PEDRO HENRIQUE NOGUEIRA

ESTABELECIMENTO DE CONTEXTO, ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA DELEGACIA REGIONAL DE SEGURANÇA PÚBLICA

LAVRAS - MG

2014

PEDRO HENRIQUE NOGUEIRA

ESTABELECIMENTO DE CONTEXTO, ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA DELEGACIA REGIONAL DE SEGURANÇA PÚBLICA

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Sistemas de Informação para a obtenção do título de Bacharel em Sistemas de Informação.

Área de concentração:

Segurança da Informação

Orientador:

Rêmulo Maia Alves

LAVRAS - MG

2014

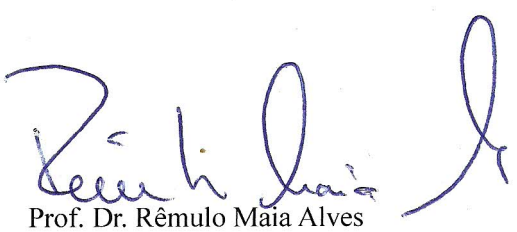
PEDRO HENRIQUE NOGUEIRA

ESTABELECIMENTO DE CONTEXTO, ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA DELEGACIA REGIONAL DE SEGURANÇA PÚBLICA

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Sistemas de Informação para a obtenção do título de Bacharel em Sistemas de Informação.

APROVADA em 21 de Novembro de 2014.

Prof. PhD. André Luiz Zambalde	UFLA
Bel. Plínio Márcio Braga Torres	UFLA



Prof. Dr. Rêmulo Maia Alves

Orientador

LAVRAS - MG

2014

AGRADECIMENTOS

Agradeço a Deus, por me conceder essa vitória em minha vida.

Agradeço à Universidade Federal de Lavras (UFLA) pela oportunidade e por todo o conhecimento transmitido.

Agradeço ao professor e orientador Rêmulo Maia Alves pela atenção concedida durante todo esse tempo, pelas críticas feitas, pelos conhecimentos repassados durante toda a minha graduação e pela amizade.

Agradeço a um grupo seleto de professores da UFLA que passaram durante a minha graduação ao qual pude adquirir muitos conhecimentos que engrandeceram minha formação profissional e moral, e que me ajudaram a construir valores éticos necessários para o desenvolvimento do pensamento reflexivo. Levarei comigo, para onde for, um pouco de cada um de vocês.

Agradeço a todos os meus amigos que fizeram parte dessa jornada, me apoiando e compartilhando a ajuda necessária nos momentos difíceis. Em especial ao Carlos Eduardo Lino pela ajuda que sempre precisei durante o curso.

Agradeço as grandes mentes da ciência que um dia pisaram neste mundo ou que ainda permanecem vivas, e que contribuíram direta ou indiretamente para a melhoria da qualidade de vida de cada um de nós. Mentes que destaco: Carl Friedrich Gauss, Isaac Newton, Nikola Tesla, Louis Pasteur, Alan Turing, Jimmy Walles, Sergey Brin e Larry Page.

Agradeço ao Armin Van Buuren, músico e produtor de trance, ritmo musical que me manteve acordado e concentrado durante todas as madrugadas para a confecção deste trabalho.

E por fim agradeço a você leitor: quem quer que seja, onde quer que esteja, que tenha se disposto a ler essa monografia por qualquer motivo que seja. Não existe texto sem leitor, e por isso a sua leitura também faz parte da produção desse trabalho.

“Não limitem seu pensamento aos sistemas existentes – imaginem o que poderia ser possível e então comecem a trabalhar para descobrir um meio de sair do estado atual das coisas e chegar lá. Ousem sonhar. O homem deve tentar alcançar o que está fora do seu alcance; senão, para que existiriam os céus?”

Vinton Gray Cerf

Coautor dos protocolos TCP/IP e considerado um dos pais da Internet

RESUMO

Atualmente a informação é um recurso muito valioso para as organizações. No setor público, a visão muda e o grande beneficiário é a sociedade, que utiliza dos serviços públicos em geral. O presente trabalho visou levantar o ambiente de uma Delegacia Regional de segurança pública quanto à segurança dos ativos de informação que ela possui, suas adequações às normas e padrões internacionais e ao processo DS5 (Garantir a Segurança dos Sistemas) do *framework* COBIT (*Control Objectives for Information and Related Technology*). Foram coletadas as informações por meio de questionários, roteiro de entrevista e observações. Os resultados obtidos mostraram que a gestão da segurança da informação está deficiente no ambiente e melhorias são necessárias. Por fim, concluiu-se que as políticas estaduais de segurança existem, mas estão centralizadas e pouco disseminadas no contexto estudado; e o que compromete as atividades da gestão de segurança da informação é a indisponibilidade de Recursos Humanos no Poder Estadual.

Palavras-chave: Segurança da Informação, Administração Pública Estadual, ABNT NBR ISO/IEC 27002:2013, ABNT NBR ISO/IEC 27005:2013, COBIT.

ABSTRACT

Currently the information is a very valuable resource for organizations. In the public sector, the view changes and the big beneficiary is the society that uses public services in general. The present work aimed at the environment of a Regional Police Station of Public Security about the safety of information assets that it owns, its adequacy to the international norms and standards and the process DS5 (Ensure Safety Systems) of the COBIT framework (Control Objectives for Information and Related Technology). Were colletcted the information through questionnaires, interview guidelines and observations. The results showed that the information security management is deficient in the environment and improvements are needed. Finally, it was concluded that State Security Policies exist, but are centralized and low disseminated in the context studied; and which undermines the activities of Information Security management is the unavailability of human resources in the State Government.

Keywords: Information Security, State Public Administration, ABNT NBR ISO/IEC 27002:2013, ABNT NBR ISO/IEC 27005:2013, COBIT.

LISTA DE FIGURAS

LISTA DE ABREVIAÇÕES

ABNT	Associação Brasileira de Normas Técnicas
BO	Boletim de Ocorrência
CIRETRANS	Circunscrições Regionais de Trânsito
CMMI	Capability Maturity Model Integration
COBIT ®	Control Objectives for Information and Related Technology
DETRAN	Departamento Estadual de Trânsito
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standartization
NBR	Norma Brasileira
PCMG	Polícia Civil de Minas Gerais
SIAL	Sistema de Apreensão e Leilão de Veículo
SEPLAG	Secretaria de Estado de Planejamento e Gestão
SGSI	Sistemas de Gestão da Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

Sem dúvida nenhuma estamos na era da informação e da economia globalizada. Sempre que estamos lendo uma revista, um jornal ou vendo um filme, estamos lidando com algum tipo de informação.

A informação é todo o dado trabalhado, útil, tratado, com valor significativo atribuído ou agregado a ele e com um sentido natural e lógico para quem usa a informação (REZENDE; ABREU, 2003). A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias (LAUREANO, 2005). Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, tem valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (QSP, 2014).

Em se tratando de segurança da informação, a ISO/IEC 27000 (2014) apresenta a seguinte definição: segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação. A adoção de uma gestão de segurança da informação se torna essencial para evitar que ocorram interrupções de qualquer espécie no setor público (Xiang et al.; 2008).

Uma estatística do Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (www.cetic.br) em relação ao setor público mostra os percentuais de práticas de segurança adotadas, conforme as Figuras 1 e 2, demonstrando o quão devem evoluir ou manter cada uma delas.

Percentual (%)		Senha para acesso a rede e aplicações			Backup			Identificação de invasões, vírus e spam		
		Sim	Não	Não sabe/ Não Respondeu	Sim	Não	Não sabe/ Não Respondeu	Sim	Não	Não sabe/ Não Respondeu
Total		96	3	1	92	7	1	90	8	1
PODER	Executivo	96	4	1	92	7	1	89	9	1
	Judiciário	100	0	0	100	0	0	97	3	0
	Ministério Público	93	3	3	97	0	3	97	0	3
	Legislativo	98	0	2	98	0	2	94	4	2
ENTE FEDERATIVO	Federal	99	0	1	99	1	1	96	3	1
	Estadual	96	4	1	92	7	1	89	9	2
PORTE	Até 249 pessoas ocupadas	94	6	1	88	10	1	89	9	3
	De 250 ou mais pessoas ocupadas	99	1	0	95	4	0	94	6	0

Figura 1 - Proporção de órgãos públicos federais e estaduais que utilizaram práticas de segurança da informação nos últimos 12 meses, por tipo de prática
Fonte: Cetic, 2014

Percentual (%)		Restrição de acesso físico aos servidores centrais			Controle dos softwares instalados nas estações de trabalho dos usuários			Suprimento de energia aos servidores centrais		
		Sim	Não	Não sabe/ Não Respondeu	Sim	Não	Não sabe/ Não Respondeu	Sim	Não	Não sabe/ Não Respondeu
Total		89	10	1	84	15	1	77	21	2
PODER	Executivo	88	11	1	83	16	1	75	22	2
	Judiciário	96	4	0	92	8	0	97	3	0
	Ministério Público	97	0	3	83	14	3	90	7	3
	Legislativo	98	0	2	96	2	2	84	14	2
ENTE FEDERATIVO	Federal	95	5	1	90	8	1	93	6	1
	Estadual	89	10	1	83	16	1	75	22	2
PORTE	Até 249 pessoas ocupadas	88	11	1	80	18	2	70	27	3
	De 250 ou mais pessoas ocupadas	93	7	0	87	13	0	81	18	1

Figura 2 - Proporção de órgãos públicos federais e estaduais que utilizaram práticas de segurança da informação nos últimos 12 meses, por tipo de prática
Fonte: Cetic, 2014

As organizações têm se planejado para evitar incidentes, reduzir riscos e maximizar lucros.

Em uma instituição pública os gestores devem buscar eficiência para atingir os objetivos e melhorar o serviço prestado para a sociedade, onde o contribuinte é uma parte do sistema.

1.1. Objetivo, Motivação e Justificativa

A Delegacia Regional em estudo trata diretamente com a sociedade na solução de diversos serviços relacionados à segurança. Ela possui 14 municípios. Na sede, ela conta com um total 53 servidores efetivos, dividindo-se em 7 delegados, 10 escrivães, 24 investigadores, 5 peritos, 3 médicos-legistas e 4 técnicos administrativos. Englobando todos os municípios a qual fazem parte, ela possui 70 servidores.

Essa Delegacia Regional atende a cidade sede através de suas diversas delegacias internas (Delegacia de Tóxicos e Entorpecentes; Delegacia de Trânsito; Delegacia de Furtos e Roubos; Delegacia Especializada de Crimes Contra a Mulher; o Idoso e a Criança; Delegacia de Defraudações e Falsificações; Delegacia de Homicídios e Delegacia de Crimes contra o Meio Ambiente). É um serviço de extrema necessidade para a sociedade o trabalho que a Polícia Civil realiza. Logo, o local em que ela realiza este trabalho tem que seguir padrões para manter a qualidade e eficiência dos serviços.

A segurança da informação em uma delegacia é de extrema importância, pois fraudes, vazamento de informação, acesso indevido aos locais e sistemas utilizados podem causar problemas aos ativos que ela possui, aos serviços prestados, e às pessoas diretamente ligadas, inclusive servidores e/ou a

população.

O objetivo geral do trabalho foi analisar o contexto de uma Delegacia Regional de Segurança Pública, verificar suas adequações às políticas e normas de segurança da informação e avaliar a maturidade do processo DS5 do COBIT.

Como objetivos específicos, o presente trabalho buscou realizar uma análise do ambiente; identificar os procedimentos adotados no tratamento da informação e alinhamento com os decretos estaduais de regulamentação da segurança de informação; classificar a informação e avaliar e priorizar os riscos eminentes encontrados com base na norma ABNT NBR ISO/IEC 27005 (2011).

A principal justificativa para a realização deste trabalho se deu pela baixa segurança da informação encontrada no ambiente. Poucos controles; pouca ou nenhuma política de gestão de ativos e uma fraca organização de delegações de competências das pessoas envolvidas nos processos. Uma Delegacia Regional deve ser exemplo ou pelo menos seguir normas e padrões básicos de segurança da informação. Acredita-se que este trabalho é importante por discutir um tema atual e muito importante no qual empresas e diversas organizações do mundo tem se preocupado e investido em segurança da informação, e buscou-se trabalhar com as versões mais recentes das normas técnicas da área. As decisões governamentais nesse quesito ainda carecem de objetividade e aplicação devido a vários fatores, e é este tema que será abordado do decorrer do trabalho.

O trabalho poderá auxiliar a delegacia na adequação do acesso e controle da informação descrito em detalhes nos decretos estaduais e a outras resoluções que estão disponíveis no sítio da Secretaria de Estado de Planejamento e Gestão do Estado de Minas Gerais.

1.2. Descrição do problema

A Delegacia Regional em estudo encontra-se com uma gestão deficitária

da informação. A credibilidade de uma instituição de segurança pública ao tratar com informação deve ser alta. Vulnerabilidades nos controles, acesso indevido a sistemas e salvaguarda de arquivos de forma precária são pontos primários encontrados ao observar o ambiente.

Ameaças intencionais como a invasão a sistemas, e acidentais por erros de usuários (fatores humanos) geram consequências, impactos na confiança e na integridade da informação e na imagem da instituição. A dificuldade de percepção dos gestores ou a ineficácia dos mesmos contribuem para a continuidade destas mesmas práticas.

1.3. Organização do trabalho

Os capítulos do presente trabalho estão organizados da seguinte forma: no capítulo 2 é apresentado o referencial teórico, onde serão abordados os principais conceitos de segurança de informação; as principais normas para o estudo da segurança da informação; o guia de boas práticas COBIT ®; um histórico da Polícia Civil e sua estrutura; os objetivos e estrutura da Secretaria de Estado de Planejamento e Gestão e as presentes normas e decretos na administração pública estadual.

O capítulo 3 apresenta a metodologia de pesquisa para o trabalho, que tem o objetivo de mostrar o tipo de pesquisa e como ela será feita no ambiente selecionado neste estudo de caso.

O capítulo 4 apresenta os resultados e a discussão da presente proposta de projeto para a disciplina de projeto orientado II.

Por fim, o capítulo 5 apresenta a conclusão do trabalho e as propostas para trabalhos futuros.

2. REFERENCIAL TEÓRICO

A evolução das tecnologias de comunicação e consequentemente o aparecimento das redes de computadores permitiu aproximar as pessoas e abrir caminho para troca de informações, sem saírem do seu lugar (ARAÚJO, 2010). Proteger a informação é essencial.

A segurança da informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003). Ela é um processo diretamente relacionado aos negócios de uma organização. Seu principal objetivo é garantir o funcionamento da organização frente às possibilidades de incidentes, evitando prejuízos, aumentando a produtividade, propiciando maior qualidade aos clientes, vantagens em relação aos seus competidores e garantido a reputação da organização (DAWEL, 2005).

Atualmente, os riscos relacionados à segurança da informação são um grande desafio para muitas organizações, uma vez que esses riscos podem ter consequências terríveis, incluindo a responsabilidade corporativa, a perda de credibilidade e danos monetários (CAVUSOGLU et al., 2004).

2.1. Conceitos relacionados e objetivos da Segurança da Informação

A Segurança da Informação possui 3 (três) principais objetivos ou três princípios básicos: Confidencialidade, Integridade e disponibilidade (Figura 3).

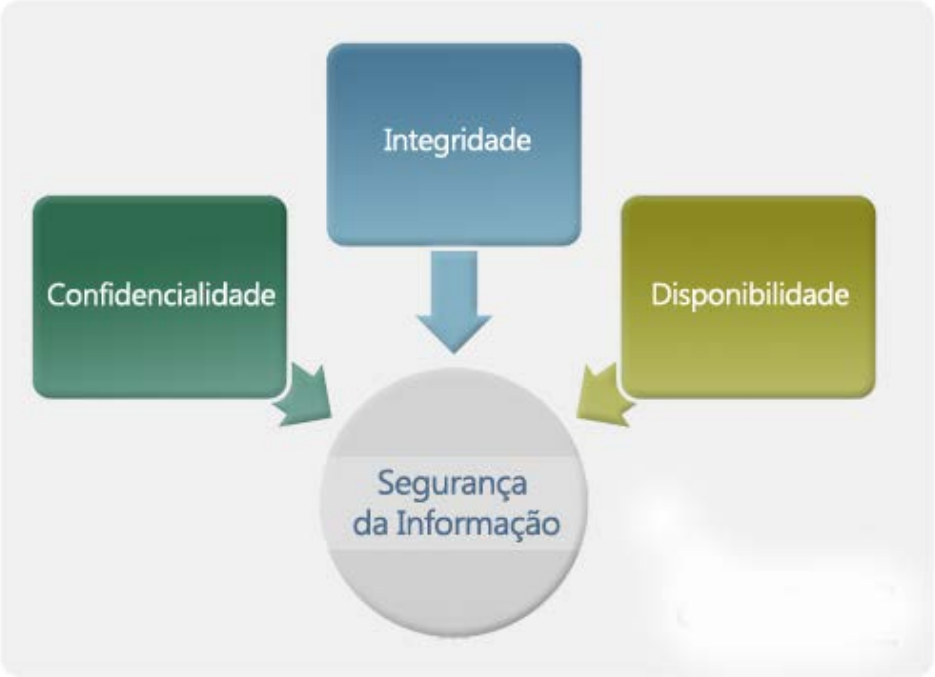


Figura 3 - Objetivos da Segurança da Informação
Fonte: Segurançadainformacao, 2014

Abaixo estão os conceitos segundo a norma ISO/IEC 27000 (2014):

- **Confidencialidade**: propriedade de que a informação não esteja disponível ou que seja revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade**: propriedade de salvaguarda da exatidão e completeza de ativos. Ou seja, "está ligada à propriedade de manter a informação armazenada com todas as suas características originais estabelecidas pelo dono da informação, tendo atenção com o seu ciclo de vida (criação, manutenção e descarte)" (SEGURANÇADAINFORMACAO, 2014).
- **Disponibilidade**: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. Ou seja, deve garantir que a informação

esteja sempre à disposição sempre que os usuários necessitarem.

Segundo a norma ISO/IEC 27000 (2014), além destes três, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas. São estas:

- **Autenticidade**: propriedade que uma entidade é o que é diz ser. Ou seja, é o princípio que diz que a origem do documento é autêntica, que ele não foi alterado no meio do caminho.
- **Responsabilidade**: dever de arcar com o próprio comportamento.
- **Não-Repúdio**: capacidade de comprovar a ocorrência de um evento ou ação alegada e suas entidades originárias. Ou seja, o emissor não pode negar a sua autenticidade.
- **Confiabilidade**: propriedade de um consistente procedimento planejado. Ou seja, é o resultado do funcionamento de todos os outros princípios.

A ausência de qualquer mecanismo de proteção ou a existência inadequada dos mesmos; a ausência ou deficiência de uma cultura de segurança; configurações mal elaboradas ou com falhas, acarretam em vulnerabilidades em uma organização. “Vulnerabilidade é uma fraqueza de um ativo ou de controle que pode ser explorado por uma ou mais ameaças” (ISO/IEC 27000, 2014).

As ameaças são “a causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização” (ISO/IEC 27000, 2014). Elas podem quebrar um, ou mais dos princípios da segurança da informação. Conforme descrito em Sêmola (2003), as ameaças podem ser classificadas quanto a sua intencionalidade e ser divididas em grupos (LAUREANO, 2005):

- **Naturais**: Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.

- **Involuntárias/acidentais**: Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados por acidentes, erros, falta de energia, etc.
- **Voluntárias/intencionais**: Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Os impactos são as potenciais consequências nos negócios de uma organização geradas por uma ou mais ameaças.

O risco é uma probabilidade de uma ameaça se concretizar. A ISO/IEC 27000 (2014) diz que o risco é o efeito da incerteza sobre os objetivos. Segundo Sêmola (2003), a equação do risco é caracterizada pela Figura 4:

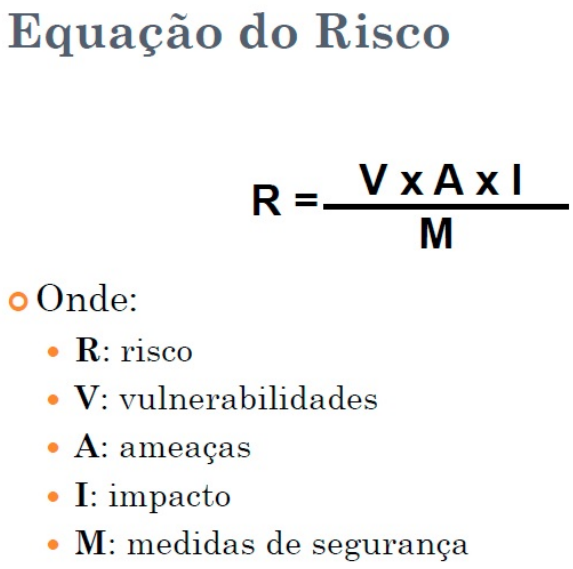


Figura 4 - Equação do risco
Fonte: Alves, 2012

2.2. Normas de Segurança da Informação

A série ISO/IEC 27000 se refere a um conjunto de normas desenvolvidas que fornecem uma estrutura para gerenciamento de segurança da informação para qualquer organização, pública ou privada, grande ou pequeno porte. Especificamente, a ISO/IEC 27000 (2014) além de conter informações básicas das normas da série, contém um glossário com a definição de termos e vocabulários bem definidos para não causar interpretações errôneas dos conceitos abordados nas normas da série 27000.

Esta norma foi publicada no dia 14/01/2014 segundo o site da Associação Brasileira de Normas Técnicas, e possui 31 páginas.

As normas da família ISO/IEC 27000 convergem para um ponto, o Sistema de Gestão de Segurança da Informação (SGSI), tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. Estão muito relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos (NORMASTECNICAS, 2014).

2.2.1. ABNT NBR ISO/IEC 27001

A norma ISO/IEC 27001 foi publicada em março de 2006 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação (CORREIA, 2014).

A norma ABNT NBR ISO/IEC 27001 (2013) foi preparada para prover requisitos para estabelecer, implementar, manter, e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A adoção do SGSI é uma decisão estratégica para uma organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais

usados, tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo (ABNT NBR ISO/IEC 27001, 2013). Esta norma pode ser usada por partes internas e externas, para avaliar a capacidade da organização em atender aos seus próprios requisitos de segurança da informação (ABNT NBR ISO/IEC 27001, 2013).

Esta norma foi atualizada e foi publicada no dia 08/11/2013 segundo o site da Associação Brasileira de Normas Técnicas e possui 30 páginas.

As novas versões contam com 14 seções de controles, 35 objetivos de controle e 114 controles mandatórios. Foram incluídas seções de Criptografia, Segurança nas Operações, Segurança nas Comunicações e Relacionamento na Cadeia de Suprimento. Dentre os novos controles destacam-se os que tratam do desenvolvimento seguro de aplicações (ESCOLA SUPERIOR DE REDES, 2013).

2.2.2. ABNT NBR ISO/IEC 27002

A norma ISO/IEC 27002 teve origem na antiga norma ISO/IEC 17799 de 2001, e essa que teve sua base a norma inglesa BS7799-1 de 1995. Ela traz o código de prática para controles de segurança da informação.

Esta norma é projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um SGSI, baseado na ABNT NBR ISO/IEC 27001 (2013) ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. Esta norma é também usada no desenvolvimento de organizações e indústrias específicas de gerenciamento de segurança da informação, levando em consideração os seus ambientes de risco de segurança da informação específicos (ABNT NBR ISO/IEC 27002, 2013).

Esta norma identifica três fontes principais de requisitos de segurança da

informação:

a) a avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócios da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
b) a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus principais parceiros comerciais, contratados e provedores de serviço tem que atender, além do seu ambiente sociocultural.
c) os conjuntos particulares de princípios, objetivos e os requisitos do negocio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

Os resultados de uma avaliação de risco ajudarão a orientar e determinar as ações de gestão apropriadas e as prioridades para gerenciar os riscos de segurança da informação e a implementação dos controles selecionados para proteger contra estes riscos (ABNT NBR ISO/IEC 27002, 2013).

Esta norma foi atualizada e foi publicada no dia 08/11/2013 segundo o site da Associação Brasileira de Normas Técnicas, e possui 99 páginas.

2.2.3. ABNT NBR ISO/IEC 27003

O propósito desta Norma é fornecer diretrizes práticas para a implantação de um SGSI, em uma organização, de acordo com a ABNT NBR ISO/IEC 27001:2005. A implantação de um SGSI geralmente é executada como um projeto (ABNT NBR ISO/IEC 27003, 2011).

Esta Norma não cobre atividades operacionais e outras atividades do SGSI, porém aborda os conceitos sobre como desenvolver as atividades após o início da operação do SGSI (ABNT NBR ISO/IEC 27003, 2011).

Com o uso desta Norma, a organização será capaz de desenvolver um processo para a Gestão da Segurança da Informação, fornecendo às partes interessadas a garantia de que os riscos aos ativos de informação são continuamente mantidos dentro dos limites de Segurança da Informação aceitáveis, conforme definido pela organização (ABNT NBR ISO/IEC 27003, 2011).

Esta norma foi publicada no dia 04/10/2011 segundo o site da Associação Brasileira de Normas Técnicas, e possui 75 páginas.

2.2.4. ABNT NBR ISO/IEC 27005

Esta norma fornece diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001 (2013). Ela é do interesse de gestores e pessoal envolvidos com a gestão de riscos de segurança da informação em uma organização e, quando apropriado, em entidades externas que dão suporte a essas atividades (ABNT NBR ISO/IEC 27005, 2011).

Esta norma foi publicada no dia 17/11/2011 segundo o site da Associação Brasileira de Normas Técnicas, e possui 87 páginas.

2.2.4.1. Gestão de Riscos

A Gestão de Riscos é uma série de atividades que se relacionam à forma como a organização lida com os riscos, abrangendo todo o ciclo de vida do

tratamento de riscos (ALVES, 2012). Conforme a Figura 5 que se encontra na norma ABNT NBR ISO/IEC 27005 (2011), o processo de gestão de risco compreende algumas etapas:

- **Estabelecimento do contexto**: definir os critérios para gestão de riscos e o escopo da gestão, das áreas envolvidas, processos, sistemas, condições de mercado, ambiente legal, entre outros (BANCO PAULISTA, 2014).
- **Identificação dos riscos**: Como o próprio nome já diz, nessa etapa são identificados os riscos a que o negócio está sujeito (LAUREANO, 2005).
- **Análise dos riscos**: Gerar listas detalhadas de vulnerabilidades, riscos e eventos que possam causar impacto aos objetivos da organização (ALVES, 2012). A Análise de Riscos deve contemplar algumas atividades, como o levantamento de ativos a serem analisadas, definições de uma lista de ameaças e identificação de vulnerabilidades nos ativos (LAUREANO, 2005).
- **Avaliação dos riscos**: etapa onde é mensurado o impacto que um determinado risco pode causar ao negócio (LAUREANO, 2005);
- **Tratamento dos riscos**: Identificação de controles, desenvolvimento do plano de ação e implantação do plano de ação (ALVES, 2012);
- **Monitoramento e análise crítica**: acompanhar os processos de gerenciamento e controle de riscos por meio de indicadores para avaliar a necessidade de ajustes em critérios, processos e instrumentos operacionais (BANCO PAULISTA, 2014).
- **Comunicação e consulta**: Conscientização dos usuários a respeito dos riscos residuais envolvidos na execução de determinadas atividades (BANCOPAULISTA, 2014).

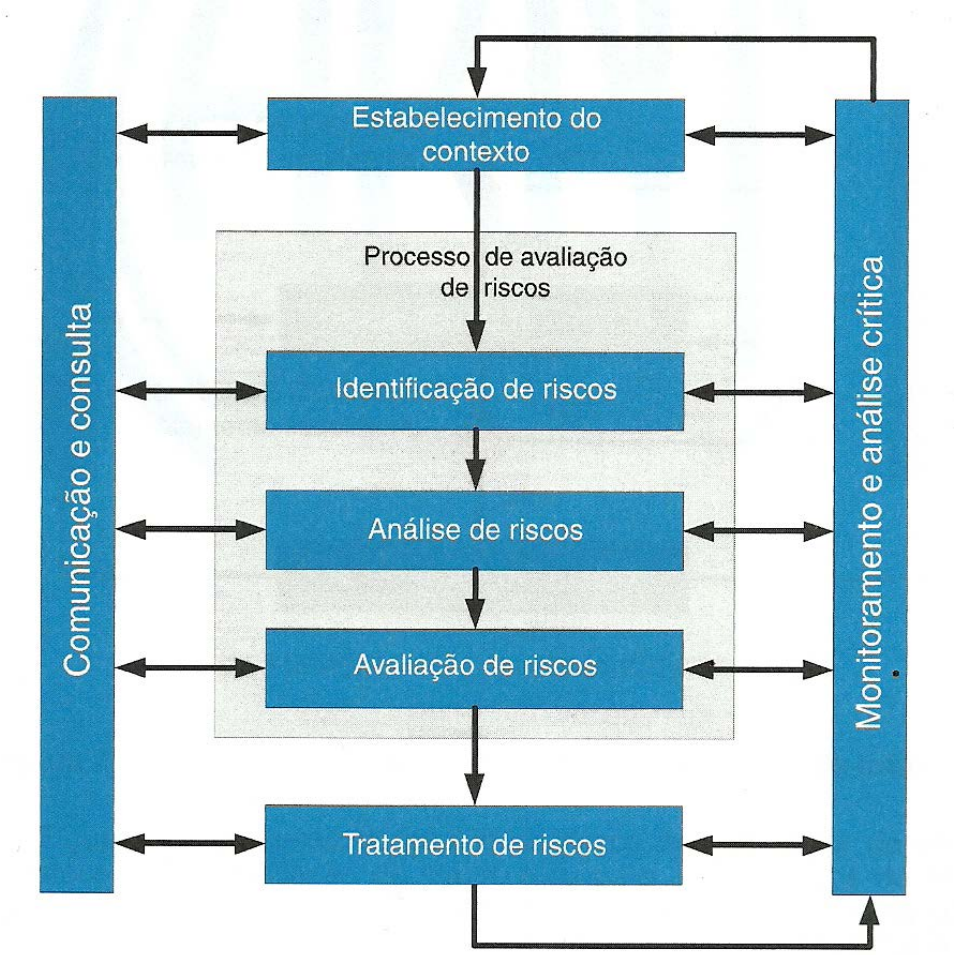


Figura 5 - O processo de gestão de riscos
Fonte: ABNT NBR ISO/IEC 27005, 2011

O processo de Gestão de Riscos de Segurança da Informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo, um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo, o plano de continuidade de negócios) (ABNT NBR ISO/IEC 27005, 2011).

Como mostra a Figura 6, o processo de Gestão de Riscos de Segurança da Informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento do risco. Um enfoque iterativo na execução do processo de 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 (ABNT NBR ISO/IEC 27005, 2011).

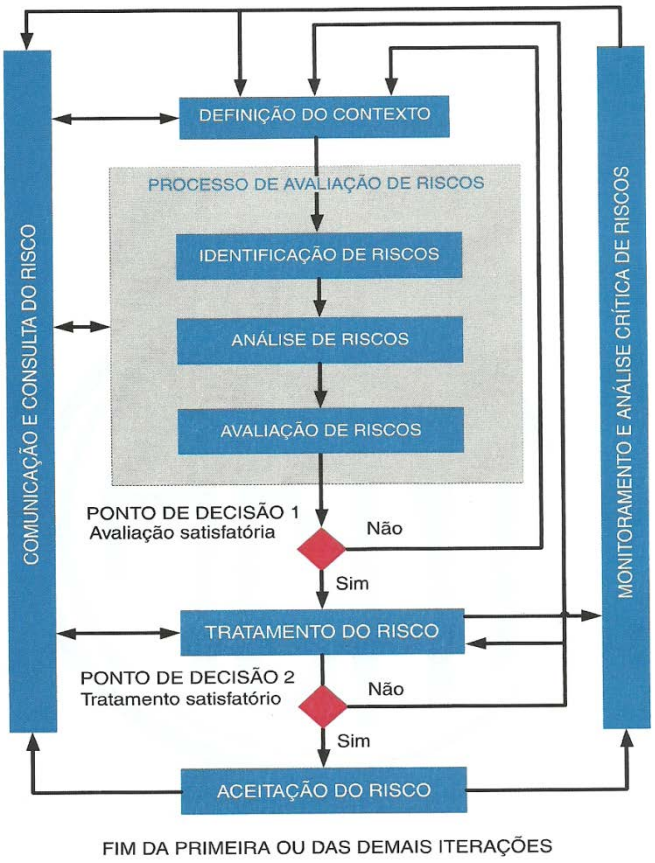


Figura 6 - Processo de Gestão de Riscos de Segurança da Informação
Fonte: ABNT NBR ISO/IEC 27005, 2011

Segundo Stoneburner (2001) citado por Laurenano (2005), a forma para descobrir se existe algum risco em um projeto e se o mesmo é aceitável, é apresentada na Figura 7:

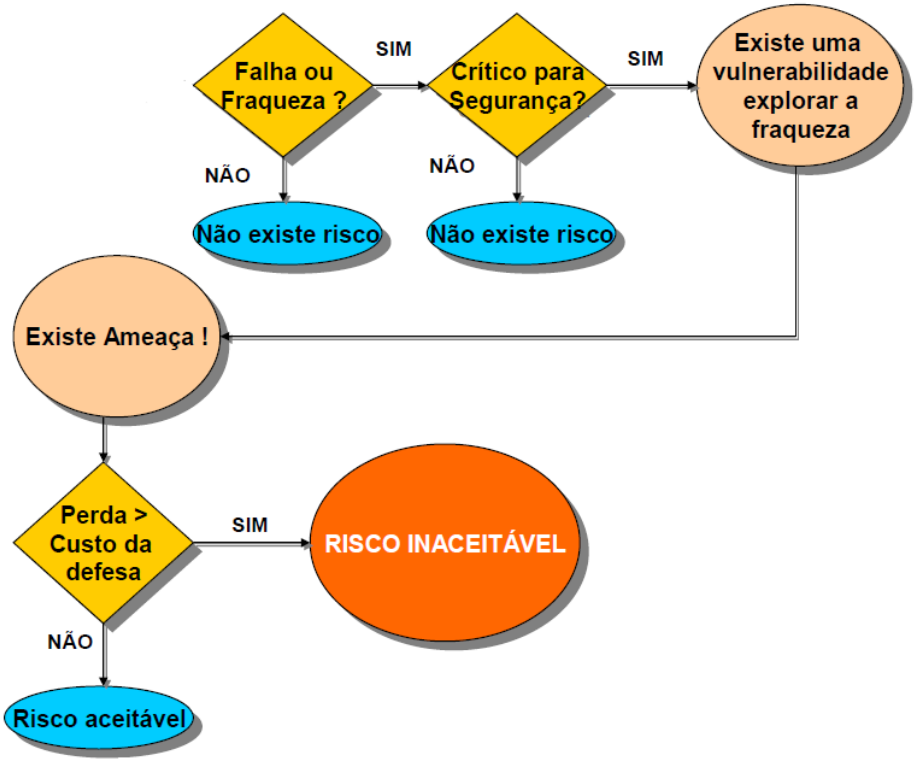


Figura 7 - Forma de avaliação de risco
Fonte: Laureano, 2005 (adaptado)

Segundo a norma ABNT NBR ISO/IEC 27005 (2011), convém que a gestão de riscos de segurança da informação contribua para:

- A identificação de riscos;
- O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- A comunicação e entendimento da probabilidade e das consequências destes riscos;

- O estabelecimento da ordem prioritária para tratamento do risco;
- A priorização das ações para reduzir a ocorrência dos riscos;
- O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão riscos;
- A eficácia do monitoramento do tratamento dos riscos;
- O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;
- A coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- O treinamento de gestores e pessoas a respeito dos riscos e das ações para mitigá-los.

2.3. COBIT

Segundo a ISACA (*Information Systems Audit and Control Association*), o COBIT é editado pelo ITGI (*Information Technology Governance Institute*) e aceito internacionalmente como uma boa prática de controle sobre informações, TI e riscos relacionados. Utiliza-se o COBIT para implantar a governança de TI e melhorar os controles de TI. Segundo o ITGI (2005), o COBIT foi projetado para ser utilizado por 4 diferentes públicos:

- Direção executiva;
- Administração do negócio;
- Administração de TI;
- Auditores.

Ele se estrutura em quatro domínios da seguinte forma conforme a Figura 8:

Figura 8 - Estrutura do COBIT
Fonte: Efagundes, 2014

Dentre as ferramentas disponibilizadas para a aplicação do COBIT encontra-se o COBIT *Management Guidelines* que provê um modelo de maturidade, semelhante ao CMMI (*Capability Maturity Model Integration*), com níveis variando de 0 (Não existente) a 5 (Otimizado) onde, em cada nível, existe uma descrição de como devem estar dispostos os processos para alcançá-los. Além disso, este modelo pode ser utilizado como um *checklist* para identificar melhorias nos processos de TI existentes na organização. Os seis níveis de maturidade com suas descrições genéricas são (ITGI, 2005):

- Nível 0: **Não existente** - Ausência total de processos identificáveis. A

organização não reconhece que há um aspecto a ser tratado.

- Nível 1: **Inicial** - Há evidências de que a organização reconhece que o aspecto existe e deve ser considerado. Entretanto, não há processos padronizados, apenas abordagens eventuais que tendem a ser aplicadas de forma isolada ou caso a caso.

- Nível 2: **Repetível** - Os processos foram desenvolvidos até o estágio em que procedimentos similares são adotados por pessoas distintas que realizam a mesma tarefa. Não há treinamento ou divulgação formal de procedimentos padronizados e as responsabilidades são deixadas a cargo das pessoas. Há um alto grau de confiança no conhecimento pessoal e consequente tendência a erros.

- Nível 3: **Definido** - Os procedimentos foram padronizados e documentados, bem como divulgados através de treinamento. Contudo, cabe às pessoas seguir tais processos, sendo pouco provável que desvios sejam detectados. Os procedimentos em si não são sofisticados, consistindo na formalização de práticas existentes.

- Nível 4: **Gerenciado** - É possível monitorar e mensurar a conformidade dos procedimentos, bem como adotar medidas quando os processos aparentarem não funcionar efetivamente. Os processos estão sob constante melhoria e propiciam boas práticas. Automação e ferramentas são utilizadas de forma limitada.

- Nível 5: **Otimizado** - Os processos foram refinados ao nível de melhores práticas, com base nos resultados de melhorias contínuas e modelagem da maturidade com outras organizações. A TI é utilizada como uma forma integrada para automatizar os fluxos, provendo ferramentas para otimizar a qualidade e a efetividade, tornando a empresa ágil para adaptações.

A Figura 9 ilustra os processos contemplados pelo COBIT:

Figura 9 - Processos do COBIT
Fonte: Bermejo, 2011

2.3.1. O processo DS5 – Garantir a Segurança dos Sistemas

O processo DS5 – Garantir a segurança dos sistemas é descrito da seguinte forma: "*Para manter a integridade da informação e proteger os ativos de TI, é necessário implementar um processo de gestão de segurança. Esse processo inclui o estabelecimento e a manutenção de papéis, responsabilidades, políticas, padrões e procedimentos de segurança de TI. A gestão de segurança inclui o*

monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança. A gestão eficaz de segurança protege todos os ativos de TI e minimiza o impacto sobre os negócios de vulnerabilidades e incidentes de segurança."

Este processo possui 11 objetivos de controle detalhados:

- DS5.1 - **Gestão da Segurança de TI**: Gerenciar a segurança de TI no mais alto nível organizacional da empresa de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio.
- DS5.2 - **Plano de Segurança de TI**: Traduzir os requisitos de negócio, de risco e conformidade, em um plano abrangente de segurança de TI, que leve em consideração a infraestrutura de TI e a cultura de segurança. O plano deve ser implementado em políticas e procedimentos de segurança, juntamente com investimentos adequados em serviços, pessoal, software e hardware. Políticas e procedimentos de segurança devem ser comunicados aos usuários e partes interessadas.
- DS5.3 - **Gestão de Identidade**: Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo. Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados. Os direitos de acesso devem ser solicitados pela gestão de usuários, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. As identidades e os direitos de acesso dos usuários devem ser mantidos em um repositório central. É necessário implementar e manter atualizadas medidas técnicas e de procedimentos com boa relação custo-benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso.

- DS5.4 - **Gestão de Contas de Usuário**: Assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário. Incluir um procedimento de aprovação de concessão de direitos de acesso pelos proprietários dos dados ou sistemas. Esse procedimento deve ser aplicado a todos os usuários, inclusive aos administradores (usuários com privilégios), usuários internos e externos, para os casos normais ou emergenciais. Os direitos e obrigações relativos ao acesso a sistemas e informações corporativos devem ser definidos em contrato para todos os tipos de usuários. Devem ser feitas revisões frequentes de todas as contas e os respectivos privilégios.
- DS5.5 - **Teste de Segurança, Vigilância e Monitoramento**: Garantir que a implementação de segurança de TI seja testada e monitorada proativamente. A segurança de TI deve ser revalidada periodicamente para garantir que o nível de segurança aprovado seja mantido. A função de monitoramento e registro de eventos (*logging*) deve possibilitar a prevenção e/ou detecção prematura de atividades anormais e incomuns que precisem ser tratadas, bem como a subsequente geração de relatórios no tempo apropriado.
- DS5.6 - **Definição de Incidente de Segurança**: Definir e comunicar claramente as características de incidentes de segurança em potencial para que possam ser tratados adequadamente pelos processos de gestão de incidentes ou gestão de problemas.
- DS5.7 - **Proteção da Tecnologia de Segurança**: Garantir que as tecnologias de segurança importantes sejam invioláveis e que as documentações de segurança não sejam reveladas desnecessariamente.
- DS5.8 - **Gestão de Chave Criptográfica**: Assegurar que sejam

estabelecidos políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada.

- DS5.9 - **Prevenção, Detecção e Correção de Software Malicioso**: Assegurar que medidas preventivas, de detecção e corretivas sejam estabelecidas corporativamente, em especial correções de segurança (*patches*) e controles de vírus, para proteger os sistemas de informação e tecnologias contra *malwares* (vírus, *worms*, *spyware*, *spam*).
- DS5.10 - **Segurança de Rede**: Garantir que técnicas de segurança e procedimentos de gestão relacionados (como firewalls, aplicativos de segurança, segmentação de rede e detecção de intrusão) sejam utilizados para autorizar o acesso e controlar os fluxos de informação entre redes.
- DS5.11 - **Comunicação de Dados Confidenciais**: Assegurar que as transações de comunicação de dados confidenciais ocorram somente por um caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovante de envio, comprovante de recebimento e não-rejeição de origem.

3. METODOLOGIA

O estudo se concentrará em uma Delegacia Regional de Segurança Pública, para ser avaliada como está a percepção da segurança da informação em uma Instituição Estadual de Minas Gerais. A cidade que se encontra esta Delegacia Regional no qual realizou-se este estudo de caso não será citada, somente será tratada de maneira genérica. A justificativa para não citar a cidade é trivial, pois os estudos vão se basear nos procedimentos de segurança da informação da mesma, e expor eles em domínio público poderiam gerar consequências comprometedoras.

A metodologia de desenvolvimento deste trabalho envolveu uma observação do ambiente e uma análise dos sistemas e políticas utilizadas. Os dados foram coletados no mês de outubro de 2014 e buscou-se verificar como são os processos internos e suas abordagens. Analisou-se as normas em estudo e o processo DS5 do COBIT para definir quais ações estão de acordo e quais não estão, e propor alterações do quadro atual da rotina do tratamento da segurança informação baseado nas vulnerabilidades encontradas. A utilização do COBIT se deu apenas como uma ferramenta de apoio na parte prática de TI (Tecnologia da Informação) da Delegacia Regional em relação aos sistemas utilizados.

Buscou-se também o apoio nas normas de segurança da informação para elencar riscos, prioridades para gerenciar o risco, e verificação dos controles que faltam ou que precisem ser aprimorados devido às vulnerabilidades encontradas. Toda a coleta de dados se deu pessoalmente e através de respostas fornecidas a questionários encaminhados pelo *chat* da rede social Facebook.

3.1. Tipo de Pesquisa

Com base no tipo de modelo proposto por Jung (2009), o trabalho em

desenvolvimento trata-se de uma pesquisa qualitativa, pois se baseia na observação cuidadosa e de caráter descritivo dos ambientes onde a informação está sendo ou onde será usada, do entendimento das várias perspectivas dos usuários ou potenciais usuários da informação, etc.

Quanto à natureza, é uma pesquisa aplicada, pois poderá ser utilizada em organizações que lidam com segurança pública.

Quanto aos objetivos, é uma pesquisa descritiva, pois tem como finalidade a observação, transcrição e análise dos dados obtidos.

Quanto aos procedimentos, é um estudo de caso único. A utilização de estudo de caso permite um melhor entendimento da situação através de uma percepção real dos problemas vivenciados.

Os métodos para coleta de dados foram a observação e questionários.

A Figura 10 mostra os tipos de pesquisa segundo Jung (2009):

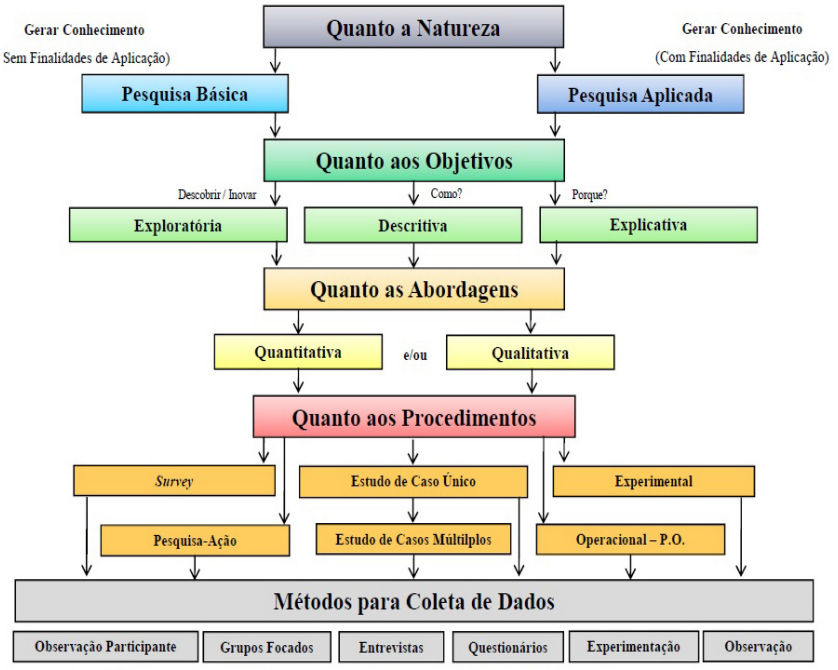


Figura 10 - Classificação dos tipos de pesquisas
Fonte: Jung, 2009

3.2. Procedimentos metodológicos

Com base nos níveis descritos na literatura, o COBIT propõe um modelo de maturidade específico para cada um dos seus processos. Cada processo possui sentenças específicas.

Conforme Ranzi e Alves (2007), as sentenças do modelo de maturidade podem se transformar em um questionário para avaliar se elas estão ou não de acordo com o encontrado (Quadro 1).

Foi avaliada cada sentença e o grau de conformidade delas na Delegacia, atribuindo 1 à sentença verdadeira e 0 à sentença falsa. Ou seja, quanto maior a conformidade com os níveis mais altos, melhor. Assim, será possível planejar e discutir ações. Cada sentença foi respondida por entrevista na presença do autor deste trabalho, do delegado regional e de um analista de sistemas servidor desta delegacia.

O gerenciamento do processo de “Garantir a segurança dos sistemas” que satisfaça ao requisito do negócio para a TI de “manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança” é:

Quadro 1 – Sentenças do nível 0 do processo DS5.
Fonte: COBIT 4.1, 2007.

0 - Inexistente quando	**Pontuação**
A organização não reconhece a necessidade de segurança da informação	
Responsabilidades não estão estabelecidas para garantir a segurança.	
Medidas de apoio à gestão de segurança de TI não estão implementas.	

Não há relatórios de segurança de TI, e não existe nenhum processo de resposta às falhas de segurança de TI.	
Não há um processo reconhecível de administração de segurança.	
Pontuação Total	
Sentenças	
Conformidade	

Continuando a realizar a análise de cada nível, é possível gerar as conformidades de cada nível e dispor destes dados em um novo quadro. No apêndice deste trabalho encontram-se todos os outros quadros de avaliação da maturidade dos outros níveis.

Com base nas normas ABNT e através da análise do ambiente, será possível realizar uma identificação dos riscos e realizar uma priorização quanto aos seus impactos e verificar onde ocorrem as vulnerabilidades nos controles e as decisões estratégicas que propiciam estas ocorrências. Através de um questionário com perguntas específicas respondidas pela internet pelo *SurveyMonkey*[1] com o link do questionário disponibilizado via *chat* pela rede social Facebook, com integrantes desta Delegacia, incluindo delegados, analistas, escrivães, técnicos e estagiários, que serviram de peso para sustentar a observação a respeito do ambiente por este autor que já vivencia por um tempo considerável os processos desta Delegacia Regional.

Pôde-se também fazer uma análise com políticas que estão consonância com a Resolução n^{o} 69, de 17 de setembro de 2009, que trata da Política de Segurança da Informação no Governo do Estado de Minas Gerais no âmbito da Administração Pública Estadual. Esta resolução encontra-se completa em anexo neste trabalho.

[1] https://pt.surveymonkey.com

3.3. A Polícia Civil de Minas Gerais e a Delegacia Regional de Segurança Pública

A Polícia Civil do Estado de Minas Gerais (PCMG) é uma das polícias do Estado de Minas Gerais, órgão do sistema de segurança pública ao qual compete, nos termos do artigo 144, § 4º, da Constituição Federal e ressalvada competência específica da União, as funções de polícia judiciária e de apuração das infrações penais, exceto as de natureza militar. A PCMG subordina-se diretamente ao Governador do Estado e integra, para fins operacionais, o Sistema de Defesa Social. Tem a sede na cidade de Belo Horizonte.

O surgimento dessa Instituição deu-se, na realidade, no período colonial, quando ainda capitania hereditária. A primeira Constituição Mineira promulgada em 31 de outubro de 1890 criou a Milícia Cívica, autorizando o Governador a prover os Cargos Policiais. No ano seguinte, em 16 de outubro de 1891, com a criação das Secretarias de Estado, os cargos policiais foram inseridos na Secretaria de Negócios do Interior e Justiça (COSTA; CHAVES, 2003).

A primeira organização policial em Minas Gerais, aprovada em 1892, compreendia a chefia de polícia, que dirigia o policiamento em todo o Estado, enquanto que o Delegado, sob seu comando administrativo, policiava o município, o subdelegado, os distritos, o Inspetor, os quarteirões. Atribuiu-se ao Chefe de Polícia o poder de nomear os Delegados e Subdelegados dentre cidadãos com qualidades necessárias ao exercício policial, probos e inteligentes. Os policiais nomeados não eram considerados, como hoje são, funcionários públicos, nem percebiam qualquer remuneração pela função delegada (COSTA; CHAVES, 2003).

No ano de 1895 era instalada nas imediações da atual igreja da Boa Viagem, a primeira Delegacia de Polícia de Belo Horizonte, com seu corpo de

guardas, conhecida por “Força Pública”, para atender a demanda da nova capital mineira. Conforme se vê na Figura 11, a unidade policial era uma rústica construção de pau a pique, ainda no antigo Curral D'el Rei. Antes da criação da Guarda Civil, o policiamento na capital era realizado pelos soldados da Força Pública, que faziam o patrulhamento através da cavalaria e infantaria, o que trazia sérias consequências com o esvaziamento dos quartéis, prejudicando os seus serviços (CYBERPOLICIA, 2014).

Figura 11 – Primeira Delegacia de Polícia de Belo Horizonte
Fonte: Cyberpolicia, 2014

A Figura 12 é de 1896 do arquivo do Museu Abílio Barreto e retrata o cotidiano da época. “Observamos os homens em seus ternos, cadeiras de palhinha, gaiolas penduradas na parede e chão batido de uma venda” (CYBERPOLICIA, 2014).

Figura 12 - Curral D'el Rey
Fonte: Cyberpolicia, 2014

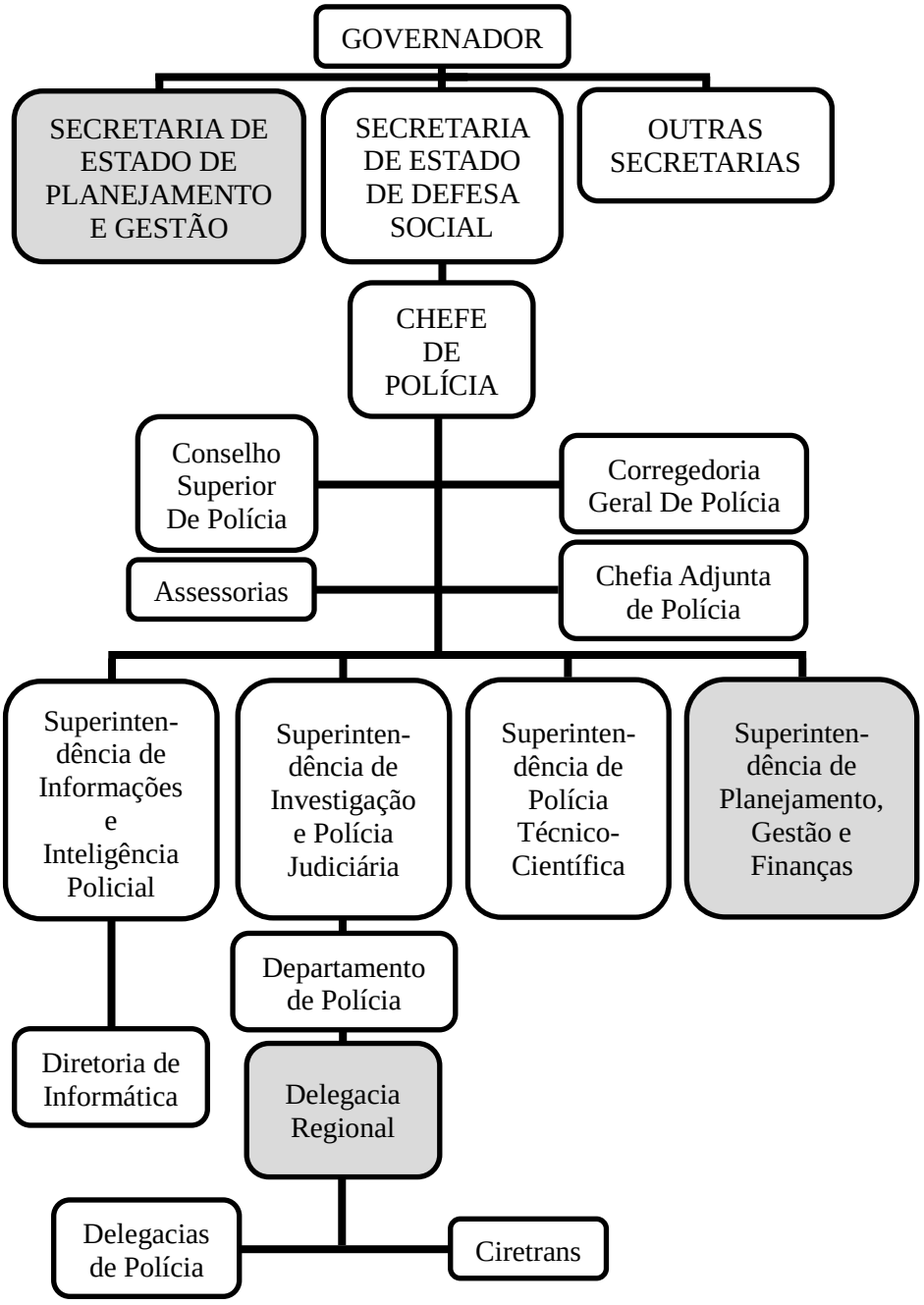
Em Minas Gerais, os chefes políticos, principalmente no interior do Estado, interferiam profundamente na permanência ou não do Delegado nas cidades compostas por seus eleitores. Com tanta influência política, somente em meados do século passado formalizaram-se os cargos na Polícia Civil e a Secretaria de Estado da Segurança Pública fora sistematizada, regulamentando-se todos os órgãos da estrutura organizacional, definindo-se competências, jurisdição e atribuições de cada um, de acordo com o âmbito de atuação (COSTA; CHAVES, 2003).

Na Figura 13 encontra-se o brasão da PCMG.

Figura 13 - Brasão da Polícia Civil de Minas Gerais
Fonte: PCMG, 2008

A Polícia Civil do Estado de Minas Gerais, dirigida pelo Chefe de Polícia Civil, desenvolve os serviços públicos da sua competência, basicamente, através das Delegacias Policiais. As delegacias distribuídas pelo território estadual são, nas suas circunscrições, o centro das investigações e pontos de atendimento e proteção à população.

O organograma simplificado da Polícia Civil de Minas Gerais foi criado por este autor com base na Lei Complementar 129 de 08/11/2013, que contém a Lei Orgânica da PCMG. Em destaque os três órgãos onde se concentrará os estudos deste trabalho.


GOVERNADOR
SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO
SECRETARIA DE ESTADO DE DEFESA SOCIAL
OUTRAS SECRETARIAS
CHEFE DE POLÍCIA
Conselho Superior De Polícia
Corregedoria Geral De Polícia
Assessorias
Chefia Adjunta de Polícia
Superinten-dência de Informações e Inteligência Policial
Superinten-dência de Investigação e Polícia Judiciária
Superinten-dência de Polícia Técnico-Científica
Superinten-dência de Planejamento, Gestão e Finanças
Departamento de Polícia
Diretoria de Informática
Delegacia Regional
Delegacias de Polícia
Ciretrans

3.3.1. Negócio

Apuração de crimes e contravenções por meio da investigação criminal cientificamente aplicada e o exercício da polícia judiciária para o esclarecimento de autoria, materialidade, motivo e circunstância, bem como a identificação civil e criminal, o registro e licenciamento de veículos, a formação e o controle de condutores, objetivando a segurança pública, a promoção de direitos e o fortalecimento da democracia.

3.3.2. Missão

Integrar a gestão coletiva da segurança pública e justiça criminal, por meio da realização eficiente da investigação criminal científica, redutora do fenômeno da violência.

3.3.3. Visão

Ser reconhecida, por sociedade e governos, como órgão essencial à construção das políticas de segurança pública e com maior índice de esclarecimento de ilícitos penais, atuando na repressão qualificada e na mediação de conflitos.

3.3.4. Valores

- Compromisso com o interesse público.
- Promoção de Direitos Humanos.
- Identificação dos cidadãos como sujeitos de direitos.
- Unidade institucional.

- Ética nas relações internas e externas.
- Valorização e qualificação profissional.
- Eficiência, qualidade, imparcialidade, transparência e efetividade dos serviços.
- Disciplina como princípio e sustentáculo do autocontrole profissional.
- Hierarquia como instrumento de gestão e controle disciplinar.

3.4. Secretaria de Estado de Planejamento e Gestão

A Secretaria de Estado de Planejamento e Gestão (SEPLAG) tem como objetivo coordenar, formular, executar e avaliar políticas que visem o desenvolvimento econômico, social e institucional de Minas Gerais. Dentre suas políticas públicas estão as que fomentam o desenvolvimento dos recursos humanos do governo Estadual, questões orçamentárias, recursos logísticos, tecnologia da informação e comunicação, modernização administrativa, saúde ocupacional, a coordenação geral das ações de governo e a gestão da estratégia governamental (SEPLAG, 2014). A Figura 14 mostra a sua página principal na *web*.

Figura 14 - Página inicial da SEPLAG na *Web*
Fonte: SEPLAG, 2014

Na Figura 15 encontra-se o organograma da SEPLAG fracionado com a Assessoria de Gestão da Informação, subordinada à Subsecretaria de Gestão da Estratégia Governamental.

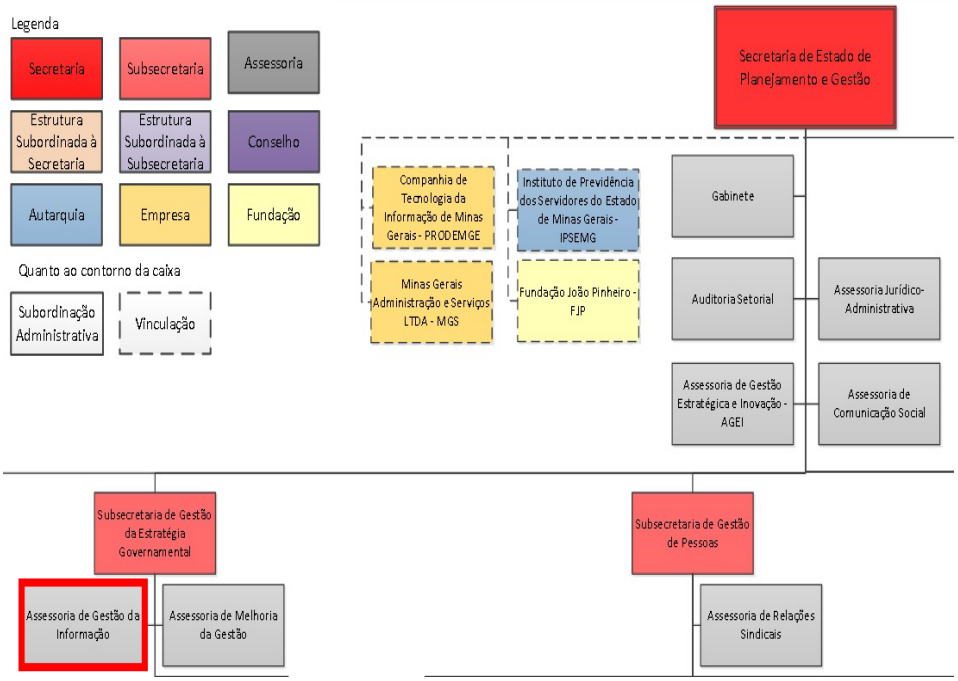


Figura 15 – Organograma fracionado da SEPLAG
Fonte: SEPLAG, 2014

Segundo o Decreto 45.794 de 02 de dezembro de 2011 que dispõe sobre a organização da Secretaria de Estado de Planejamento e Gestão, esta Assessoria é detalhada na Subseção I:

Art. 25. A Assessoria de Gestão da Informação tem por finalidade estruturar o ambiente informacional no âmbito da SEPLAG, mediante a implementação de práticas de Gestão da Informação, Inteligência Estratégica e Gestão do Conhecimento, em conformidade com as diretrizes estabelecidas pela Subsecretaria de Gestão da Estratégia Governamental, competindo-lhe:

I - identificar, analisar e acompanhar a evolução das necessidades informacionais na SEPLAG, propondo e gerindo instrumentos e ferramentas para atendimento às demandas priorizadas pela Direção Superior;

II - identificar, tratar e sistematizar conteúdos informacionais, otimizando o processo de estruturação, qualificação e disseminação da informação no âmbito da SEPLAG e do Governo do Estado de Minas Gerais, com vistas a obter uma visão consolidada dos avanços do governo e comunicá-los com transparência;

III - elaborar produtos de informação e de inteligência acerca da atuação estratégica do Governo do Estado no tocante aos planos, programas, projetos e ações governamentais, de modo a subsidiar o processo decisório; e

IV - coordenar a gestão do conhecimento na SEPLAG, mediante a estruturação de políticas e a implementação de práticas voltadas para o compartilhamento de ideias e conhecimento.

3.5. Superintendência de Planejamento, Gestão e Finanças da PCMG

Conforme a Lei Complementar 129 de 08/11/2013, que contém a Lei Orgânica da PCMG, ela se incumbe de:

Art. 44. A Superintendência de Planejamento, Gestão e Finanças tem por finalidade coordenar e executar o planejamento logístico, gerenciar o orçamento, a contabilidade e a administração financeira, gerir os recursos materiais e a administração de pessoal, competindo-lhe:

I - elaborar a proposta orçamentária da PCMG e acompanhar sua execução financeira, bem como viabilizar a prestação de contas da PCMG;

II - coordenar, orientar e executar as atividades de administração e pagamento de pessoal, expedir certidões funcionais, realizar averbações e preparar atos de posse e de aposentadoria;

III - controlar o cadastro de pessoal, a lotação e a vacância de cargos da PCMG;

IV - admitir, organizar, orientar e supervisionar a prestação de serviços terceirizados de apoio administrativo para os órgãos e unidades da PCMG, consistentes nas atividades de conservação, limpeza, segurança e vigilância patrimonial, transportes, copeiragem, reprografia, abastecimento de energia e água, manutenção de instalações e suas dependências;

V - guardar e manter controle de bens apreendidos ou arrecadados que não se vinculem a inquérito policial ou termo circunstanciado de ocorrência e realizar os respectivos leilões, inclusive de bens inservíveis para a PCMG, nas hipóteses legais, com a contabilização e destinação dos recursos para manutenção da PCMG;

VI - coordenar o sistema de administração de material, patrimônio e logística, inclusive adquirir, controlar e prover bens e serviços para órgãos e unidades da PCMG;

VII - manter a gestão de arquivo e de documentos e atuar na preservação da memória institucional da PCMG;

VIII - prover a atualização, a manutenção e o abastecimento da frota de veículos da PCMG;

IX - gerenciar a elaboração e celebração dos termos de doação, convênio, contrato e instrumento congênere.

3.6. Segurança da Informação na Administração Pública Estadual

A segurança da informação na Administração Pública Estadual possui 18 documentos relacionados para instruir todos os órgãos do Estado a protegerem seus ativos de informação de vulnerabilidades. O Quadro 2 contém estes documentos.

Quadro 2 – Principais documentos de Segurança da Informação do Estado de Minas Gerais.
Fonte: SEPLAG, 2014.

REGULAMENTO/NORMA	ASSUNTO
Decreto Estadual nº 44.998, de 30 de dezembro de 2008.	Institui a Política de Tecnologia da Informação e Comunicação no Governo do Estado de Minas Gerais, cria o Sistema de Governança de Tecnologia da Informação e Comunicação e o Comitê Executivo de Tecnologia da Informação e Comunicação no âmbito da Administração Pública Estadual.
Decreto Estadual nº 45.241, de 10 de dezembro de 2009.	Dispõe sobre o acesso às novas ferramentas interativas da *Web* 2.0 em uso nos órgãos e entidades da Administração Pública Estadual.
Decreto Estadual nº 45.969, de 24 de maio de 2012.	Regulamenta o acesso à informação no âmbito do Poder Executivo.
Decreto Estadual nº 46.226, de 24 de abril de 2013.	Dispõe sobre o uso de correio eletrônico institucional no âmbito da Administração Pública Direta, Autárquica e Fundacional do Poder Executivo.
Resolução Conjunta SEPLAG/SEF/PRODEMGE/Intendência nº 8.648, de 28 de junho de 2012.	Institui Grupo de Trabalho para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gerenciamento de Segurança da Informação no âmbito da Cidade Administrativa de Minas Gerais.
Resolução Seplag nº. 071, de 28 de novembro de 2003.	Dispõe sobre padronização e utilização dos Serviços de Correio Eletrônico Oficial dos Órgãos e Entidades do Poder

	Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.
Resolução Seplag n° 002, de 19 de janeiro de 2006.	Institui o Comitê Multidisciplinar de Segurança da Informação da Secretaria de Estado de Planejamento e Gestão - CMSI, e dá outras providências.
Resolução Seplag nº. 060, de 26 de setembro de 2006.	Institui as Normas de Segurança da Informação na Secretaria de Estado de Planejamento e Gestão.
Norma de Utilização da Internet	Estabelece os regulamentos para o uso da Internet na SEPLAG.
Norma de Utilização da Estação de Trabalho.	Estabelece os regulamentos para a utilização de estações de trabalho da SEPLAG
Norma de Utilização de Senhas.	Estabelece os regulamentos para a utilização de senhas de acessos à rede corporativa da SEPLAG
Termo de Responsabilidade - Estação de Trabalho.	Possui o formulário com o termo de responsabilidade
Resolução Seplag n° 69, de 17 de setembro de 2009.	Institui a Política de Segurança da Informação no Governo do Estado de Minas Gerais no âmbito da Administração Pública Estadual.
Resolução Seplag n° 72, de 21de setembro de 2009.	Regulamenta a Política de Segurança da Informação no que se refere à utilização da Tecnologia da Informação e Comunicação pelos técnicos dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.
Resolução Seplag n° 73, de 21 de	Regulamenta a Política de Segurança da Informação no

setembro de 2009.	que se refere à utilização da Tecnologia da Informação e Comunicação pelos usuários dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.
Resolução Seplag nº 017, de 11 de maio de 2010.	Institui o arranjo decisório e a matriz de responsabilidades das ações de Tecnologias da Informação e Comunicação no Estado de Minas Gerais.
Resolução Seplag nº 63, de 14 de setembro de 2011.	Institui o Manual de Desenvolvimento e Aquisição de Sistemas Seguros - MDASS com o objetivo de promover o aprimoramento da segurança da informação em sistemas utilizados pelos órgãos e entidades do Governo de Minas Gerais.
Resolução Conjunta Seplag/Sef/PRODEMGE/Intendência nº 8924, de 29 de maio de 2013.	Institui a norma de gestão de administradores das unidades organizacionais do domínio do Active Directory no âmbito da Cidade Administrativa de Minas Gerais.

4. RESULTADOS E DISCUSSÃO

4.1. O Ambiente – Estabelecimento de Contexto

A Delegacia Regional tem seu principal ativo de informação: os inquéritos policiais. São eles que contêm grande parte do trabalho da Polícia Civil. O acesso aos inquéritos normalmente se dá pelo delegado, que tem o acesso exclusivo a eles; pelos escrivães; pelos investigadores; e pelos estagiários, que comumente são chamados de escrivães *ad/hoc* e que auxiliam o trabalho dos delegados e da delegacia como um todo. Nestes inquéritos são anexados diversos documentos e/ou provas documentais que podem ser ou não significativos para a resolução de um crime.

Outro ativo que pode ficar fora de um inquérito policial quando se trata de casos mais leves e de pouca relevância, mas que pode conter documentos ou objetos apreendidos são os boletins de ocorrências (BO's) tradicionais que a Polícia Militar destina à delegacia. Cada delegacia interna se responsabiliza por armazenar e arquivar estes BO's.

O que se pode notar é a precariedade da infraestrutura para armazenar grande quantidade de boletins de ocorrência de forma organizada e segura. Armários sem trinco, gavetas enferrujadas, salas sem ventilação e algumas com umidade acabam dificultando a atividade de armazenamento seguro e facilitando o acesso indevido por funcionários não autorizados ou até pessoas comuns, e que por consequência, podem acabar retirando o que vem anexado aos BO's, o que pode ser objetos, documentos, etc.

Mais um ativo de informação existente é o Sistema Interno do DETRAN (Figura 16), este que possui políticas bem mais rígidas ao controle de acesso. Para obter um *Login* é necessário um ofício de um delegado e direcioná-lo para o Centro de Controle de Divisão de Ciretran's em Belo Horizonte. Aprovado o

acesso, a hierarquia de acessos é definida para o usuário, pois há funções que ele não está autorizado a realizar, como por exemplo, a opção de cancelamento de comunicação de venda do veículo abaixo.

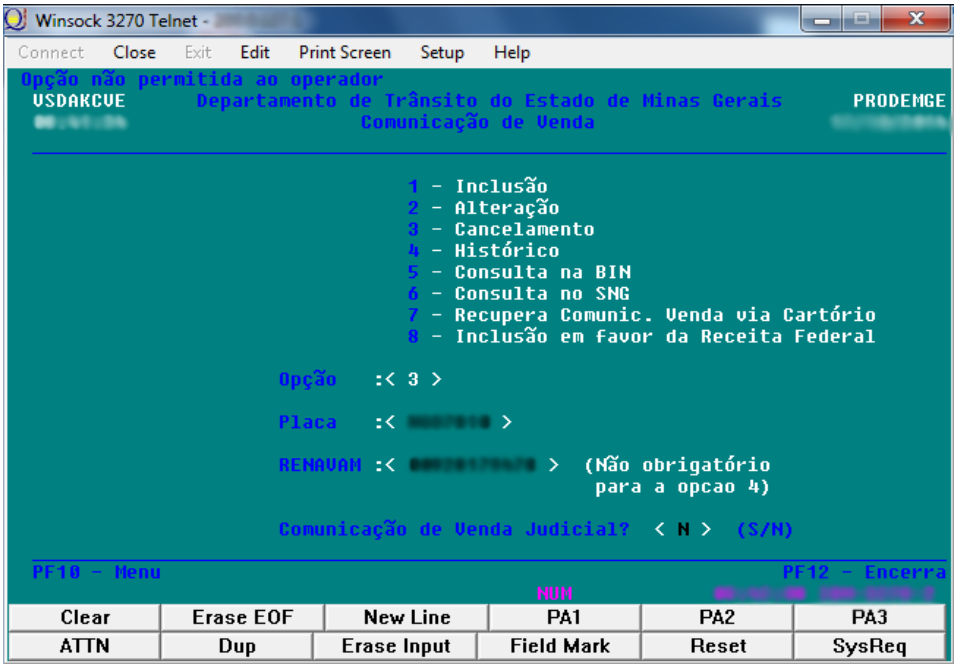


Figura 16 - Exemplo de uma hierarquia de acessos no Sistema
Fonte: PCMG, 2014

O que comumente ocorre neste caso e que é de grande risco, é o acesso por outro usuário utilizando o *Login* ativo da pessoa, pois a mesma se esquece de fazer o procedimento de *Logoff* ou de encerrar o uso do programa. Muitos o utilizam, saem para realizar outra tarefa e outro usuário mal-intencionado utiliza o sistema para realizar procedimentos irregulares na senha do funcionário que ali estava. Este sistema também armazena LOG's de registro em um banco de dados externo para futuras auditorias. Um dos outros diversos sistemas ligados ao DETRAN está o SIAL (Sistema de Apreensão e Leilão de Veículo). Ele já não possui a falha de deixar as sessões abertas. Após um determinado período de inatividade ele a encerra automaticamente (Figura 17).

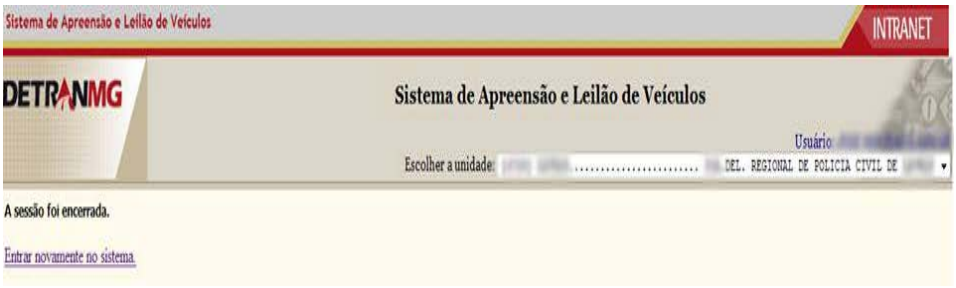


Figura 17 - Sessão encerrada automaticamente pelo SIAL
Fonte: PCMG, 2014

Outros ativos de TI que a delegacia possui estão presentes: computadores pessoais, roteadores, impressoras, *switches* e rack. O *Switch* principal fica em um rack devidamente trancado, mas a chave do mesmo permanece na fechadura da porta. Alguns computadores não têm placa patrimonial e não possuem lacres nas tampas de acesso ao interior das mesmas.

A delegacia possui duas redes de telecomunicações para acesso. Possui uma rede interna da polícia civil, onde é possível o acesso à intranet; e uma rede cedida gratuitamente por um provedor local para acesso convencional a internet. Ambas as redes que ligam os dispositivos internos são cabeadas. É utilizado também o acesso via rede wireless, que é protegida com senha utilizando o algoritmo WPA2, garantindo, portanto, mais segurança e confiabilidade neste quesito.

Em relação aos acessos, somente salas com armamentos e a sala da inteligência são protegidas o dia todo, pois somente pessoas autorizadas podem entrar. Outras salas que possuem informação e dados importantes, mas que o acesso não pode ser proibido o dia todo, utilizam-se de cofres reforçados para guardar o que é necessário. Somente pessoas autorizadas podem ter acesso à combinação do cofre. Nas demais salas o acesso é liberado aos funcionários. Salas estas que ainda podem conter informações sigilosas, mas que devido à péssima infraestrutura encontrada e a falta de locais, elas têm o acesso liberado,

pois não há mais locais para armazenar estes ativos.

4.2. Classificação da informação

Os inquéritos têm classificação segundo o teor de seu conteúdo. Segundo o artigo 20 do código processual penal, diz que “a autoridade assegurará no inquérito o sigilo necessário à elucidação do fato ou exigido pelo interesse da sociedade”. A resolução nº 69 da SEPLAG estabelece inciso terceiro do artigo quarto:

III - classificação da informação: as informações devem ser classificadas de forma a serem protegidas adequadamente;

No parágrafo segundo do inciso sétimo do mesmo artigo estabelece:

§ 2º *Até que seja estabelecida uma norma geral, as informações devem ser classificadas, em sigilosa, restrita e pública, por cada órgão ou entidade responsável por sua salvaguarda, no âmbito de sua competência, de acordo com os termos previstos em Lei.*

O que se encontra na prática é um controle informal desta resolução, pois muitos funcionários não sabem ao certo quais documentos e informações são públicos, restritos ou sigilosos, e não há um controle disso. A secção 8.2 da norma ABNT NBR ISO/IEC 27002 trata da classificação da informação e possui o objetivo:

- Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Possui o controle:

- Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificações ou divulgação não autorizada.

Nas diretrizes desta mesma norma é estabelecido: convém que os proprietários de ativos de informação sejam responsáveis por sua classificação; convém que o esquema seja consistente em toda a organização, de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma. O que falta no momento para ser realizado este controle são servidores disponíveis, o que no momento a Delegacia Regional não possui.

4.3. Análise do processo DS5 do COBIT

Após a avaliação das sentenças do COBIT, o Quadro 3 foi montado juntamente com o gráfico explicativo (Gráfico 1):

Quadro 3 – Conformidades do processo DS5.

DS5 – Garantir a Segurança dos Sistemas	
Nível	**Conformidade**
0	60%
1	100%
2	50%
3	28,57%
4	8,33%
5	0%

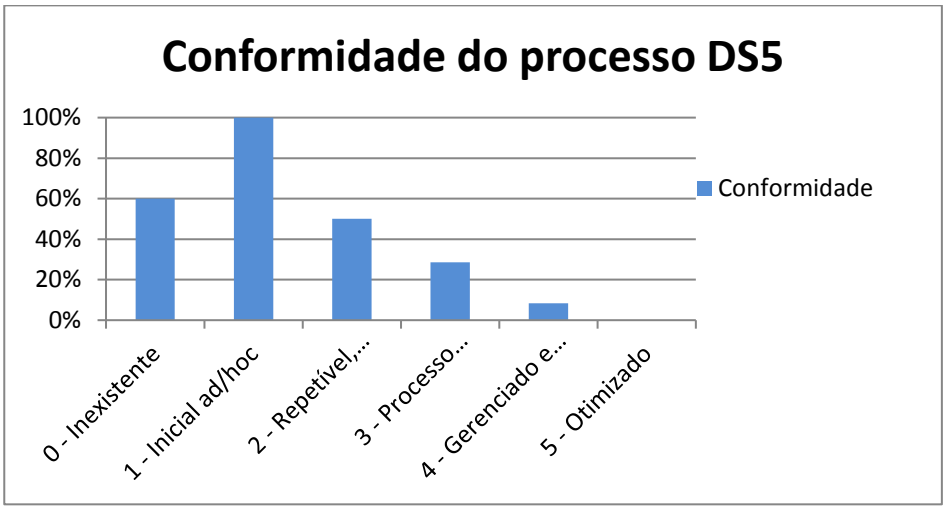


Gráfico 1 – Nível de maturidade de cada nível

Pode-se notar que a segurança dos sistemas utilizados ainda está em um ponto básico segundo o COBIT. Mas isso não quer dizer ausência total ou parcial de segurança dos sistemas, pois a conformidade com o nível inicial - que está após o nível inexistente - está em 100%. E também existem conformidades posteriores com certo nível tolerável.

4.4. Avaliação e priorização de Riscos

Com base na observação, na análise da norma ABNT NBR ISO/IEC 27005 que sugere algumas ameaças e no questionário respondido pelos integrantes de diversos setores internos da Delegacia, pode-se notar os riscos na percepção dos entrevistados quanto à probabilidade de ameaças (Gráfico 2).

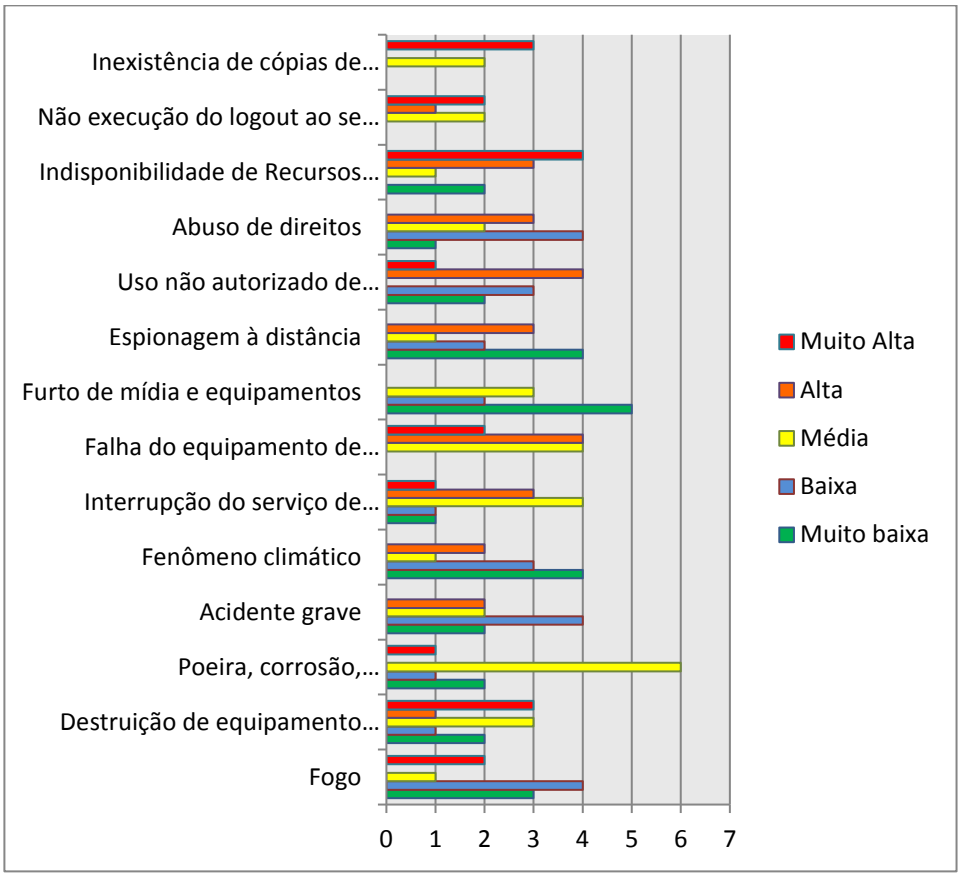


Gráfico 2 - Probabilidades de Ameaças ocorrerem.

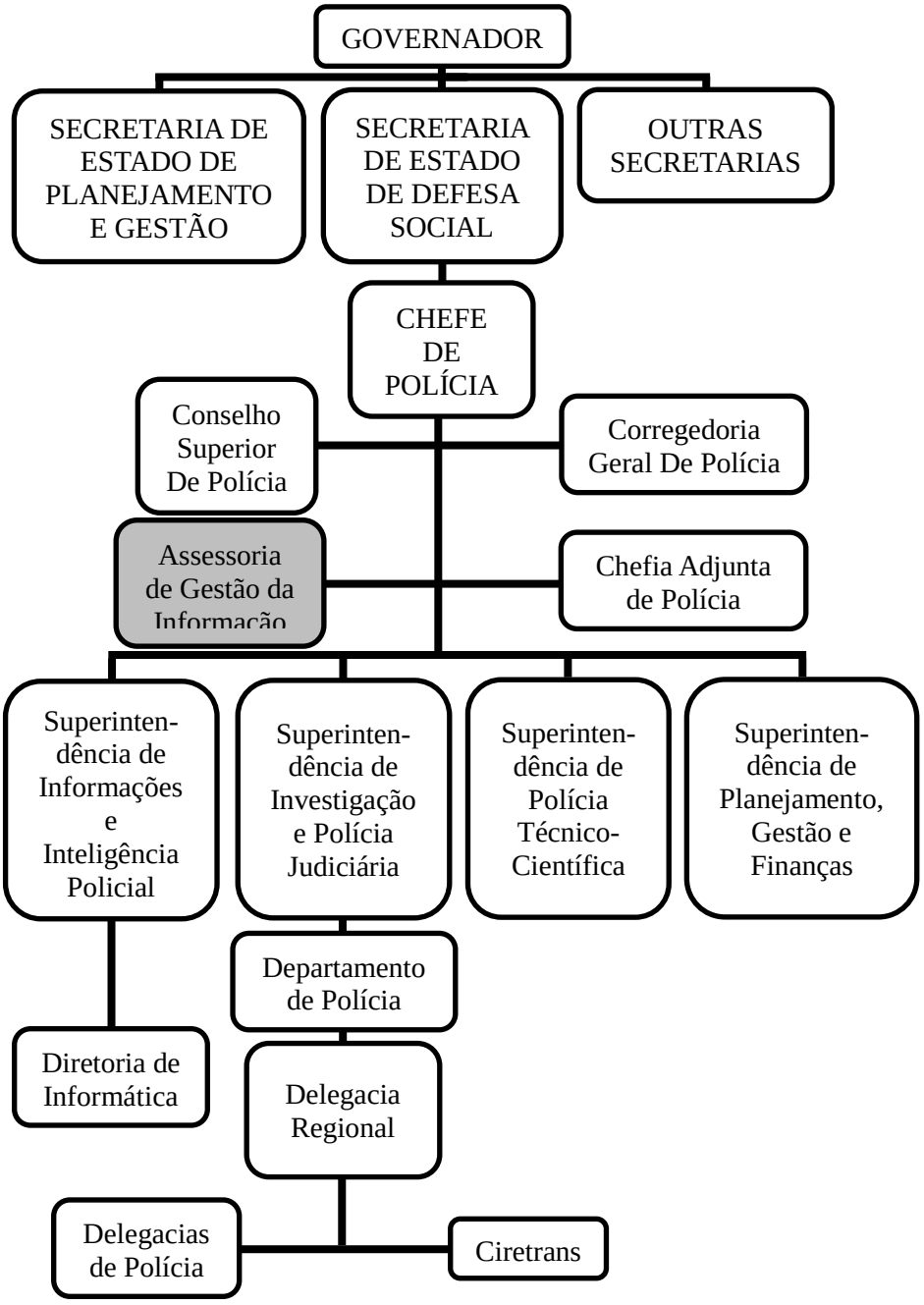
No apêndice encontra-se todos os demais gráficos utilizados e o Gráfico 2 detalhado.

É possível verificar de início a maior quantidade avaliada como Muita Alta em Indisponibilidade de Recursos Humanos, seguida respectivamente por Inexistência de Cópias de Segurança e Destruição de Equipamento ou Mídia. Categorizado como Alta, estão respectivamente as Falhas em Equipamentos de Telecomunicação e Uso Não Autorizado de Equipamento. Controles de segurança podem ser propostos com base nessa avaliação. Conforme a forma de avaliação do risco proposta por Laureano (2005), teria que ser feita uma análise

de custos para verificar se o risco é aceitável ou não, da mesma forma com a Inexistência de Cópias de Segurança. Quase todos os riscos se convergem para a Indisponibilidade de Recursos Humanos, devendo, portando, ser sanada em curto prazo, pois riscos inaceitáveis podem acontecer, pois a perda pode ser maior que o custo da defesa, ou seja, o custo da contratação de pessoal geraria impactos no orçamento, mas em longo prazo outros riscos seriam eliminados, como por exemplo, falha do equipamento de telecomunicação e controle dos ativos, pois haveria (m) servidor (es) encarregado (s) para tal tarefa.

4.5. Proposta de novo organograma

Como a Gestão de Segurança não deve ficar subordinada à órgãos onde o comando está sob Delegados, convém criar uma assessoria juntamente com as existentes com funcionários qualificados para tratar destes assuntos especificamente para a PCMG ajudaria a otimizar processos e separaria competências de maneira clara, por deixar servidores realizarem essa atividade específica e sem sobrecarga de trabalho. Mas para isso, a SEPLAG teria que autorizar contratação por concurso de mais servidores com competências específicas para realizar as atividades necessárias.


GOVERNADOR
SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO
SECRETARIA DE ESTADO DE DEFESA SOCIAL
OUTRAS SECRETARIAS
CHEFE DE POLÍCIA
Conselho Superior De Polícia
Corregedoria Geral De Polícia
Assessoria de Gestão da Informação
Chefia Adjunta de Polícia
Superinten-dência de Informações e Inteligência Policial
Superinten-dência de Investigação e Polícia Judiciária
Superinten-dência de Polícia Técnico-Científica
Superinten-dência de Planejamento, Gestão e Finanças
Departamento de Polícia
Diretoria de Informática
Delegacia Regional
Delegacias de Polícia
Ciretrans

5. CONCLUSÕES

Verificou-se que o Estado de Minas Gerais não investe o necessário em políticas de treinamento e infraestrutura para melhor tratar e gerenciar a informação, pelo menos no interior do Estado. Novas estratégias de processos devem ser adotadas para melhorar o fluxo e também o controle da informação. Fazer uma classificação da informação faz-se necessário, para restringir o acesso de pessoas não autorizadas a determinados dados que podem ser sigilosos devido a alguma investigação que esteja em andamento, pois alguém do ambiente interno pode conseguir um acesso fácil e conseguir obter estes dados caso algum funcionário tenha o intuito de agir com má fé. Ainda há um caminho a se percorrer, e parecem faltar decisões estratégicas de efetiva implantação em todo o Estado, talvez por ineficiência ou talvez por falta de recursos.

Ao contrário do que o autor acreditou ao início deste trabalho, o Estado de Minas Gerais já contempla várias políticas de segurança da informação bem definidas por várias resoluções e decretos estaduais, e que estão são de livre acesso a qualquer pessoa, incluindo servidores e cidadãos, no sítio da SEPLAG, mas não é divulgado internamente. Nota-se no resultado da pesquisa que 100% dos respondentes desconhecem a norma que trata de segurança da informação.

Verificou-se também que a SEPLAG é o órgão maior responsável pelas estratégias de gestão do Estado, e cabe a ela definir os procedimentos a serem adotados. A Assessoria de Gestão da informação, órgão subordinado da Subsecretaria de Gestão da Estratégia Governamental contém competências que a colocam como a responsável pela gestão da segurança da informação. Pode-se observar que está faltando a esta Assessoria realizar o que está presente em suas competências, que é a *"disseminação da informação no âmbito da SEPLAG e do Governo do Estado de Minas Gerais"*, mas de forma eficaz, onde todos os órgãos do Estado possam ser contemplados. Nota-se que a Administração

Pública Estadual possui uma ramificação muito extensa de órgãos, e fazer que políticas que no momento estão centralizadas em Belo Horizonte chegar a pequenos órgãos em municípios pequenos e com eficiência é uma tarefa árdua e onerosa.

Outro problema de grande urgência e que já foi tratado no trabalho é a indisponibilidade de recursos humanos no contexto da Polícia Civil, que se encontra atualmente sucateada. Déficits de funcionários são encontrados em qualquer delegacia do Estado, e não é diferente na que foi estudada. Com tamanha carga de trabalho e poucos recursos, é quase impossível gerir internamente de forma adequada a segurança da informação e diversos outros serviços prestados à população. Isso é resolvido somente com a contratação de pessoal, onde só o governador pode autorizar novos concursos, com base em diversas leis de responsabilidade fiscal que a SEPLAG apresenta com previsões futuras de gastos nos cofres públicos.

As organizações sempre estão vulneráveis a inúmeras ameaças e problemas, e na literatura são fornecidas várias maneiras para se resolver, analisar e tentar amenizar estes problemas. Os gestores devem sempre dar atenção em segurança, pois é um ponto crítico para as organizações. Fica exposto que, muitas vezes, por não haver um plano bem definido quanto à segurança, os gestores até conhecem os problemas, mas os ignoram, com um pensamento de que eles em determinado aspecto nunca irão acontecer na instituição.

Este trabalho está limitado a uma instituição pública, mas pode ser referência para qualquer outra organização como proposta para trabalhos futuros. E também mostrou que as normas técnicas sugerem processos contínuos para a evolução, crescimento e qualidade dos processos de segurança da informação em geral, e usá-las só trará benefícios tanto para o setor privado ou público.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, F. H. S. **Avaliação Da Maturidade Dos Processos De Segurança Da Informação Em Uma Instituição De Ensino Superior Pública Federal.** Monografia de graduação. UFLA, 2014.

ALVES, R. M. **Segurança da informação**. Slides da disciplina Segurança e Auditoria em Sistemas de Informação. Universidade Federal de Lavras. 2013.

ARAÚJO, T.; Costa, J.; Gonçalves, A.; Rodrigues, I. **A rede GÉANT e as tendências de desenvolvimento das novas redes de comunicação em fibra óptica.** Universidade Nova de Lisboa, Faculdade de Ciências e Tecnologia, Portugal, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27001. **Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002. **Tecnologia da Informação - Técnicas de segurança – Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27003. **Tecnologia da Informação - Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação**. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005. **Tecnologia da Informação - Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, 2011.

BANCOPAULISTA. **Relatório Circular 3.678 - Gerenciamento de riscos**. Disponível em:

<https://www.bancopaulista.com.br/docs/Gerenciamento_de_Riscos_BANCO_PAULISTA.pdf>. Acesso em: 02 nov. 2014.

BERMEJO, P. H. S. **Framework para governança de TI**. DCC – UFLA. 2011.

CAVUSOGLU, H.; CAVUSOGLU, H.; RAGHUNATHAN, S. **Economics of IT Security Management: Four Improvements to Current Security Practices, Communications of the Association for Information Systems**. 2004, p. 65-75.

CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO – **TIC Governo Eletrônico 2013, Órgãos Públicos Federais e Estaduais**. Disponível em: <http://cetic.br/tics/governo/2013/orgaos/B6/>. Acesso em: 24 out. 2014.

CORREA, R. M. **Um estudo de caso sobre a Gestão da segurança da informação Em uma empresa privada**. Monografia de graduação. UFLA, 2014.

COSTA, P. L., CHAVES, P. G. S. **O papel da Polícia Civil no processo de envelhecimento da população na cidade de Belo Horizonte - Minas Gerais: a Delegacia especializada de proteção ao idoso – DEPI.** Disponível em: <http://www.ibccrim.org.br/artigo/625-Artigo:-O-papel-da-pol%C3%ADcia-civil-no-processo-de-envelhecimento-da-popula%C3%A7%C3%A3o-na-cidade-de-Belo-Horizonte-Minas-Gerais:-a-Delegacia-especializada-de-prote%C3%A7%C3%A3o-ao-idoso--DEPI>. Acesso em: 28 out. 2014.

CYBERPOLICIA. **História da Polícia Operacional Investigativa - A Polícia através das décadas em Minas Gerais**. Disponível em: <http://www.cyberpolicia.com.br/index.php/historia/decadas/164-primeiras-decadas#>. Acesso em: 28 out. 2014.

DAWEL, G. A. **A segurança da informação nas Empresas**. Ampliando horizontes além da tecnologia. Rio de Janeiro: Ed. Ciência Moderna, 2005.

EFAGUNDES. **O que é o COBIT?** Disponível em: <http://www.efagundes.com/Artigos/COBIT.htm>. Acesso em: 27 out. 2014.

ESCOLA SUPERIOR DE REDES. **Atualizadas as normas 27001 e 27002 - Técnicas de Segurança.** Disponível em: <http://esr.rnp.br/noticias/atualizadas-as-normas-27001-e-27002-tecnicas-de-seguranca>. Acesso em: 31 out. 2014.

INTERNATIONAL STANDARD. ISO/IEC 27000. **Information technology — Security techniques — Information security management systems — Overview and vocabulary**. Third Edition, 2014.

ITGI. Information Technology Governance Institute. **COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models.** Rolling Meadows: ITGI, 2007.

JANSSEN, L. A. **Instrumento de avaliação de maturidade em processos de segurança da informação: estudo de caso em instituições hospitalares**. Dissertação (Mestrado) — PUCRS, 2008. Disponível em: <http://repositorio.pucrs.br/dspace/bitstream/10923/1240/1/000400421-Texto%2bCompleto-0.pdf>. Acesso em: 27 out. 2014.

JUNG, C. F. **Metodologia aplicada a projetos de pesquisa: Sistemas de Informação & Ciência da Computação**. Taquara, 2009. 1 CD-ROM.

LAUREANO, M. A. P. **Gestão de Segurança da Informação**. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 30 out. 2014.

LEFFA. **Normas da ABNT Citações e Referências Bibliográficas**. Disponível em: <http://www.leffa.pro.br/textos/abnt.htm#4.1>. Acesso em: 24 out. 2014.

MINAS GERAIS. **Lei Complementar 129 de 08/11/2013, que contém a Lei Orgânica da Polícia Civil do Estado de Minas Gerais**. Disponível em: <https://www.almg.gov.br/consulte/legislacao/completa/completa-nova-

min.html?tipo=LCP&num=129&comp=&ano=2013&texto=original>. Acesso em: 30 out. 2014.

NORMASTECNICAS. **SÉRIE ISO 27000**. Disponível em: <http://www.normastecnicas.com/iso/serie-iso-27000/>. Acesso em: 30 out. 2014.

PCMG. **Polícia Civil do Estado de Minas Gerais**. Disponível em: <https://www.policiacivil.mg.gov.br/>. Acesso em: 28 out. 2014.

PLANEJAMENTO.MG. **Segurança da informação**. Disponível em: <http://planejamento.mg.gov.br/gestao-governamental/gestao-de-tecnologia-da-informacao/seguranca-da-informacao>. Acesso em 29 out. 2014.

PWC. **Uma defesa ultrapassada Principais resultados da Pesquisa Global de Segurança da Informação 2014 – The Global State of Information Security® Survey 2014**. Disponível em: <http://www.PwC.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 28 out. 2014.

QSP. **Sistemas de Gestão da Segurança da Informação**. Disponível em: <http://www.qsp.org.br/siso_27000.shtml>. Acesso em 28 nov. 2014.

RANZI, T. A. D.; ALVES, E. M. **Governança de TI: avalição de maturidade do COBIT em uma empresa global**. Universidade Federal de Santa Catarina. 2007. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAA&url=https%3A%2F%2Fprojetos.inf.ufsc.br%2Farquivos_projetos%2Fprojeto_442%2FArtigo.doc&ei=6PpOVL6MHc-1sQSxqIK4DQ&usg=AFQjCNFHQHR03OnEecRUsANUl5qsSvFrmw&sig2=TQyQVxOJAheTSe64ilDouA&bvm=bv.77880786,d.cWc&cad=rja>. Acesso em 28 out. 2014.

REZENDE, D. A.; ABREU, A. F. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. 3ª ed. São Paulo, (2003).

SEGURANCADAINFORMACAO. **Fundamentos e Conceitos da Segurança da Informação, Módulo Security Solutions.** Disponível em: <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>. Acesso em: 30 out. 2014.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 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: 30 out. 2014.

XIANG, W.; WANG, Y.; ZHANG, Z. **The research on business continuity planning of e-government based on information security risk management**. In: Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on. 2008. p. 446–450.

APÊNDICE A

Os quadros a seguir apresentam os resultados obtidos em cada nível de maturidade do COBIT.

Quadro 4 – Sentenças do nível 1 do processo DS5.

1 – Inicial / *ad hoc* quando	**Pontuação**
A organização reconhece a necessidade de segurança de TI.	1
A consciência da necessidade de segurança depende principalmente das pessoas.	1
A segurança de TI é tratada de forma reativa e não é mensurada.	1
As falhas de segurança de TI detectadas geram acusações internas, pois a atribuição de responsabilidades é obscura.	1
As respostas às falhas de segurança de TI são imprevisíveis.	1
Pontuação Total	5
Sentenças	5
Conformidade	100%

Quadro 5 – Sentenças do nível 2 do processo DS5.

2 – Repetível, porém Intuitivo quando	**Pontuação**
As responsabilidades pela segurança de TI são atribuídas por um coordenador de segurança de TI, apesar da autoridade do gestor do coordenador ser limitada.	0
A consciência da necessidade de segurança é fragmentada e limitada.	1
Embora informações relevantes de segurança sejam produzidas pelos sistemas, elas não são analisadas.	1
Serviços terceirizados podem não tratar das necessidades	0

específicas de segurança da organização.	
Políticas de segurança estão sendo desenvolvidas, mas as habilidades e ferramentas são inadequadas.	0
Os relatórios de segurança de TI são inconsistentes, mal elaborados ou impertinentes.	1
Treinamento em segurança está disponível, mas depende da decisão de cada funcionário.	0
A segurança de TI é considerada principalmente como sendo de responsabilidade e domínio de TI, e a empresa não percebe a segurança da TI como parte do seu domínio.	1
Pontuação Total	4
Sentenças	8
Conformidade	50%

Quadro 6 – Sentenças do nível 3 do processo DS5.

3 – Processo Definido quando	**Pontuação**
A conscientização de segurança existe e é promovida pela Direção.	0
Os procedimentos de segurança de TI são definidos e alinhados com a política de segurança de TI.	0
As responsabilidades pela segurança de TI são atribuídas e entendidas, mas não são consistentemente impostas.	0
Um plano de segurança de TI e soluções de segurança são resultado de análises de risco.	0
O relatório de segurança não tem foco em negócio.	1
Testes de segurança são realizados de forma *ad hoc* (por exemplo, teste de intrusão).	1

O treinamento em segurança é disponibilizado para a TI e para o Negócio, mas é agendado e controlado informalmente.	0
Pontuação Total	2
Sentenças	7
Conformidade	28,57%

Quadro 7 – Sentenças do nível 4 do processo DS5.

4 – Gerenciado e Mensurável quando	**Pontuação**
As responsabilidades pela segurança de TI são claramente atribuídas, gerenciadas e impostas.	0
Avaliações críticas de riscos e impactos de segurança são executadas consistentemente.	0
As práticas e políticas de segurança são complementadas com perfis básicos específicos.	0
É mandatória a submissão aos métodos de promoção de conscientização da segurança.	0
A identificação, a autenticação e a autorização do usuário são padronizadas.	1
Certificações de segurança são buscadas por equipes responsáveis pela auditoria e o gerenciamento de segurança.	0
Os testes de segurança são realizados utilizando padrões e processos formalizados visando melhorar os níveis de segurança.	0
Os processos de segurança de TI são coordenados com a área corporativa de segurança da informação.	0
Os relatórios de segurança estão alinhados aos objetivos de negócio.	0
O treinamento em segurança de TI é ministrado às equipes de negócios e de TI.	0

O treinamento em segurança da TI é planejado e gerenciado para atender às necessidades do negócio e aos perfis de riscos de segurança definidos.	0
Os objetivos e métricas da gestão de segurança foram definidos, porém ainda não são mensurados.	0
Pontuação Total	1
Sentenças	12
Conformidade	8,33%

Quadro 8 – Sentenças do nível 5 do processo DS5.

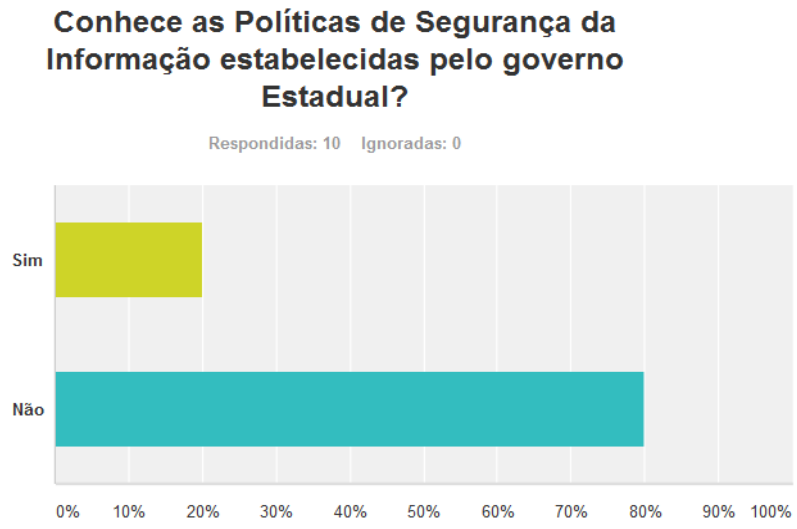
5 – Otimizado quando	**Pontuação**
A segurança de TI é de responsabilidade conjunta das Direções de Negócio e de TI e está integrada aos objetivos corporativos de segurança.	0
Os requisitos de segurança de TI são claramente definidos, otimizados e incluídos em um plano de segurança aprovado.	0
Os usuários e clientes são gradativamente responsáveis pela definição dos requisitos de segurança, e as funções de segurança são integradas às aplicações no estágio de planejamento.	0
Os incidentes de segurança são prontamente tratados com procedimentos formalizados de resposta a incidentes apoiados por ferramentas automatizadas.	0
São realizadas avaliações de segurança críticas periódicas para verificar a efetividade da implementação do plano de segurança.	0
As informações sobre ameaças e vulnerabilidades são sistematicamente coletadas e analisadas.	0
Os controles adequados para minimizar riscos são prontamente comunicados e implementados.	0

Testes de segurança, análise de causa-raiz dos incidentes de segurança e identificação proativa de riscos são utilizados em processos de melhoria contínua.	0
Os processos de segurança e tecnologia estão integrados em toda organização. Métricas de gerenciamento de segurança são coletadas e comunicadas.	0
A Direção utiliza essas métricas para ajustar o plano de segurança como parte do processo de melhoria contínua.	0

Pontuação Total	0
Sentenças	10
Conformidade	0%

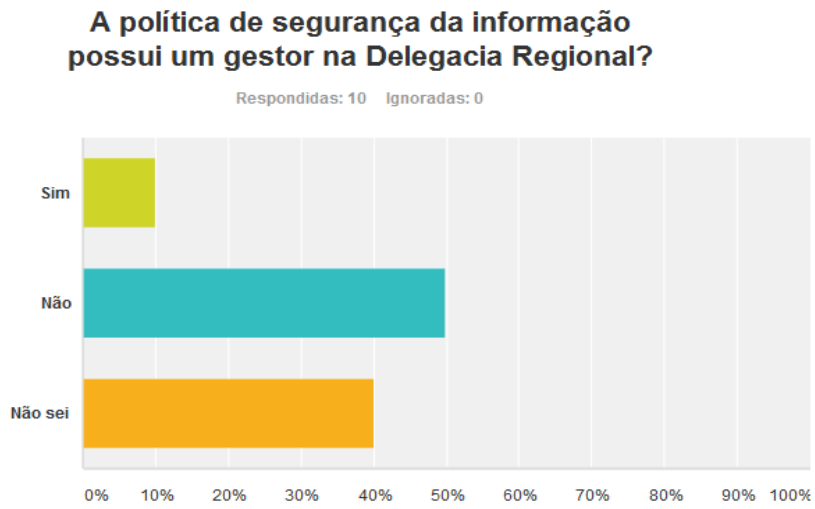
APÊNDICE B

Questionários adotado no **SurveyMonkey**.



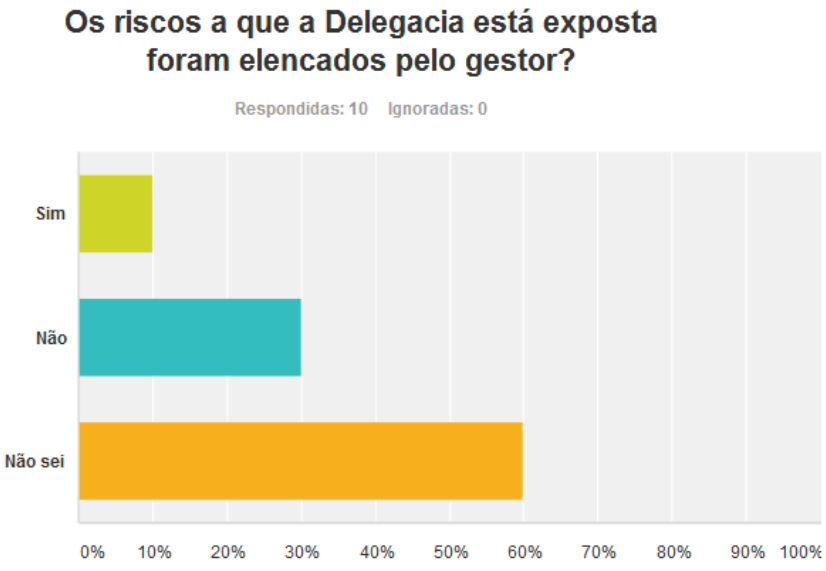
Opções de resposta	Respostas	
Sim	20,00%	2
Não	80,00%	8
Total		10

Figura 18 - Conhecimento das Políticas de Segurança
Fonte: SurveyMonkey, 2014



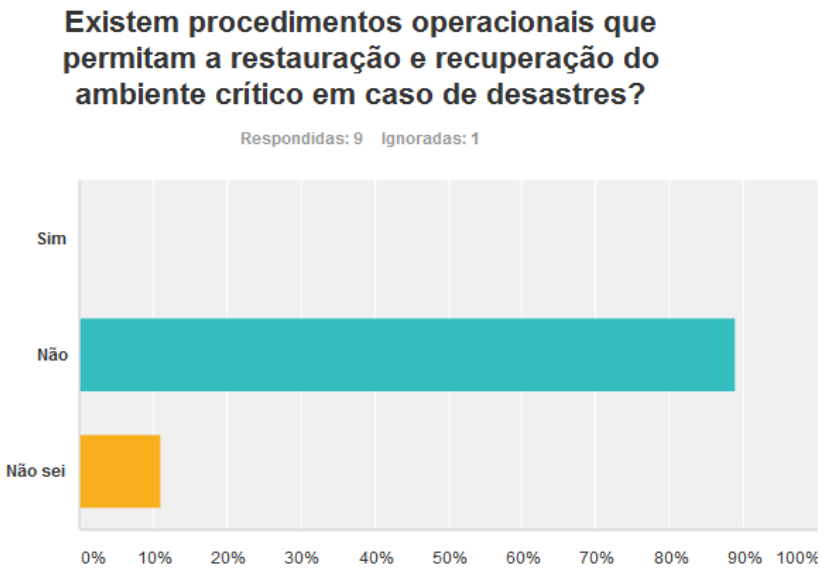
Opções de resposta	Respostas	
Sim	10,00%	1
Não	50,00%	5
Não sei	40,00%	4
Total		10

Figura 19 - Existência de Gestor
Fonte: SurveyMonkey, 2014



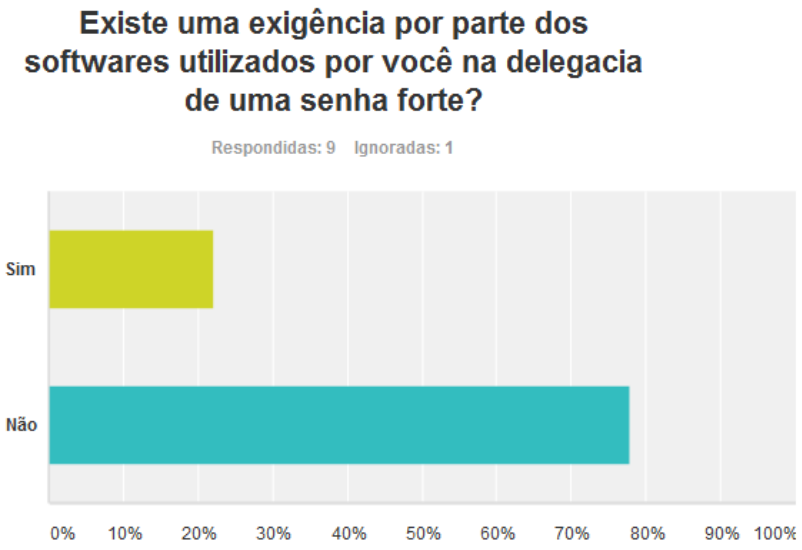
Opções de resposta	Respostas	
Sim	10,00%	1
Não	30,00%	3
Não sei	60,00%	6
Total		10

Figura 20 - Riscos elencados
Fonte: SurveyMonkey, 2014



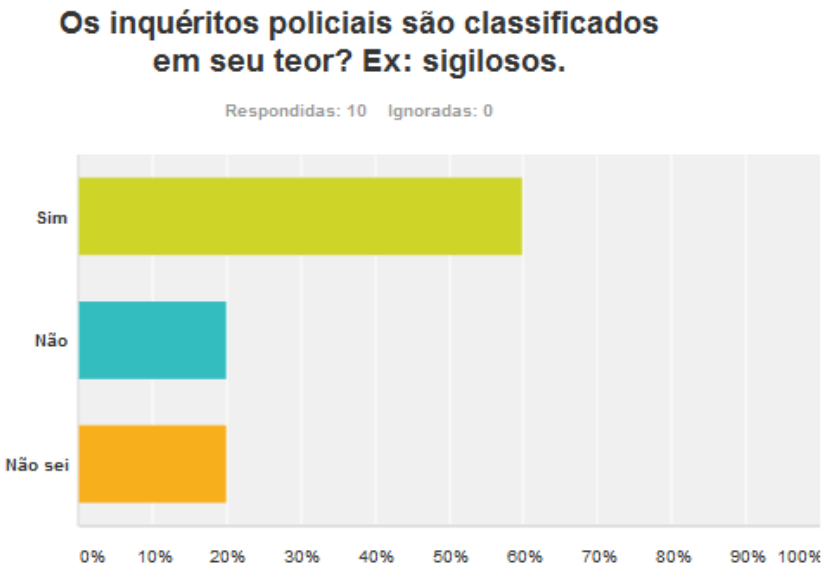
Opções de resposta	Respostas	
Sim	0,00%	0
Não	88,89%	8
Não sei	11,11%	1
Total		9

Figura 21 - Recuperação de desastre
Fonte: SurveyMonkey, 2014



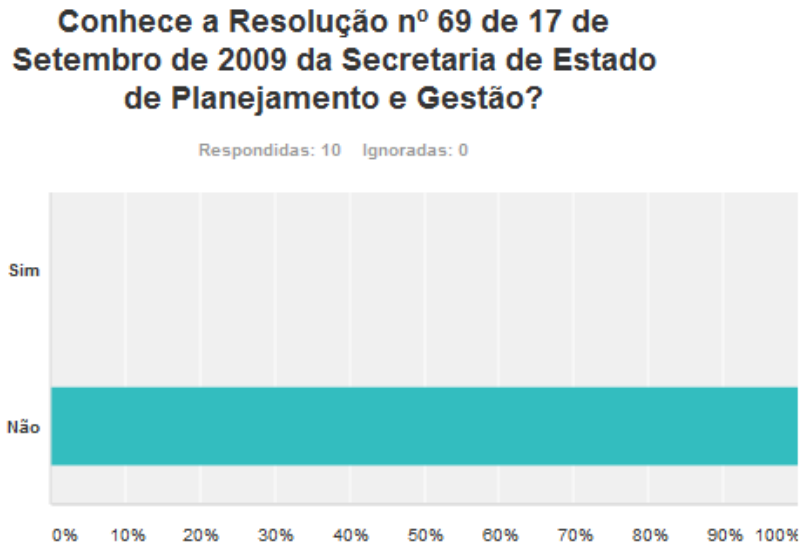
Opções de resposta	Respostas	
Sim	22,22%	2
Não	77,78%	7
Total		9

Figura 22 - Criação de senha forte
Fonte: SurveyMonkey, 2014



Opções de resposta	Respostas	
Sim	60,00%	6
Não	20,00%	2
Não sei	20,00%	2
Total		10

Figura 23 - Classificação de inquéritos
Fonte: SurveyMonkey, 2014



Opções de resposta	Respostas	
Sim	0,00%	0
Não	100,00%	10
Total		10

Figura 24 - Conhecimento da Resolução
Fonte: SurveyMonkey, 2014

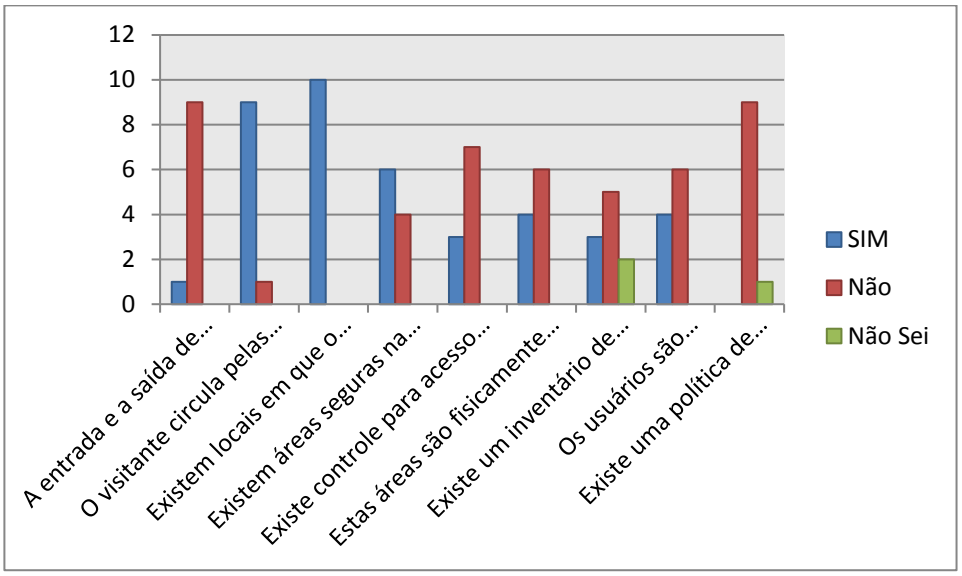


Gráfico 2 – Avaliação de conformidades.

Questões adotadas:

- A entrada e a saída de visitantes são registradas?
- O visitante circula pelas dependências da delegacia sozinho?
- Existem locais em que o público geral não tem acesso?
- Existem áreas seguras na Delegacia?
- Existe controle para acesso a estas áreas seguras?
- Estas áreas são fisicamente trancadas e periodicamente verificadas?
- Existe um inventário de todos os ativos (equipamentos, arquivos, pessoas) importantes?
- Os usuários são administradores das máquinas?
- Existe uma política de backup?

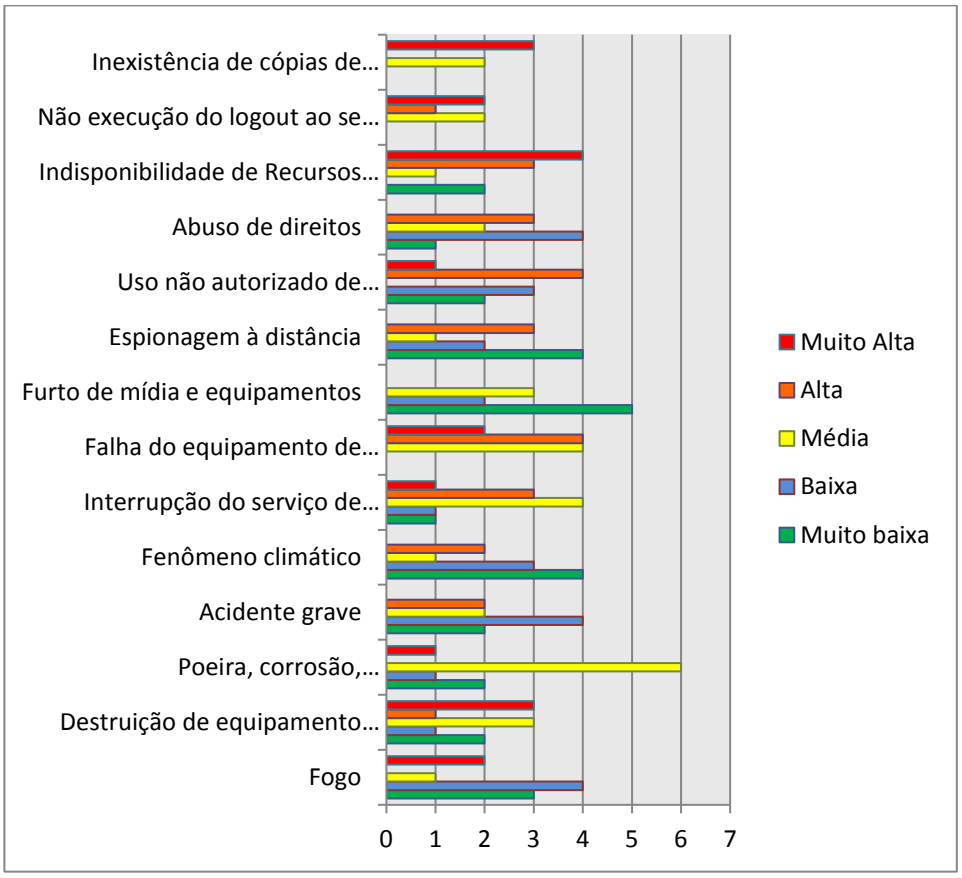


Gráfico 3 – Probabilidades de Ameaças ocorrerem.

Questões adotadas:

- Fogo
- Destruição de equipamento ou mídia
- Poeira, corrosão, congelamento
- Acidente grave
- Fenômeno climático
- Interrupção do serviço de energia
- Falha do equipamento de telecomunicação
- Furto de mídia e equipamentos

- Espionagem à distância
- Uso não autorizado de equipamento
- Abuso de direitos
- Indisponibilidade de Recursos Humanos
- Não execução do logout ao se deixar uma estação de trabalho desassistida
- Inexistência de cópias de segurança (backups)

Questão aberta proposta:

Na sua opinião, em relação à segurança da informação, qual (is) ponto (s) você destacaria que a Delegacia deve priorizar para eliminar o (s) risco (s) mais evidente (s) e por quê? (Na segurança da informação pode se destacar ambiente físico, eventos naturais, pessoal interno, ataques digitais, políticas de acesso, invasão de sistemas, políticas de backup, falta de execução de normas e procedimentos de segurança, etc.)

RESPOSTA 1- Falta de pessoal.
RESPOSTA 2- Investir em recursos humanos.
RESPOSTA 3- Criação de senhas e de políticas de backup.
RESPOSTA 4- Melhor informações aos usuários dos sistemas da delegacia regional!!!
RESPOSTA 5- Melhoria no sistema de cabeamento, formatação e análise periódica dos equipamentos por técnicos especializados!
RESPOSTA 6- Criar uma política de administração das máquinas e realizar backups periódicos.
RESPOSTA 7- Principalmente politicas de acesso e criação de backups.
RESPOSTA 8- Contratar mais pessoal e pessoal especializado.

ANEXO

RESOLUÇÃO Nº. 69, DE 17 DE SETEMBRO DE 2009

Institui a Política de Segurança da Informação no Governo do Estado de Minas Gerais no âmbito da Administração Pública Estadual.

A SECRETÁRIA DE ESTADO DE PLANEJAMENTO E GESTÃO, no uso da atribuição que lhe confere o 93, §1º, inciso III, da Constituição do Estado e o art. 16 do Decreto nº. 44.998, de 30 de dezembro de 2008, e considerando a necessidade de estabelecer diretrizes para uma Política de Segurança da Informação,

RESOLVE:

Art.1º Fica instituída a Política de Segurança da Informação do Estado de Minas Gerais, constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pelos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.

Art.2º A Política de Segurança da Informação se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública no âmbito dos órgãos e entidades da Administração Pública Estadual.

Art.3º Para efeitos desta Resolução se aplicam os seguintes conceitos:

I - segurança da Informação: conjunto de medidas para o estabelecimento de controles necessários à proteção das informações do Estado durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais visando à garantia da continuidade dos processos e serviços do Estado e a preservação de seus aspectos básicos, a saber: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

II- confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;

III- integridade: salvaguarda da exatidão e completeza da informação;

IV- disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes;

V- autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui;

VI- legalidade: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

VII- usuário: toda pessoa a qual se aplica a Política de Segurança da Informação do Estado de Minas Gerais.

Art.4º A Política de Segurança da Informação tem como diretrizes:

I - gestão de riscos: os órgãos e entidades do Governo do Estado de Minas Gerais devem adotar o modelo de gestão de riscos para o Sistema de Gestão de Segurança da Informação;

II - proteção da informação: as informações geradas, adquiridas, armazenadas, processadas, transmitidas e descartadas pelas unidades administrativas devem ter mecanismos de proteção adequados, de forma a resguardar sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

III - classificação da informação: as informações devem ser classificadas de forma a serem protegidas adequadamente;

IV - controle de acesso às informações: toda informação utilizada pelas unidades administrativas deve ter seu acesso controlado de acordo com a sua classificação;

V - educação em segurança da informação: os usuários devem ser instruídos a respeito da correta utilização das informações e dos recursos computacionais disponibilizados pelo Estado;

VI - responsabilidade pela segurança da informação: o usuário é responsável pela segurança das informações as quais tenha acesso;

VII - gestão de continuidade do negócio: os órgãos e entidades são responsáveis por elaborarem e manterem um plano de continuidade de negócios, de acordo com as suas necessidades, de forma a reduzir os impactos decorrentes da interrupção de serviços causada por desastres ou falhas da segurança.

§1º Os mecanismos de proteção devem estar em conformidade com a legislação vigente, com o Código de Conduta Ética do Servidor Público e da Alta Administração Estadual, e com a versão vigente da série 27000 da ISO.

§ 2º Até que seja estabelecida uma norma geral, as informações devem ser classificadas, em sigilosa, restrita e pública, por cada órgão ou entidade

responsável por sua salvaguarda, no âmbito de sua competência, de acordo com os termos previstos em Lei.

§ 3º As informações referentes aos cidadãos, que estejam sob a custódia do Estado, devem ter seus acessos controlados e restringidos, visando a garantir, assim, o direito individual e coletivo das pessoas, a inviolabilidade de sua intimidade e o sigilo de suas informações, nos termos previstos em Lei.

SS4º O usuário deve notificar à área responsável pela segurança da informação em casos de suspeita ou violação das regras ou em caso de falhas de Segurança da Informação.

Art.5º Para os fins deste Decreto compete:

I - ao Comitê de Tecnologia da Informação e Comunicação:

a) coordenar as ações necessárias para a implantação do Modelo de Gestão de Segurança da Informação;

b) avaliar periodicamente a Segurança da Informação, por meio da análise de indicadores;

II - à área responsável pela Segurança da Informação:

a) identificar necessidades específicas de Segurança da Informação e propor as implementações necessárias;

b) elaborar documentos necessários à Segurança da Informação;

c) elaborar e manter indicadores de Segurança da Informação;

d) elaborar, manter e implementar o plano de continuidade dos negócios;

e) elaborar programas de treinamento e de conscientização em Segurança da Informação;

f) analisar os incidentes de segurança da informação e recomendar as correções necessárias.

III - à Auditoria-Geral do Estado e às unidades setoriais e seccionais de auditoria compete zelar pelo cumprimento do disposto nesta Resolução.

Art.6º O usuário que não cumprir as normas estabelecidas nesta Resolução estará sujeito às penalidades previstas em Lei.

Art.7º Normas complementares a essa Resolução serão expedidas por meio de Resoluções da Secretaria de Estado de Planejamento e Gestão - Seplag.

Art.8º Esta Resolução entra em vigor na data de sua publicação.

Belo Horizonte, 17 de setembro de 2009

Renata Vilhena

Secretária de Estado de Planejamento e Gestão