NORMAS DE SEGURANÇA DA INFORMAÇÃO APLICADA A UM ÓRGÃO PÚBLICO

WAGNER SALAZAR PIRES: mestre em Ciência da Computação pela UFMG e Analista do Ministério Público de Minas Gerais. Suas áreas de interessem incluem Gerenciamento de Projetos, Direito Constitucional, Administrativo, Tributário e Contabilidade.

RESUMO: Não há uma norma única que atenda a todos os requisitos de um órgão público ou organização, assim, os assuntos abordados no trabalho, normas da família ISO/IEC 27000 (segurança da informação), devem ser utilizados em conjunto de forma complementar. O presente trabalho apresenta uma visão geral de algumas destas normas e faz uma relação da aplicação delas ao Ministério Público de Minas Gerais (MPMG).

Palavras-chaves: ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 e MPMG.

1 - INTRODUÇÃO

Informação, por si só, é um termo de difícil definição. Por sua complexidade, o assunto vem sendo abordado por estudiosos diversos. No século passado, a Ciência da Informação tomou para si tal responsabilidade, propondo uma abordagem abrangente que envolve tantas questões sociais quanto questões relacionadas a novas tecnologias. Por possuir esse perfil de considerar importantes questões de diversos ângulos, a Ciência da Informação tem se apresentado com um campo de pesquisa frutífero, cujos desafios são constantes [1].

Este século vem sendo marcado pela transição e por transformações profundas, com impactos extensos em todas as áreas. A criação e disseminação de novas tecnologias, com a multiplicação de redes interconectadas de computadores e fomento das mídias interativas, e consequente desenvolvimento de outras formas de transmissão de conteúdo, além dos livros, têm levado a novas experiências e formas de interação e aprendizagem e formação [2].

A Tecnologia da Informação (TI) evidencia-se pela contínua expansão e por uma forte concorrência entre empresas de todos os setores. Em virtude disso, para que essas entidades possam permanecer nesse meio, elas precisam desenvolver produtos e serviços que, de algum modo, se destaquem e conquistem a credibilidade de seus clientes [3]. Um ponto fundamental para atingir esse objetivo refere-se a segurança e governança da informação.

A informação encontra-se nos ativos que envolvem a organização e que têm valor para o seu negócio, desta forma a proteção desta informação deve ser feita tendo em conta estes ativos. Os ativos podem ser físicos (arquivos, bibliotecas, cofres que contém informação relevante), tecnológicos (recursos informáticos como sistemas de informação, e-mails, intranets) e humanos (pessoas que fazem parte das atividades das organizações). Acerca desse posicionamento, SOLMS, em [3], observa-se que:

> “A segurança da informação é estruturada e organizada dentro da empresa. A importância desta dimensão está no fato de focar os vários tipos de melhores práticas para gestão da Segurança da Informação no qual cada estágio é vinculado a um propósito da estrutura organizacional, incluindo algum tipo de fórum sobre segurança informacional que é essencial para o bom andamento das implementações. Esta dimensão não se refere somente aos aspectos da estrutura organizacional, mas também aos aspectos da segurança da informação voltados para as responsabilidades no trabalho, a comunicação com relação às regras de segurança e ao envolvimento dos gestores com a segurança da informação”.

A Segurança da Informação (SI) consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade), é confiável (integridade) e autêntica (autenticidade). Já a Gestão de Segurança de Informação (GSI) busca o alinhamento entre as necessidades organizacionais de segurança e o gerenciamento dos sistemas de informação, não apenas no que concerne ao emprego de tecnologias, mas com ênfase em aspectos de risco, política organizacional, processos e métodos de gestão aplicáveis ao desenvolvimento, operação e manutenção de sistemas. Essa ideia foi desenvolvida de modo a se tornar o padrão global de SI: o conjunto de normas da família ISO/IEC 27000.

Desta forma, o decorrer do artigo realiza um estudo das normas da família ISO/IEC 27000 e descreve a aplicação destes conceitos apresentados no Ministério Público de Minas Gerais. O Ministério Público é uma instituição permanente, essencial à função jurisdicional do estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis.

2 - NORMAS REFERENTES À SEGURANÇA DA INFORMAÇÃO

Atualmente, a Informação assume-se como um dos principais ativos das organizações. Diariamente é originado um grande volume de informação que convém que seja tratada de forma conveniente, consoante o valor que representa para a organização. Assim sendo, a Segurança da Informação assume cada vez mais um papel preponderante no sucesso das organizações. Saber quanto e como investir em segurança é o desafio que se coloca às empresas nos dias de hoje.

A ISO/IEC 27000 também conhecida como família de normas ISO 27000 é uma série de padrões relacionados à temática de Segurança da Informação. A série oferece melhores práticas e recomendações sobre a gestão da informação, riscos e controles dentro do contexto de uma estratégia global do SGSI.

A série possui deliberadamente um escopo amplo, que abrange mais do que apenas a autenticidade, confidencialidade, disponibilidade ou questões de segurança técnica. É aplicável a organizações de todos os tamanhos e feitios. Todas as organizações são incentivadas a avaliar os seus riscos de segurança da informação, em seguida, implementar controles de segurança apropriados de acordo com as suas necessidades, usando orientações e sugestões quando aplicado.

As normas da família ISO 27000 utilizam fortemente o ciclo de Planejamento, Execução, Controle e Ação (PDCA da sigla em inglês), idealizado por Shewhart e mais tarde aplicado por Deming [4]. A Figura 1 ilustra esse ciclo que é composto por um conjunto de ações em sequência, dada pela ordem estabelecida pelas letras que

compõem a sigla: P (*plan*: *planejar*), D (*do*: fazer, executar), C (*check*: verificar, controlar), e finalmente o A (*act*: agir, atuar corretivamente).

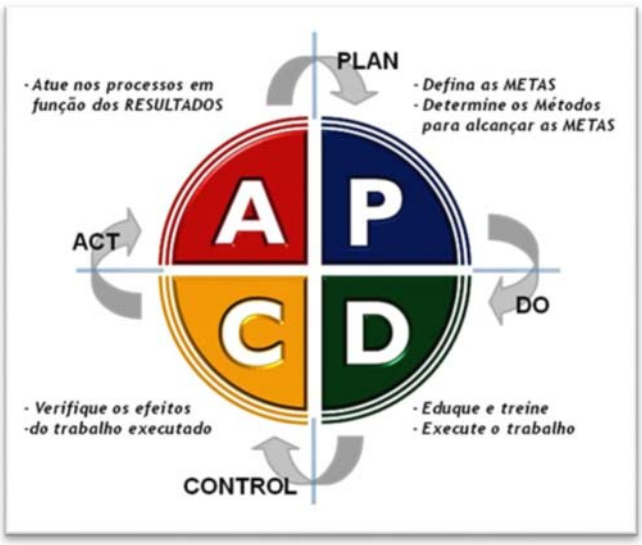

Figura 1 - Ciclo PDCA

Com relação as normas que fazem parte do escopo do presente trabalho, a série ISO 27000 constitui um padrão de certificação de sistemas de gestão promovido pelo *International Organization for Standardization* (ISO), neste caso aplica-se à implementação de Sistemas de Gestão de Segurança da Informação (SGSI), através do estabelecimento de uma política de segurança, de controlos adequados e da gestão de riscos. No decorrer desta seção é apresentado as normas ISO/IEC 2700, ISO/IEC 2701, ISO/IEC 2702 e ISO/IEC 2705.

Existem outras normas na série ISO 27000, como a ISO/IEC 27003 que contém um conjunto de diretrizes para a implementação do SGSI, ISO/IEC 27004 que define métricas de medição para a gestão da segurança da informação, dentre outras que fogem ao escopo do trabalho proposto.

2.1 - ISO/IEC 27000

A ISO/IEC 2700 apresenta uma série de termos e definições que são utilizados pelas demais normas da família 27000 [5]. Assim, nessa norma é definido um vocabulário comum para evitar diferentes interpretações de conceitos técnicos e de gestão. Devido a importância desse vocabulário, destaca-se alguns termos:

Controlo de acesso – meios para assegurar que o acesso a ativos está autorizado e restringido com base no trabalho e em requisitos de segurança;

Responsabilidade – responsabilidade de uma entidade pelas suas ações e decisões;

Ativos – qualquer coisa que tenha valor para a organização (informação, software, o próprio computador, serviços, as pessoas, entre outros);

Atacar – tentar destruir, alterar, expor, inutilizar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo;

Autenticação – prestação de garantia de que uma característica reclamada por uma entidade é correta;

Autenticidade – propriedade que nos diz que uma entidade é aquilo que realmente afirma ser;

Disponibilidade – propriedade de ser acessível e utilizável por uma entidade autorizada;

Confidencialidade – propriedade que garante que a informação não está disponível ou revelada a indivíduos não autorizados, entidades ou processos;

Controlar – meio de gestão de risco, incluindo as políticas de procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou de natureza legal;

Ação corretiva – ação para eliminar a causa de uma não conformidade detectada ou outra situação indesejável;

Diretriz – recomendação do que é esperado que seja feito a fim de alcançar um objetivo;

Segurança da Informação – preservação da confidencialidade, integridade e disponibilidade das informações;

Sistema de Gestão de Segurança de Informação – parte do sistema de gestão global, com base numa abordagem de risco de negócio, para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação;

Risco de Segurança da Informação – potencial que uma ameaça explore uma vulnerabilidade de um ativo ou grupo de ativos e, assim, cause danos à organização;

Integridade – propriedade de proteger a exatidão de ativos;

Sistema de Gestão – âmbito das políticas, procedimentos, diretrizes e recursos associados para alcançar os objetivos de uma organização;

Política – intenção e direção geral como formalmente expressas pela gestão;

Processo – conjunto de atividades inter-relacionadas ou interativas que transformam insumos em produtos;

Risco - combinação da probabilidade de um evento e das suas consequências;

Evento – ocorrência de um determinado conjunto de circunstâncias;

Análise de risco – uso sistemático de informações para identificar fontes e estimar a ocorrência de um risco;

Gestão de risco – atividades coordenadas para dirigir e controlar uma organização em relação a um determinado risco;

Ameaça – causa potencial de um incidente indesejado, o que pode resultar em danos para um sistema ou entidade;

Vulnerabilidade – fraqueza de um ativo ou controle, que pode ser explorada por ameaça.

2.2 - ISO/IEC 27001

O padrão mais conhecido na família é o ISO/IEC 27001 que fornece requisitos para um SGSI. Foi a primeira da série ISO 27XXX, publicada pela *International Organization for Standardization* (ISO) em outubro de 2005 e substituiu a norma BS 7799-2 para certificação de SGSI. A ISO 27001 apresenta conceitos de alto nível, e por essa razão, possibilita as organizações estabelecerem seus critérios específicos de auditoria de gestão [6].

As atividades demandadas na área de segurança da informação vêm sendo amplamente discutidas no setor de TI. A adoção de um SGSI é uma decisão estratégica para uma organização. A norma ISO/IEC 27001:2013 foi preparada para prover um modelo de processos para implementar, manter e melhorar o SGSI de uma organização. Esta norma define 114 controles agrupados em 14 domínios, que são enumerados a seguir:

1. Políticas de segurança da informação
2. Organização de segurança da informação
3. Segurança na gestão de recursos humanos
4. Gestão de ativos
5. Controle de acesso
6. Criptografia
7. Segurança física e ambiental
8. Segurança de operações
9. Segurança de comunicações
10. Aquisição, desenvolvimento e manutenção de sistemas
11. Relações com fornecedores
12. Gestão de incidentes de segurança da informação
13. Aspectos de segurança da informação na gestão da continuidade do negócio
14. Conformidade

A norma ISO/IEC 27002 traz, praticamente, estes mesmos conceitos, porém com um nível de detalhamento maior. Assim, neste artigo, optou-se por explicá-los na Seção 2.3. A norma ISO/IEC 27001 também contém um conjunto de cláusulas relativas à definição de regras e requisitos de cumprimento, a saber:

- **Contexto da organização**: a organização deve determinar as questões internas e externas que são relevantes para o SGSI.
- **Liderança**: a alta direção deve demonstrar sua liderança e comprometimento em relação ao SGSI.
- **Planejamento**: a organização deve planejar ações para contemplar riscos e oportunidades.
- **Apoio**: a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI.
- **Operação**: a organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos de segurança da informação e à avaliação e tratamento dos riscos.
- **Avaliação de desempenho**: a organização deve avaliar o desempenho da segurança da informação e a eficácia do SGSI, monitorando, medindo, analisando e realizando auditoria interna.
- **Melhoria**: a organização deve reagir à não conformidade e melhorar continuamente a eficácia do SGSI.

É importante salientar que embora a norma ISO/IEC 27001:2013 seja a referência mais completa sobre as demandas de segurança da informação no setor de TI, ela precisa ser adaptada aos objetivos da instituição, aos seus requisitos de segurança, processos, empregados, tamanho e estrutura.

A Figura 2, extraída de [7], ilustra o mapeamento entre o ciclo PDCA e os objetivos da normal hora em comento.

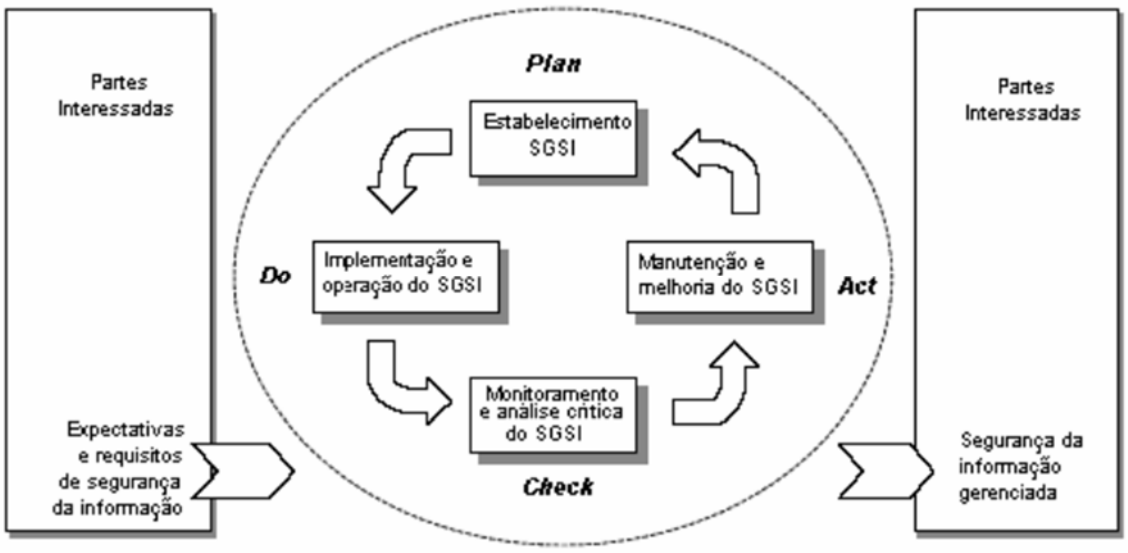

Figura 2 - Ciclo PDCA e a norma ISO/IEC 27001

Plan (Planejar) (estabelecer o SGSI): Estabelecer política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação para entregar resultados conforme as políticas globais de uma organização e objetivos.

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

Check (Checar) (monitorar e revisar o SGSI): Avaliar e, onde aplicável, medir o desempenho de um processo contra a política do SGSI, objetivos e experiência prática e relatar os resultados para a gerência para revisão.

Act (Agir) (manter e melhorar o SGSI): Tomar as ações corretivas e preventivas, baseado nos resultados da auditoria interna do SGSI e revisão gerencial ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

2.3 - ISO/IEC 27002

Com origem no governo britânico, a norma BS7799 é a base para a norma ISO/IEC 17799 que veio a tornar-se ISO/IEC 27002. O Código de Boas Práticas ISO/IEC 27002 fornece uma estrutura para avaliar os sistemas de gestão de segurança da informação baseada em um conjunto de diretrizes e princípios que têm sido adotadas por empresas, governos e organizações empresariais em todo o mundo [8].

Em [1] é destacado que o *framework* de controles ISO permite aos profissionais de segurança da informação ter uma abordagem consistente e metódica, ao avaliar os processos de segurança nas organizações, infraestrutura de tecnologia, ou processos.

Os benefícios da segurança da informação estão na prevenção de perdas financeiras que a empresa pode ter, no caso da ocorrência de riscos de segurança da informação. Para que um sistema de informação seja considerado seguro, deve atender a quatro características:

- Integridade – A informação só poderá ser modificada por quem está autorizado e de maneira controlada;
- Confidencialidade – A informação só deverá estar disponível para quem está autorizado;
- Disponibilidade – A informação deverá estar disponível quando for necessária;
- Não repúdio – O uso ou modificação da informação por parte de uma pessoa autorizada deve ser irrefutável, ou seja, a pessoa não poderá negar a ação.

A norma ISO/IEC 27002 está estruturada em 14 seções, sendo que cada uma dessas é constituída por categorias de segurança da informação, e cada categoria tem um objetivo de controle definido, um ou mais controles que podem ser aplicados para atender ao objetivo de controle, as descrições dos controles, as diretrizes de implementação e informações adicionais.

Política de segurança da informação: o objetivo é fornecer orientação e apoio às ações da gestão de segurança da informação sobre os requisitos de negócios e as leis e regulamentos pertinentes. A gerência deve estabelecer uma política clara e de acordo com os objetivos do negócio e demonstrar seu apoio e comprometimento com a segurança da informação através da publicação e manutenção de uma política segurança da informação para toda a organização.

Organização da segurança da informação: deve estabelecer uma estrutura de gestão a fim de iniciar e monitorar a implementação da segurança da informação dentro da organização. A administração deve adotar a política de segurança da informação, atribuir funções de segurança e de coordenação, bem como fiscalizar a execução da política de segurança em toda a organização. Se necessário, a organização deve estabelecer e facilitar o acesso às fontes de referência especializadas para garantir a atualização dos envolvidos sobre as tendências do setor, a evolução das normas e métodos de avaliação, e fornecer as ferramentas adequadas para a manipulação de resultados segurança. Seu objetivo deve ser a promoção de uma abordagem multidisciplinar para a segurança da informação, que, por exemplo, envolva a cooperação e colaboração dos gestores, usuários, administradores, designers de aplicação, auditores e especialistas em segurança da informação, em áreas como gestão segurança e de riscos.

Gestão de ativos tem por objetivo: alcançar e manter uma política de proteção adequada para os ativos da organização. Para que isso seja possível, devem ser identificados os proprietários para todos os ativos e atribuir a responsabilidade pela manutenção de controles adequados. A implementação de controles específicos pode ser delegada pelo proprietário caso seja conveniente. No entanto, o proprietário continua responsável pela proteção adequada dos ativos. O termo “proprietário” identifica um indivíduo ou entidade responsável, com a aprovação dos mecanismos de direção, para controlar a produção, desenvolvimento, manutenção, utilização e segurança de ativos.

Segurança em recursos humanos: o objetivo é garantir que os funcionários, fornecedores e usuários de terceiros entendam suas responsabilidades, e esteja apto a desempenhar suas funções, além de reduzir o risco de roubo, fraude e mau uso de recursos. As responsabilidades de segurança devem ser definidas antes da contratação, com a descrição adequada do trabalho e suas condições. Todos os funcionários, prestadores e usuários de terceiros devem ser selecionados adequadamente, especialmente para trabalhos sensíveis com acesso a informações. Funcionários, fornecedores e usuários de prestadores de serviços de processamento de informações devem assinar um acordo sobre seus papéis e responsabilidades relacionadas com a segurança.

Controle de acesso: deve gerir o acesso à informação, recursos e processos de negócios com base nas necessidades de segurança e do negócio da organização. A regulamentação para as políticas de controle de acesso deve considerar a distribuição das informações e autorizações, devendo para isso, estabelecer procedimentos para atribuição de permissões de acesso aos sistemas e informações.

Criptografia: o objetivo é assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação. Assim, deve ser desenvolvida e implementada uma política para uso de controles criptográficos para a proteção da informação.

Segurança física e de ambiente: o objetivo é impedir o acesso físico não autorizado, dano ou interferência nas instalações e informações da organização. Os serviços de processamento de informações sensíveis devem ser realizados em áreas seguras e protegidas, em um perímetro de segurança definido por barreiras e controles de entrada adequada. Estas áreas devem ser fisicamente protegidas contra acesso não autorizado, danos e interferências. A proteção fornecida deve ser proporcional aos riscos identificados. Para evitar a perda, dano, roubo ou comprometimento de ativos e interrupção das atividades da organização, os equipamentos devem ser protegidos contra ameaças físicas e ambientais. A proteção dos equipamentos é necessária para reduzir o risco de acesso não autorizado à informação e à proteção contra perda ou roubo. Da mesma forma, deve-se a considerar controles especiais para proteção contra ameaças contra estruturas físicas e a garantia de serviços como eletricidade e infraestrutura local.

Segurança das Operações: deve ser garantido a operação segura e correta dos recursos de processamento da informação. Os procedimentos de operação devem ser documento e disponibilizados para todos os usuários que necessitam deles.

Segurança nas comunicações: o objetivo é assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam. As redes devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

Aquisição, desenvolvimento e manutenção de sistemas de informação: deve garantir que a segurança é parte integral dos sistemas de informação. Os sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócio, aplicações de uso geral, serviços e aplicações desenvolvidas pelos usuários. A concepção e implementação de sistemas de informação que dão apoio aos processos de negócio das empresas podem ser cruciais para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação. Todos os requisitos de segurança devem

ser identificados na fase de levantamento de requisitos de um projeto e ser justificados, documentados e aceitos como parte de todo o processo para um sistema de informação.

Relacionamento com Fornecedor: o objetivo é garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.

Gerenciamento de incidentes de segurança da informação: deve garantir que os eventos e falhas de segurança associados aos sistemas de informação sejam identificados e comunicados o mais breve possível, permitindo assim a elaboração de medidas corretivas oportunas. Todos os funcionários, fornecedores e terceiros devem estar cientes dos procedimentos de comunicação de diferentes tipos de eventos e pontos fracos que possam ter impacto sobre a segurança dos ativos organizacionais.

Aspectos da segurança da informação na gestão da continuidade do negócio: a continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização.

Conformidade legal: tem por objetivo, evitar a violação de qualquer lei, estatuto, regulamento ou obrigações contratuais e de quaisquer requisitos de segurança. A concepção, funcionamento, utilização e gestão dos sistemas de informação podem estar sujeitos a requisitos legais, de segurança regulamentares e contratuais. Os requisitos legais específicos devem ser aconselhados por um advogado da organização ou profissionais qualificados.

2.4 - ISO/IEC 27005

A norma ISO/IEC 27005 foi publicada em junho de 2008 e apresenta as diretrizes para o gerenciamento dos riscos de segurança da informação. Utiliza diversos conceitos da norma ISO/IEC 27000, já descritos no início deste capítulo. Esta norma descreve todo o processo necessário para a gestão de riscos de segurança da informação e as atividades necessárias para a perfeita execução da gestão [9]. Apresenta práticas para gestão de riscos da segurança da informação. As técnicas nela descritas seguem o conceito, modelos e processos globais especificados na norma ISO/IEC 27001, descrita na Seção 2.2, além de apresentar a metodologia e avaliação e tratamento dos riscos requeridos pela mesma norma.

De acordo com a norma, o processo de gestão de riscos de segurança da informação é composto pelas atividades mostradas na Figura 3.

Definição do contexto: define o escopo e os limites que serão levados em consideração na gestão de riscos. Deverão ser descritos os processos que fazem parte do escopo, garantindo a identificação dos ativos relevantes para a gestão dos riscos. Além disso, a definição do contexto inclui determinar os critérios gerais de aceitação dos riscos para a organização e as responsabilidades para a gestão de riscos.

A atividade de Análise/Avaliação de Riscos é subdividida em outras três atividades: Identificação de riscos; Estimativa de riscos; e Avaliação de riscos. **Identificação de riscos**: identifica os eventos que possam ter impacto negativo nos negócios da organização. Devem ser identificados os ativos, suas vulnerabilidades e as ameaças que podem causar danos aos ativos. Identifica as consequências que as perdas de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos. **Estimativa de riscos**: atribui valor ao impacto que um risco pode ter e a probabilidade de sua ocorrência, de forma qualitativa ou quantitativa. Estimar o risco

através da combinação entre a probabilidade de um cenário de incidente e suas consequências. **Avaliação de riscos**: determina a prioridade de cada risco por meio de uma comparação entre o nível estimado do risco e o nível aceitável estabelecido pela organização. O ponto de decisão 1, visto na Figura 3, verifica se a avaliação dos riscos foi satisfatória, conforme os critérios estabelecidos pela organização. Caso não seja satisfatória, a atividade pode ser reiniciada de forma que se possa revisar, aprofundar e detalhar ainda mais a avaliação, assegurando que os riscos possam ser adequadamente avaliados.

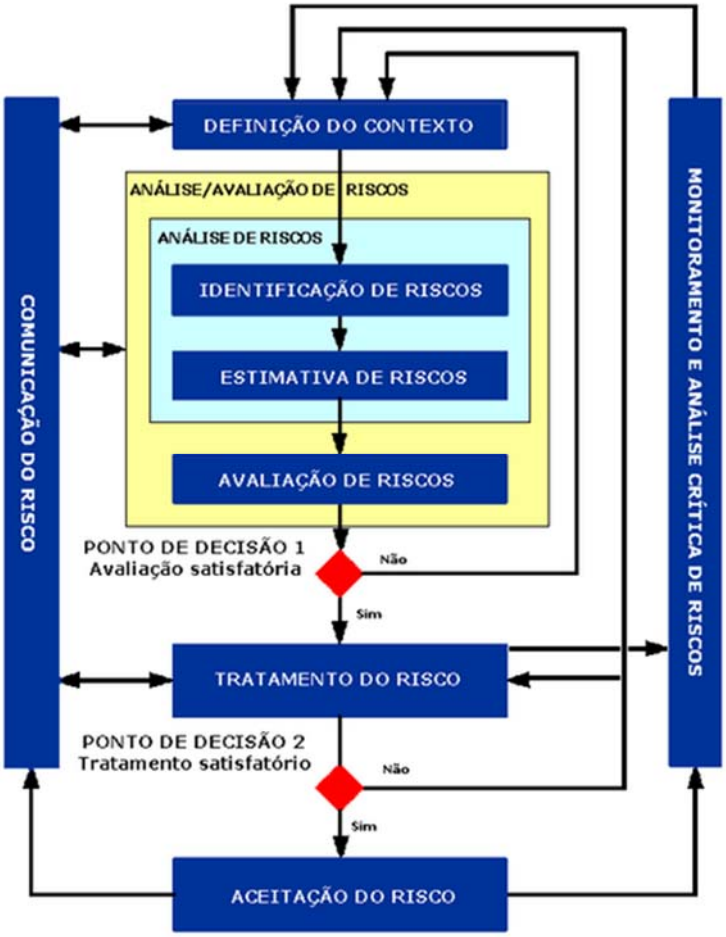

Figura 3 - Processo de gestão de riscos em segurança da informação

Tratamento do risco: implementa controles para reduzir, reter, evitar ou transferir os riscos. Se o tratamento do risco não for satisfatório, ou seja, não resultar em um nível de risco residual que seja aceitável, deve-se iniciar novamente a atividade ou o processo até que os riscos residuais sejam explicitamente aceitos pelos gestores da organização.

Aceitação do risco: registrar formalmente a aprovação dos planos de tratamento do risco e os riscos residuais resultantes, juntamente com a responsabilidade pela decisão.

Comunicação do risco: desenvolve planos de comunicação dos riscos para assegurar que todos tenham consciência sobre os riscos e controles a serem adotados.

Monitoramento e análise crítica de riscos: monitora continuamente os riscos e seus fatores a fim de identificar eventuais mudanças no contexto. Certifica que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriados nas circunstâncias presentes.

A norma ISO/IEC 27005 não inclui uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a cada organização definir a melhor abordagem conforme o contexto na qual está inserida.

3 - SEGURANÇA DA INFORMAÇÃO NO MINISTÉRIO PÚBLICO DE MINAS GERAIS

Segundo o relatório técnico [10], realizou-se uma análise sintetizada com o objetivo verificar falhas e acertos na gestão da segurança da informação no MP. A Tabela 1, extraída de [10], apresenta a análise de todas as respostas obtidas para cada um dos domínios da norma ISO 27001. Esta tabela é composta dos domínios da norma, do conjunto das perguntas efetuadas no levantamento, do cálculo de respostas positivas e do indicador da situação, apresentado nas cores verde (se o conjunto das respostas for acima de 50%), vermelho (se o conjunto das respostas for abaixo de 50%) e amarelo (se o conjunto das respostas for igual a 50%).

Domínio segurança da informação conforme ISO 27001:2013	Perguntas do levantamento	Respostas positivas	Situação: verde: >50% positiva vermelha: <50%positiva amarelo:=50%
1-Políticas de segurança da informação	9,10,17,18,19	43%	
2-Organização de segurança da informação	11,15,16,46,49-1,49-2,49-3,49-4,49-5	33%	
3-Segurança na gestão de recursos humanos	13,14	29%	
4-Gestão de ativos	25,26,27,30	68%	
5-Controle de acesso	48-2,48-3,48-4,48-5,48-6,48-10	79%	
6-Criptografia	45	61%	
7-Segurança física e ambiental	33, 34, 35, 36, 37, 38, 51-4	81%	
8- Segurança de operações	29,31,32,39,40,48-1,48-5,48-8,48-9, 51-1,51-2,51-3,51-5	65%	
9-Segurança de comunicações	50-1,50-3,50-4,50-5,50-6,50-7	79%	
10-Aquisição, desenvolvimento e manutenção de sistemas	28,48-11	33%	
11-Relação com fornecedores	20	47%	
12-Gestão de incidentes de segurança da informação	41,43,48-7	30%	
13-Aspectos de segurança da informação na gestão da continuidade de negócios	22,23,24,47	19%	
14-Conformidade	21,44	50%	

Tabela 1 - Situação geral da segurança da informação conforme domínios da norma ISO/IEC 27001.

Percebe-se pela Tabela 1, que de forma geral o MP apresenta uma boa gestão da segurança da informação nos domínios associados às questões operacionais e ambientais tais como a gestão dos ativos, a segurança nas operações e nas comunicações e a segurança física.

No entanto, o MP não apresenta uma boa gestão da segurança da informação nos domínios relacionados à definição de políticas e procedimentos de segurança da informação, gestão dos recursos humanos, gestão de incidentes, gestão de continuidade de negócios e conformidade com requisitos legais e contratuais.

Tais constatações confirmam que mesmo não havendo uma equipe dedicada à segurança da informação, as atividades operacionais são razoavelmente bem executadas com a equipe existente. Porém, as questões procedimentais e reguladoras ficam prejudicadas e apontam a necessidade de ações para melhorias neste campo.

A Figura 4, também extraída de [10], apresenta uma visualização das principais ferramentas de segurança implantadas. Com uma alta porcentagem, destaca-se a implantação de *firewall*, sistemas de antivírus em *desktops*, gerenciamento de autenticação e controle de acesso de rede. Com uma baixa porcentagem, destaca-se a implantação de sistemas de *data loss prevention*, análise de vulnerabilidade, sistema de revisão de código e sistema de monitoramento de eventos e incidentes.

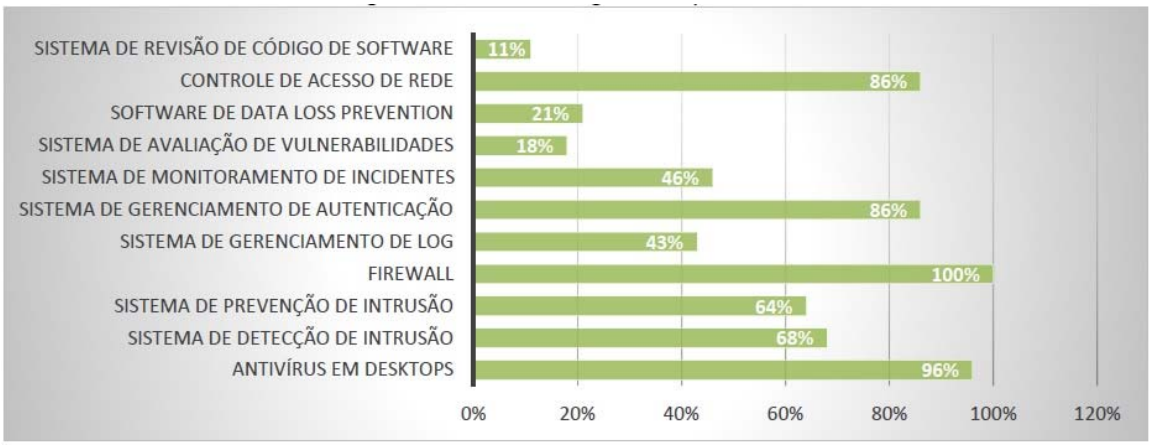

Figura 4 - Situação geral da segurança da informação conforme domínios da norma ISO/IEC 27001

4 – CONCLUSÕES

O mundo nunca mais foi o mesmo após o surgimento dos computadores e após a evolução da Internet. No mundo atual globalizado, a Internet presta um importante serviço, contribuindo para agilizar ainda mais este processo de globalização. As organizações, habituadas cada vez mais a esta realidade digital, passam a depender dela de forma vital. A informação passa a ser considerada um ativo das empresas, um patrimônio.

Neste prisma, percebe-se a importância da Segurança da Informação para um órgão público. A proteção de seus dados a qualquer custo sob pena de grandes prejuízos é um tema atual. Seguindo esta tendência, surgem tecnologias que prometem elevado nível de segurança e proteção, e a cada dia as organizações se conscientizam

mais e mais da importância e necessidade de protegerem seus dados. Isto justifica a atual preocupação do MPMG com a segurança da informação.

Segundo [10], as principais dificuldades encontradas na gestão de segurança da informação do MPMG estão relacionadas à governança da segurança nos seus aspectos de política, organização, gestão de recursos humanos, manutenção de sistemas, relação com fornecedores, continuidade de negócios, gestão de incidentes e conformidade. A proposta de quantitativo de pessoas para execução das atividades de segurança não englobam as questões operacionais, uma vez que não é apenas a equipe da área de segurança que zela pela informação na instituição. O gerenciamento operacional diário, a gestão das comunicações, a segurança física, o controle de acesso, a gestão dos ativos foi bem avaliados no levantamento, o que corrobora esta afirmação.

REFERÊNCIAS

[1] – Luciana Emirena dos Santos Carneiro. Gestão da Informação e do Conhecimento no âmbito das práticas de segurança da Informação: Pessoas, Processos e Tecnologia. Belo Horizonte - MG, Brasil, 2012.

[2] – M. Silva, Educação online. 2. Ed, São Paulo: Edições Loyola, 2006.

[3] – Paula Geralda B. C., Ambiente de Aprendizado para Educação em Gerenciamento de Projetos, Universidade Federal de Pernambuco, 2005.

[4] – Fernandes, A.A. e Abreu, V.F., Implantando a Governança de TI – da Estratégia à Gestão dos Processos de Serviços, 3 Ed, ISBN: 9788574524863.

[5] – Diana Luísa Rocha Santos e Rita Maria Santos Silva, Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001, Faculdade de Engenharia da Universidade do Porto, Porto, Portugal,2012.

[6] – Jon Hall, Frameworks for IT Management, ISO 27001 - Information Security Management Systems, Zaltbommel, Netherlands, 2006.

[7] – Humphreys e Edward. Implementing the ISO/IEC 27001 Information Security Management System Standard, Artech House, Inc., Norwood, MA, USA, 2007.

[8] – Alexandre Cavalcante Alencar, COBIT, ITIL e ISO/IEC 27002 Melhores Práticas para Governança de Tecnologia da Informação,
Faculdade Lourenço Filho, Fortaleza - CE, Brasil, 2010.

[9] – Edson Kowask Bezerra, Gestão de Riscos de TI NBR 27005, Escola Superior de Redes – RNP, Rio de Janeiro - RJ, Brasil, 2013.

[10] – Daniel Silva Carnevalli e Lilian Noronha Nassif, Análise da demanda de serviços e do quantitativo de pessoal no Ministério Público para a área de segurança da informação, Departamento de Informática - MPMG, Belo Horizonte/MG, Brasil, 2015.