas que levem a um melhor entendimento do sistema atual e quais melhorias devem ser realizados do ponto de vista dos gestores e colaboradores da Unidade Policial.

3.3 Visitas Técnicas

Visitas rotineiras para visualização do ambiente e um melhor entendimento dos processos realizados.

3.4 Integração aos Processos

Participar dos processos internos da polícia, visando melhor conhecimento dos procedimentos adotados. Buscar verificar de forma ativa os problemas encontrados, as possíveis soluções, nível de comprometimento dos colaboradores e realizar relatórios periódicos para utilização como parâmetro no desenvolvimento do Manual.

3.5 Identificação e Tratamento dos Ativos

Identificar os ativos da Unidade Policial, classificando-os, e separando-os por níveis de prioridade, para possibilitar um tratamento específico, garantindo a utilização de Politicas de Segurança mais seguras. Pode-se verificar na figura 1, logo abaixo a matriz de risco, apresentando os principais ativos a serem analisados.

Matriz de Risco da Polícia Civil de Chavantes					
Componentes	**Ativos**	**Vulnerabilidade**	**Ameaça**	**Dano/Impacto**	**Risco %**
Físico	Arquivo Morto	8	8	8	64
	Prédio	7	4	5	20
	Hardware	8	6	8	48
	Servidor	7	8	7	56
Humano	Funcionário	6	8	5	40
	Terceirizado	7	6	7	42
	Usuário	5	7	5	35
	Fornecedor	4	4	8	32

Figura 1 – Matriz de Risco

Fonte: Elaborado pelos autores

	Baixa	Média	Alta
Vulnerabilidade	0 a 3	4 a 7	8 a 10
Ameaça	**Natural** 0 a 3	**Involuntária** 4 a 7	**Voluntária** 8 a 10
Dano/Impacto	**Pequeno** 0 a 3	**Médio** 4 a 7	**Grande** 8 a 10

Figura 2 – Tabela de Criticidade

Fonte: Elaborado pelos autores

3.6 Descrição do Ambiente

O ambiente analisado é uma unidade da Polícia Civil do Estado de São Paulo, onde na mesma, trabalham nove pessoas, sendo divididas em:

- **Delegado:** responsável por todos dentro desta unidade, fazendo com que o trabalho seja realizado de forma correta, e respondendo por qualquer ocorrência, crime ou atos que venham a ser praticados na região de sua jurisdição.
- **Investigador:** policial especializado em realizar trabalho externo (rua), efetuando investigações a respeito de crimes, roubos, desaparecimento de pessoas, e esclarecendo os mesmos a ordem em que aparecem.
- **Escrivães:** policiais também treinados e aprovados em concurso público, porém treinados para trabalhar na parte administrativa, realizando todo trabalho burocrático dentro da instituição, ouvindo pessoas envolvidas em crimes, elaborando Boletins de Ocorrências e todo trâmite policial.
- **Papiloscopista:** policial responsável pela parte de identificação do indivíduo por meio das “papilas”, ou seja, impressões digitais, sendo

esta área responsável por retirar impressões digitais para elaboração de RGs e na identificação de suspeitos.

- **Auxiliares Administrativos:** funcionários públicos municipais admitidos em concurso público que prestam serviços na unidade policial, realizando trabalho administrativo, mediante convênio entre a Prefeitura Municipal e a Delegacia.
- **Policiais:** pessoal responsável em efetuar o patrulhamento das ruas, e localizar e apreender pessoas suspeitas, efetuando turnos de trabalho variados.
- **Faxineira:** contratada por firma terceirizada, responsável pela parte de limpeza e conservação do prédio.
- **Setor de Trânsito:** pessoal responsável pela emissão de documentos e emplacamento de veículos, bem como aplicação de multas oriundas de infrações de trânsito.
- **Estagiário(a):** estudante do último ano do curso de Direito, aprovado(a) pela FUNDAP (Fundação de Desenvolvimento Administrativo), que realiza estágio em Unidade Policial, visando aprimorar seu conhecimento, ajudando também na parte de elaboração de Boletins de Ocorrência e Inquéritos Policiais.

No prédio existem oito salas, sendo cinco no primeiro andar e três no segundo, que dividem os setores da delegacia. Duas delas ficam logo na entrada: uma para atendimento ao público e elaboração de Boletins de Ocorrência e outra para um Escrivão. Na sala do escrivão fica também o rack da Prodesp, órgão responsável pela intranet.

Nos fundos existem três salas: uma para o Delegado, uma para outro Escrivão e uma para o Investigador, isso tudo até então no primeiro andar.

No andar superior existem mais três salas: uma para o Setor de Trânsito, uma para serviços de Papiloscopista (elaboração de RG), e uma reservada para o Arquivo Morto.

Em todas as salas, com exceção da sala do Papiloscopista e do Arquivo Morto, existe um ou mais computadores sendo usados com sistemas Linux e Windows XP.

Existem quatro extintores espalhados por todo o prédio, porém na sala do arquivo morto não existe extintor. Não existem saídas de emergência, porém, o portão dos fundos é bem amplo e fica sempre aberto no horário de expediente.

O prédio conta ainda com um link externo para acesso a internet, o qual o acesso ao mesmo é feito em cinco dos oito computadores.

Os Boletins de Ocorrência são elaborados em um sistema conhecido como **RDO** (Registro Digital de Ocorrência), tendo dessa forma um registro eletrônico e um físico das ocorrências, sendo os eletrônicos armazenados em banco de dados externo de manutenção da matriz da Policia Civil do Estado de SP.

3.7 Inquéritos Policiais

Os Inquéritos Policiais onde são registrados todos os delitos cometidos por um indivíduo, são guardados apenas em formato físico (papel), não havendo nenhum responsável direto por seu arquivamento. Todos os funcionários da delegacia tem acesso ä sala de Arquivo Morto, podendo manusear os documentos lá contidos de qualquer maneira, sem nenhum controle de acesso aos mesmos.

4 RESULTADOS E DISCUSSÕES

Neste capítulo**,** serão expostos os problemas encontrados com relação a Segurança da Informação, em uma das Unidades da Polícia Civil do Estado de São Paulo, conforme avaliação feita através da aplicação de questionários e visitas técnicas até o local. A pesquisa elaborada aponta quais pontos estão vulneráveis na unidade avaliada possibilitando assim estabelecer os requisitos necessários para sua proteção. Esses pontos irão fazer parte do manual de implementação de politicas de segurança da Informação.

4.1 Segurança da Informação

Com relação a Segurança da Informação, embasados nos capítulos anteriores onde foram descritos os requisitos para sua obtenção, notou-se na figura 8 abaixo, que (67%) dos funcionários da Unidade Policial afirmam que desconhecem

o responsável pela Segurança da Informação, e (33%) dizem que existe um responsável pela Segurança da Informação, mostrando que cada funcionário segue um procedimento próprio não estando amparados por nenhuma política de SI.

Figura 1 – Conhecimento sobre o responsável pela Segurança da Informação

Fonte: Elaborado pelos autores

4.2 Importância dos documentos

No ambiente analisado notou-se que (78%) dos colaboradores acreditam que os inquéritos policiais trazem informações de maior importância para a polícia, sendo que este se encontra em formado físico (papel), e outros (22%) acreditam que todos os documentos são importantes, não vendo maior prioridade em um ou em outro, conforme mostra figura 2 a seguir:

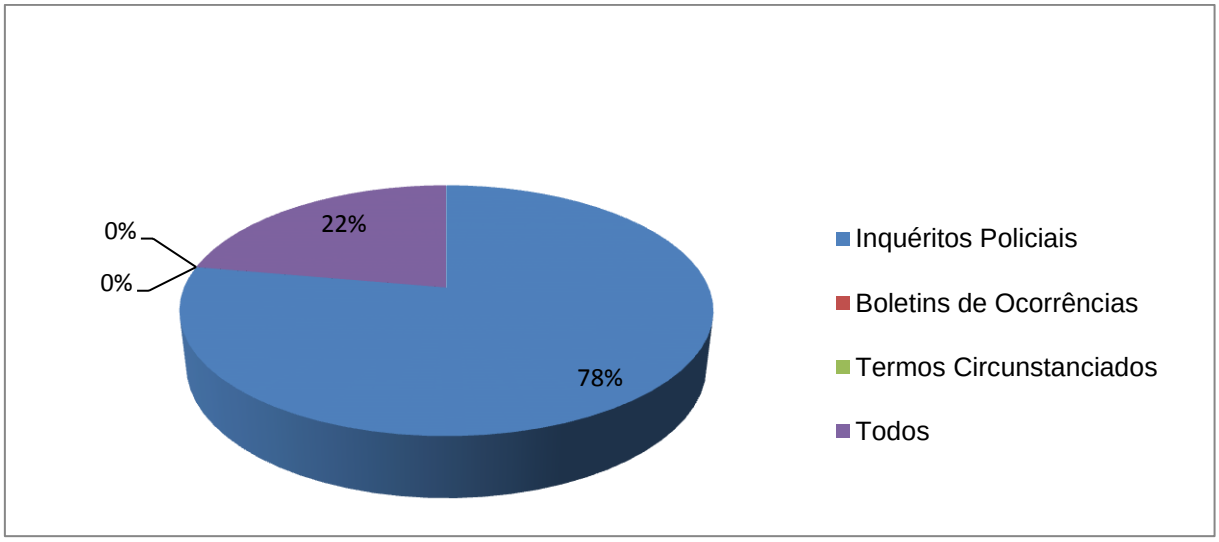

Figura 2 – Documentos mais importantes na visão dos colaboradores
Fonte: Elaborado pelos autores.

Para os inquéritos policiais que neste caso, obtiveram maior grau de importância, cuidados especiais devem ser tomados para que a vida útil desses documentos perdure pelo maior tempo possível e que sua reposição também seja feita para que sempre esteja disponível a futuras consultas.

4.3 Setores que requerem maior atenção

Pode-se verificar que nas organizações, existem setores ou departamentos que requerem mais atenção que outros. Isto se deve ao fato de possuírem informações ou arquivos importantes e que são vitais para a organização e que devem ser armazenados e manuseados com mais cautela, pois caso ocorra à perda ou extravio dos mesmos, e não se possua uma cópia, sua recuperação está comprometida.

Tanto em grandes corporações, como em pequenas, deve-se ser direcionada a devida atenção aos setores que guardam informações importantes.

Seguindo este conceito, na Unidade Policial analisada nota-se na figura 3 abaixo, que (86%) dos funcionários disseram que o arquivo morto onde ficam guardados os inquéritos policiais é o setor que requer maior atenção, contra (14%) que dizem que os arquivos pertencentes ao setor de investigações denotam maior importância.

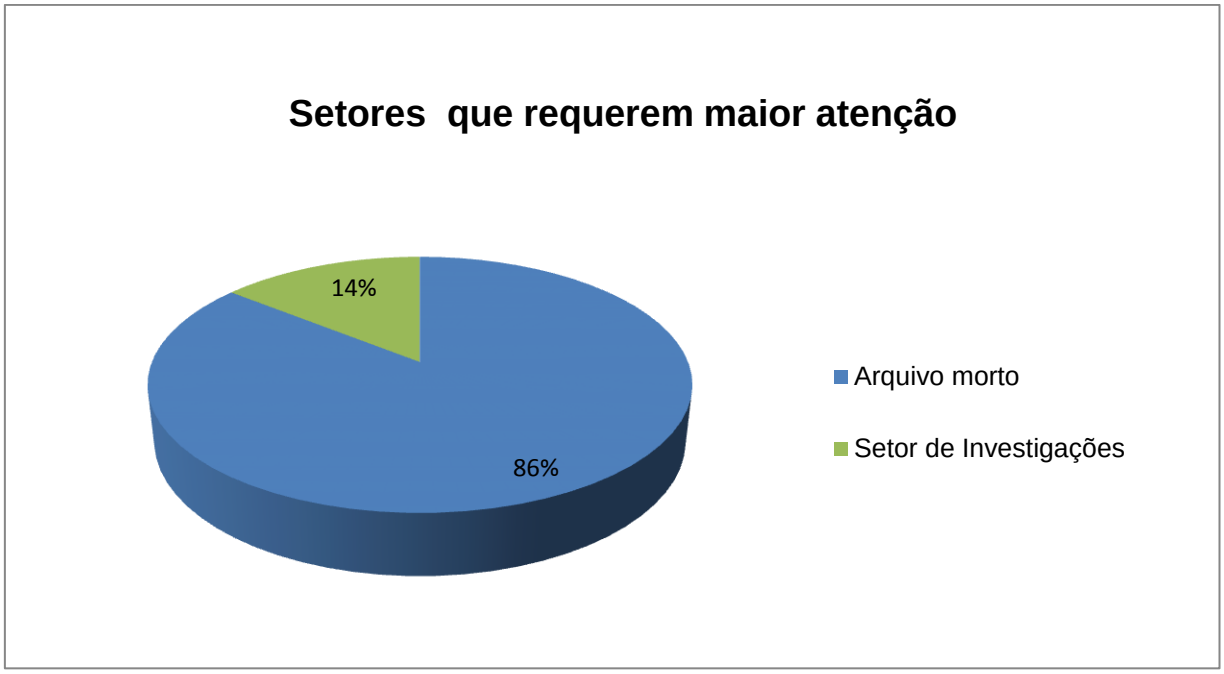

Figura 3 - Setores que requerem maior atenção

Fonte: Elaborado pelos autores

4.4 Descarte das informações

O descarte das informações é algo muito importante para o provimento de um ambiente seguro, pois faz parte do processo e da vida útil dos ativos. Muitas organizações se preocupam com várias áreas de suas empresas, mas deixam pequenas lacunas vulneráveis que possibilitam que pessoas mal intencionadas adquiram informações sigilosas e façam uso de forma ilícita. Dessa forma se faz necessário um correto descarte das informações contidas nas empresas e organizações inseridas no mercado atual, visto que hackers tem vasculhado até mesmo o lixo de grandes empresas, à procura de qualquer tipo de dados ou informações para tirarem proveito dessas lacunas deixadas na segurança, invadindo sistemas e se apoderando dos dados e informações neles contidos.

Na Unidade Policial assim como em várias empresas, esse problema também ocorre e mesmo havendo um procedimento, para descarte de informações, muitos funcionários não utilizam de forma correta. Pode-se observar claramente na figura 13 na próxima página, que há divergências na utilização correta do descarte das informações, pois (56%) dos funcionários dizem não se preocuparem com o

descarte das informações e (44%) que se preocupam e fazem bom uso do procedimento.

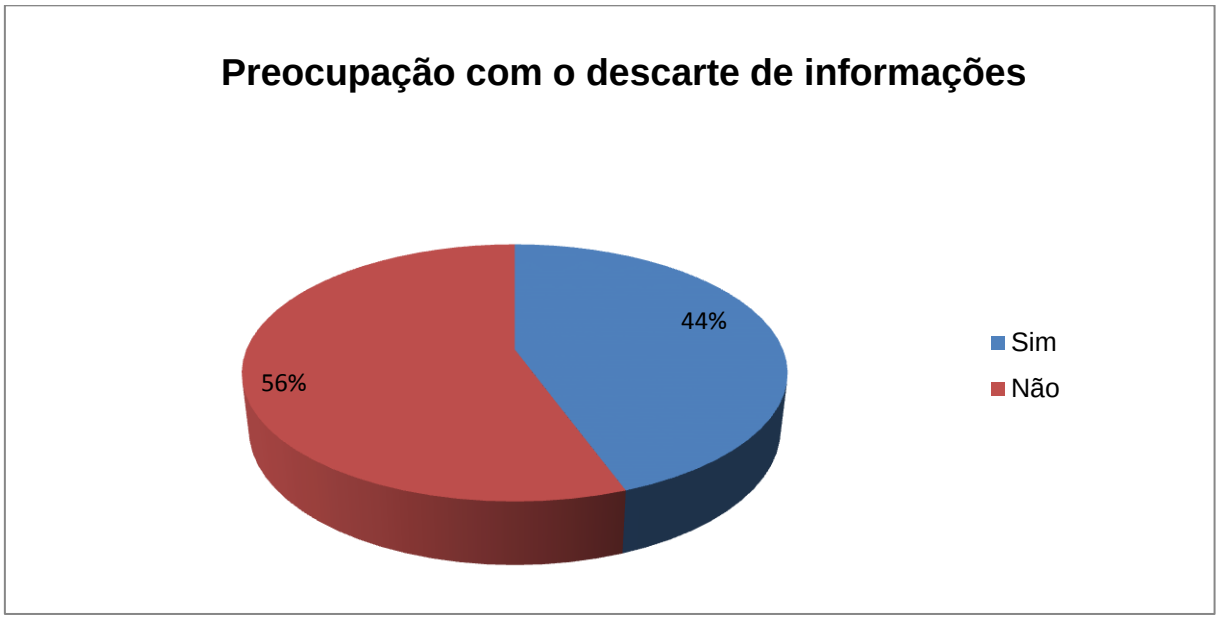

Figura13– Preocupação com o descarte de informações

Fonte: Elaborado pelos autores

5 CONSIDERAÇÕES FINAIS

Mesmo com a grande quantidade de evidências que mostram a necessidade de proteção dos ativos dentro das organizações, ainda existem empresas que fazem uso de seus recursos sem tomarem os devidos cuidados para o provimento de um ambiente seguro. Isso é gerado pela falta de uma politica de segurança da informação ou até mesmo pela falta de conscientização e treinamento aos envolvidos nos processos.

Pode ser observado na pesquisa que alguns dos fatores que contribuíram para a ocorrência dos problemas apresentados, são gerados pela falta de um responsável pela segurança das informações e de regras e procedimentos que sejam disseminados a todos os colaboradores da Unidade Policial. Essa falha encontrada gera um nível crítico a segurança dos ativos, devido ao desconhecimento do real valor do que está sendo manipulado e cada usuário acaba aderindo a regras e procedimentos próprios, tornando os processos não padronizados.

Outro ponto de destaque são os acessos ao sistema e aos espaços físicos, que não possuem restrições especiais. São utilizadas por grande parte dos funcionários senhas compartilhadas, característica que não condizem com o real valor da senha que é de ser única e intransferível. Quanto ao espaço físico existe transição de pessoal de maneira indiscriminada, ficando as informações desses locais disponíveis a qualquer funcionário.

Esse trabalho teve uma grande relevância dentro da Unidade Policial onde foi aplicado visto que, o delegado responsável, após visualizar o resultado mostrou interesse por sua implementação, passando a dar maior importância as suas informações.

MANUAL DE IMPLEMENTAÇÃO

SEGURANÇA DAS INFORMAÇÕES

Procedimentos:

- Eleger um responsável pelos dados;
- Autenticar todos os usuários;
- Disponibilizar aos usuários apenas o necessário para desempenhar suas funções;
- Controle de entrada e saída dos setores;
- Realizar cópias de segurança;
- Manter as informações em mais de um local;
- Ambientes Climatizados;
- Equipamentos de prevenção de incêndios;
- Realizar treinamentos e palestras;
- Divulgar a todos os setores da UP os procedimentos a serem seguidos;

ACESSO AS SALAS

Procedimentos:

- Acesso autorizado somente ao funcionário do setor.
- Manter a sala fechada na ausência do responsável.

ARMAZENAMENTO DE DOCUMENTOS

Procedimentos:

- Registrar quantidade de páginas;
- Encaminhar ao setor responsável;
- Separar e ordenar os documentos;
- Gerar um número de registro ao documento;
- Classificar por nível de importância;
- Identificar o responsável, o dia e horário do arquivamento;
- Realizar o arquivamento em local específico.

DA RETIRADA DE ARQUIVOS

Procedimentos:

- Solicitar ao setor responsável os documentos;
- Verificação de quantidade de páginas do documento retirado;
- Identificar o motivo da solicitação;
- Registrar nome, data e horário da retirada;
- Validade para devolução dos arquivos;
- Conferir quantidade de páginas do documento devolvido;
- Registrar nome, data e hora da devolução;
- Realocar em seu local específico.

MANUSEIO DAS INFORMAÇÕES

Procedimento:

- Não ingerir alimentos durante o manuseio de informações;
- Manter uma boa higiene pessoal;
- Não danificar;
- Não realizar cópias sem autorização;
- Não divulgar ou utilizar para fins pessoais;
- Manter o sigilo das informações.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação, Rio de Janeiro: ABNT, 2005.

ARANHA, Ana Carolina. A sociedade e a segurança da informação. Microsoft Technet. Disponível em: http://technet.microsoft.com/pt-br/library/cc668426.aspx. Acesso em: 02 Out 2012.

ARTIGOS JURÍDICOS. Inquérito Policial. Disponível em: http://www.advogado.adv.br/artigos/2001/emerson/inqpolicial.htm. Acesso em: 02 Nov 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação – Guia Prático para Elaboração e Implementação 2 Ed. Rio de Janeiro: Ciência Moderna., 2008.

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

FONTES, Edison Luiz Gonçalves. Segurança da Informação: O usuário faz a diferença. São Paulo: Saraiva, 2006.

ISO/IEC 13335-1:2004 – Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. 2004.

PEIXOTO, Mário C.P.P. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006.

SCRIBD. Disponível em: <http://pt.scribd.com/doc/52566307/Apostila-Gestao-de-Seguranca-da-Informacao> Acesso em 14 Março 2013.

SUA PESQUISA.COM, Sumérios. História dos Sumérios, Suméria, Mesopotâmia, Cultura, Civilização, Escrita Cuneiforme. Disponível em: http://www.suapesquisa.com/pesquisa/sumerios.htm . Acesso em 17 Abril, 2013.