FÁBIO AMARO OLIVEIRA

UM ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA ORGANIZAÇÃO PÚBLICA

LAVRAS – MG

2014

FÁBIO AMARO OLIVEIRA

UM ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA ORGANIZAÇÃO PÚBLICA

Trabalho de Conclusão de Curso de Graduação apresentado ao Colegiado do Curso de Bacharelado em Sistemas de Informação, para obtenção do título de Bacharel.

Orientador:

Prof. Rêmulo Maia Alves

LAVRAS - MG

2014

FÁBIO AMARO OLIVEIRA

ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA ORGANIZAÇÃO PÚBLICA

Trabalho de Conclusão de Curso de Graduação apresentado ao Colegiado do Curso de Bacharelado em Sistemas de Informação, para obtenção do título de Bacharel.

APROVADA em 26 de novembro de 2014.

Dr. Marluce Rodrigues Pereira

Clessius Wallace Sandy

Dr. Rêmulo Maia Alves (Orientador)

LAVRAS-MG
Novembro/2014

AGRADECIMENTOS

Gostaria de agradecer, em primeiro lugar, a Deus pela oportunidade de realizar meu sonho e alcançar mais essa vitória.

Ao meu orientador Rêmulo Maia Alves, que me orientou com seus conhecimentos e grande experiência na área, o que foi fundamental para elaboração deste trabalho.

Agradeço aos meus amados pais, Diana e Moisés, pelo apoio, incentivo, educação e orações.

Aos meus irmãos Renan (in memoriam) eu nunca vou me esquecer de você, te amo... e Diego pela admiração e companheirismo que nos fazem caminhar juntos.

A minha esposa Jaciara pelo incondicional apoio, amor, carinho e por estar sempre ao meu lado nos momentos mais difíceis de minha vida.

A minha filha recém-nascida Amanda, que me incentiva e me faz querer buscar novas vitórias.

Ao comandante da 6ª Cia Ind MAT, Ageu Evangelista Ferreira – Major PM, juntamente com Sgt PM Clessius e Cb PM João Bosco.

Aos meus amigos que me acompanharam durante essa batalha e principalmente meu amigo Alessandro Botelho pelo companheirismo e ajuda nessa caminhada que nos fez chegar a essa vitória juntos.

Por fim, agradeço a todos que não citei, mas que colaboraram com mais esta conquista em minha vida.

RESUMO

A elaboração da Política de Segurança da Informação é um diferencial estratégico para as organizações que se preocupam com a informação, as tecnologias que suportam essas informações, as pessoas, os processos e o ambiente como um todo e querem cuidar para que um incidente de segurança não ocorra com nenhum desses ativos. Neste trabalho é apresentado um estudo de caso sobre a gestão da segurança da informação em uma empresa pública, sendo esta a Sexta Companhia Polícia Militar Independente de Meio Ambiente e Trânsito Rodoviário (6ª Cia Ind MAT), unidade pertencente a Polícia Militar de Minas Gerais (PMMG). O intuito do trabalho foi desenvolver uma Política de Segurança da Informação a partir das normas ABNT ISO/IEC DA SÉRIE 27000, análise CIDAL e das vulnerabilidades relativas aos ativos da informação. Caso seja aprovada pela alta direção da organização, a política deverá ser publicada e divulgada a todo seu público interno, tanto para parte tática como operacional, mostrando que é necessário preocupar com segurança da informação a todo instante.

Palavras-chave: Política de Segurança da Informação, normas ABNT ISO/IEC DA SÉRIE 27000, Análise CIDAL.

ABSTRACT

The development of the information security policy is a strategic advantage for organizations that are concerned with the information, technologies that support this information, people, processes and the environment as a whole and want to care for a security incident does not occur with any of these assets. In this paper a case study on the management of information security in a public company is presented, which is the 6th Co. Ind MAT, facility owned by the Military Police of Minas Gerais. The aim of the study was to develop a security policy information from the standards ISO / IEC 27000 SERIES, analysis CIDAL and vulnerabilities related to information assets. If approved by the top management of the organization, the policy should be published and disseminated throughout its domestic audience, both for tactical and operational part, showing that it is necessary to worry about information security at all times.

Keywords: information security policy, standards ISO / IEC 27000 SERIES, Analysis CIDAL.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

6ª CIA PM IND MAT	Sexta Companhia Polícia Militar Independente de Meio Ambiente e Trânsito Rodoviário
ABNT	Associação Brasileira de Normas Técnicas
B.O	Boletim de Ocorrência
BOs	Boletim de Ocorrência Simplificado
COBIT	Control Objectives for Information and Related Technology
ERP	Enterprise Resource Planning
IEC	International Electrotechnical Comission
ISO	International Organization for Standardization
IS	Incidente de Segurança
NBR	Norma Brasileira
PDCA	Planejar, Fazer, Checar, Agir
PMMG	Polícia Militar de Minas Gerais
PN	Processo de Negócio
REDS	Registro de Defesa Social
RDS	Relatório Diário de Serviço
SGSI	Sistema de Gestão de Segurança da Informação
SIDS	Sistema Integrado de Defesa Social
SIU	Sistema Informatizado Unificado
TI	Tecnologia da Informação
Wi-Fi	Wireless Fidelity

SÚMARIO

1. INTRODUÇÃO

As empresas na atual conjuntura do mercado devem estar atentas às novas tecnologias que são desenvolvidas a cada dia e como elas podem ser incorporadas para melhorar seus sistemas e facilitar suas atividades. Sendo assim, garantir a proteção de um conjunto de informações, preservar o valor que elas possuem para a organização e fazer com que a segurança das informações torne-se uma das principais estratégias e ponto de atenção das empresas.

A gestão da segurança da informação faz com que uma empresa pública ou privada, possa garantir que o funcionamento de seus sistemas fique menos vulnerável contra invasores que estão em busca de informações essenciais para o negócio da organização ou querem causar algum dano.

Nesse sentido, com o crescimento da necessidade de estar conectado a uma rede de computadores, através da internet, para realização de trabalhos essenciais, tanto administrativos quanto operacionais, faz com que os recursos de hardware e software das empresas fiquem expostos a ameaças tanto no âmbito interno como externo. As tecnologias aumentam o conforto e a facilidade para os usuários, podendo trazer com elas vulnerabilidades que devem ser identificadas e tratadas, diminuindo ao máximo os riscos e perigos.

A falta de uma Política de Segurança da Informação bem definida para a organização pode acarretar em falhas de segurança nos sistemas e nos processos de negócio. Com isso, podem causar impactos dos mais variados níveis, indo do acesso indevido a sistemas restritos, perda de dados importantes dos processos de negócio, ou em um nível mais crítico, colocar em risco a vida de terceiros, bem como a vida de integrantes da corporação, através do vazamento de informações sigilosas.

Devido à necessidade de se ter uma maior segurança e proteger as informações, as tecnologias que dão suporte a essas informações, as pessoas, os

processos e os ambientes, é fundamental que a empresa tenha uma Política de Segurança da Informação que esteja pautada nos princípios básicos de confidencialidade, disponibilidade e integridade, para assim poder fazer a gestão de riscos.

Nesse contexto, este trabalho vem mostrar um estudo de caso sobre a Gestão da Segurança da Informação na Sexta Companhia de Polícia Militar Independente de Meio Ambiente e Trânsito Rodoviário (6ª CIA PM IND MAT), sendo uma companhia pertencente à Polícia Militar de Minas Gerais (PMMG), que é uma empresa pública estadual.

1.1 Motivação

A motivação para a elaboração deste estudo vem da importância que a segurança da informação exerce para 6ª Cia Ind MAT, bem como para todo tipo de empresa que está no mercado, sujeito aos riscos e ameaças que estão presentes no dia-a-dia de uma organização. As vulnerabilidades são inerentes a qualquer empresa que utiliza tecnologia, principalmente quando estas expõem seus sistemas de informação e comunicação ao estarem conectados à rede mundial de computadores.

É importante o entendimento mais aprofundado das normas existentes na literatura para identificar a existência e como está estabelecida a gestão da segurança da informação no setor de (Tecnologia da Informação) da empresa pública estudada.

1.2 Justificativa

A justificativa para elaboração deste trabalho manifesta-se na importância de levantar os pontos de ameaças e vulnerabilidades dos ativos de

informação, para que se possa ajudar na elaboração de uma Política de Segurança da Informação, auxiliando nas diretrizes/fundamentos básicos de segurança, podendo atender as necessidades da organização, e que sirva de referência para melhorar a segurança de outras empresas.

Com relação a isso, visa auxiliar a organização no levantamento de seus pontos negativos e que podem ser solucionados com melhorias estabelecidas dentro das normas NBR ISO/IEC 27000.

1.3 Objetivos

O objetivo principal deste trabalho é realizar um estudo de caso sobre gestão da segurança da informação no setor de TI de uma empresa pública, levando em consideração o que é proposto nas normas da série NBR ISO 27000.

Como objetivos específicos pretendem-se:

1) Identificar os pontos de vulnerabilidade, relacionados às ferramentas computacionais, às pessoas, aos processos e ao ambiente.
2) Analisar a segurança da informação em relação ao ambiente empresarial, orientando e apoiando a alta direção a estabelecer uma Política transparente de Segurança da Informação para toda a organização. Com isso, conscientizar todo o nível estratégico da organização a respeito da importância de se ter uma Política de Segurança da Informação capaz de garantir a confidencialidade, integridade e disponibilidade necessárias às informações.
3) Elaborar um relatório com as melhores práticas relativas à gestão da segurança da informação.

1.4 Estrutura do Documento

Com relação à disposição do texto, o trabalho está organizado em 5 capítulos, sendo o capítulo 1 composto pela introdução, o capítulo 2 é composto pelo referencial teórico que faz uma contextualização geral sobre segurança da informação, Política de Segurança da Informação, ativos da informação, vulnerabilidades, ameaças, incidente de segurança, probabilidade, impacto e controle e por último aborda sobre as normas ABNT NBR ISO/IEC 27000.

No capítulo 3 é apresentada a metodologia de pesquisa que vem mostrar os métodos, técnicas, procedimentos e a identificação quanto à descrição dos tipos de pesquisas utilizados.

Os resultados e discussão encontram-se no capítulo 4, e objetivam dar uma melhor visão a todos os níveis da organização em relação às vulnerabilidades e falhas para que possam ser melhoradas. No capítulo 5, é apresentada a conclusão sobre o estudo realizado e tudo o que foi observado em relação a TI e a segurança da informação.

2. REFERENCIAL TEÓRICO

2.1 Segurança da Informação

Conforme Campos (2007), na década de 1980 surgiram às teorias relacionadas ao conceito de sociedade do conhecimento ou da informação. A informação é um elemento base essencial na geração de conhecimentos, facilitando na tomada de decisões, gerando eficiência nos negócios e agilidade em cada uma das atividades organizacionais.

De acordo com Fernandes (2010a), o conceito de informação pode ser definido sob duas perspectivas: como estrutura, pode ser conceituada como um conjunto de dados ou registros representados em uma determinada forma/ordem que lhes permitem ser entendidos; e como processo, a informação pode ser entendida como o resultado da interação entre agentes capazes de interpretar e decidir. Não obstante, a informação caracteriza-se como um ativo com grande importância para as organizações, visto que a mesma ajuda, e por vezes determina a tomada de decisões, a coordenação e o controle que se tem da organização e de seus negócios.

A segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Os ativos são recursos, pessoas, bens e serviços, que a empresa possui e que geram receita (SÊMOLA, 2003).

A mudança e o crescimento da tecnologia da informação dos computadores tomam conta dos ambientes de escritório, quebram paradigmas e acesso local à informação, e chegam a qualquer lugar do mundo através dos notebooks e da rede mundial de computadores: a internet (SÊMOLA, 2003).

Um ponto importante na segurança informacional em um ambiente empresarial é o tráfego das informações por esse ambiente. Essa troca de

informação é essencial para os diversos processos de trabalho, visto que a mesma é compartilhada com os demais usuários. Nos mais variados ambientes, as informações podem ser encontradas de inúmeras maneiras, podem estar escritas, impressas, em um banco de dados (rede local), em mídias, etc. As informações também trafegam em redes internas e externas (Intranet e Internet), portanto, surge à necessidade de que as informações estejam sempre bem seguras (CAMPOS, 2007).

Ainda conforme Campos (2007), a segurança é implantada pela necessidade do administrador em reduzir os riscos oferecidos às informações, com objetivo de proporcionar um nível aceitável de garantia. A segurança das informações tem que ser bem estabelecida e organizada de forma que um sistema de segurança da informação atenda a três princípios básicos: Confidencialidade, Integridade e Disponibilidade. Se um desses itens falharem, seja por ter sido desrespeitado, atacado, falha nos equipamentos ou por outro motivo qualquer, então se tem uma quebra de segurança da informação, ou seja, temos uma incidência de segurança da informação.

Os três princípios fundamentais da segurança da informação, segundo Salvador (2013) são:

Confidencialidade (sigilo): É a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las. Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não autorizadas.

Integridade: Esse princípio destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais, indevidas ou acidentais. Em outras palavras, é a garantia de que a informação que foi armazenada é a que será recuperada.

Disponibilidade: É a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo. Em outras palavras, é a garantia que a informação sempre poderá ser acessada.

Segundo Canaver (2012) outros aspectos complementares a estes três são:

Autenticidade: garante que a informação efetivamente foi criada ou manipulada por quem reivindica sua autoria. Exemplo: uso de uma senha de acesso.

Legalidade: permite garantir alguns aspectos interessantes. Um deles é a compatibilidade com as leis, regulamentos e normas que cercam o ambiente onde a mesma é utilizada. O outro aspecto atual é a não repudiação de auditoria, ou seja, mesmo que um usuário tente negar que realizou uma determinada transação qualquer que ele efetivamente tenha realizado, isso não seja possível através de algum mecanismo de comprovação com documentos digitais particulares. A Autenticidade também contribuiu para a obtenção desta característica.

O ciclo de vida da informação diz respeito a todos os momentos onde a informação é exposta a riscos, e agora já podemos dizer, de comprometimento de um ou mais aspectos de segurança citados acima. Estes momentos são vivenciados quando os ativos da empresa sejam eles físicos tecnológicos ou humanos, fazem da informação disponível, alimentando os processos de negócio e fazendo a empresa funcionar.

Em uma corporação, a segurança está ligada a tudo o que manipula direta ou indiretamente a informação (inclui-se aí também a própria informação e os usuários), e que merece proteção.

2.2 Políticas de Segurança da Informação

Segundo Silva, Carvalho e Torres (2003), Política de Segurança da Informação "... é um conjunto reduzido de regras que definem, em linhas gerais, o que é considerado pela empresa como aceitável ou inaceitável, contendo ainda referencias às medidas a impor aos infratores. Esta política deverá referenciar todas as outras políticas existentes na empresa que contenham regras de segurança, bem como fazer alusão às normas de segurança".

Nesse sentido, a Política de Segurança da Informação é fundamental para normatizar as estratégias vinculadas à segurança dos sistemas de uma empresa. Estas normas possibilitam, entre outras coisas, fiscalizar acessos não autorizados e incorretos.

Recomenda-se a criação de uma comissão responsável pela Política de Segurança da Informação, para divulgação, atualização e distribuição das normas de segurança dentro da empresa. Tal divulgação pode ser através de folhetos entregues aos funcionários no processo de admissão e/ou educação continuada, distribuídos por emails, através de cartazes, ou até mesmo palestras.

O documento que descreve as normas deve conter, no mínimo, os seguintes itens:

- Definição da segurança da informação;
- Resumo das metas e importâncias;
- Comprometimento da direção da empresa;
- Definição das responsabilidades na gestão da segurança;
- Registro das políticas que devem ser seguidas;
- Conformidade com a legislação e cláusulas de contratos existentes.

Para Sêmola (2003), uma Política de Segurança estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e

descarte das informações, dentro do nível de segurança estabelecido sob medida pela e para a empresa.

2.2.1 Ativos de Informação

Conforme Campos (2007), as organizações têm na informação um elemento essencial para todos os processos de negócio, sendo, portanto, um bem ou ativo de grande valor. A informação existe e é suportada em diversos meios, tais como em equipamentos, cadernos, livros, na cabeça das pessoas, em cabos de rede de computadores, Wi-Fi (rede sem fio), entre outros. Assim, é possível afirmar que a informação é tão importante quanto o próprio meio que a suporta, que a mantém segura e que permite a sua existência.

As organizações classificam seus bens patrimoniais como ativos e da mesma maneira a informação e os mecanismos de comunicação, devem ser classificados como ativos de informação, tendo um grande valor. Em muitas organizações maiores, esse valor é maior do que o dos bens concretos (CAMPOS, 2007).

2.2.2 Vulnerabilidade

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável (BUGS, 2012).

2.2.3 Ameaças

Ameaça é algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade. Ameaça pode ser uma pessoa, uma coisa, um evento ou uma ideia capaz de causar dano a um recurso, em termos de confidencialidade, integridade, disponibilidade (SALVADOR, 2013).

Ameaças externas: São representadas por todas as tentativas de ataque e desvio de informações vindas de fora da empresa. Normalmente essas tentativas são realizadas por pessoas com a intenção de prejudicar a empresa ou para utilizar seus recursos para invadir outras empresas.

Ameaças internas: estão presentes, independentemente das empresas estarem ou não conectadas à Internet. Podem causar desde incidentes leves até os mais graves, como a inatividade das operações da empresa.

2.2.4 Incidente de Segurança da Informação

O incidente de segurança da informação pode ocorrer quando uma ameaça externa ou interna explora as vulnerabilidades dos ativos de informação, expondo a vulnerabilidade de um dos três princípios fundamentais que regem a segurança da informação, quebrando a confidencialidade, integridade ou disponibilidade.

2.2.5 Probabilidade

Probabilidade refere-se “à chance de uma falha de segurança ocorrer, que pode ser estimado verificando o grau das vulnerabilidades encontradas nos ativos de informação e o grau das ameaças que possam explorar as vulnerabilidades” (CAMPOS, 2007).

De acordo com Campos (2007), a probabilidade de ocorrer um incidente de segurança é estimada a partir da relação do grau da ameaça e o grau da vulnerabilidade. Como exemplo, ameaças consideradas de alto grau temos os vírus e o acesso livre aos servidores, já como ameaças de baixo grau podemos citar os meteoros que podem cair na superfície da Terra. Com relação às vulnerabilidades de alto grau, tem-se uma rede local de computadores ligada à Internet; e as vulnerabilidades de baixo grau, armários sem tranca, onde se guardam mídias de instalações e de backup. Esses graus são sempre relativos, pois mesmo as mais baixas vulnerabilidades poderão representar probabilidades consideráveis se o grau de ameaça for muito grande.

2.2.6 Impacto

Os impactos referem-se aos problemas e prejuízos que um incidente de segurança causa quando, de fato, ocorrem em uma organização. Quando ocorre um impacto, de um mesmo incidente de segurança da informação, este pode ser diferente em organizações diferentes, dependendo do tipo de negócio ou do plano de contingência (CAMPOS, 2007).

2.3 Controle

Conforme Campos (2007), o controle deve ser exercido, principalmente, em cima das vulnerabilidades que existem nos ativos, que normalmente estão dentro do raio de ação, já que as ameaças são agentes externos, que normalmente estão fora do raio de ação. De fato, as medidas de segurança da informação, na prática, são voltadas para a diminuição das vulnerabilidades que podem ser encontradas nos ativos de informação das empresas.

Deve ser feito um controle de segurança da informação, onde poderá ser usado um mecanismo para diminuir a vulnerabilidade de um ativo de

informação, sejam sobre um equipamento, os funcionários ou um processo. Os tipos de controle mais encontrados são: senhas de acessos, Política de Segurança da Informação, contratos de responsabilidades sobre uso da informação, sistemas de firewall (controle contra invasões por hackers via rede) e Proxy, acesso físico aos equipamentos e as salas onde ficam os servidores, monitoramento de infecção por vírus, entre outros meios de controle (CAMPOS, 2007).

2.3.1 Control Objectives for Information and Related Technology (COBIT)

O COBIT (2007) tem um conjunto de ferramentas eficazes focadas no controle dos processos, dando o diagnóstico do que fazer, mas não como fazer, questão que terá de ser resolvida com a ajuda das melhores práticas de outras metodologias. É um modelo abrangente, sua utilização independe da plataforma de TI utilizada, ou ramo da empresa. O COBIT é um instrumento de apoio para desenhar, melhorar ou auditar processos, dizendo o que o processo deve ter ou fazer.

O COBIT é composto por quatro áreas distintas (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, Monitoração e Suporte). Em cada uma destas áreas é definida uma série de processos que visam garantir o controle de todas as etapas. Ele possui 34 objetivos de controle de alto nível e 215 objetivos de controle detalhados (processos), sendo atualmente o framework mais completo para governança de TI (ITGI, 2007).

O COBIT orienta sobre as melhores práticas de gestão para cada área da organização de TI, Entretanto, não descreve detalhadamente os procedimentos, mesmo porque cada organização tem suas próprias características. Alinhado aos modelos (COSO, ITIL, ISO/IEC 27001(17799) e Lei Sarbanes-Oxley (SOX)), abrangente e aplicável para auditoria e controle de processos em TI desde o

planejamento até a monitoração e a auditoria de todos os processos (ITGI, 2007).

2.3.2 Os Princípios Básicos do COBIT

- Efetividade: A informação deve ser entregue de forma correta, consistente e em formato útil.
- Eficiência: A informação deve ser provida por meio do uso otimizado dos recursos.
- Confidencialidade: A informação deve ser protegida contra acesso não autorizado.
- Integridade: Precisão e completude de informações.
- Disponibilidade: Informações disponíveis sempre que necessário.
- Conformidade: As informações devem obedecer a leis, regulamentos e cláusulas contratuais aos quais os processos de negócio estão sujeitos.
- Confiabilidade: Informações adequadas para que a organização exercite suas atividades de negócio.
- Aplicações: Sistemas automatizados e procedimentos manuais que processam informações.
- Informação: Dados capturados, processados e gerados por sistemas de informação, em qualquer formato usado pelo negócio.
- Infraestrutura: Recursos tecnológicos (hardware, sistemas operacionais, sistema de banco de dados, redes, etc.) e instalações físicas que suportam o processamento das aplicações.
- Pessoas: Equipe necessária para planejar, organizar, adquirir, implementar, entregar, suportar, monitorar e avaliar sistemas de informação e serviços de TI.

2.3.3 As Características do COBIT

As características de acordo com o ITGI (2007) são:

- Foco no negócio: alinhamento entre objetivos de negócio e objetivos de TI.
- Orientação a processos: organização das atividades de TI em um modelo de processos.
- Baseado em controles: definição de objetivos de controle a serem considerados ao gerenciar os processos.
- Direcionamento a medições: Uso de identificadores e modelos de maturidade.

2.3.4 Modelo de Maturidade do COBIT

De acordo com o ITGI (2007), no COBIT existe uma forma que auxilia os gestores, a saber, como sua organização se situa no mercado, em relação aos concorrentes, as melhores práticas existentes e identificar o que é necessário para alcançar um nível de gestão adequado para os processos de TI.

Para cada processo de TI é relacionado um dos níveis do modelo de maturidade:

- **Não existente:** Carência completa de qualquer processo reconhecido:
- **Inicial:** A organização reconhece que tem problemas, porém os mesmos são resolvidos pontualmente, sem padronização.
- **Repetidos:** Os problemas são resolvidos com envolvimento da TI, inclusive o nível de gerência. Porém não existe um processo definido, tendo práticas de governança como meta. As informações concentram-se nos indivíduos.

- **Definido:** Definido e documentado uma estrutura de processo para supervisão da gerência, baseado nos princípios das boas práticas.
- **Administrado:** Nesta etapa são tomadas ações corretivas quando existem desvios dos objetivos. Os processos estão seguindo seu fluxo normal e podem ocorrer melhorias nestes, quando necessário.
- **Otimizado:** Boas práticas de governança são seguidas. Há uma harmonia entre a TI e objetivos da empresa existindo um controle efetivo das estratégias de TI.

2.3.5 Governança de TI

A governança de TI está relacionada ao desenvolvimento de um conjunto estruturado de competências e habilidades estratégicas que pode ser entendida como a autoridade e responsabilidade pelas decisões referentes ao uso da TI. A administração de TI, com seus processos de planejamento, organização, direção e controle, tem como objetivo garantir a realização bem sucedida dos esforços para o uso da TI, desde a sua definição com o alinhamento estratégico, influenciado pelo contexto, até a mensuração dos seus impactos no desempenho empresarial (SCHEIN, 1989).

2.4. NORMAS ABNT ISO/IEC DA SÉRIE 27000

2.4.1 ABNT NBR ISO/IEC 27001:2006

Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas

necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização. É esperado que este e outros sistemas de apoio mudem com o passar do tempo. Espera-se também que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (ISO/IEC 27001, 2006).

2.4.1.1 Abordagem de Processo

Uma organização precisa identificar e gerenciar muitas atividades para assim poder funcionar efetivamente. Qualquer atividade que faz uso de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo. Frequentemente a saída de um processo forma diretamente a entrada do processo seguinte (ISO/IEC 27001, 2006).

A abordagem de processo para a gestão da segurança da informação apresentada nesta Norma encoraja que seus usuários enfatizem a importância de:

a) Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) Monitoração e análise crítica do desempenho e eficácia do SGSI;

d) Melhoria contínua baseada em medições objetivas.

Esta Norma adota o modelo conhecido como "Plan-Do-Check-Act" (PDCA), que é aplicado para estruturar todos os processos do SGSI. A figura 1 ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações

necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e suas expectativas (ISO/IEC 27001, 2006).

Plan (planejar) (estabelecer o SGSI) Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Do (fazer) (implementar e operar o SGSI) Implementar e operar a política, controles, processos e procedimentos do SGSI.

Check (checar) (monitorar e analisar criticamente o SGSI) Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

Act (agir) (manter e melhorar o SGSI) Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

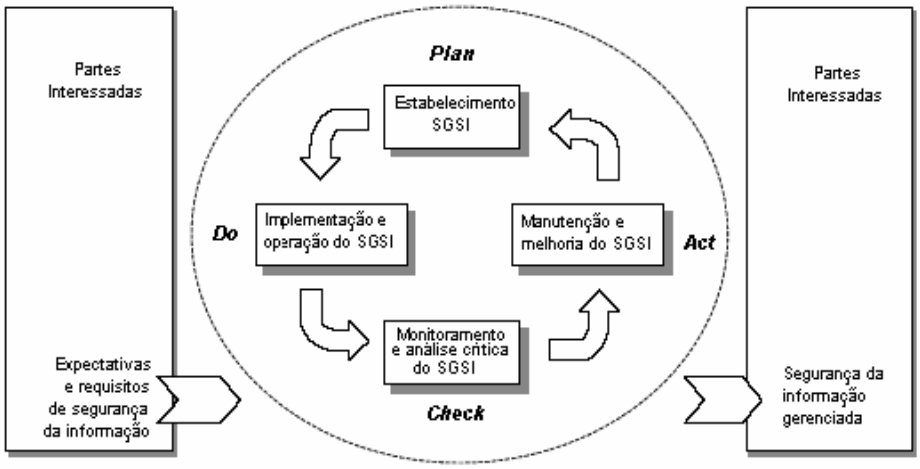

Figura 1 - Modelo PDCA Aplicado aos Processos do SGSI

Fonte: ISO/IEC 27002 (2005)

2.4.2 ABNT NBR ISO/IEC 27002:2005

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.

O código de boas práticas ISO/IEC 27002 fornece uma estrutura para avaliar os sistemas de gestão de segurança da informação, baseada em um conjunto de diretrizes e princípios que têm sido adotadas por empresas, governos e organizações empresariais em todo o mundo (ISO/IEC 27002, 2005).

A ISO/IEC 27002 está estruturada em 11 seções, cada uma destas é constituída por categorias de segurança da informação, sendo que cada categoria tem um objetivo de controle definido, um ou mais controles que podem ser aplicados para atender ao objetivo de controle, as descrições dos controles, as diretrizes de implementação e informações adicionais.

A norma apresenta 39 objetivos de controles (categorias) e 133 controles de segurança que são divididos da seguinte forma: Política de Segurança da Informação, organização da segurança da informação, gestão de ativos, segurança em recursos humanos, segurança física e de ambientes, gerenciamento das operações e comunicações, controles de acesso, aquisição, desenvolvimento e manutenção de sistemas de informação, gerenciamento de incidentes de segurança da informação, gerenciamento da continuidade do negócio e conformidade legal.

2.4.3 ABNT NBR ISO/IEC 27005:2008

Esta Norma está de acordo com os conceitos especificados na ABNT NBR ISO/IEC 27001 e foi elaborada para facilitar uma implementação satisfatória da segurança da informação tendo como base a gestão de riscos.

O conhecimento dos conceitos, modelos, processos e terminologias descritos na ABNT NBR ISO/IEC 27001 e na ABNT NBR ISO/IEC 27002 é importante para um entendimento completo desta Norma Internacional.

Esta Norma Internacional se aplica a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização como um todo (ISO/IEC 27005, 2008).

2.4.3.1 Contextualização

Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. Convém que essa abordagem seja adequada ao ambiente da organização e em particular esteja alinhada com o processo maior de gestão de riscos corporativos. Convém que os esforços em relação à segurança lidem com riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários. Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI (ISO/IEC 27005, 2008).

Convém que a gestão de riscos de segurança da informação contribua para:

- Identificação de riscos
- Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência
- Comunicação e entendimento da probabilidade e das consequências destes riscos

- Estabelecimento da ordem prioritária para tratamento do risco
- Priorização das ações para reduzir a ocorrência dos riscos
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas e informadas sobre a situação da gestão de riscos
- Eficácia do monitoramento do tratamento do risco
- Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los

2.4.3.2 Visão Geral do Processo de Gestão de Riscos de Segurança da Informação

O processo de gestão de riscos de segurança da informação consiste na definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica de riscos (ISO/IEC 27005, 2008, p.8).

O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo ou a uma área específica da organização, por exemplo: um departamento, uma localidade, um serviço, a um sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle efetivo, como o plano de continuidade de negócio (ISO/IEC 27005, 2008).

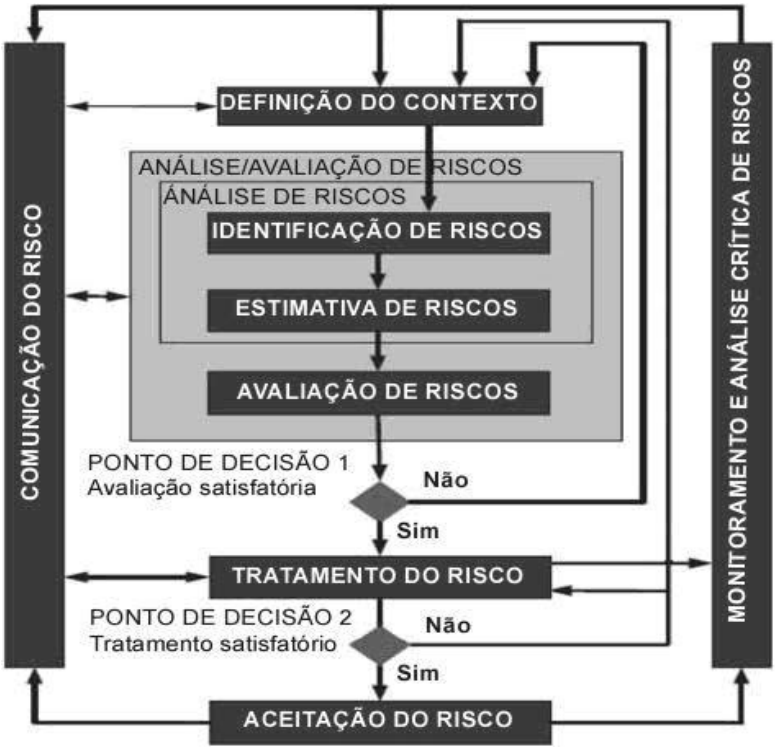

Figura 2 - Processo de Gestão de Riscos de Segurança da Informação

Fonte: ABNT ISO/IEC 27005(2008)

Na figura é ilustrado o Processo de Gestão de Riscos de Segurança da Informação de acordo com a norma ABNT ISO/IEC 27005, onde mostra as atividades de análise/avaliação de riscos e/ou de tratamento do risco como um todo, sendo realizadas mais de uma vez. Um enfoque iterativo na execução da análise/avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. O enfoque iterativo permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados. (ISO/IEC 27005, 2008)

Durante o processo de gestão de riscos de segurança da informação, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados. Mesmo antes do tratamento do risco, informações sobre riscos identificados podem ser muito úteis para o gerenciamento de incidentes e ajudar a reduzir possíveis prejuízos. A conscientização dos gestores e pessoal no que diz respeito aos riscos, à natureza dos controles aplicados para mitigá-los e as áreas definidas como de interesse pela organização, auxiliam a lidar com os incidentes de segurança e eventos não previstos da maneira mais efetiva. Convém que os resultados detalhados de cada atividade do processo de gestão de riscos de segurança da informação, assim como as decisões sobre a análise/avaliação de riscos e sobre o tratamento do risco (representadas pelos dois pontos de decisão na Figura 2), sejam documentados. (ISO/IEC 27005, 2008)

3. DESENVOLVIMENTO

A metodologia de pesquisa visa apresentar os métodos, técnicas e procedimentos, para possibilitar a realização da pesquisa e obter resultados que possam ser úteis para a empresa estudada, descrevendo os tipos de pesquisa.

3.1 Descrições da Pesquisa

No que diz respeito à metodologia para o desenvolvimento deste trabalho, quanto à natureza, será utilizada uma pesquisa aplicada que visa gerar conhecimentos úteis e de forma prática para solução de problemas específicos da empresa, envolvendo interesses locais e que possam ser posteriormente aplicados.

Quanto aos objetivos, foram realizadas pesquisas do tipo exploratórias que tem como objetivo a visualização inicial e familiaridade com os problemas, através do contato direto com as pessoas, ambiente de estudo dos sistemas, sendo tudo relacionado e necessário à pesquisa. O estudo de caso e as pesquisas bibliográficas buscam resgatar o conhecimento através do estudo em livros, artigos científicos e normas relativas ao tema proposto e a observação do ambiente estudado, o que permite uma visão mais ampla sobre o assunto.

Quanto às abordagens, o trabalho consistirá em uma pesquisa qualitativa, pois não utilizará de métodos e técnicas estatísticas. Utilizará do levantamento de informações relacionadas aos problemas de segurança da informação relativos aos processos de negócios utilizados no ambiente da organização.

Quanto aos procedimentos metodológicos, será feito a análise da organização e avaliação dos riscos, propondo uma Política de Segurança da Informação para a 6ª Cia Ind MAT, realizado um estudo sobre 04 sistemas relacionados a TI e que são muito importantes para a organização estudada.

Através disso, fazer o mapeamento dos sistemas, realizando o levantamento dos ativos descritos, identificação de ameaças e vulnerabilidades visíveis. Analisar a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade (Análise CIDAL) e fazer a gestão de riscos relacionados à segurança da informação. Foi elaborada uma proposta para a aquisição de equipamentos de TI, sendo que os valores foram obtidos através de pesquisa de preços praticados no mercado.

3.2 Análise da Organização

3.2.1 Caracterização da Organização

A Sexta Companhia Independente de Meio Ambiente e Trânsito Rodoviário (6ª Cia Ind MAT), pertence à Polícia Militar de Minas Gerais (PMMG), com sede na cidade de Lavras/MG, onde gerencia e participa diretamente da segurança pública. Suas áreas de atuação compreendem a fiscalização de Meio Ambiente e do Trânsito Rodoviário, abrangendo uma área com 44 municípios e 03 distritos no Sul de Minas Gerais. A Cia mantém convênios com outros órgãos como DER (Departamento de Estradas de Rodagem de Minas Gerais), DPRF (Departamento de Polícia Rodoviária Federal), IBAMA (Instituto Brasileiro de Meio Ambiente e dos Recursos Naturais Renováveis), IMA (Instituto Mineiro de Agropecuária) e prefeituras, realizando operações em conjunto com esses órgãos. Na área operacional, são registrados BO (Boletim de Ocorrência), exercendo o poder de polícia ao realizar prisões de acordo com as leis e em casos necessários são lavrados autos de infrações em ambas as áreas de fiscalização. Já na parte administrativa, que compreendem as áreas estratégica e tática, são gerenciadas e controladas as operações, ocorrências e as atividades operacionais, além disso, é desenvolvida

toda a parte administrativa como análise de índices estatísticos, escalas de serviço do efetivo empregado em festas e no dia a dia operacional, controle de recursos, gestão de TI, divulgação de resultados e informações para órgãos de comunicação, etc.

A 6ª Cia foi fundada em 06/09/2006 em Lavras/MG e seu ramo de negócio é Segurança Pública, sendo uma unidade estruturada com uma rede interna de computadores, na qual funciona para fornecer internet a todas as seções, com um servidor próprio que foi configurado com um número de IP fixo, acessível no padrão HTTP por meio de um navegador de qualquer ponto da rede interna e pela internet.

- Empresa: Polícia Militar de Minas Gerais/6ª Cia Independente de Meio Ambiente e Trânsito Rodoviário.
- Empresa de grande porte: Hoje a Polícia Militar de Minas Gerais possui um efetivo de aproximadamente 50.000 policiais, sendo que a 6ª Cia conta com um efetivo de 137 Policiais, distribuídos entre as áreas administrativas, policiamento Rodoviário e de Meio Ambiente e 01 funcionário civil.
- Ramo de negócio: Segurança Pública.
- Ano de fundação da PMMG: A corporação tem a sua origem no Regimento Regular de Cavalaria de Minas, em 9 de junho do ano de 1775, com 239 anos de existência. Já a 6ª Cia foi fundada em 06/09/2006 em Lavras/MG e completou 8 anos.

3.2.2 Levantamento dos Sistemas e Avaliação de Riscos

O estudo identificou quatro sistemas relacionados à área de gestão de TI e que são utilizados pela 6ª Cia, sendo o SIU um processo pioneiro na área e está sendo desenvolvido pela organização estudada em parceria com a UFLA. Foi

realizada uma breve descrição das funcionalidades, mapeando parte do fluxo de informação e realizando a análise CIDAL para os processos. Todavia por se tratar de uma organização do ramo de Segurança Pública existem informações de caráter confidencial, e que não foi possível ter acesso. A obtenção das informações se deu por meio de entrevistas com os usuários e desenvolvedores do sistema.

3.2.2.1 Descrição dos Sistemas

Intranet da Policia Militar de Minas Gerais (PMMG) - O portal de intranet da PMMG foi desenvolvido pela Diretoria de Tecnologia e Sistemas da PMMG para realizar todo o controle administrativo da corporação em todo o estado de Minas Gerais. O sistema é disponibilizado via web e todos os policiais tem acesso ao sistema através de qualquer computador com acesso a internet. O nível de acesso é dado de acordo com a função do usuário no sistema. O sistema seria o equivalente a um ERP (Enterprise Resource Planning) para uma corporação privada. O sistema é mantido pelo Centro de Tecnologia e Sistemas da PMMG, que cuida do aprimoramento e manutenção. A intranet da PMMG agrupa os diversos subsistemas utilizados na administração da corporação, como controle de folha de pagamento de todos os policiais e bombeiros, gerenciamento de ocorrências de todo estado, controle das viaturas, entre muitos outros. Devido a sua importância vital para a administração de toda PMMG, existe uma tolerância máxima de 2 horas para inoperância do sistema, após esse período, grandes prejuízos podem ocorrer. A princípio o operacional, que é o policiamento em si, não fica comprometido, mas o não funcionamento deste sistema por um grande período de tempo compromete o funcionamento de toda a corporação, pelo fato do serviço administrativo depender desse processo, sendo que o serviço administrativo é quem irá dar suporte ao serviço operacional.

Sistema Informatizado Unificado (SIU) - é o sistema desenvolvido pela 6ª. CIA Ind MAT da PMMG para gerenciamento e controle das ocorrências e atividades na sua área de atuação, que abrange 44 municípios e três distritos no Sul de Minas Gerais. Todos os policiais pertencentes a essa companhia são obrigatoriamente cadastrados no sistema. Cada usuário possui um nível de acesso diferenciado, sendo este garantido de acordo com a função no sistema. O Sistema possui um administrador geral com acesso irrestrito, dois moderadores com acesso parcial, e os demais usuários acesso restrito a inserção de dados no sistema. O sistema é disponibilizado via web e os usuários cadastrados acessam o sistema através de seu login e senha. Os usuários cadastram no sistema o número do boletim de ocorrência, as imagens do local do fato que vincula a coordenada geográfica obtida por GPS no aparelho celular. Estes são de grande importância estratégica para a 6ª Cia e consequentemente para a PMMG, por gerar diversos relatórios geoestatísticos, que auxiliam no processo de controle, gerenciamento, auxilio na criação de políticas de prevenção de acidentes de trânsito, infrações de trânsito e ambientais, além de contribuir para o contínuo processo de aperfeiçoamento dos serviços prestados. Os dados são armazenados no servidor localizado na sede da 6ª CIA Ind MAT da PMMG. As informações cadastradas no sistema são de caráter sigiloso, podem somente ser acessadas por terceiros através de mandado judicial. A Polícia Militar possui Código de Ética e Estatuto próprio que proíbe a divulgação de informações confidenciais, sendo seu descumprimento considerado uma infração, o que inibe o vazamento de informação através do "ativo" pessoas. O servidor fica localizado em ambiente protegido em uma área de segurança do (8º Batalhão da PMMG), todavia este sistema não possui proteção contra desastres naturais. Também foi verificada a realização sistemática de backup, porém o processo não é automatizado e as cópias são armazenadas no mesmo espaço físico e no mesmo prédio de servidor.

Os backups não possuem um padrão para toda a 6ª Cia, sendo que este sistema ainda está em fase de teste e os ajustes estão sendo realizados.

Portal Corporativo Regional da 6ª Região da Polícia Militar - O portal corporativo regional foi desenvolvido pela 6ª Região da PMMG em parceria com a UFLA (Universidade Federal de Lavras), sendo a primeira região dentro do estado de Minas Gerais a disponibilizar um portal que oferece os serviços de divulgação de informações das ocorrências policiais de destaque, divulgação de eventos, denúncias e notícias de interesse geral ocorridas nas cidades que abrangem uma área com 44 municípios e 03 distritos no Sul de Minas Gerais, pertencentes à região. O sistema do portal também possui a área restrita aos militares cadastrados, através de uma intranet PM, administrada e controlada pela região, com acesso restrito através de login e senha, com níveis de acesso diferenciado, sendo este garantido de acordo com a função que cada um exerce no sistema. A intranet regional é utilizada para serviços administrativos, cadastrar os Relatórios Diários de Serviço (RDS) das unidades, bem como tratar de informações de interesse do público interno. A autenticação desse sistema é simples uma vez que não existe criptografia e nenhuma entidade certificadora. O Sistema possui um gestor, dois administradores pleno, com acesso irrestrito, dois moderadores com acesso parcial, e o restante do efetivo policial, que são os militares de todas as cidades pertencentes a 6ª Região tem acesso restrito à inserção de dados no sistema, como cadastro de eventos, boletins periódicos, mural de recados e outros serviços, para que sejam efetuadas as rotinas administrativas e informações exclusivas ao público interno. O servidor do portal está hospedado no campus da UFLA, no prédio da DGTI (Diretoria de Gestão de tecnologia da informação) com as mesmas regras de segurança que são implantadas para os seus servidores, como uma sala refrigerada, acesso restrito com sistema biométrico, câmera de segurança e pessoal identificado por

crachás, sendo tudo monitorado 24h. O sistema possui um backup automatizado e uma cópia parcial/manual realizado em uma mesma sala do prédio principal da 6ª Região de forma esporádica, onde não possui extintor e nenhum outro sistema que pode prevenir situações iniciais de emergência como princípios de incêndio. A 6ª Região mesmo já disponibilizando esse portal desde 2003, não possui hoje uma Política de Segurança da Informação, apenas memorandos e um Plano inicial de Continuidade de Negócios. O firewall utilizado é o disponibilizado pela UFLA.

Sistema Integrado de Defesa Social (SIDS) - É um sistema modular, integrado, que reúne os seguintes órgãos da segurança pública em Minas Gerais: a Subsecretaria de Administração Prisional (SUAPI) da Secretaria de Estado de Defesa Social (SEDS), a Polícia Militar de Minas Gerais (PMMG)/6ª Cia Ind MAT, a Polícia Civil de Minas Gerais (PCMG) e o Corpo de Bombeiros Militar de Minas Gerais (CBMMG). Trata-se de um sistema que permite a gestão das informações de defesa social relacionadas às ocorrências policiais e de bombeiros, à investigação policial, ao processo judicial e à execução penal, respeitada as atribuições legais e autonomias administrativas dos órgãos que as compõem. Através do SIDS (Sistema Integrado de Defesa Social) é confeccionado o REDS (Registro de Defesa Social) que são os Boletins de Ocorrência informatizados e outros registros de interesse interno da corporação e se constitui como uma importante ferramenta para direcionar a política de integração das organizações de defesa social do Estado de Minas Gerais, na medida em que informatiza as bases de dados e fornece instrumentos para suporte de uma decisão gerencial estratégica. Informatizando processos, o sistema é capaz de agilizar rotinas e acelerar a coleta, disseminação e localização de informações, trazendo para o cotidiano dos trabalhos novos instrumentos tecnológicos e a possibilidade do estabelecimento de metas conjuntas para a

redução dos índices de criminalidade em Minas Gerais. Vale ressaltar que o SIDS não contém um plano de contingência para segurança da informação elaborado e documentado. As medidas de contingência são tomadas por decisão do nível superior. Torna-se de extrema importância um plano de contingência para o sistema, visto que ele abrange não só a PMMG, mas também a Polícia Civil, SUAPI e o corpo de bombeiros. O sistema SIDS estando inoperante compromete significativamente a atividade operacional que utiliza esse sistema para confecção dos relatórios de atividade (RAT), Boletim de ocorrência (BO), Boletim de ocorrência simplificado (BOs) e a ficha de acidente com viatura.

3.2.3 Mapeamento das Entradas e Saídas

Nas figuras 3, 4, 5, 6 são apresentados os mapeamentos das entradas e saídas dos processos de cada Sistema de Informação existente na organização.

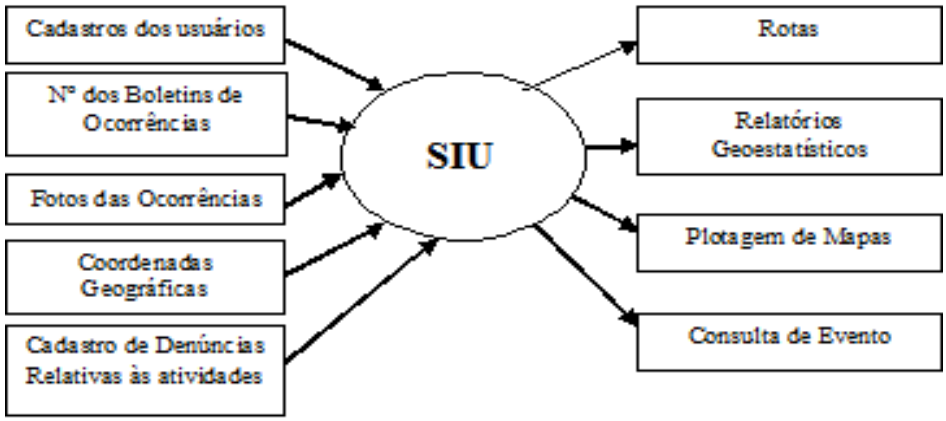

Figura 3 – Entradas e Saídas do SIU

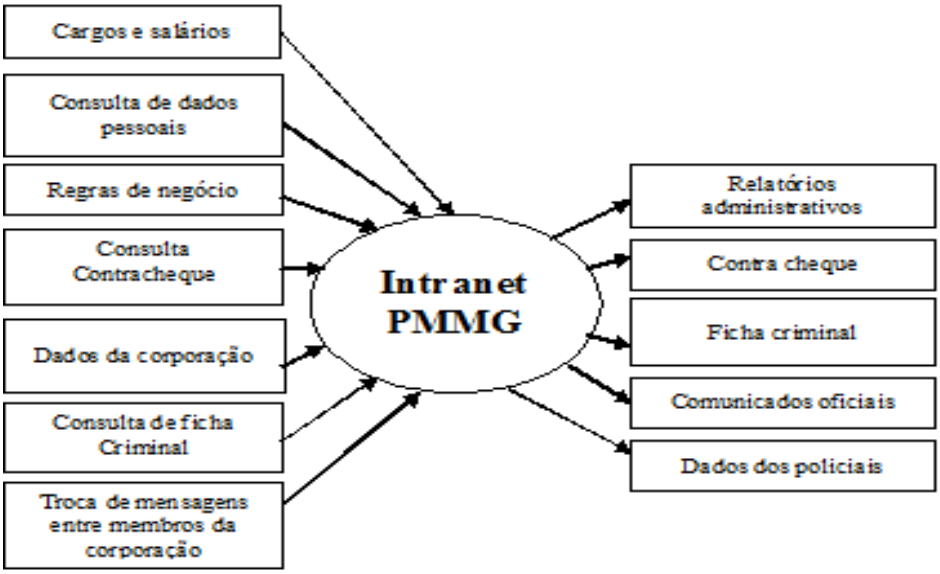

Figura 4 – Entradas e Saídas da Intranet PMMG

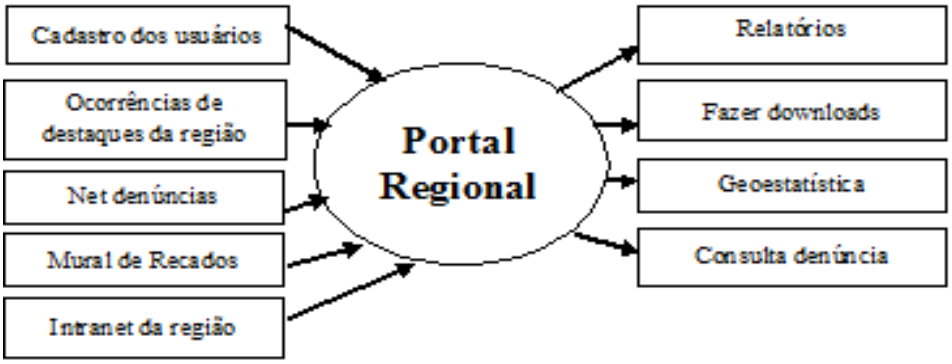

Figura 5 – Entradas e Saídas do Portal Regional

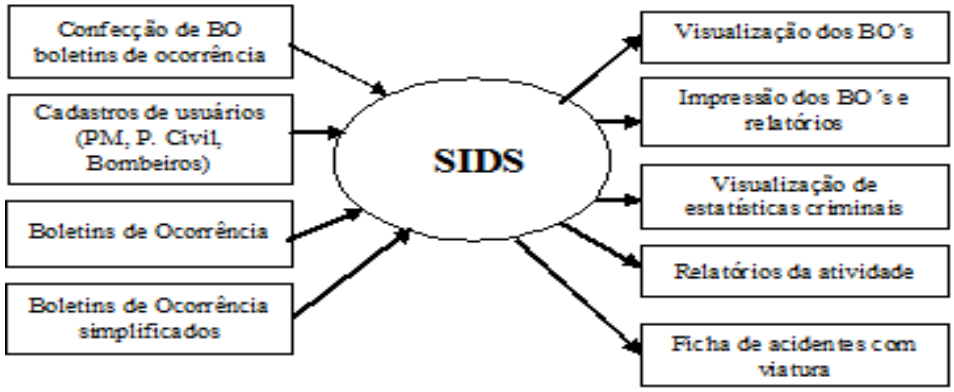

Figura 6 – Entradas e Saídas do SIDS

3.2.4 Elenco de Ativos Descritos

Tabela 1 - Elenco de Ativos Descritos

Elementos	Intranet
Físico	Salas, Mobiliário infraestrutura de dados.
Tecnológico	INTRANET (Sistema).
Físico – Tecnológico	Computadores, servidor com ar condicionado, equipamentos de conectividade.
Humano	Gestores, Policiais.
	SIU
Físico	Salas, Mobiliário.
Tecnológico	SIU (Sistema).
Físico – Tecnológico	Computadores, servidor, equipamentos de conectividade.
Humano	Gestores, Policiais
	Portal Corporativo
Físico	Salas, Mobiliário, infraestrutura de dados.
Tecnológico	Portal Regional (Sistema).
Físico – Tecnológico	Computadores, servidor, equipamentos de conectividade.
Humano	Gestores, Policiais.
	SIDS
Físico	Salas de grande porte para guardar os servidores locais e mobiliários.
Tecnológico	SIDS (Sistema).
Físico – Tecnológico	Computadores, servidor, equipamentos de conectividade, técnicos e Analistas de TI.
Humano	Gestores, Policiais.

3.2.5 Correlação de Ativos com Ciclo de Vida

Tabela 2 - Correlação de Ativos com Ciclo de Vida

	Ativo	Fase Ciclo	Informações
Intranet	Salas, Mobiliário, infraestrutura de dados	Armazenamento	Todas
	Infraestrutura de dados, equipamentos de conectividade	Transporte	Todas
	Computadores	Manipulação	Somente Informações que o usuário tem acesso
	Servidores	Armazenamento	Todas
	Gestor	Manipulação	Todas
	Gestor	Descarte	Qualquer informação que não seja mais necessária para os sistemas
	Policiais	Manipulação	Somente Informações que o usuário tem acesso
SIU	Salas, Mobiliário, infraestrutura de dados	Armazenamento	Todas
	Infraestrutura de dados, equipamentos de conectividade	Transporte	Todas
	Computadores	Manipulação	Somente Informações que o usuário tem acesso
	Servidores	Armazenamento	Todas
	Gestor	Manipulação	Todas
	Gestor	Descarte	Qualquer informação que não seja mais necessária para os sistemas
	Policiais	Manipulação	Somente Informações que o usuário tem acesso
Portal Regional	Salas, Mobiliário, infraestrutura de dados	Armazenamento	Todas
	Infraestrutura de dados, equipamentos de conectividade	Transporte	Todas
	Computadores	Manipulação	Somente Informações que o usuário tem acesso
	Servidores	Armazenamento	Todas
	Gestor	Manipulação	Todas
	Gestor	Descarte	Qualquer informação que não seja mais necessária para os sistemas

SIDS	Salas de grande porte, mobiliário.	Armazenamento	Todos os gestores, técnicos, gerentes administrativos, policiais (em forma visível).
	Servidores		Apenas os técnicos e os analistas de TI responsáveis pela manutenção
	Televisores	Monitoramento	Técnicos
	Sistema SIDS	Armazenamento	Analistas de TI
	Computadores	Armazenamento	Todos
	Gestores, técnicos, analistas de TI.	Manipulação	Todas
	Salas de grande porte, mobiliário.	Armazenamento	Todos os gestores, técnicos, gerentes administrativos, policiais (em forma visível).

3.2.6 Análise CIDAL

A norma ABNT ISO/IEC 27002:2005, que apresenta um código de prática para a gestão de segurança da informação, define que a segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, legalidade, não repúdio e confiabilidade, podem também estar envolvidas (ABNT, 2005).

Tabela 3 - Análise CIDAL

Índice	Nível	Enquadramento
1	**Não considerável**	A ocorrência de um incidente de segurança (IS) no sistema é absorvida integralmente através de um Plano de Continuidade de baixo custo sem prejuízo algum à atividade produtiva
2	**Relevante**	A ocorrência de um IS no sistema em análise demanda ações reativas programadas perceptíveis em outros, podendo causar impactos de baixa monta, como pequenos atrasos ou prejuízos financeiros absorvíveis, porém indesejados
3	**Importante**	Um IS no sistema em avaliação provoca a redução imediata de sua operacionalidade normal, causando prejuízos diários. Demanda ações reativas emergenciais para que a extensão de seus impactos não afetem outros sistemas e metas da empresa

4	**Crítico**	Os impactos de um IS podem ser percebidos em vários sistemas associados, demandando iniciativas reativas não previstas anteriormente, causando a necessidade de esforços adicionais e redução da capacidade produtiva de toda ou grande parte da empresa. Compromete metas. A ausência ou demora na reação pode transformar o evento em vital.
5	**Vital**	A ocorrência de um IS deste tipo no sistema em análise pode atingir toda a empresa e seus parceiros, causando impactos irreversíveis e demandando ações emergenciais que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa.

Tabela 4 - Análise CIDAL dos Sistemas

Intranet	**C**	**I**	**D**	**A**	**L**
1					
2					
3					
4					
5					
SIU	**C**	**I**	**D**	**A**	**L**
1					
2					
3					
4					
5					
Portal Corporativo	**C**	**I**	**D**	**A**	**L**
1					
2					
3					
4					
5					
SIDS	**C**	**I**	**D**	**A**	**L**
1					
2					
3					
4					
5					

No sistema Intranet, os itens Integridade e Disponibilidade são considerados Vitais, uma vez que o sistema armazena todas as informações utilizadas pela PMMG em nível operacional, gerencial e estratégico, sendo que estas devem ser precisas e estar sempre à disposição quando se fazem necessárias. Nesse sentido, dados incorretos ou indisponíveis, podem acarretar em operações errôneas causando prejuízos morais e financeiros, impactando na imagem da corporação. A Confidencialidade e Autenticidade foram consideradas Críticos, pois o sistema armazena dados sobre a corporação, dados pessoais dos policiais, fichas criminais, dados sobre operações, dados sobre o patrimônio, entre muitas outras informações de caráter sigiloso, pois um vazamento dessas informações podem gerar efeitos catastróficos, como processos judiciais, ou mesmo comprometer a integridade física dos policiais. No quesito Legalidade, que é Importante, sendo que a PMMG possui Código de Ética e Estatuto Interno da corporação que regem sobre o comportamento do policial, sendo que entre os vários tópicos, existe um tópico que incide sobre o vazamento de informação sigilosa, onde caso um incidente ocorra, o policial poderá responder tanto militarmente como civilmente pelos danos causados por essa ocorrência.

No sistema SIU, os itens Confidencialidade, Disponibilidade e Autenticidade foram considerados Relevantes, por se tratar de um sistema destinado a inteligência da PMMG, o sistema somente manipula informações de caráter público ou reservado, são informações que serão disponibilizadas para a população futuramente na forma de relatórios. A indisponibilidade do sistema não compromete as operações da organização. Existe grande tolerância nesse quesito, uma vez que os dados podem ser armazenados para então serem descarregados no sistema. Por se tratar de um sistema que realiza análise geoestatística dos dados lá armazenados a Integridade dos dados é considerada Crítica e precisa ser garantida, uma vez que erros aqui podem causar o

direcionamento errado das operações, e decisões erradas por parte do comando, causando prejuízos financeiros e a imagem da corporação. No quesito Legalidade é importante, sendo que a PMMG possui Código de Ética e Estatuto Interno, que disciplinam a conduta dos policiais e como deve ser seu comportamento, entre os vários tópicos. Existe um tópico que incide sobre o vazamento de informação sigilosa, relacionando qual sanção disciplinar o militar irá enquadrar caso um incidente ocorra, o policial poderá responder tanto militarmente como civilmente pelos danos causados por essa transgressão disciplinar.

No sistema Portal Corporativo Regional, a Confidencialidade e Disponibilidade são Críticos, pois o sistema trabalha e armazena dados importantes dos policiais da região, bem como informações de pessoas envolvidas em tipo de infrações ou crimes que não podem ser divulgadas sem um devido tratamento e em forma de resultados. Já os sistemas precisam estar disponíveis para que as atividades administrativas sejam realizadas, a fim de garantir a boa execução da atividade fim que é o policiamento. A Integridade é Vital, uma vez que os dados não podem estar incorretos ou indisponíveis para que sejam realizadas as operações, sendo que caso ocorra irá causar prejuízos à imagem da corporação podendo ter outros resultados como até o risco a integridade física de terceiros ou do próprio policial, caso a informação não esteja mais íntegra no momento de realizar uma intervenção em uma ocorrência. A Autenticidade e Legalidade são Importantes, sendo que todos os outros processos precisam ter autenticidade para garantir que a pessoa ou sistema que está acessando a informação realmente é quem diz ser e está autorizado a acessá-la. Já a PMMG possui Código de Ética e Estatuto Interno, que informam como o policial deve se comportar, uma vez que pode ser punido e enquadrado no vazamento de informação sigilosa, onde caso um incidente ocorra, o policial

poderá responder tanto militarmente como civilmente pelos danos causados a imagem da corporação ou fato que resulta grande transtorno.

No sistema SIDS, são Vitais a Integridade, Legalidade e a Autenticidade dos dados contidos no sistema, pois as ocorrências cadastradas devem ser consistentes e íntegras. Não deverá de forma alguma haver redundâncias ou inconsistências de dados, devido ao fato que as ocorrências estão interligadas a Leis públicas e Federais. Devido à disponibilização dos boletins de ocorrência para o público mediante número do boletim e poder serem feitas pesquisas e impressões, a Confidencialidade e a Disponibilidade dos dados foram classificados como fatores Importantes, ou seja, elas devem estar disponíveis, mas mediante mandado judicial elas podem ser retiradas do sistema a qualquer momento. Se a pessoa tiver o número do BO e o nome da pessoa envolvida ela já pode acessar os dados da ocorrência, tornando-se os dados menos confidenciais.

3.2.6.1 Conclusões da Análise CIDAL dos Sistemas

Para calcular a média, foram somados os valores de cada um dos itens, confidencialidade, integridade, disponibilidade, autenticidade e legalidade referenciados na Tabela 4 – Análise CIDAL e dividido por cinco, encontrando a média de cada um dos sistemas.

- O sistema Intranet teve média: 4.2, sendo considerado um processo (Crítico), uma vez que ele é utilizado para controlar grande parte da área administrativa, bem como dar suporte as áreas operacionais tanto da 6ª Cia, em suas atividades, como em todos as outras unidades da PMMG no Estado, interligando a corporação através da troca de mensagens e todo tipo de ferramentas e publicações que se faça necessária. A demora em solucionar um incidente de segurança

nesse processo pode agravar, vindo a se tornar vital para empresa, o que leva a necessidade de um empenho maior em resolver o incidente através de esforços adicionais.

- O sistema SIU teve média: 2.6, sendo considerado um processo (Relevante), uma vez que é considerado apenas um processo de negócio que está sendo desenvolvido pela 6ª Cia e que ajuda a melhorar a resposta às ocorrências da área especializada, realizando o geoprocessamento das informações, sendo um sistema que pode ser estendido para todo Estado. Em um primeiro momento, um incidente de segurança nesse processo de negócio irá gerar pequenos prejuízos absorvíveis, que não irá causar tantos problemas para o desenvolvimento das atividades, ocorrendo apenas pequenos atrasos na geração de informações estatísticas.
- O sistema Portal Corporativo teve média: 3.8, sendo considerado (Importante), pelo fato de ser uma ferramenta para divulgação das ocorrências policiais na 6ª Região da Polícia Militar, aproximando e divulgando os bons serviços prestados a população. Esse processo de negócio pioneiro na 6ª RPM, já está sendo implantado em outras Regiões do Estado, sendo utilizado também pela 6ª Cia, uma vez que a unidade faz parte da 6ª Região. Um incidente de segurança nesse processo torna-se importante, uma vez que ele também tem uma intranet regional, sendo uma ferramenta para realização dos serviços administrativos e operacionais através dessa área restrita aos integrantes da PMMG.
- O sistema SIDS teve média: 4.2, sendo considerado (Crítico), uma vez que atualmente, os boletins de ocorrência e alguns outros documentos são confeccionados de forma informatizada na 6ª Cia e em todo o Estado de Minas Gerais, através desse sistema e com isso

faz com que um incidente nesse processo seja de grande relevância tanto para a área operacional, que necessita desse sistema 24 horas por dia e não irá conseguir confeccionar os boletins de ocorrência, quanto para a área administrativa que não irá conseguir levantar os pontos que precisam de uma maior atenção por parte da fiscalização policial, sendo considerado assim um processo crítico para todas as unidades da corporação.

3.3 GUT

A matriz GUT **(**sigla para Gravidade, Urgência e Tendência) são parâmetros usados para estabelecer prioridades na eliminação de problemas, especialmente se forem vários e relacionados entre si. A técnica de GUT foi desenvolvida com o objetivo de orientar decisões mais complexas. É um sistema usado quando desejamos priorizar os itens obtidos através do brainstorming (GRIMALDI; MANCUSO, 1994).

Tabela 5 - Matriz GUT

	Gravidade	Urgência	Tendência
1	Entre 1 - 2,3	Tolerância acima 120h	Não há menção no sistema
2	Entre 2,4 - 3,7	Tolerância entre 24h e 120h	Possibilidade de agravamento prevista no sistema
3	Entre 3,8 - 5	Tolerância inferior 24h	Previsão de incremento

Tabela 6 - Matriz GUT Sistema Intranet

	Gravidade (CIDAL)	Urgência	Tendência	Total
Intranet	3	3	3	27

Tabela 7 - Matriz GUT Sistema SIU

	Gravidade (CIDAL)	Urgência	Tendência	Total
SIU	2	3	2	12

Tabela 8 - Matriz GUT Sistema Portal Corporativo

	Gravidade (CIDAL)	Urgência	Tendência	Total
Portal Corporativo	3	3	2	18

Tabela 9 - Matriz GUT Sistema SIDS

	Gravidade (CIDAL)	Urgência	Tendência	Total
SIDS	3	3	2	18

Através da análise GUT, foi visualizado que com a análise dos quatro processos de negócio utilizados pela 6ª Cia, caso ocorra um incidente de segurança no qual afete todos esses processos utilizados, devem ser priorizados aqueles com maior importância e que podem gerar um maior impacto para as atividades, caso fiquem inoperantes por horas. Dessa forma, a solução dos problemas deve respeitar a importância dos sistemas de acordo com a gravidade, tendência e urgência, sendo a Intranet vista como o principal sistema e que precisa ser dada uma maior importância, já o sistema SIU, visto dentro dos critérios GUT é o que tem uma menor priorização entre esses sistemas.

3.4 BIA

A Análise de Impacto nos Negócios (BIA) tem com principal função identificar e documentar o impacto que poderá ser causado por uma interrupção nas atividades que suportam os produtos e serviços da organização (BCI, 2007 b).

As funções/atividades são consideradas críticas quando a sua inoperabilidade é considerada inaceitável. Outro fator que altera a classificação em crítico ou não critico é a legislação em vigor. O BIA permite a escolha da melhor estratégia para cada sistema, iniciando-se sempre pelo mais crítico (de maior risco).

Tabela 10 - BIA

	Policial/ Gerente do Sistema	Incêndio/ Desastres Naturais	Pane Elétrica	Ataque ao Sistema/ Vazamento de Info. Confidencial	Tolerância
Intranet	X	X	X	X	4 horas
SIU	X	X	X	X	48 horas
P.Corpor.	X	X	X	X	24 horas
SIDS	X	X	X	X	24 horas

Em relação à análise BIA, foi verificada através de pesquisas e conversas com funcionários responsáveis por realizar tarefas/atividades nesses sistemas, a tolerância no caso de um incidente, sendo constatado que o sistema Intranet é considerado crítico para a corporação, em um dia normal de expediente, não podendo ficar mais de 4 horas inoperante, causando prejuízos a partir disso.

3.5 Análise SWOT

3.5.1 Pontos Positivos da Organização

- A empresa possui um código de ética e disciplina e memorandos internos que auxiliam no controle da segurança da informação, principalmente em relação ao controle do ativo pessoa.

- Com relação à segurança do ativo informação, a empresa possui um documento recente, sendo este a Resolução interna da Polícia Militar de Minas Gerais, Nº 4320 de 16/07/2014 que regulamenta o direito de acesso à informação no âmbito da PMMG.
- Existem câmeras de segurança que além de gravar, transmitem qualquer movimentação em um monitor de 40 polegadas que fica na sala de operações da unidade, onde 24 horas por dia tem um policial armado de serviço. As gravações ficam armazenadas por um período de 30 dias.
- O gestor/administrador do sistema trabalha na seção de inteligência da empresa, o que facilita o acesso a novas tecnologias, bem como uma relação mais estreita com o nível estratégico.

3.5.2 Pontos Negativos da Organização

- Há poucos investimentos no setor de TI da empresa, principalmente na área de segurança da informação.
- A organização possui mão de obra especializada, porém não existe um setor de tecnologia da informação na 6ª Cia.
- O gestor acumula outras funções na empresa além daquelas relativas à segurança da informação.
- A organização não possui uma Política de Segurança da Informação.
- A rede lógica não possui servidor, bem como firewall.
- Alguns pontos de RJ45 estão expostos, sendo um ponto de grande vulnerabilidade para o acesso não autorizado da rede interna.
- O servidor do sistema SIU, está em uma sala que não é totalmente segura, onde não possui ar condicionado.

- O servidor SIU utiliza firewall nativo do Windows e antivírus freeware
- As informações da empresa estão fragmentadas em células e cada célula realiza seu backup manualmente sem nenhum critério padronizado.
- Os backups ficam no mesmo prédio que o servidor, o que pode ser perdido em caso de um incêndio, desastre natural ou qualquer outro desastre que venha a danificar o prédio todo.
- Os backups não são automatizados e quando realizados, são executados por pessoas sem domínio do conhecimento necessário para salvaguardar as informações.
- Não há um controle efetivo do nível estratégico quanto aos backups realizados.
- Não há um controle efetivo do nível estratégico quanto ao uso de mídias graváveis ou transmissão de informação pela rede mundial de computadores.
- O prédio onde fica a sala do servidor e algumas salas de computadores de registros de BO não possuem extintores de incêndio.
- O link que conecta à rede mundial de computadores (fibra ótica) está em uma sala de registro de BO, separada apenas por uma divisória de madeira do tipo MDF com porta, porém não é fechado até o teto.
- A sala do link não possui controle de acesso a pessoas não autorizadas.
- Falta a identificação com crachás de pessoas que estejam realizando algum trabalho ou prestando serviços no interior da unidade.
- As edificações são facilmente acessíveis tanto advindos do 8º BPM, quanto da entrada principal da 6ª Cia.

3.5.3 Oportunidades

- A localização da sede da 6ª Cia fica em uma cidade universitária, onde tem a possibilidade de conseguir estagiários dos cursos relacionados a sistemas de informação e computação. Na referida Universidade, funcionam cursos de graduação e pós-graduação direcionados à área de TI e de estrutura de redes.
- O bom relacionamento da 6ª Cia com professores da Universidade Federal de Lavras, inclusive com convênios de colaboração celebrados entre as instituições.

3.5.4 Ameaças

- Acesso e captura de dados sigilosos e ou protegidos por pessoas não autorizadas.
- Invasão do servidor SIU pela rede interna ou externa, pelo baixo nível de segurança do firewall, senhas e protocolo.
- Fácil e irrestrito a possibilidade de cópias dos diversos dados e informações pelo ativo pessoa.
- Acesso facilitado aos links e pontos de conexão através dos RJ45 e pela fibra ótica que chega a 6ª Cia de forma aérea.
- Perdas ou extravio dos backups realizados em mídias removíveis por fatores humanos ou naturais pela ausência de local seguro para guarda.

3.6 Plano de Segurança

O plano de segurança é um documento dinâmico (em permanente atualização) que reflete a prevenção dos riscos na organização. Os objetivos que devem presidir à sua elaboração são:

- Demonstrar o compromisso assumido pelos responsáveis máximos da organização, do seu empenho na prevenção dos riscos;
- Orientar todos os colaboradores da organização, em matéria de segurança, higiene e saúde;
- Servir de guia de implementação dos métodos de identificação, avaliação e controle de riscos;
- Avaliar o desempenho da função prevenção na organização.

Por se tratar de uma organização que depende do bom funcionamento de sua infraestrutura tecnológica, o plano de segurança será voltado para eficácia e eficiência desta.

A seguir serão apresentadas possíveis medidas que irão ajudar no bom funcionamento dos sistemas da organização em estudo.

3.6.1 Elementos do Plano de Segurança

O plano de segurança sugerido para esta organização possui os seguintes elementos:

1. Atividades previstas,
2. Cronograma,
3. Estimativa de prazo para realizar a atividade,
4. Custo estimado,
5. Pessoas responsáveis pelas atividades,
6. Setores/departamentos alvos,
7. Outras informações e sugestões

3.6.1.1 Atividades Previstas

A. Implementação de um servidor de backup separado: Definição de estações de trabalho críticas, como por exemplo, o servidor, que deve ter um no-break próprio e estar separado fisicamente dos computadores principais.
B. Implementação de um sistema no-break (inclui gerador e reforma na sala do servidor): Um sistema no-break de boa qualidade que receba manutenção periódica por parte de uma empresa especializada e que siga alguma norma de controle de qualidade, como por exemplo, ITIL. Esse sistema deverá ser capaz de suprir a necessidade de funcionamento de toda a infraestrutura relativa ao software. Contratação de um provedor de internet auxiliar independente de energia elétrica, como por exemplo, algum que possua a tecnologia 4G. Contrato com a empresa de energia local para que a manutenção nas redes elétricas que afetem a 6ª Cia seja providenciada com uma tolerância menor ou igual à 2 horas.
C. Elaboração de um Plano de Administração da Crise (PAC): Ao ocorrer uma pane elétrica, os recursos de controle entrarão em ação automaticamente. No entanto, por tratar-se de uma situação indesejada, que reduz a capacidade operacional da empresa, ações contingenciais são necessárias. Deve-se então, criar um documento que contenha todas as informações e procedimentos para ação durante um incidente (todos os envolvidos devem estar cientes dos procedimentos).
D. Elaboração de um Plano de Continuidade Operacional (PCO): Deve focar na tolerância do PN. Para garantia de continuidade do Software GRC, primeiramente o Gestor de TI deve acionar a empresa conveniada de fornecimento de geradores e colocá-la de sobre aviso para o atendimento da ocorrência em questão, obter uma estimativa de tempo para manutenção e solicitar geradores caso esse tempo seja acima do tolerado pelo sistema. Na eventual necessidade dos geradores o responsável pelo plano deve guiar os

técnicos até o setor responsável e acompanhar o procedimento de instalação dos geradores a fim de evitar sabotagem.

E. Elaboração de um Plano de Recuperação de Desastres (PRD): Tem uma importância fundamental no Plano de Contingências, porque visa à avaliação da eficiência e a eficácia dos controles, de forma a evitar que novas ocorrências reduzam a capacidade operacional do recurso contingenciado. Assim são eventos importantes no PRD em questão: tempo de tolerância suportado pelo sistema e estimativa de prejuízos gerados pela paralisação. Em reuniões futuras com o corpo administrativo trazer a tona o problema e propor um controle mais rigoroso ou mudança de contrato com a empresa de energia, caso essa venha a não cumprir com o combinado.

F. Auditoria de capacitação: A capacitação de todos os profissionais selecionados para trabalhar nos setores auditados será avaliada a fim de identificar possíveis vulnerabilidades decorrentes do não profissionalismo dos mesmos.

3.6.1.2 Cronograma

Tabela 11 - Cronograma

	Mês 1				Mês 2				Mês 3				Mês 4				Mês 5				Mês 6			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
C																								
D																								
E																								
B																								
A																								
F																								

3.6.1.3 Tabela de Estimativas

Tabela 12 - Estimativa de Custos

Atividades	Ordem no Cronograma	Prazo (dias)	Responsáveis	Setor	Custo (R$)
A	5	40	P4 -Seção de Transporte e Manutenção	Setor de suporte de TI Gestão de contratos e convênios	14mil
B	4	40	P4 -Seção de Transporte e Manutenção	Setor de suporte de TI Gestão de contratos e convênios	12mil
C	1	90	P3 -Seção de Planejamento	Administrativo Gestão de contratos e convênios Gestão de Ti	3mil
D	2	90	P3 -Seção de Planejamento	Administrativo Gestão de contratos e convênios Gestão de Ti	3mil
E	3	90	P3 -Seção de Planejamento	Administrativo Gestão de contratos e convênios Gestão de Ti	3mil
F	6	50	P3 -Seção de Planejamento estratégico	Órgão de auditoria	180/h

A organização possui 5 seções, sendo elas divididas em P1(Seção de pessoal), a P2(Seção de Inteligência), P3(Seção de Planejamento), P4(Seção de transporte e manutenção) e a P5(Seção de divulgação de notícias e organização de eventos.

As seções P3 e P4 foram utilizadas para coletados dados para fazer a estimativa de custos referenciada na Tabela 13. A P3 é responsável por fazer o planejamento de todas as atividades de gestão de contratos e convênios dentro da organização, tanto na área administrativa quanto operacional, já a P4 é a parte mais responsável pelo suporte e manutenção dos sistemas e aquisição de materiais.

Para a organização em questão foi traçado um cronograma de 180 dias, onde a sequência de atividades foi escolhida de acordo com sua relevância e a dependência das outras atividades em relação a ela. A atividade C, D e E foram consideradas de relevância e importância, já que é pré-requisito para a implementação da infraestrutura tecnológica, recebeu um prazo maior para que seja efetuada com planejamento e qualidade adequados. Em seguida, no intuito de assegurar o backup dos dados críticos da organização, sugere-se a implementação de um servidor de backup automatizado num espaço físico separado e com um no-break próprio. Por fim, é realizada uma auditoria de capacitação com o objetivo de identificar os funcionários mais capacitados para trabalhar com o plano de segurança e realizar um treinamento daqueles que ainda não estão aptos para trabalhar na área.

3.6.1.4 Custos

Os custos aqui apresentados foram obtidos através de tomada de preços no mercado no mês março de 2014.

Implementação de um servidor de backup separado: A solução prevê a instalação de um servidor robusto para suportar a demanda de serviços. A exemplo do servidor Dell Power Edge T620 no valor de R$9.000,00 (nove mil reais). É previsto também um servidor de armazenamento externo ao prédio principal para que tenham dados seguros caso haja desastre natural no servidor principal. O servidor Dell Power Edge T420 no valor de R$4.500,00 (quatro mil e quinhentos reais) supre essa necessidade. Para uma solução extra, prevemos a contratação de um plano de backup de dados na Nuvem. Total: R$14.000,00.

Implementação de um sistema no-break (inclui gerador): A organização necessita de equipamentos de contenção às falhas de energia elétrica como, por exemplo, No-breaks eficientes com sistemas de alertas e geradores movidos a combustíveis como diesel e/ou gasolina. Um No-break da marca SMS com recurso e eficiência necessários possui valor de R$1.000,00 (mil reais). E um gerador automático custa em média de R$2.000,00 (dois mil reais). De acordo com a avaliação feita na organização, não havia extintores de incêndio no local do servidor e não havia controle de acesso à sala onde se localizam os equipamentos de TI. Será então necessária uma reforma determinando um local específico para os equipamentos de TI com acesso restrito com fechadura digital com leitor biométrico. Um projeto de incêndio (planta de incêndio, taxas administrativas e equipamentos de incêndio) custa em torno de R$3.500,00 (três mil e quinhentos reais). Total: R$12.000,00.

3.6.1.5 Responsáveis

A formação da equipe responsável pela análise e implementação do Plano de Segurança de Informação deve levar em consideração o grau de conhecimento tecnológico exigido pelas atividades, a experiência dos envolvidos em relação aos processos afetados e o nível de autonomia e

autoridade necessário para a obtenção ágil das informações e a negociação com outros setores ou com elementos externos a organização, tais como empresas fornecedoras de energia.

3.6.1.6 Setor/Departamentos Envolvidos

As diferentes atividades previstas no Plano de Segurança irão exigir dedicação por parte dos envolvidos, sejam membros da equipe de implementação ou funcionários dos setores envolvidos alocados em atividades específicas.

Com relação às Atividades A e B, devido à natureza tecnológica envolvida, será necessário o envolvimento do setor de suporte de tecnologia de informação da 6ª. CIA IND MAT da PMMG, bem como do setor de contratos e convênios, para negociação do contrato com os fornecedores de energia.

As Atividades C, D e E devem envolver o corpo administrativo, o setor de gestão de contratos e convênios e o setor de gestão de TI para aprovação das medidas definidas em cada um dos planos elaborados, aprovação dos controles a serem adotados e negociação com fornecedores. Após a conclusão e aprovação dos planos, é importante o apoio do setor de comunicação interna da 6ª. CIA, para garantir a disseminação de informações sobre as decisões tomadas e o funcionamento dos processos de segurança não apenas aos setores afetados, mas que possam ser acessados e conhecidos a todos os membros da organização.

3.6.1.7 Informações Complementares

Em um âmbito de abrangência superior ao das Atividades do Plano de Segurança, é altamente recomendado que a organização busque adotar *frameworks* de governança de informação e, que representam por si um padrão

de qualidade e que também sejam capazes de gerar enormes benefícios para a organização. Entre as opções de interesse, destacam-se:

- **ITIL**: O foco principal do ITIL é fornecer as definições de melhores práticas e critérios para as operações de gestão. Mais especificamente, ITIL se concentra principalmente na definição do funcional, atributos operacionais e organizacionais que precisam estar no local para as operações de gestão a ser totalmente otimizado em duas categorias principais: **Serviço de Apoio de Gestão (Service Support) e Prestação de Serviços de Gestão (Service Delivery). Service Support** inclui Service Desk, Incidentes, Problemas, Configuração, Gerenciamento de Mudança e Liberação, enquanto que os **Service Delivery** inclui nível de serviço, financeiro, capacidade, Continuidade e disponibilidade de serviço. Cada categoria inclui critérios de definição de boas práticas para muitas áreas, incluindo suporte organizacional, integração de componentes, gestão da comunicação, capacidade de produto, qualidade de execução e qualidade de serviço ao cliente. Se o objetivo é melhorar continuamente a eficiência das operações de TI e qualidade de atendimento ao cliente, **ITIL** seria provavelmente a melhor aposta.
- **COBIT**: O COBIT é um guia para a gestão de TI recomendado pelo ISACF (Information Systems Audit and Control Foundation, www.isaca.org). O COBIT inclui recursos tais como um sumário executivo, um framework, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do COBIT são recomendadas pelos peritos em gestão de TI que ajudam a otimizar os investimentos de TI e fornecem métricas para avaliação dos resultados. O COBIT independe das plataformas de TI adotadas nas

empresas. O COBIT está dividido em quatro domínios: Planejamento e organização, Aquisição e implementação, Entrega e suporte e Monitoração.

- **PMBOK** : O PMI (Project Management Institute) é a uma organização sem fins lucrativos de profissionais da área de gerenciamento de projetos. O PMI visa promover e ampliar o conhecimento existente sobre gerenciamento de projetos assim como melhorar o desempenho dos profissionais e organizações da área. As definições e processos do PMI estão publicados no PMBOK (Guide to the Project Management Body of Knowledge). Esse manual define e descrevem as habilidades, as ferramentas e as técnicas para o gerenciamento de um projeto. O gerenciamento de projetos compreende cinco processos – Início, Planejamento, Execução, Controle e Fechamento, bem como nove áreas de conhecimento: Integração, escopo, tempo, custo, qualidade, recursos humanos, comunicação, análise de risco e aquisição.
- Como um complemento, é interessante estudar a adoção de certificação de maturidade de processos, tais como o MPS-BR ou CMMI. Ambos os modelos possuem níveis de maturidade que definem a capacidade da empresa em trabalhar em projetos grandes e complexos

4. RESULTADOS

A elaboração desse estudo de caso é de grande valia para a organização estudada, uma vez que levantou diversos pontos críticos sobre a segurança da informação e que precisam, com urgência, de uma maior atenção devido ao valor da informação e as suas vulnerabilidades.

Foi observado que a organização utiliza de quatro sistemas (Intranet, SIDS, Portal Regional e SIU), relacionados a TI. Estes tem uma grande importância para o desenvolvimento das atividades tanto administrativas quanto operacionais, sendo que os três primeiros são utilizados pela 6ª Cia tendo uma abrangência estadual, já o último, teve início dentro da 6ª Cia e está sendo desenvolvido em parceria com a Universidade Federal de Lavras, sendo um processo pioneiro em todo Estado e que está chamando a atenção de outras unidades e do comando geral da PMMG.

Controlando os ativos da informação e os principais riscos que eles trazem, podemos reduzir em muito as ameaças que são inerentes ao mundo da rede mundial de computadores.

Os fatores relacionados à falta de segurança da informação apontados dentro da organização, relacionados às normas ABNT ISO/IEC DA SÉRIE 27000 e outras referências, são de considerável importância, uma vez que os referidos processos de negócio manipulam dados de toda corporação, de seus integrantes, dos sistemas utilizados pela PMMG e também dados pessoais de cidadãos envolvidas nos diversos tipos de ocorrências em todo Estado.

Nesse sentido, caso ocorra uma invasão nos sistemas da organização, além do prejuízo financeiro incalculável, a perda de credibilidade e confiança por parte da população pode estar a um passo de se tornar realidade, devido a falhas simples e outras que necessitam de um pouco mais de recursos, mas que podem ser corrigidas pela organização, antes que um incidente ocorra. Havendo

uma quebra nos sistemas de segurança, dados pessoais de colaboradores e demais pessoas estariam em risco.

Com isso, mudanças em relação à segurança dos ativos da informação são necessárias e precisam estar em constante aperfeiçoamento, diminuindo assim as vulnerabilidades da organização que são mais fáceis de serem corrigidas e aumentam em muito a segurança da informação. Com relação a isso, as ameaças são inúmeras e a cada dia surgem novas, ficando impossível fazer segurança da informação se preocupando em tentar combater essas ameaças.

Diante do estudo foi elaborada uma Política de Segurança da Informação que será entregue ao nível estratégico da organização, dando uma melhor visão sobre as vulnerabilidades e falhas mais nítidas e que precisam ser corrigidas o mais rápido possível, demandando de recursos financeiros relativamente viáveis devido à importância que a organização exerce dentro do contexto do Estado, para que seja estudada e verificada a possibilidade de sua implantação.

Caso seja aprovada pela alta direção da organização, a política deverá ser publicada e divulgada a todo seu público interno, tanto para o nível tático como operacional, mostrando que é necessário preocupar com segurança da informação a todo instante.

Em relação a isso, que a elaboração deste trabalho possa ser útil não só para a organização estudada, mais sim que sirva de referência para se tentar melhorar os níveis de segurança da corporação como um todo, bem como a segurança de outras empresas, uma vez que tenham seus processos pautados em sistemas de informação e queiram melhorá-los. Com isso, tornando-se mais competitiva, segura e capaz de aproveitar as tecnologias que estão disponíveis e são oferecidas a cada dia, com responsabilidade de todas as pessoas envolvidas, não colocando a organização em risco.

4.1 Proposta de Política de Segurança da Informação

A partir da necessidade de melhorar a segurança da informação na 6ª Cia, foi elaborado um estudo relacionado aos riscos, ameaças e as vulnerabilidades dos ativos da informação na organização, uma vez que ela não possui uma Política de Segurança da Informação. A elaboração da Política de Segurança é um diferencial estratégico para as organizações que se preocupam com a informação, as tecnologias que suportam essas informações, as pessoas, os processos e o ambiente como um todo e querem cuidar para que um incidente de segurança não ocorra com nenhum desses ativos.

O mercado está cada vez mais inseguro para qualquer organização, independente do setor que ela atua, devido à diversidade de problemas referentes aos ativos da informação, dos crimes digitais que já existem e surgem a cada dia, aumentando o risco para todas. Nesse sentido, dentro da constante evolução da informática, a presente Política de Segurança da Informação proposta deve ser periodicamente revisada e atualizada.

Dessa forma, a organização precisa proteger toda a informação envolvida nos processos de negócio e gerada no desempenho de suas atividades. Sendo assim, a partir do estudo da organização em relação às normas ABNT ISO/IEC DA SÉRIE 27000, análise CIDAL e das vulnerabilidades relativas aos ativos da informação, foi elaborada esta Política de Segurança da Informação e apresentada como proposta a alta administração, uma vez que a organização ainda não possui.

4.1.1 Utilização da Internet

- Aos usuários dos recursos computacionais da 6ª Cia, é permitido "navegar" na Internet em sites oficiais, do governo e que estejam

diretamente relacionados às necessidades do serviço policial e ao bom andamento das atividades tanto operacionais quanto administrativas.

4.1.2 A Divulgação da Política de Segurança

- A organização terá a obrigação de divulgar a todos os seus funcionários a Política de Segurança, enviando uma cópia na caixa de mensagens de cada integrante da 6ª Cia pela Intranet, bem como deve ser impressa uma cópia para cada seção.
- A divulgação da política deve ser clara e ampla, para que todos os funcionários tenham acesso a suas informações e possam compreendê-las.
- Todos os funcionários da 6ª Cia devem assinar um termo confirmando que tomaram conhecimento da Política de Segurança da Informação em sua íntegra, para evitar alegações de desconhecimento.
- Quaisquer alterações que venham a ocorrer na Política de Segurança da Informação da organização devem ser comunicadas aos seus funcionários em um período antes da mesma ser implantada, para que os funcionários possam ficar cientes bem como adaptarem-se as elas.

4.1.3 A Proteção da Informação

- Toda informação que for considerada de caráter sigiloso pela organização pode ser enviada ou recebida via Internet, desde que esteja devidamente protegida por métodos criptografados e de renomada eficácia.

- O servidor deve estar protegido em um espaço físico fechado, com dispositivos de segurança, bem refrigerado e que tenha o acesso restrito ao gestor/administrador do sistema, comandante da 6ª Cia ou pessoas previamente autorizadas pelos mesmos.
- As cópias de backup e o servidor devem estar localizados em espaços físicos diferentes, evitando assim que caso ocorra um incêndio, inundação ou qualquer tipo de desastre natural, possa vir a danificar ou mesmo destruir ambos os arquivos.
- As informações, as tecnologias que suportam essas informações, os processos de negócio e os ambientes computacionais ou que possuam equipamentos necessários ao bom desenvolvimento das atividades no dia a dia da organização, devem ser manipulados com responsabilidade e de forma a manter seu perfeito funcionamento.
- Os dados relativos a veículos, autores, vítimas, envolvidos ou qualquer outro tipo de dados relativos a ocorrências não devem ser divulgados na Internet em sites de bate papo, redes sociais, mídia ou qualquer outro canal de comunicação que não seja os sites de responsabilidade da PMMG, através da sessão de comunicação P5, evitando a perda de credibilidade e confiança por parte da população.
- Deve-se ter um cuidado redobrado com informações de caráter sigilo para a organização, sobre operações ou mesmo os dados dos integrantes da corporação, uma vez que o vazamento dessas informações possa colocar em risco a vida dos militares ou da população, sendo que a 6ª Cia Ind MAT é um órgão que trabalha diretamente com a segurança pública, devendo essas serem manipuladas com a maior segurança possível.

- O direito de acesso à informação no âmbito da 6ª Cia PM Ind MAT será regulamentado de acordo com a resolução Nº 4320, de 16 de Julho de 2014 da PMMG.

4.1.4 Controle de Acesso

- Todo usuário da 6ª Cia para conseguir entrar na Internet, deve realizar o acesso através do login e senha para a liberação de seu uso.
- O gestor ficará responsável de fornecer um login e senha provisórios aos visitantes ou profissionais que estejam realizando algum tipo de manutenção nos sistemas informatizados.
- O Proxy irá fazer o controle de determinados sites proibidos, sendo permitido o acesso a sites de assuntos relacionados ao bom andamento do serviço policial.
- Toda vez que o um policial ou funcionário civil acessar o sistema fica registrado seus dados de login e senha, sendo que o log é preenchido com todas as informações do acesso.
- Ex: Hora de inicio, término e todas as funções que são executadas durante aquele acesso.
- No caso dos policiais, o acesso é liberado após a colocação do número de polícia e senha que é pessoal e intransferível.
- Dentro do processo de negócio SIU existem níveis diferenciados de acesso, sendo estes liberados de acordo com as seções e a função que cada militar exerce dentro da corporação, ficando a cargo do gestor controlar a liberação ou restrição do acesso dentro do sistema, nesses vários níveis, aos funcionários.
- Toda vez que for necessário à realização de manutenção no PN SIU, sistemas informatizados, de telefonia e internet, a empresa prestadora

de serviços deverá enviar previamente os dados do(s) funcionário(s) (RG, CPF, função), para que seja conferido no momento de sua apresentação.

- Toda pessoa que estiver realizando algum trabalho ou mesmo prestando serviços de qualquer natureza no interior da Unidade, deverá obrigatoriamente ser identificada por crachá, após o cadastro de seus dados em uma ficha que ficará arquivada.
- Em dias úteis e dentro do horário comercial de funcionamento da 6ª Cia, a responsabilidade por controlar o acesso de pessoas aos sistemas, fica a cargo do gestor/administrador do sistema ou pessoa autorizada por ele, ficando o plantão da unidade responsável nos casos excepcionais e fora do expediente normal e devidamente orientado pelo gestor/administrador do sistema.

4.1.5 Tráfego de Informações

- Toda informação obtida via Internet deve ser considerada suspeita até ser confirmada por outra fonte de informação que a originou.
- Todo tipo de arquivo ou software trazido por usuários em dispositivos móveis ou obtido por download fora da rede da 6ª Cia deve ser submetido à verificação de vírus antes de ser aberto ou executado, mesmo que a origem do mesmo seja de fonte “conhecida” pela organização.
- Quaisquer dispositivos móveis como smartphone, celular, PDA, console portátil, ultra móbile PC, ultrabook, notebook, netbook, laptop, coletor de dados, etc, que forem conectados nos computadores e outros dispositivos ligados à rede devem ser precedidos pela verificação completa de um antivírus.

4.1.6 A gestão da Segurança da Informação

- Deve fazer revisões de forma a propor diretrizes, memorandos, normas e procedimentos relativos à segurança da informação.
- Solicitar junto a alta administração a disponibilidade de recursos para que seja implantado um servidor de backup e um sistema de no-break.
- Elaborar um Plano de Administração da Crise (PAC), Plano de Continuidade Operacional (PCO), Plano de Recuperação de Desastres (PRD), que irão dar condições para a organização se recuperar de um incidente.
- Estudar propostas de modificações na Política de Segurança da Informação encaminhadas pelos usuários dos sistemas, bem como pelas demais áreas da organização.
- Avaliar a efetividade dos processos, supervisionando e analisando os sistemas e dispositivos relacionados à segurança da informação.
- Planejar, elaborar e coordenar a execução de estratégias, planos e ações voltadas à segurança das informações.
- Implementar controles físicos, administrativos e tecnológicos, identificando as vulnerabilidades existentes, para assim poder realizar o tratamento adequado dos riscos.
- Tratar adequadamente as informações de eventos e incidentes de segurança que venham a ocorrer, determinando ao gestor as respectivas ações corretivas ou de contingência que cada caso necessite.

4.1.7 Políticas de Backup

- Implantação de um servidor de backup para toda a rede da 6ª Cia, a fim de padronizar a realização de backups e tornar a sua execução automatizada.
- O nível estratégico deve determinar quais são as informações e os dados críticos da organização que precisam ter certa prioridade ao realizar cópias periódicas de segurança.
- Os militares da área operacional e os administrativos quando trabalharem naquela área, são responsáveis pela geração de informações dos locais de registro de ocorrências ou operações que irão alimentar o SIU (Sistema Informatizado Unificado), uma vez que esses registros devem ser descarregados ao final de cada turno de serviço no sistema.
- É de responsabilidade do gestor/administrador da TI da 6ª Cia a execução de backups periódicos, dos dados armazenados nos servidores, sendo que esta ação deve ser realizada no mínimo semanalmente.
- Deve ser estabelecido um horário em que os sistemas estejam sendo menos utilizados para serem realizadas as tarefas de cópias de segurança, sendo que dessa forma não irá afetar o tráfego de informações nem a disponibilidade dos serviços.

4.1.8 Fica Terminantemente Proibido

- Repassar qualquer tipo de informação de exclusividade da 6ª Cia, para terceiros ou mesmo facilitar que outras pessoas a consiga.

- Utilizar os sistemas ou dispositivos físicos para realizar atividades particulares e que não estão previstas dentro das atividades operacionais e administrativas.
- Manipular qualquer tipo de documento eletrônico ou não, meios magnéticos ou mesmo o desvio de informações para o uso próprio ou de terceiros a fim de obter vantagens.
- Obter indevidamente acesso a recursos de qualquer natureza, que não seja de responsabilidade do indivíduo.
- Instalação de qualquer software ou hardware que não seja de conhecimento e consentimento do setor de TI.

4.1.9 Penalidades

- O não cumprimento das determinações estabelecidas pela Política de Segurança da Informação da 6ª Cia Ind MAT, sujeita o infrator às penalidades previstas no código de ética da PMMG, memorando e normas internas da organização estabelecidas para proteger os ativos da informação.

5. CONCLUSÃO

Com o trabalho realizado pôde-se perceber que a segurança dos sistemas de informação de uma organização, na maioria das vezes, é um setor crítico para o negócio e por ser tão importante, deve-se dar a devida atenção e planejar-se da melhor forma possível. Além disso, pôde-se observar que a atividade de planejamento da mesma é muito complexa e envolve uma série de fatores quase sempre negligenciados pelas organizações, mas que podem acarretar em grandes prejuízos financeiros, de segurança pessoal e perda de credibilidade das pessoas no mercado em que ela atua.

Para se evitar um incidente de segurança da informação é importante elaborar uma gestão dessa segurança, preocupando-se com os ativos da informação, sobretudo a vulnerabilidade relativa às pessoas, o que pode ser diminuída através de uma Política de Segurança da Informação efetiva e que não fique apenas no papel. É fundamental que a execução da presente Política de Segurança da Informação seja fielmente implantada e constantemente monitorada pelos principais gestores.

Foi observado que a 6ª Cia Ind MAT apesar de não possuir uma Política de Segurança da Informação definida, possui algumas normas e leis que estão dispersas em meio a inúmeros documentos que a polícia produz, e que se reunidos e divulgados ao público interno poderiam ajudar em muito na segurança da informação.

Devido às informações de algumas áreas serem de caráter confidencial e restrito não foi possível aprofundar um pouco mais nas questões da segurança da informação ou mesmo em métodos de segurança que são empregados.

Por fim, é importante ressaltar a necessidade que todos os setores e funcionários da organização estejam a par das normas e procedimentos pré-

estabelecidos, ou seja, é necessário que todos tenham a cultura de segurança e não só o conhecimento que ela é importante.

Trabalhos futuros

Em relação a trabalhos futuros, fica a oportunidade de acompanhar e analisar a implantação da Política de Segurança proposta, melhorando e complementando o documento, corrigindo deficiências ou falhas que por ventura não foram observadas.

É necessário que sejam aplicados questionários como métricas para verificar se a Política de Segurança está sendo bem empregada e aceita pelos funcionários, bem como o nível de comprometimento e interesse do público interno em relação à segurança, além de realizar uma auditoria de capacitação para selecionar todos os profissionais aptos a trabalhar no setor de TI.

Com relação à ocorrência de um incidente de segurança da informação é necessário que sejam desenvolvidos o Plano de Recuperação de Desastres (PRD), Plano de Continuidade Operacional (PCO) e Plano de Administração da Crise (PAC), uma vez que foi verificado neste trabalho que a organização estudada não possui esses planos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27001. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.** Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002. **Tecnologia da informação - Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005. **Tecnologia da informação - Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio de Janeiro, 2008.

BCI. Good Practice Guidelines 2008: **A Management Guide to Implementing Global Good Practice in Business Continuity Management** – Section 2: Understanding the Organization. 2007 b.

BUGS, Wagner. 2012. **Segurança da Informação.** Disponível em http://www.wagnerbugs.com.br/arquivos/material/seguranca_informacao.pdf. Acesso em 26 mai. 2014.

CAMPOS, André L. N. 2007. **Sistema de segurança da informação: controlando os riscos**. Florianópolis: Visual Books.

CANAVER, Gustavo. 2012. **Segurança da informação – Ciclo de vida da informação.** Disponível em http://gustavocanaver.wordpress.com/tag/cidal. Acesso em 22 abr. 2014.

FERREIRA, F. N. F; ARAUJO, M. T. **Política de Segurança da Informação: Guia prático para elaboração e implementação.** Rio de janeiro: Ciência Moderna, 2ª Ed. 2008.

FERNANDES, J. H. C. 2010a. **Módulo: Sistemas, Informação e Comunicação - Curso de especialização em gestão da segurança da informação e comunicações**. Universidade de Brasília.

GRIMALDI, R.; MANCUSO, J. H. **Qualidade Total**. Folha de São Paulo e SEBRAE, 6ª e 7ª fascículos, 1994.

ITGI (Steering Committee and IT Governance Institute). **Cobit Framework, Technical Report**, 2007.

MINAS GERAIS (ESTADO) Lei n.º 14.310, de 19 de junho de 2002, que dispõe sobre **o Código de ética e disciplina dos militares do estado de Minas Gerais (CEDM).**

POLICIA MILITAR DE MINAS GERAIS (PMMG). **Intranet PM.** Disponível em https://intranet.policiamilitar.mg.gov.br/AutenticacaoSSO/login.action. Acesso em 10 out. 2014.

POLICIA MILITAR DE MINAS GERAIS (PMMG). **Portal Corporativo Regional.** Disponível em http://www.pmmg.portalregional.mg.gov.br/. Acesso em 14 out. 2014.

POLICIA MILITAR DE MINAS (PMMG). **Sistema Informatizado Unificado (SIU).** Disponível em http://187.109.55.161:8080. Acesso em 12 out. 2014.

POLICIA MILITAR DE MINAS GERAIS (PMMG). **Sistema Integrado de Defesa Social.** Disponível em **https://web.sids.mg.gov.br/reds/.** Acesso em 10 out. 2014.

POLICIA MILITAR DE MINAS GERAIS (PMMG). RESOLUÇÃO Nº 4320, de 16 de julho de 2014. **Regulamenta o direito de acesso à informação no âmbito da Polícia Militar de Minas Gerais.**

SALVADOR, Gustavo. 2013. **Entendendo os fundamentos da segurança da informação.** Disponível em http://www.profissionaisti.com.br/2013/10/entendendo-os-fundamentos-da-seguranca-da-informacao. Acesso em 21 abr. 2014.

SCHEIN, Edgar. **Organizational Culture and Leadership**. San Francisco, Jossey Bass Publications. 2ª Ed. 1989

SÊMOLA, M. 2003. **Gestão da segurança da informação:** visão executiva da segurança da informação. Elsevier. 1ª Ed. Rio de Janeiro.

SILVA, Pedro T.; CARVALHO, Hugo; TORRES, Catarina B. Segurança dos sistemas de informação: **Gestão estratégica de segurança empresarial.** 1ª Ed. Portugal: Centro Atlântico, 2003.

UNIVERSIDADE FEDERAL DE LAVRAS. Biblioteca da UFLA. **Manual de normalização e estrutura de trabalhos acadêmicos:** TCC, monografias, dissertações e teses. Lavras, 2010. Disponível em: <http://www.biblioteca.ufla.br/site/index.php>. Acesso em: 16/10/2014.