Eduardo de Oliveira Vasconcelos

GESTÃO DA SEGURANÇA DA INFORMAÇÃO NO SERVIÇO PÚBLICO ESTADUAL DE MINAS GERAIS: estudo de caso em um órgão estatal de pesquisa

Belo Horizonte
2017

Eduardo de Oliveira Vasconcelos

GESTÃO DA SEGURANÇA DA INFORMAÇÃO NO SERVIÇO PÚBLICO ESTADUAL DE MINAS GERAIS: estudo de caso em um órgão estatal de pesquisa

Monografia apresentada ao curso de Especialização em Administração Pública, Planejamento e Gestão Governamental da Fundação João Pinheiro, como requisito parcial para a obtenção do título de especialista.

Orientador: Max Melquiades da Silva

Belo Horizonte
2017

Eduardo de Oliveira Vasconcelos

Gestão da segurança da informação no serviço público estadual de Minas Gerais

Monografia apresentada à Escola de Governo Professor Paulo Neves de Carvalho da Fundação João Pinheiro como requisito para obtenção do título de Especialista *lato sensu* em Administração Pública, Planejamento e Gestão Governamental.

Banca Examinadora

_____

Prof. Max Melquíades da Silva. Orientador

_____

Prof.ª Marconi Laia

Belo Horizonte, 06 de junho de 2017.

RESUMO

A Tecnologia da Informação tornou-se fundamental para a desenvolvimento e melhora na prestação de serviços públicos. A Tecnologia da Informação aperfeiçoou os processos administrativos, diminuiu a burocracia e aumentou a transparência e controle social dos serviços ofertados e por esses motivos as organizações que utilizam a Tecnologia da Informação precisam proteger suas informações de ameaças que possam comprometer ou interromper os serviços prestados à Sociedade Neste contexto, insere-se a Segurança da Informação que objetiva minimizar os riscos provenientes destas ameaças através de um Sistema de Gestão da Segurança da Informação e prover a continuidade dos serviços. Diante da relevância do assunto, o trabalho propôs como objetivo principal analisar o Sistema de Gestão da Segurança da Informação de uma organização pública. Objetivos específicos como análise das políticas de segurança da informação, avaliação da gestão de riscos, avaliação do comprometimento dos usuários finais e da alta direção, efetividade do Sistema de Gestão de Segurança da Informação do órgão e alinhamento às normas referência no assunto também serão abordados no estudo. Para o atingimento destes objetivos, foi feita uma entrevista com o gestor da Tecnologia da Informação da instituição e aplicado um questionário aos servidores utilizadores de sistemas informatizados e microcomputadores no órgão. O estudo revelou que devido à particularidade do órgão, as normas utilizadas não foram criadas especialmente para a tratarem o assunto: Segurança da Informação. Apesar disto, a organização possui um ótimo nível de Segurança da Informação devido aos controles (políticas) implementados.

Palavras chave: Tecnologia da Informação, Segurança da Informação, Políticas de Segurança da Informação, Gestão de Riscos da Tecnologia da Informação.

ABSTRACT

Information Technology has become fundamental for development and improvement in the provision of public services. Information Technology improves administrative processes, diminishes bureaucracy and increases the transparency and social control of third party services and their elements as organizations that use Information Technology and protect their information from threats that compromise or disrupt services provided to the Company In this context, it includes an Information Security that aims to minimize risks through threats through an Information Security Management System and provide a continuity of services. Given the relevance of the work, the main objective of the paper is to analyze the Information Security Management System of a public organization. Specific objectives such as information security policy analysis, risk management evaluation, end-user and senior management commitment assessment, effectiveness of the organization's Information Security Management System, and alignment of standards. For the accomplishment of the objectives, an interview with the manager of the Information Technology of the institution was carried out and a questionnaire was applied to the users of the computerized systems and microcomputers in the organ. The study revealed that, due to the particularity of the body, the standards were not specially created for this purpose: Information Security. Despite this, an organization has an optimal level of information security of the implemented controls.

Keywords: Information Technology, Information Security, Information Security Policies, Information Technology Risk Management.

AGRADECIMENTOS

Agradeço a minha mãe, que além de mãe é amiga, irmã mais velha, ouvinte, psicóloga e, muitas vezes, pai. Ela é a minha orientadora na vida. Ela é a responsável por todo o meu esforço e dedicação. Ensinou-me a trilhar os caminhos corretos na vida e sem ela, eu nada seria. Poderia escrever um livro com agradecimentos e mesmo assim as palavras ali contidas não seriam o bastante.

Em especial, agradeço ao meu orientador Professor Me. Max Melquíades ou simplesmente Max, por sua sensatez, serenidade, incentivo e objetividade na condução das orientações. Ele foi o responsável por me mostrar os caminhos a trilhar, os quais muitas vezes por minha inexperiência se mostraram inextricáveis e desafiadores. Sem ele, este trabalho não estaria concluído.

“O insucesso é apenas uma oportunidade para recomeçar com mais inteligência.”
Henry Ford

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANVISA	Agência Nacional de Vigilância Sanitária
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infraestructure Library*
OMS	Organização Mundial da Saúde
ONA	Organização Nacional de Auditoria
SGSI	Sistemas de Gestão da Segurança da Informação
SI	Sistema da Informação
SIC	Segurança da Informação e Comunicação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

O dinamismo nas negociações advindo da informatização dos processos organizacionais na sociedade contemporânea modificou diversos paradigmas e as empresas que acompanharam essa evolução digital notaram que a informação se transformou em um importante recurso e ativo estratégico. O ponto focal a ser observado é reconhecer que a informação e processos, redes e pessoas estão relacionadas e são importantes para alcançar os objetivos da organização. Em virtude disto, a informação tem recebido atenção especial das organizações, pois em um ambiente altamente competitivo, ela se transformou no elemento motriz capaz de ditar o sucesso ou fracasso nos negócios.

Hoje a Tecnologia da Informação (TI) está difundida e encrostada em todos os aspectos de negócios empresariais, internos ou externos, além de estar presente nos diversos setores da atividade econômica. As organizações têm assistido cada vez mais a tramitação de suas informações por meio de sistemas informatizados e grande parte desses sistemas utilizam algum meio tecnológico de propagação, e geralmente, este meio se encontra interconectado com outros diversos sistemas destas mesmas corporações.

Diante do contexto em que está inserida a informação, é notadamente observado a necessidade de sua proteção em todas as etapas do seu ciclo de vida, o que envolve: geração, exibição, manutenção, tutela, transformação, atualização, destruição, entre outras. Além disso, a informação deve possuir a natureza agregadora conforme elencado anteriormente e por isso, ela necessita de alta qualidade pois sua falta pode incorrer em decisões que possam gerar prejuízos às organizações.

Para tal, atualmente no mercado, existem diversas ferramentas (Normas técnicas, *frameworks*[1], bibliotecas, manuais, cartilhas, *softwares*, Leis) abertas ou proprietárias disponíveis, que utilizam técnicas para proteger a informação, desmembra-la em categorias onde seu tratamento poderá receber o nível cuidado esperado e, em

[1] É um conjunto de objetos que colaboram para realizar um conjunto de responsabilidades para um domínio de subsistema de aplicativos.

alguns casos, auxiliar através de controles no tratamento contra uma interrupção causada por um problema ou incidente.

O arcabouço constante no campo da Segurança da Informação e Comunicação (SIC) será a responsável por fundamentar as diretrizes constantes neste trabalho. Devido a isso, a definição de segurança da informação se torna necessária e apesar da publicação ser antiga, datada em 16/04/2000, definição publicada no *Diário Oficial da União* tem seu conteúdo completo e de fácil entendimento:

> [...] proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (DOU, 2000)

O serviço Público assim como as organizações privadas também mantem sua informação dentro de sistemas de gestão da tecnologia da informação com o intuito de prover uma maior transparência e atender a sociedade de maneira eficaz e eficiente. Uma das iniciativas governamentais foi a criação do Governo Eletrônico, que proveu maior transparência em seus serviços, além de aumentar a facilidade de comunicação com o cidadão e tornar seus serviços mais ágeis e dinâmicos. O setor público se fez valer da potencialidade conseguida com a amplitude que a Internet possui nos usuários finais, entretanto juntamente com essa exposição existe um conjunto de riscos que ela pode propiciar.

Diante do contexto, introduz-se o problema ao qual o trabalho se propõe a resolver: conhecer e analisar as práticas e políticas de gestão de segurança da informação em um órgão público do estado de Minas Gerais.

Perante o problema exposto, o objetivo geral do trabalho será verificar e analisar o sistema de gestão da segurança da informação no órgão e seu alinhamento às **normas**[2].

[2] Normas ISO/IEC 27000/2014; ANBT ISO/IEC 27001/2013; ANBT ISO/IEC 27002/2013; ANBT ISO/IEC 27005/2011.

O presente estudo pretende verificar os seguintes objetivos específicos, no órgão analisado, estão sendo contemplados:

- Analisar a aplicação de boas práticas de Segurança da Informação nos sistemas de gestão da tecnologia da informação.
- Verificar o nível de conhecimento dos usuários, tidos como elo mais fraco do sistema, em relação às práticas de segurança da informação.
- Analisar aderência e alinhamento das políticas de Segurança da Informação do órgão com as normas mais utilizadas e conhecidas no mercado.
- Avaliar o comprometimento e a visão da alta direção com relação a um Sistema de Gestão de Segurança da Informação.

A metodologia utilizada será uma pesquisa exploratória no órgão afim de analisar a existência e efetividade de um SGSI. A intenção da pesquisa é executar um estudo de caso amplo e detalhado no órgão e auxilia-lo no preenchimento de lacunas em sua segurança com o intuito de minimizar os riscos de decorrentes da utilização da TI em seu dia a dia. A abordagem utilizada será qualitativa e quantitativa. A abordagem qualitativa será feita através de análise do Sistema de Gestão da Segurança da Informação e da política de segurança da informação existente no órgão. Será verificado também a aderência do SGSI organizacional com relação às diretrizes da Norma ABNT ISO/IEC 27000/2014. Os requisitos para estabelecimento, implementação, melhoria e manutenção do SGSI serão observados a luz da Norma ABNT ISO/IEC 27001:2013. Os controles existentes, sua implementação, diretrizes e objetivos do SGSI serão analisados sob a ótica da Norma ABNT ISO/IEC 27002/2013. A análise envolverá a observância da gestão de riscos de TI do órgão, o processo de avaliação e tratamento de risco e seu nivelamento com a Norma ABNT ISO/IEC 27005/2011. A gestão dos ativos da organização será analisada também sob a luz da Biblioteca de Infraestrutura de Tecnologia de Informação (ITIL), em sua 3ª versão. O levantamento de dados para análise quantitativa será realizado através de questionários endereçados aos usuários dos sistemas de TI e alguns gestores.

O referido estudo está distribuído em cinco capítulos que são subdivididos da seguinte forma. O primeiro capítulo apresenta uma pequena introdução

sobre o tema proposto, bem como, o problema, objetivo e metodologia orientadora que serão usados no trabalho.

O segundo capítulo expõe a revisão de literatura e embasamento teórico sobre o tema proposto com a intenção de amparar as decisões sobre possíveis soluções para o assunto. Nele conceitos sobre o arcabouço da Segurança da Informação são elucidados e as técnicas de enfrentamento para o problema são propostas e elencadas com a intenção de familiarizar o leitor sobre o tema.

O terceiro capítulo apresentará a metodologia utilizada no trabalho, o tipo e a forma de pesquisa e como ocorrerá a obtenção dos dados necessários para a análise do problema proposto. Ademais, para fins de auxilio e esclarecimento será aplicado um questionário (Anexo 1) aos usuários (servidores públicos) selecionados da organização. Além disto, será feita uma entrevista semiestruturada com o gestor da área de TI a fim de elucidar possíveis dúvidas sobre a segurança da informação do órgão.

No quarto capítulo, as práticas sobre Gestão da Segurança da Informação no órgão do estado de Minas Gerais escolhido e serão levantadas através de uma pesquisa exploratória a existência e abrangência das políticas de Segurança da Informação na unidade governamental. Além disso, serão analisadas as particularidades do órgão e as suas relações com as políticas de Segurança da Informação, o comprometimento dos usuários de Sistemas da Informação, a análise dos controles existentes, a existência dos processos de análise, avaliação e tratamento de risco, a conformidade com normas referência como a ISO/IEC 27002/2013 e a existência e análise do plano de continuidade de negócio. Os dados levantados serão condensados com a intenção de evidenciar se o órgão possui um nível satisfatório de eficiência nas políticas da Segurança da Informação.

No quinto capítulo, serão apresentadas as considerações finais que terão sua fundamentação em consonância com os dados levantados no capítulo anterior, analisando os resultados de acordo com as normas[2] referência no assunto. O trabalho constatou que diferentemente do setor privado, a organização pública estudada não conduz de forma estratégica o tema segurança da informação. As normas técnicas da ABNT pouco foram aplicadas nos requisitos ou controles do sistema de gestão da

segurança da informação. Além disto, serão expostas as limitações encontradas no trabalho como, por exemplo, o pequeno número de participantes que responderam ao questionário enviado diante do número expressivo de funcionários que o órgão possui em seu quadro funcional. O assunto possibilitou a confirmação que algumas propostas de trabalho futuras poderiam sem criadas para adentrar no objetivo principal ou nos objetivos específicos. Entre elas pode-se citar: o aumento da abrangência do estudo com a utilização de novas fontes (normas, *frameworks*[1], bibliotecas) de orientação, a comparação entre a forma como a segurança da informação é tratada tanto pelas organizações do setor privado e as organizações da Administração Pública do estado de Minas Gerais. A intenção possibilitaria um *benchmark* do assunto entre algum órgão da organização pública e uma empresa do setor privado.

2 O ARCABOUÇO DA SEGURANÇA DA INFORMAÇÃO

O desenvolvimento dos serviços oferecidos pela Administração Pública, em todas as esferas, atualmente, é dependente da informação para o alcance de forma eficiente e eficaz de seus objetivos. Devido a isso, um setor de TI é imprescindível a qualquer unidade governamental pública seja ela de direito público ou privado. Porém, uma informação para agregar valor ao negócio, auxiliar no serviço operacional, atingir os objetivos estratégicos ou dinamizar qualquer outra área da organização, necessita ter um nível de qualidade, tal que, todos os itens elencados anteriormente facilmente serão alcançados.

A Gestão de Sistemas de Segurança da Informação é amplamente difundida na literatura técnica da Tecnologia da Informação e por esse motivo serão condensados diversos conceitos, manuais, *frameworks*[1], bibliotecas, normas dos mais variados conteúdos com a intenção de direcionar, embasar e desenvolver o tema.

2.1 Princípios da Segurança da Informação

Para que a completude dos objetivos da Segurança da Informação seja atingida, seus atributos básicos: Integridade, Confidencialidade e Disponibilidade precisam ser observados.

Figura 1 – Atributos básicos da Segurança da Informação

Fonte: Portal GSTI. *Overview* da certificação ISSO 27002 *Foundation*.

Será utilizada para fins de definição dos sustentáculos da Segurança da Informação a Biblioteca de Infraestrutura de Tecnologia da Informação, comumente conhecida pelo seu acrônimo, ITIL, em sua versão 3, datada do ano de 2011. A ITIL é referência em administração de ativos de TI e é largamente utilizada com sucesso nas organizações de cunho privado. Seu objetivo principal é prover boas práticas de gerenciamento de serviços de TI em organizações que possuam operações de TI ou pretendam aplicar melhorias nelas. Segundo o glossário da ITIL, a **integridade** é "um princípio que garante que dados e itens de configuração somente sejam modificados por pessoas e atividades autorizadas considerando todas as possíveis causas de modificação, incluindo falhas de hardware e software, eventos ambientais e intervenção humana". A **confidencialidade** compreende "o princípio que requer que dados devam somente ser acessados por pessoas autorizadas". A **disponibilidade** refere-se à "habilidade de um serviço de TI ou outro item de configuração de desempenhar a sua função acordada quando requerido. A disponibilidade é determinada pela confiabilidade, sustentabilidade, funcionalidade do serviço, desempenho e segurança".

2.2 Requisitos de um Sistema de Gestão da Segurança da Informação

O estabelecimento, implementação, manutenção e melhoria contínua de um SGSI requer que alguns requisitos permaneçam alinhados com as necessidades da organização. Logo, é imprescindível que a organização classifique os seus requisitos de segurança da informação. A Norma ABNT ISO/IEC 27002/2013 dita que existem três fontes elementares de requisitos da segurança da informação:

- A avaliação de riscos para a organização. Ela tipifica as ameaças aos ativos, e as suas vulnerabilidades, além de realizar a estimativa das chances de ocorrências das ameaças e os seus impactos para os negócios organizacionais.
- A legislação vigente, estatutos, regulamentações e cláusulas contratuais as quais a organização está sujeita inclusive seu ambiente sociocultural.
- Princípios, objetivos e requisitos de negócio com relação ao desenvolvimento de todo o ciclo de vida da informação com o intuito de apoiar os tomadores de decisão da organização.

Os objetivos destes sistemas de gestão da informação podem ser os mais diversos e, dentre eles, conforme preconiza a Norma ISO/IEC 27001/2011, podemos citar:

- Prover informações de qualidade que possam ser utilizadas principalmente no auxílio ou suporte na tomada de decisão dos seus detentores.
- Assistir a organização a alcançar suas metas estratégicas ou índice de excelência gerencial.
- Conceder benefícios que possam garantir uma execução eficiente da sua missão.
- Agregar e gerar valor ao negócio.
- Conservar os riscos de negócio em um nível aceitável.

Como preconizado na ABNT ISO/IEC 27001/2013, convém que o SGSI esteja contido e integrado aos demais processos da organização e sua estrutura administrativa. Além disto, a Segurança da Informação necessita ser avaliada relativamente em projetos de processos da organização, seus sistemas de informação e controles.

Porém, anterior ao estabelecimento de um SGSI a organização, através de seus gestores, deve definir interna e externamente as questões fundamentais que possam vir a comprometer o bom funcionamento organizacional e distanciem do alcance dos seus objetivos. Esse contexto organizacional é o ambiente propício para a inserção do SGSI bem como a análise dos seus resultados.

Definido o contexto de atuação do SGSI, convém que controles sejam definidos no processo de sua implementação. Segundo com a Norma ABNT ISO/IEC 27002/2013, "a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware"*. A Norma orienta as organizações a implementarem controles de segurança da informação Normalmente aceitos e conhecidos, que podem ser estabelecidos em organizações de todos os tamanhos, bem como, de todos os setores onde transitam informações de diferentes formatos, eletrônico, físico e verbal. Tais controles devem ser analisados e selecionados com base

na probabilidade e intensidade dos danos aos negócios ocasionados pela quebra da segurança nos sistemas da organização.

2.2.1 Benefícios de um Sistema de Gestão da Segurança da Informação

Os benefícios obtidos com a implantação de um Sistema de Gestão da Segurança da Informação são extensos, de acordo com a Norma ABNT ISO/IEC 27000/2014 e entre eles podemos citar:

- Estabelecimento de uma metodologia clara de Gestão da Segurança da Informação.
- Redução do risco de perda, roubo ou alteração da informação.
- O acesso à informação feito através de protocolos de segurança.
- Confiança e regras claras para todos os envolvidos de uma organização.
- Aumento de segurança em relação à gestão de processos.
- Conformidade com a legislação vigente sobre informação pessoal, propriedade intelectual.
- Os riscos e os seus controles são continuamente verificados e melhorados perenemente.
- Garantia de qualidade e confidencialidade.

2.2.2 Fatores de sucesso para segurança da informação

Outro fator importante para que um Sistema de Gestão da Segurança da Informação seja efetivo em uma organização é o comprometimento da alta direção em todas as áreas abrangidas pelo SGSI. Esta mentalidade deve estar incutida em todos os membros que devem perceber os benefícios obtidos por um SGSI. As organizações necessitam de um modelo de governança efetiva e comprometida pois, segundo o *framework*[1] COBIT, a governança compreende diferentes tipos de atividades, por conseguinte, serve a diferentes propósitos:

- Garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados.
- Define a direção através de priorizações e tomadas de decisão.
- Monitora o desempenho e a conformidade com a direção e os objetivos estabelecidos na organização.

A menção ao *framework*[1] COBIT, em sua 5ª edição, é importante pois ele possui áreas e domínios que estão alinhados a outras normas e entre elas, temos a ABNT ISO/IEC 27000/2014 que será usada constantemente neste trabalho. A gestão atua no seguimento das diretivas impostas pela governança através do planejamento, desenvolvimento, execução e monitoramento das operações internas da organização. A governança intenciona a aplicação da TI para atender às demandas e objetivos atuais e futuros dos negócios e das partes interessadas. A principal diferença entre a governança e a gestão está no foco e lugar de atuação. A governança TI

> [...] é a estrutura de relacionamentos, processos e mecanismos usados para desenvolver, dirigir e controlar estratégias e recursos de TI de maneira a melhor atingir as metas e objetivos de uma organização. É um conjunto de processos que visa adicionar valor a uma organização, ao passo que equaciona elementos de risco e de retorno associados a investimentos de TI. A governança de TI é, ao fim e ao cabo, uma responsabilidade do grupo de dirigentes e gestores executivos (SETHIBE; CAMPBELL; MCDONALD, 2007, p. 833).

Verifica-se que a governança de TI está mais focada analisar os impactos organizacionais através de um desenvolvimento de um plano estratégico onde eles possam se alinhar aos objetivos institucionais da organização e atendam aos interesses dos atores internos e externos à organização. A Tabela 1, descreve os principais elementos da governança e da gestão de TI.

Quadro 1 – Governança de TI versus Gestão de TI

GOVERNANÇA DE TI	GESTÃO DE TI
Foco interno e externo	**Foco interno**
Visão do conjunto da organização	**Visão departamental e individual**
Futuro	**Presente**
Estratégias	**Operações e projetos**
Geração de benefícios	**Custos e qualidade**
Investimento sábio	**Prestação de contas**
Delegação	**Controle (hands-on)**

Fonte: Liu e Ridley (2005).

Os modelos de governança de TI seguidos pelo setor público estão preconizados e elaborados por organizações privadas. Um exemplo disto, é o *framework*[1] COBIT, já citado anteriormente. Tal fato, deve-se à falta de modelos de governança de TI criados exclusivamente para o setor público. A natureza peculiar vivida pela Administração Pública se difere do setor privado, o que a torna mais complexa (LIU, RIDLEY, 2005, p. 3).

2.3 Ameaças de TI

Toda a informação que é administrada e processada por uma organização pode ser alvo de algum ataque maliciosos, erro ou um desastre natural (enchente, incêndio, terremoto) e está propícia a possuir vulnerabilidade inerentes a sua natureza e uso (ISO/IEC 27000:2014).

A utilização de SGSI objetiva controlar, administrar e direcionar as atividades de TI em uma organização de forma a diminuir os riscos de TI provenientes de ameaças internas ou externas e atingir seus objetivos. O risco de segurança da informação está relacionado à capacidade que as ameaças têm em expor vulnerabilidade de um ativo de informação ou grupo de ativos de informação e, desta maneira, ocasionar algum prejuízo para a organização ou gerar alguma incerteza no alcance dos seus objetivos. Outro ponto importante a se acrescentar é que o risco pode ser positivo ou negativo. Geralmente, o risco está expresso em termos de uma junção entre as consequências de um evento e a probabilidade de ocorrência do mesmo.

Uma ameaça é uma causa potencial de ocorrência de um incidente indesejado que pode resultar em danos ao SI ou a organização (ISO/IEC 27000:2014). Uma ou mais ameaças podem gerar uma vulnerabilidade que se entende como uma fraqueza do sistema. Ela pode ser explorada e beneficiar o invasor que poderá ter acesso ou controle dos ativos da organização.

Deste modo, as ameaças são tratadas pelo processo de administração de riscos que visa a aplicação sistemática de políticas, procedimentos e práticas de gestão do risco através das atividades de comunicação, consulta, estabelecimento do contexto e

identificação, análise, avaliação, tratamento, acompanhamento e revisão dos riscos (ISO/IEC 27000:2014).

2.4 Políticas e controles de segurança da informação

As políticas de segurança da informação auxiliam a organização a alcançar seus objetivos estratégicos através da implementação de controles de segurança da informação baseando-se em seu contexto, estimulando uma diminuição dos riscos provenientes de ameaças e vulnerabilidades através de uma segurança da informação eficiente e eficaz. De acordo com a norma ISO/IEC 27002/2013, "a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*".

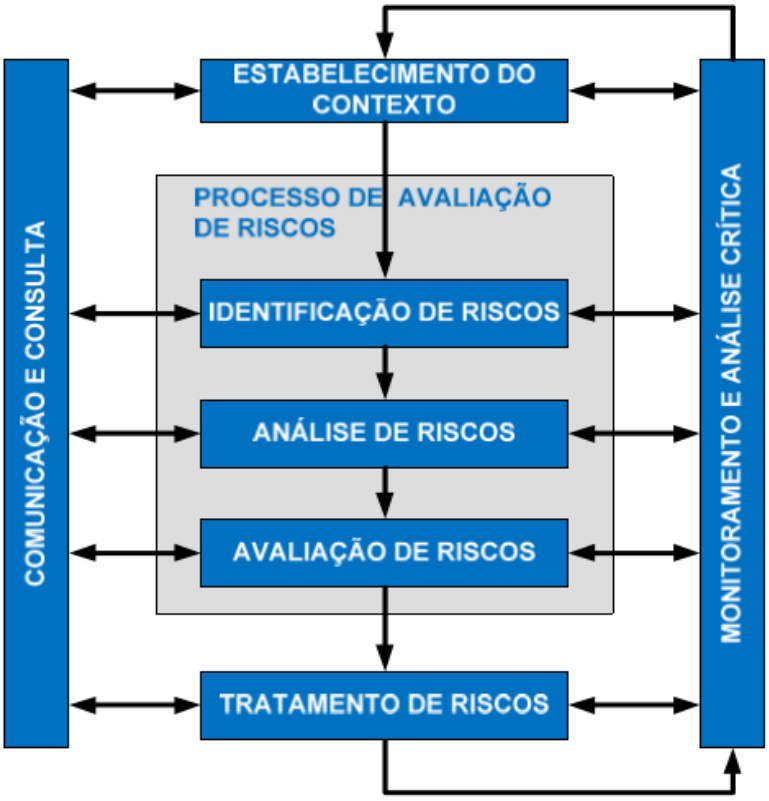
A intenção da política de segurança da informação é ajudar a direção e direcionar a segurança da informação atentando aos requisitos de negócios, as leis e regulamentações a serem seguidas e proteger a organização de ameaças atuais e futuras. A política de segurança da informação deve receber, após sua definição, a aprovação da alta direção. Após isso, ela deve ser publicada e transmitida aos usuários, neste caso, os funcionários e empregados públicos e todos aqueles que fazem uso e manipulam informações na organização.

A política deve conter a definição, objetivos e princípios norteadores para os elementos relacionados à segurança da informação, atribuir responsabilidades, gerais e especificas, aos atores que foram definidos e a metodologia para tratar exceções e desvios. A granularização de alguns tópicos exige a implementação de controles específicos com o intuito de aumentar e especificar o nível de segurança da informação em certos grupos de interesse De acordo com a norma anteriormente citada, alguns tópicos são: controle de acesso, classificação e tratamento da informação, segurança física e do ambiente, backup, proteção contra códigos maliciosos, controles criptográficos, segurança nas comunicações, proteção e privacidade da informação de identificação pessoal.

2.5 A gestão de riscos

A gestão de riscos é um fator constantemente tratados nos diversos conteúdos que versam sobre a Segurança da Informação. A intenção é oferecer técnicas e abordagens que possam reduzir os riscos inerentes a um sistema informatizado pois ao contrário de que se pensa, a sua eliminação total é dificilmente conseguida. De acordo, com a Norma ISO/IEC 27005/2011 que fora especificamente criada para a gerenciar os riscos de segurança da informação de uma organização, a gestão de riscos é composta por "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". A interpretação do conceito leva a conclusão de que a gestão de riscos é um processo que envolve diversas etapas e isso é facilmente comprovado conforme mostrado abaixo a figura extraída da Norma em questão.

Figura 2 – O processo de gestão de riscos



Fonte: ABNT NBR ISO/IEC 27005:2011.

2.5.1 A análise de contexto

Após a análise e determinação do contexto, os critérios básicos e limites da segurança da informação, e a coordenação do processo de gestão de riscos de segurança da informação podemos passar para a próxima etapa da gestão de riscos.

Entretanto, é necessária uma definição de risco com a finalidade de esclarecer seu significado. De acordo com a Norma criada especificamente para a sua gestão, "um risco é a combinação das consequências advindas da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo".

2.5.2 O processo de avaliação de riscos

Adentrando o invólucro que é o processo de avaliação de riscos, etapa por seguinte, verifica-se que ele é um processo complexo e consiste nas seguintes atividades: Identificação de riscos, análise de riscos e avaliação de riscos. A primeira atividade a ser desempenhada é a identificação de riscos que segundo a Norma ISO/IEC 27005/2011 tem o propósito de "[...] determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer". A fase de identificação necessita da inclusão dos riscos estejam ou não sob os cuidados da organização, ainda que não seja possível identificar a fonte ou causa dos mesmos. Vale lembrar que esta fase deve fornecer informações satisfatórias para a próxima etapa do processo de avaliação de riscos.

A sistemática de análise de riscos pode ser qualitativa ou quantitativa ou ainda uma conciliação de ambas. Ela pode ter diversos níveis de penetração, sob a análise da sensibilidade dos ativos, o alcance das ameaças descobertas ou de incidentes já ocorridos dentro da organização. Deve-se avaliar as consequências das violações da Segurança da Informação e as possíveis perdas ou o comprometimento dos ativos da organização. Em suma, nesta etapa os riscos devem ser valorados, quantitativa ou qualitativamente, de acordo com os ativos atingidos e impacto ocasionado sobre os negócios.

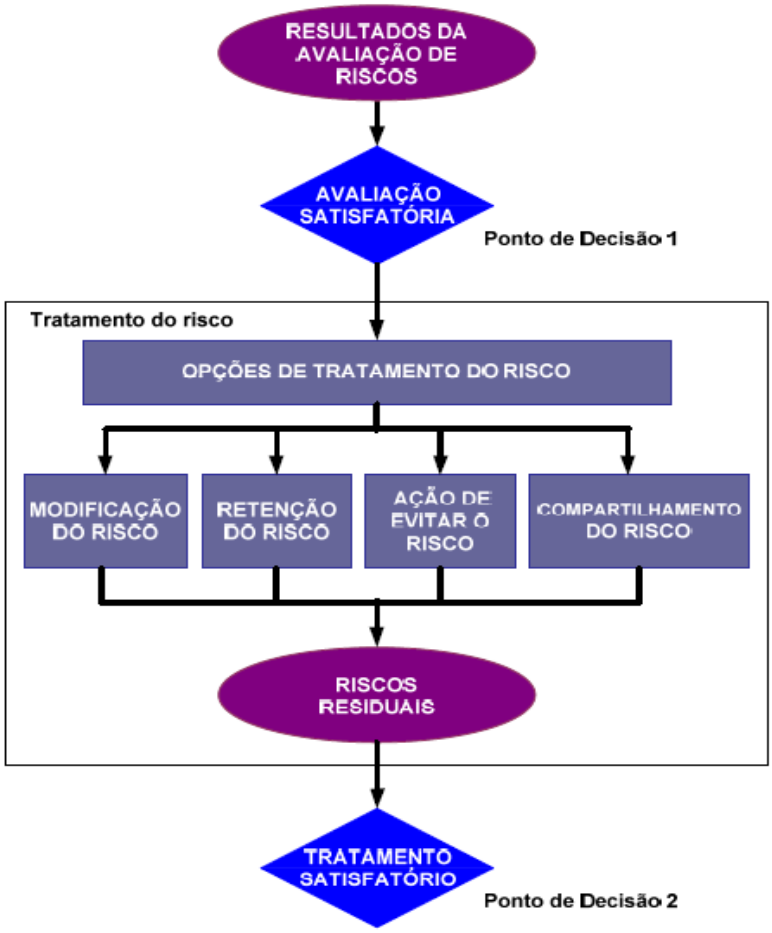
A última etapa do processo é a avaliação de riscos, ela consiste em utilizar os critérios de avaliação de riscos de acordo com o seu nível e estejam alinhados com o contexto escolhido na gestão de riscos de segurança da informação e os objetivos estratégicos da organização. Nesta etapa, a aceitação do risco é definida de acordo com fundamentos fixados na avaliação. Está etapa se torna importante pois sua saída é uma lista de riscos priorizada atendendo aos critérios estabelecidos no processo de avaliação de riscos.

Vale lembrar que todo o processo de avalição de riscos pode ser iterada quantas vezes se julgar necessário, pois o risco deve ser analisado até que se encontre em um nível mínimo possível ou um nível aceitável de acordo com os critérios definidos e recebam uma avaliação satisfatória.

2.5.3 O tratamento de riscos

Os resultados obtidos no processo anterior servem de entrada para a próxima fase do processo de gestão de riscos: o tratamento de riscos. Nesta fase, o risco será examinado e quatro ações, de acordo com resultado do processo de avaliação de riscos, podem ser tomadas. As opções de tratamento, exibidas abaixo na figura 3, são conhecidas através do acrônimo MATE (Mitigar, Aceitar, Transferir, Evitar) e podem ser usadas combinando mais de uma ação.

Figura 3 – Atividade de tratamento do risco



Fonte: ABNT NBR ISO/IEC 27005:2011.

A criação de um plano de tratamento de risco é indicada, pois, o plano "define, identifica claramente a ordem de prioridade em que as formas específicas de tratamento do risco convêm serem implementadas, assim como os seus prazos de execução" (ISO/IEC 27005/2011). Após a definição do plano, há a necessidade de determinar os riscos residuais que devem levar em consideração critérios do processo de avaliação de riscos.

Esmiuçando as possíveis ações a serem tomadas diante de um risco, temos a ação de mitigar que é a redução de um risco até um nível aceitável, aceitar é quando o risco foi aceito de acordo com os critérios estabelecidos da organização. Riscos aceitos são aqueles que não foram totalmente resolvidos após o processo de gestão de riscos e que seu nível pode ser tolerado pela organização, não impactando assim, os seus negócios. O processo de transferir um risco ocorre quando há a transferência da gestão do risco a terceiros que podem de maneira mais efetiva. Evitar o risco age nas atividades ou condições que podem gerar o risco e sua intenção foca em modificar as condições geradoras do risco.

2.6 O Plano de Continuidade de Negócios

Após o término do processo de gestão de riscos, é imprescindível que a organização crie um plano de continuidade de negócio. Ele será responsável por definir condições, ações e atores que agirão caso haja uma interrupção dos serviços. O plano se torna necessário pois ele determinará quais ações serão tomadas caso algum serviço seja interrompido de forma súbita ou inesperada. Segundo a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2008), a continuidade de negócios é uma capacidade estratégica e tática de uma organização de se planejar e responder a incidentes de grandes proporções, desastres ou interrupções de negócios significativas, para conseguir continuar suas operações em um nível aceitável previamente definido. Neste assunto, pode-se utilizar como base orientadora para a formulação de um plano de continuidade de negócios, a norma presente na Administração Pública Federal, NC 06 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES do Gabinete de Segurança Institucional da Presidência da República, lançada em 11 de novembro de 2009. Logicamente que o plano deverá ser adaptado ao contexto de cada organização.

O plano de continuidade de negócios engloba medidas de caráter preventivo e recuperativo. Vale destacar que os riscos aos quais as organizações estão sujeitas, se modificam com o tempo, contudo, alguns riscos são mais comuns, como por exemplo, a possibilidade de desastres naturais (furacões, terremotos, enchentes, tempestades de raios).

O Plano de Continuidade do Negócio tem como objetivo: manter a integridade e a disponibilidade dos dados da organização. Além disso, adiciona-se o propósito de garantir o funcionamento dos sistemas de gestão de tecnologia da informação sejam reparados, quando da ocorrência de situações fortuitas, tão logo quanto possível diminuindo assim os impactos causados pela interrupção.

2.6.1 Elaboração de um Plano de Continuidade do Negócio

O sucesso do plano de continuidade depende de alguns aspectos que devem ser analisados antes da sua elaboração propriamente dita:

- Exposição organizacional quanto aos riscos, possibilidade de ocorrência e as consequências decorrentes. Deve-se levar em consideração o nível do dano e o tempo necessário para a sua recuperação.
- Impactos advindos da interrupção dos serviços oferecidos.
- Identificação e priorização de processos críticos, recursos e sistemas.
- Prazo máximo para o restabelecimento de processos, recursos e sistemas.
- Meios alternativos para a recuperação dos processos, recursos e sistemas.
- Mensuração dos custos e benefícios de cada um desses meios.

Convém que o Plano de Continuidade do Negócio contenha informações e entre elas podemos citar:

- Situações responsáveis por ativar o Plano e os seus procedimentos de ativação.
- Metodologias devem ser seguidas após o fato gerador do incidente ocorrer. Exemplo: contato com autoridades apropriadas.

- Acomodações secundárias caso a principal venha a se tornar inoperante. Tais locais devem ser inventariados com relação aos bens disponíveis na instalação.
- Nível de priorização dos *softwares* de acordo com a sua importância e criticidade para a organização. Deve-se levar em consideração os ativos tangíveis (sistemas de TI) e intangíveis (imagem).
- Entrada em operação em um nível aceitável de serviços críticos da organização.
- Disponibilização de documentação de instalação reserva de aplicativos críticos (sistemas operacionais) e suprimentos de informática (servidores).
- Identificação das dependências externas ao negócio.
- Procedimentos necessários para a instalação dos serviços em instalações secundárias.
- Atores responsáveis por comandar e executar cada uma das ações mencionadas no plano. Convém determinar substitutos sempre que necessário.
- Contratos e acordos que são parte integrantes do plano no tocante a recuperação de serviços.
- Responsáveis, seus dados e formas de contato.
- Organizações responsáveis por disponibilizar os bens necessários para a restauração dos serviços.

Assim como descrito como fator imprescindível para o sucesso de SGSI, o comprometimento da alta direção da organização com o Plano de Continuidade do Negócio é fundamental, pois, de acordo com o manual de boas práticas em segurança da informação do TCU, o "plano é de responsabilidade direta da alta administração, é um problema corporativo, pois trata de estabelecimento de procedimentos que garantirão a sobrevivência da instituição como um totó e não apenas da área de informática". Vale lembrar que, muitos termos são relativos ao negócio da organização e não apenas à tecnologia da informação. A alta administração, entre outros deveres, deve:

- Constituir uma equipe de segurança exclusiva para elabora, implementar, divulgar, treinar, testar, manutenir e coordenar o Plano de Continuidade do Negócio.
- Determinar o responsável pelas demandas, negociações e assuntos relacionados ao plano que forem necessários para o seu eficiente andamento.

- Firmar acordos de cooperação com outras organizações.
- Assinar contratos direcionados para o restabelecimento dos serviços.
- Decidir sobre o orçamento disponibilizado para assegurar a execução do Plano.

2.6.2 Funcionamento do Plano de Continuidade do Negócio

A garantia de eficácia do Plano de Continuidade do Negócio desdobra-se em três requisitos: treinamento e conscientização dos atores envolvidos; testes (integrais e parciais) periódicos do Plano; processo de manutenção e melhoria contínua.

2.6.2.1 Treinamento e conscientização dos atores envolvidos

A efetividade do Plano de Continuidade do Negócio está intimamente ligada com o comprometimento dos atores envolvidos. As atividades instrutivas e de conscientização auxiliam no entendimento das ações necessárias ao seu sucesso e importância. Os funcionários conhecer suas responsabilidades especificas em situações de contingência. Desta forma, o treinamento deve ser teórico e práticos, incluindo assim simulações. Outras maneiras de conscientização podem ser utilizadas, como por exemplo: folhetos, *workshops*, palestras. Todas as formas de conscientização devem tentar incutir nos participantes a mentalidade de que eles são elementos ativos no programa de segurança da organização.

2.6.2.2 Testes do Plano de Continuidade do Negócio

O Plano deve ser testado frequentemente, pois isso determina sua efetividade e necessidade de atualização. Deve haver um planejamento sobre como e quando o Plano deverá ser testado. Ele poderá ser testado de forma integral, aproximando a situação emergencial fictícia da realidade; ou parcialmente para testar procedimentos, controles ou atividades especificas. Os resultados realimentarão o próprio Plano e determinarão a necessidade de adequação ou alteração dos seus componentes. De acordo com o manual de boas práticas do TCU, os testes também devem assegurar que todos os envolvidos na recuperação e os alocados em outras funções críticas possuam conhecimento do Plano.

2.6.2.3 Melhoria continua do Plano de Continuidade do Negócio

Modificações em procedimentos, requisitos, processos ou situações adversas devem motivar alterações no Plano. Tais atualizações regulares são fundamentais para atingir a efetividade do Plano. Algumas mudanças organizacionais, de contexto, de legislação, normativas, geográficas, contratuais, entre outras podem acionar o gatilho para uma atualização do Plano de Continuidade do Negócio.

2.7 As boas práticas de Segurança da Informação

As boas práticas de SI contribuem para que os riscos inerentes da TI sejam minimizados. Desta forma, o uso dos sistemas da TI poderá agregar valor ao negócio e beneficiar todos os usuários desses sistemas.

2.7.1 Controles de acesso

As organizações que gerem, administrem e expõem informação devem assegurar que o acesso a tais informações seja feito de forma segura. Os controles de acesso, físico ou lógico (virtual), salvaguardam equipamentos (hardware), aplicativos e arquivos contra a modificação (integridade), apresentação indevida (confidencialidade) e perda (disponibilidade). Entretanto, diferentemente de estruturas físicas que podem ser mais facilmente controladas pois sua materialidade provém isto, as estruturas lógicas são mais complexas, pois elas transitam através de um ambiente e fronteiras difíceis de controlar.

Para aumentar a segurança dita anteriormente, podemos utilizar os controles de acesso, que de acordo com o manual de boas práticas de segurança da informação criado pelo Tribunal de Contas de União (TCU), são “um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador”. Vale destacar que, o controle lógico devido a sua complexidade possui duas maneiras distintas: proteção dos recursos computacionais e controle dos usuários aos quais receberão privilégios e acesso aos recursos. O controle lógico deve avaliar a real necessidade de acesso do usuário aos recursos computacionais e através de técnicas

como identificação e autenticação do usuário prover uma ou diversas formas de confirmação de identidade. Tal confirmação de identidade está diretamente alinhada com confidencialidade, um dos pilares da segurança da informação.

2.7.1.1 Motivos da proteção dos recursos computacionais

Os motivos pelos quais os recursos computacionais (aplicativos, arquivos de dados, utilitários e sistema operacional) devem ser protegidos são diversos. Entre eles podemos citar:

- A alteração do código fonte pode comprometer a lógica de negócio, logo, deve haver a proteção do código através de técnicas conhecidas como por exemplo: ofuscamento ou geração de arquivos binários. Tais técnicas viam a proteção com o objetivo de impossibilitar a modificação de funções e a lógica do software, bem como conhecer a dinâmica interna de um sistema.
- Acesso a base de dados deve ser controlado, pois, o acesso não autorizado pode expor ou comprometer informações estratégicas ou operacionais da organização. Além disso, a sua proteção impede que dados possam ser apagados ou alterados de forma prejudicial.
- A restrição ao acesso de utilitários e função do *kernel* (núcleo) do sistema operacional deve ser restrito, pois eles têm privilégios para alterar configurações de segurança e isso pode comprometer todo o sistema onde há um sistema de gestão de tecnologia da informação. Logo, o perfil de administrador do sistema operacional deve ser dado apenas a pessoas autorizadas.
- A proteção do sistema ou mecanismo que armazena as senhas. A utilização de senhas garante a autenticidade do usuário e a violação do mecanismo pode privilegiar usuários não autorizados a executarem transações incompatíveis para o seu verdadeiro nível de privilégio.
- A utilização de um sistema de registro de ação dos usuários. A forma mais conhecida e amplamente empregada é registrar as operações através de *logs*. Eles podem ser usados para identificar usuários presentes no sistema e auxiliarem em auditorias.

2.7.1.2 Objetivos dos controles de acesso lógico

Os propósitos dos controles de acesso lógico visam certificar que os princípios básicos da segurança da informação estão sendo atendidos. De acordo com a manual de boas práticas do TCU, o entendimento do controle de acesso deve ser orientado sobre a ótica de "funções de identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos; e prevenção de acessos não autorizados". Em resumo, os objetivos são:

- Limitação de acesso aos recursos computacionais apenas por pessoas autorizadas.
- Privilegiar através de níveis, usuários de acordo sua função e suas responsabilidades.
- Monitorar o acesso a recursos computacionais sensíveis.
- Disponibilizar aos usuários apenas os recursos computações necessários para a execução de suas tarefas.

2.7.1.3 Identificação e autenticação de usuários

A identificação e autenticação de usuários em sistemas computacionais pode ser feita por uma série de mecanismos: cartão, *tokens*, biometria, certificação digital ou *logon*, entretanto, o *logon* é o mecanismo mais conhecido e utilizado devido a sua facilidade de implementação e administração. O processo é bem simples e prático e possibilita a identificação e autenticação através de identificador único, comumente conhecido como ID, que provê a identificação do usuário e uma senha responsável pela autenticação.

O processo deve ser arquitetado para exteriorizar apenas o necessário com relação às informações do sistema o que evita a exposição desnecessária de informações ao usuário. Uma sistemática eficiente deve, como prescrito no manual de boas práticas do TCU:

- Comunicar que o acesso deve ser feito apenas por pessoas autorizadas.

- Coibir a identificação do sistema ou suas aplicações e só permitir após o término do processo de *logon.*
- Evitar a exibição de informações através de mensagens de ajuda que possam facilitar pessoas não autorizadas a terminar o processo.
- Requerer a completitude das informações para prosseguimento do procedimento não informando qual parâmetro de entrada está incorreto.
- Fixar um número máximo (recomendadas três tentativas) de tentativas incorretas, registrando as tentativas incorretas, estabelecendo um intervalo para novas tentativas.
- Estabelecer um tempo para a sessão do usuário após a entrada no sistema.
- Exibir informações de *logon* anteriores com sucesso como: endereço IP, data e hora.

2.7.1.4 Orientações sobre o uso de senha

O funcionamento do controle de senhas depende do entendimento sobre as boas práticas acerca da criação de senhas e as políticas organizacionais a respeito do assunto. De acordo com a Cartilha de Segurança para Internet, criada pelo Comitê Gestor da Internet no Brasil (CGI.br), "uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar".

As responsabilidades do usuário consistem em: preservar a confidencialidade de suas senhas, não as compartilhar em hipótese alguma, evitar o seu registro em lugares que possam ser facilmente acessíveis a pessoas estranhas ou usuário mal-intencionados e não criar senhas com caracteres sequenciais, repetidos e que se refiram a dados pessoais. Convém que as senhas sejam modificadas regularmente a fim de aumentar a sua confidencialidade. A cartilha do CGI.br, mencionada anteriormente, determina que um período entre sessenta e noventa dias é considerado uma boa pratica. Os usuários devem procurar, sempre que possível, serviços que ofereçam o recurso de criptografia.

2.7.1.5 Concessão de senhas aos usuários

A concessão de senhas, conforme determina a ISO/IEC 27002/2013, deve ser regida por um processo de gerenciamento formal. Este processo envolve:

- Assinatura de uma declaração por parte dos usuários. Esta declaração versa sobre o comprometimento do usuário em manter a confidencialidade de todas as senhas sob os seus cuidados. Está declaração poder ser anexadas aos termos e condições da contratação.
- Garantir a obrigação de alteração, no primeiro acesso ao sistema, da senha temporária que fora disponibilizada ao usuário.
- Estabelecer métodos de verificação da identidade do usuário antes do fornecimento da senha temporária, de substituição ou nova.
- Disponibilizar autenticação secreta temporária aos usuários de forma segura, evitando mensagens de e-mail sem a utilização de textos cifrados.
- Notificação por parte dos usuários a respeito do recebimento da informação de autenticação secreta.

2.7.2 Criptografia

A criptografia é um conjunto de técnicas e procedimentos para codificar, ou cifrar informações legíveis por meio de algoritmos conhecidos e realmente eficientes que convertem um texto legível em um texto inelegível ou comumente conhecido como texto cifrado. A processo de criptografia é uma via de mão dupla pois ele pode ser usado para cifrar ou decifrar informações.

A utilização da criptografia protege a confidencialidade, autenticidade e a integridade da informação, além de reduzir os riscos à sua utilização, e por isso seu uso deve ser encorajado, adequado e efetivo. O desenvolvimento e implementação de uma política que contemple controles criptográficos na organização é aconselhável.

A política de criptografia da organização, no momento de sua produção, pode ser provida da indicação dos seguintes itens:

- O gerenciamento do uso dos controles criptográficos na organização e seus princípios gerais.
- A avaliação de risco proveniente do algoritmo de criptografia utilizado. O nível de proteção deve ser identificado para tal.
- A utilização da criptografia para proteger informações sensíveis transportadas nos diversos meios e formas.
- A metodologia utilizada na proteção das chaves criptográficas e a recuperação de informações cifradas elencando os procedimentos quando houver perda, dano ou comprometimentos dessas chaves.
- A definição de papéis e suas respectivas responsabilidade.
- A adoção de padrões a serem seguidos durante sua implementação.
- Análise de leis ou regulamentações e restrições nacionais nas técnicas criptográficas escolhidas.

A utilização e escolha de controles criptográficos adequados devem ser auxiliadas por um especialista e caso a organização não o tenha, é aconselhável busca-lo em outras unidades governamentais pois a escolha correta dos controles alcança com sucesso os objetivos da Política de Segurança da Informação.

2.7.3 A segurança física e do ambiente.

Os locais onde as informações são processadas e armazenadas também devem receber proteção, pois a sua violação pode prover acesso físico inadequado e não autorizado, o que compromete a segurança não só da instalação, mas também de todo o sistema que gerencia a informação da organização e especialmente a informação. O objetivo é prevenir o acesso não autorizado através da clara definição de perímetros de segurança onde estão estabelecidos os recursos responsáveis pelo processamento de informações.

Algumas diretivas podem ser consideradas convenientemente nos perímetros de segurança física:

- Definição clara da localização e capacidade de acordo com o resultado da avaliação de riscos e requisitos de segurança para o perímetro.
- Construção de paredes robustas e todas as portas devem possuir mecanismos de controle (barras, alarmes, fechaduras).
- Implantação de locais de identificação pessoal antes do perímetro como por exemplo: uma recepção para controlar o acesso físico.
- Construção, quando possível, de obstáculos físicos.
- Proteção contra incêndio e que as portas corta-fogo possuam alarme e sejam monitoradas e testadas simultaneamente com as paredes. O funcionamento de todo dispositivo contra incêndios deve estar de acordo com normas nacionais e internacionais aceitáveis.
- Instalação de sistemas que detectem intrusos em todas as áreas que possam ser usadas para acessar o perímetro.
- Segregação das áreas de processamento de informação gerenciadas pela organização das áreas gerenciadas por terceiros.

Podem ser utilizadas barreiras múltiplas para a obtenção de um nível maior de proteção física. Devido a economicidade, existe a possibilidade de várias organizações ocuparem um mesmo local, caso isso ocorra, precauções especiais devem ser tomadas utilizando por exemplo: cartões de controle ou PIN (*Personal Identification Number).* A possibilidade de desastres naturais, incidentes e ataques maliciosos deve ser analisada e ações de defesa devem ser projetadas e implantadas.

2.8 A gestão de TI e sua relevância no setor público

A inserção da Tecnologia da Informação na Administração Púbica alterou de forma significativa a sua interação com o cidadão e principalmente sua forma de trabalho. A TI, antigamente, não era tratada como um mecanismo capaz de melhorar o desempenho das organizações, a tendência era tratar a TI como uma ferramenta auxiliar, uma variável meramente interveniente a ser considerada na análise do desempenho da administração pública e dos governos (CEPIK, CANABARRO, POSSAMAI, 2010). Os diversos obstáculos a serem ultrapassados na busca de um nível melhor de eficácia e eficiência fizeram com que a Administração Pública buscasse uma

profunda transformação, através da Tecnologia da Informação, em seus processos e serviços ofertados. O grande desafio, sobretudo, era prestar serviços públicos de qualidade, respondendo a altura às requisições demandadas pela Sociedade. Dentro deste contexto, a gestão de TI na Administração Pública evoluiu ao longo dos tempos, muito por causa da necessidade de adequação às mudanças, atualizações ou criação de novas legislações ou normas. Entre elas, podemos citar, a Lei 10.520/2002, conhecida como a Lei do Pregão Eletrônico e a Lei 8.666/93, a Lei da Licitação.

Com a era da Internet, a quantidade de criação e compartilhamento de informações e dados foi excessivamente aumentada por inúmeras fontes. Atualmente, a TI é uma ferramenta fundamental para a transformação da administração pública, deixando de ser objeto apenas de gestão para ser objetos de governança (CEPIK, CANABARRO, POSSAMAI, 2010).

Essa mudança de paradigma nos serviços públicos é facilmente evidenciada por diversos dados que comprovam o valor significativo gasto ao longo dos anos com serviços de TI, por exemplo, no governo federal. A tabela 1 apresenta os órgãos da Administração Pública Federal que estão entre os maiores demandadores de serviços de TI no quesito valor.

Tabela 1 – Valores empenhados (2016) em serviços de TI acima de 4 milhões por órgãos do estado de Minas Gerais.

ÓRGÃO	Valor
Secretaria de Estado da Fazenda	**38.284.766,07**
Fundo Especial do Poder Judiciário de Estado	**34.687.899,88**
Cidade Administrativa	**20.488.817,04**
Secretaria do Estado de Planejamento e Gestão	**19.812.314,62**
Fundo Estadual de Saúde	**9.913.924,96**
Polícia Militar do Estado	**8.997.993,54**
Fundação de Amparo à Pesquisa do Estado	**8.918.006,30**
Departamento de Trânsito	**8.323.903,72**
Fundação Centro de Hematologia e Hemoterapia de MG	**5.979.908,84**
Defensoria Pública do Estado	**4.654.012,95**
Junta Comercial do Estado	**4.435.192,76**
Procuradoria Geral de Justiça	**4.419.811,67**

Fonte: Portal da transparência

Dito isso, a informação se tornou um dos principais ativos de uma organização (privada ou pública) e sua exposição em todas as esferas, interna e externa,

aumenta os riscos de violação e é neste universo onde se insere a Segurança da Informação, matéria que se tornou fundamental para a integridade dos dados públicos.

Devido à importância da informação, ela precisa ser protegida e conforme enunciado na Norma ABNT ISO/IEC 27001/2013, “a adoção de um Sistema de Gestão de Segurança da Informação é uma decisão estratégica para uma organização”. A utilização, conforme a própria Norma anunciada anteriormente, é necessária pois “o Sistema de Gestão da Segurança da Informação (SGSI) preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos [...]”.

2.9 Considerações finais

Diante do exposto em todo o capítulo, nota-se que a implementação de uma gestão da segurança da informação nas organizações é complexa, estratégica e necessita de um bom nível de conhecimento acerca do assunto. As várias etapas necessárias para o atingimento de um nível satisfatório obrigam o empenho de todos os usuários dos sistemas de TI, bem como, a alta direção deve incutir o compromisso de todos os usuários para que os controles e procedimentos de segurança sejam seguidos e respeitados.

A segurança da informação é alcançada pela implementação de conjunto de controles, incluindo as políticas de segurança da informação (ABNT ISO/IEC 27002/2013). A formulação das políticas da segurança da informação incluindo a seleção, implementação e gerenciamento dos controles de segurança informação que serão aplicados na organização estarão norteadas sob a luz da norma ABNT ISO/IEC 27002/2013.

A governança de TI é um elemento importante no ciclo de vida de um SGSI, pois sua implementação parte de uma decisão estratégica corpo de gestores e tomadores de decisão da organização e deve estar alinhada ao negócio e objetivos da organização. O *framework*[1] COBIT, em sua quinta versão, é referência no mercado no quesito governança de TI em razão de possuir boas práticas e existir entre os seus princípios a focalização do elemento de uma maneira bastante esclarecedora e objetiva.

Os ativos em qualquer organização podem ser o objeto de ameaças e uma forma de minimizar a probabilidade de ocorrência de ataque perpassa pela utilização de boas práticas de segurança da informação. Porém, este ponto só é alcançado quando usuários de sistemas de informações se comprometem a segui-las. Dito isso, o estudo verificará da aplicação de boas práticas de segurança da informação no órgão e elas receberam uma análise baseadas na norma ABNT ISO/IEC 27002/2013.

Um dos pontos focais de um SGSI é a redução de riscos presentes na tecnologia da informação, protegendo assim a informação da organização. Conforme prescrito na norma ABNT ISO/IEC 27002/2013, um SGSI considera uma visão holística e coordenada dos riscos de segurança da informação da organização. Entretanto a norma ABNT ISO/IEC 27005/2011 não determina uma metodologia especifica para a gestão de riscos de segurança da informação da organização, ela fornece diretrizes para o processo de Gestão de Riscos facilitando a implementação apropriada da segurança da informação apoiando em uma abordagem orientada pela gestão de riscos.

A maior parte dos controles contidos neste capítulo não são obrigatórios, entretanto, a sua implementação aumenta a possibilidade de sucesso do Sistema de Gestão da Segurança da Informação em alcançar seu objetivo: a proteção de toda a informação da organização.

3 METODOLOGIA

Este estudo foi realizado em uma organização[3] pública estadual de Minas Gerais que objetiva o fortalecimento do Sistema Único de Saúde através da proteção e promoção da saúde. A instituição produz oito tipos de soros antitóxicos e uma vacina – a meningocócica C. A organização fornece serviços de vigilância sanitária que incluem, entre outros: monitoramento de água e alimentos, análise de resíduos de agrotóxicos em alimentos; análise de resíduos de medicamentos veterinários em alimentos; vigilância da qualidade de medicamentos; vigilância da qualidade de cosméticos; monitoramento de hemocentros; monitoramento de Águas de Hemodiálise. Outro serviço ofertado pela instituição são exames diagnósticos, em Minas Gerais e no Brasil, de várias doenças como tuberculose, dengue, febre amarela, raiva, Chagas e muitas outras.

Dito isso, diante da grande quantidade de serviços elencados anteriormente oferecidos pelo órgão nota-se o quão importante e estratégico ele é para o estado de Minas Gerais e o Brasil, a sua relevância no cenário nacional foi o fator preponderante para a sua escolha. Inclui-se também diversos estudos e a realização de pesquisas em: Inteligência Artificial, seleção *in vitro* utilizando cultivo celular para ensaios pré-clínicos na cadeia de desenvolvimento de novos fármacos; produção de anticorpos monoclonais.

O objetivo principal do trabalho é conhecer e analisar as práticas e políticas de gestão de segurança da informação no órgão. Para o atingimento deste objetivo, foi elaborado e aplicado aos funcionários da organização um questionário composto de quatorze questões, sendo todas fechadas utilizando a escala *likert* e uma entrevista semiestruturada, composta de vinte e uma perguntas, com o assessor chefe da assessoria de Tecnologia da Informação da organização.

As questões do questionário procuraram levantar informações sobre o conhecimento acerca das boas práticas de segurança da informação constantes no órgão, problemas relacionados com a violação de segurança em seus computadores, o impacto dessa violação em relação ao tempo médio que seus computadores ficaram inoperantes

[3] O nome da organização será mantido em sigilo para não expor os atores envolvidos no estudo e pela sensibilidade e criticidade do tema.

e informações afetadas ou perdidas, a quantidade de vezes durante a semana que os funcionários utilizam algum sistema informatizado (*software*) para a realização do seu trabalho e seu entendimento quanto a importância do seu trabalho para organização e a segurança da informação no seu dia a dia funcional. O questionário foi aplicado a sessenta e oito funcionários e não objetivou aferir o nível de conhecimento dos usuários sobre tecnologia da informação, sistemas informatizados e segurança da informação. A aplicação do questionário se deu através da ferramenta Google Docs, pois as limitações dos formatos de dados que podem ser usados com esse *software* são menos restritas (FLICK, 2009).

Foi determinado junto a gerência de TI algumas áreas estratégicas de negócios da organização e após esta escolha, foi enviado um e-mail a cem servidores desses departamentos, e dentre este universo de servidores, sessenta e oito responderam o questionário. Segundo dispõe GIL (2010), essa forma de amostragem é baseada na viabilidade e ocorre quando os sujeitos são selecionados por disponibilidade ou proximidade. Logo, não há definição de critérios de participação dos respondentes pois, o questionário fora enviado a diversos funcionários da instituição de forma heterogênea, independente de variáveis como: o departamento de lotação do servidor, conhecimento sobre do tema tratado no estudo, idade, sexo, etc. Vale ressaltar que a análise quantitativa realizada não tem pretensões universalizantes, pois não se trata de uma amostragem aleatória. Trata-se apenas de um estudo de caso.

A entrevista semiestruturada visou coletar informações a respeito da existência e a administração de um sistema de gestão de segurança da informação, a presença de boas práticas de segurança da informação, o alinhamento da segurança da informação a alguma norma em especial, o alinhamento da alta direção com a segurança da informação e o gerenciamento de incidentes na organização.

Devido ao contexto de análise do Sistema de Gestão da Segurança da Informação da organização foi adotado o procedimento metodológico da pesquisa exploratória através dos métodos de pesquisa: qualitativos e quantitativos. Os dados foram coletados e analisados com o intuito de auxiliar no esclarecimento e compreensão do instrumento de pesquisa (BOGDAN & BIKLEN, 1994). A aplicação do questionário e da entrevista semiestruturada objetivaram a verificação de aspectos fundamentais

através da perspectiva dos participantes e sua diversidade e aumentar a variedade de abordagens e de métodos de pesquisa (FLICK, 2009, p. 23).

A entrevista semiestruturada serviu de base para as análises dos requisitos utilizados pelo órgão para a criação do seu SGSI, seleção dos controles de segurança da informação, gestão de riscos de segurança da informação, gerenciamento de incidentes. Os resultados das análises foram utilizados para verificar: a consonância dos requisitos escolhidos com a norma ABNT ISO/IEC 27001/2013 responsável por determinar os requisitos necessários para cobrir todo o ciclo de vida de um SGSI; o alinhamento dos controles de segurança da informação à luz da ABNT ISO/IEC 27002/2013; a conformidade da gestão de riscos de segurança da informação com a norma ABNT ISO/IEC 27005/2011 responsável por fornecer diretrizes para a Gestão de Riscos de Segurança da Informação de uma organização; a forma de gerenciamento de incidentes e sua aderência ao ITIL. Os resultados da entrevista semiestruturada atuarão de forma qualitativa e serão usados para compreender e interpretar alguns comportamentos na instituição, a opinião e expectativas do entrevistado.

Os resultados das respostas do questionário serão utilizados para verificar a correlação entre o conhecimento das políticas de segurança da informação do órgão, sua aplicação no dia a dia e o número de incidentes, suas causas e os impactos. A intenção foi levantar a efetividade e eficácia do Sistema de Gestão do Segurança da Informação da instituição. Ademais, os resultados tratarão da forma quantitativa do estudo e serão tabulados de forma absoluta com a intenção de apontar numericamente a frequência de determinados comportamentos dos funcionários, entretanto, a análise quantitativa não possibilita universalizar os resultados encontrados.

4 ANÁLISE E INTERPRETAÇÃO DOS DADOS

As duas fontes de dados (questionário e entrevista) anteriormente citadas foram utilizadas como base para a interpretação dos dados do estudo. Segundo Uwe Flick (2009), a interpretação de dados é a essência da pesquisa qualitativa, embora sua importância seja vista de forma diferenciada nas diversas abordagens.

4.1 A entrevista semiestruturada

A entrevista semiestruturada foi feita com o assessor chefe da assessoria de Tecnologia da Informação. Ele respondeu a vinte e uma perguntas que visaram analisar a segurança da informação, as boas práticas de segurança da informação, o envolvimento da alta direção na segurança da informação, a percepção do gestor a respeito do comprometimento dos usuários com a segurança e o gerenciamento dos incidentes na instituição.

4.1.1 O Sistema de Gestão de Segurança da Informação

A instituição não possui um Sistema de Gestão de Segurança da Informação (SGSI) e apoia sua segurança da informação na utilização de boas práticas de segurança da informação. O entrevistado, sobre a existência de um SGSI respondeu: "Não existe um sistema, mas sim boas práticas de segurança da informação". A seguir, foi indagado sobre as fontes que serviram de base para a implementação, manutenção ou melhoria contínua da segurança da informação.

Apesar de não possuir um SGSI bem definido, existem as práticas que são baseadas em *compliances*[4] dos negócios da instituição, elas também são regidas por normas específicas as quais a instituição deve seguir para atuar no contexto em que está inserida. Desta forma, a norma ABNT NBR ISO/IEC 27001/2013 responsável por determinar os requisitos necessários para o estabelecimento, implementação, manutenção e melhoria contínua de um SGSI não poderá ser utilizada em sua totalidade, limitando o estudo apenas a algumas partes da norma.

4.1.2 A governança e gestão de TI

[4] Conformidade com normas legais, regulamentos externos e internos, políticas e diretrizes estabelecidas.

A governança e a gestão de TI atuam em contextos distintos e, consequentemente, possuem objetivos diferentes. Por tal motivo, convém que haja a sua separação. O *framework*[1] COBIT é ideal para orientar qualquer organização com relação ao assunto pois há entre os seus princípios a separação das áreas. A instituição não segue uma norma, política ou *framework*[1] e não há a separação das áreas. Sobre o comprometimento e visão da alta direção o entrevistado respondeu: "A visão ainda é fraca, uma vez que o *turnover*[5] da alta direção é alto, e geralmente esse assunto é delegado para a assessoria de TI. O comprometimento é alinhado com o que é apresentado de demanda, ou seja, acontece de acordo com o que a gente fala que precisa ser feito, mas a passos lentos".

Assim como disponibilizado no manual de boas práticas em segurança da informação do TCU o a alta direção da organização deve participar do processo de elaboração das políticas de segurança da informação, por isso, o comprometimento da alta direção deve existir. Vale lembrar que o processo de elaboração das políticas de segurança da informação deve ter participação da alta direção, pois, conforme dispõe o manual, convém que a sua aprovação seja feita pelo mais alto dirigente da instituição.

4.1.3 Os controles de segurança da informação

A inexistência de um SGSI não impossibilita a implementação dos controles à luz da ABNT NBR ISO/IEC 27002/2013. Dito isso, a entrevista focou em fatores que proporcionassem uma análise das boas práticas de segurança da informação presentes na organização seguindo a norma citada anteriormente como fonte de orientação. Segundo a norma, os "controles podem ser selecionados desta norma ou de outros conjuntos de controles, ou novos controles podem ser projetados para atender necessidades específicas, conforme apropriado".

Durante a entrevista fora indagado a fonte dos controles selecionados e o entrevistado respondeu que os controles são baseados no Sistema de Gestão da Qualidade da organização (ISO 9001), ITIL e os *compliances* descritos anteriormente. Com a intenção de verificar o alinhamento a respeito da atualização dos controles

[5] Renovação ou rotatividade dos membros da alta direção.

existentes na instituição, foi perguntado sobre a atualização, validação e melhoria dos controles a intervalos de tempo definidos. O entrevistado respondeu que existe um intervalo de tempo definido para a validação, atualização e melhoria dos controles, complementou dizendo que os controles têm um prazo de revisão definido individualmente e finalizou dizendo que existe um sistema que gerencia toda a documentação e ciclo de vida destes controles.

4.1.4 As boas práticas de segurança da informação na Instituição

A entrevista mostrou que o grande foco da organização consiste em aplicar boas práticas de segurança da informação aliadas aos controles que em sua grande maioria são transparentes ao usuário. Apenas a varredura rotineira do sistema de antivírus em mídias disponíveis não ocorre de forma transparente, apesar da programação das rotinas acontecerem independente da ação do usuário. A política de segurança em mídias móveis (*pendrive*, HD, CD-ROM, DVD) ocorre de maneira obrigatória e automática, independendo da vontade do usuário.

Outra boa prática de segurança da informação implementada na organização é sua política de *backup*, que até o momento da entrevista se mostrou robusta e confiável. As boas práticas de segurança da informação são disseminadas na instituição através de treinamentos e campanhas sistêmicas, sobre segurança no ambiente, na operação com TI e assunto correlatos, com periodicidade de três meses, até o ano de 2016. No ano de 2017 houve uma mudança na periodicidade, que passou a ser mensal. Tal periodicidade mostra a preocupação da organização e do setor de TI em conscientizar os funcionários sobre a importância da segurança da informação para a realização de suas atividades diárias em sistemas de TI.

Conforme preconiza a ITIL, convém que a organização gerencie ativamente seus itens de configuração, que compreende qualquer componente ou ativo de serviço que necessite ser administrados de forma a entregar um serviço de TI. Para atender a esse controle, a organização utiliza o *software* Kaspersky para o gerenciamento de inventário de software nas máquinas cliente. Desta forma, o administrador possui o controle de todos os softwares instalados na máquina do cliente

protegendo a máquina de instalações de *softwares* piratas sem licença o que possibilitaria a exploração de alguma vulnerabilidade.

A grande parte das boas práticas de segurança da informação ocorrem de maneira transparente para os usuários, segundo o entrevistado, o entendimento dos riscos e o respeito às boas práticas disseminadas são os aspectos fundamentais que dependem do usuário para o sucesso da segurança da informação na organização. Diante disto, o comprometimento e aderências às políticas de segurança da informação foi objeto de questionamento. Como frisado pelo entrevistado o comprometimento e aderência às políticas e práticas de segurança da informação possui um nível médio, pois o corpo profissional é muito heterogêneo (idade, formação acadêmica, formação profissional, etc.) na instituição, entretanto, houve uma melhora do comprometimento e aderência devido a disseminação do conhecimento e ações mais ríspidas com relação ao tema.

4.1.5 Gerenciamento de incidentes

O gerenciamento de incidentes na organização segue, de acordo com o entrevistado, métodos internos, mesclados com a técnica PDCA (*Plan – Do – Check – Act)* e boas práticas da ITIL. O PDCA também conhecido como Ciclo de Deming é um modelo cíclico que possui 4 etapas e busca aumentar o nível de maturidade em um determinado processo. A metodologia é muito utilizada na ITIL, porém focada no processo de Melhoria Contínua de Serviço.

A ITIL possui um processo específico para o gerenciamento de incidentes em uma instituição. Para que o processo obtenha um nível aceitável de sucesso a ITIL recomenda que exista uma central de serviços para que o incidente receba o tratamento adequado e que todo o seu ciclo de vida possa ser acompanhado por um responsável. A instituição ainda não possui uma central de serviços para a resolução dos incidentes do dia a dia, nem para o registro e acompanhamento dos incidentes durante o seu ciclo de vida, mas de acordo com o entrevistado a concepção de uma central é um projeto para o ano de 2017. O pequeno número de incidentes nos últimos seis meses pode ser o motivo da ausência de uma central de serviços na instituição. Conforme falado pelo entrevistado, houve somente dois incidentes neste período.

Apesar da carência de uma central de serviços, a instituição possui uma base de eventos e erros conhecidos, além de procedimentos para o atendimento de processos como expressado pelo entrevistado. Tal base é crucial, pois será utilizada pelo Gerenciamento de Incidentes para a resolução de futuros incidentes que possuam a mesma causa. Ademais, a base de erros conhecidos quebra o paradigma "ilha de conhecimento" pois, desta forma, a resolução de um problema não estará mais vinculada a um funcionário, e sim, documentada e disponível para qualquer pessoa que tenha acesso à base de maneira sistemática. Por fim, fora indagado sobre a existência da relação entre prioridade de tempo limite de resolução de um incidente. O entrevistado respondeu que a relação existe na organização.

4.1.6 Gestão de riscos de TI

A gestão de riscos da instituição existe, porém, transcrevendo as palavras do entrevistado é superficial e está alinhada com a ISO 9001. A norma ABNT NBR ISO/IEC 27005/2011 é focada na gestão de riscos de TI. A norma ISO 9001 foi criada com o intuito de estabelecer requisitos para o Sistema de Gestão da Qualidade de uma organização. O objetivo é proporcionar um nível maior de confiança aos clientes da instituição. Desta forma, a norma não se encaixa de maneira adequada para a gestão de riscos de TI além de não ser a mais indicada para tratar o assunto.

Uma peça fundamental da gestão de riscos é o plano de continuidade de negócios. Entre as perguntas direcionadas ao gestor de TI, foi perguntado se a instituição possuía um plano e qual a norma foi usada como orientadora para a sua confecção. O entrevistado respondeu: "Sim, possui, pois é uma exigência dos *compliances* dos negócios: ANVISA, OMS, INMETRO e ONA. A existência de um plano de continuidade dos negócios já é um ponto positivo para a gerência de riscos da instituição, porém, sua análise mais profunda focando na norma ABNT NBR ISO/IEC 27005/2011 que foi criada para atingir esse objetivo não é possível devido a critérios de segurança da própria organização.

O diagnóstico resultante da entrevista é que a segurança da informação ainda não é tratada estrategicamente na organização, a alta direção ainda não está comprometida com o tema, a instituição precisa criar uma gestão de riscos de segurança

da informação e alinhar sua gestão da segurança da informação às normas especificas criadas.

4.2 O questionário sobre segurança da informação

O questionário sobre segurança da informação foi aplicado através do *software* Google Docs e foi respondido por sessenta e oito funcionários da autarquia estadual. O questionário objetivou aferir o conhecimento sobre a política de segurança da informação da organização, quantidade semanal do uso de algum tipo de sistema informatizado (*software)*, verificar o conhecimento e execução das políticas de segurança da informação por parte dos funcionários, levantar informações sobre violações de segurança da informação sofridas pelos respondentes e seus impactos e indagar sobre a visão que o respondente tem a respeito do nível de importância do assunto tratado no estudo e seu trabalho cotidiano.

4.2.1 A utilização de sistemas informatizados na Instituição

A organização estudada não tem como atividade fim o uso de computadores e sistemas informatizados no dia a dia funcional. Entretanto, quase a totalidade (66 respondentes) dos respondentes utilizam algum tipo de sistema informatizado para a realização de seus trabalhos, 1 respondente utiliza entre 3 ou 4 vezes por semana e 1 não utiliza.

O resultado comprova o argumento que a TI está enraizada no cotidiano de qualquer organização. A TI tornou-se uma ferramenta fundamental para ampliação e efetivação do objetivo global da Administração Pública: prover aos cidadãos e a sociedade bens e serviços públicos de qualidade. Outro fator a ser considerado é que sessenta e oito respondentes, o que representa 98,5% do total, consideram seu trabalho importante ou muito importante para o funcionamento da organização.

4.2.2 As boas práticas de segurança da informação

As boas práticas de segurança da informação estão presentes no órgão conforme falado pelo gesto de TI da organização. Elas são difundidas através de diversos mecanismos como campanhas mensais a respeito do assunto. Porém, para uma maior efetividade do tema, a contribuição dos funcionários é essencial. Diante disto, o questionário procurou explorar o assunto através de cinco perguntas.

4.2.2.1 Conhecimento sobre políticas de segurança, sua importância e uso na criação de senhas

Primeiramente, foi perguntando o nível de conhecimento sobre as políticas da informação existentes no órgão. A prevalência das respostas tendeu para o conhecimento total e parcial, respectivamente, 29,4% e 58,8%. Isto demonstra que os esforços e campanhas frequentes surtiram o efeito desejado e perseguido pelos gestores de TI da organização.

A escolha das senhas utilizadas no acesso dos serviços na rede do órgão seguiu as políticas de segurança da informação em 91,2% dos entrevistados, restando apenas 4,4% para aqueles que não seguiram nenhuma política de segurança da informação do órgão para a definição de suas senhas e 4,4% não souberam responder. Verifica-se que muitos usuários seguem as recomendações da Cartilha de Segurança para a Internet publicada pelo CGI.br que preconiza que as senhas devem ser escolhidas de acordo com as políticas organizações.

Outra política observada no questionário foi a política de *backup* por parte dos funcionários. A intenção foi verificar a existência de cópias de segurança dos arquivos necessários para a realização do trabalho diário. Neste contexto, 79,4% dos respondentes disseram que possuem *backup* dos arquivos, 16,2% disseram não ter alguma cópia de segurança e 4,4% não tem conhecimento. Conforme sugerido pela norma ABNT ISO/IEC 27002/2013 convém que procedimentos como cópias de segurança (*backup)* sejam documentados e disponibilizados a todos os usuários que necessitem deles.

No universo dos respondentes, 86,8% deles consideravam o assunto segurança da informação muito importante, 11,8% importante e apenas 1,5% não tinham conhecimento sobre a importância da segurança da informação. Isto resultado demonstra que o público alvo das campanhas sistêmicas sobre o tema entende o nível de relevância do assunto. Conforme preconiza o controle conscientização, educação e treinamento em segurança da informação da norma ABNT ISO/IEC 27002/2013, convém que todos os funcionários da organização recebam treinamento, educação e

conscientização apropriados e as atualizações regulares das políticas e procedimentos organizacionais relevantes para a s suas funções.

4.2.2.2 Aspectos preventivos e conhecimento sobre vírus de computador

Os vírus de computador estão entre os males mais comuns entre os violadores de segurança. Devido a isso, duas perguntas focaram o assunto, com o intuito de elucidar possíveis hipóteses sobre o assunto. De acordo com o gestor de TI da autarquia, a varredura do antivírus ocorre de maneira transparente para o usuário e esse pode ser o motivo pelo qual 8,8% disseram que não tem conhecimento sobre a existência de antivírus em seu computador e apenas 1,5% respondeu não possuir antivírus no computador.

Todavia, a grande maioria, 89,7% informou que possui antivírus em seu computador. O objetivo da pergunta seguinte relacionada ao assunto foi verificar o cuidado preventivo por parte dos funcionários na execução do antivírus antes da abertura de algum arquivo oriundo de alguma mídia móvel. As respostas foram variadas sendo que 39,7% sempre realizam a varredura, 25% na maioria das vezes, 8,8% ocasionalmente, 7,4% raramente e, por fim, 19,1% nunca realizam a varredura. Isto demonstrou um ponto negativo na pesquisa, pois, conclui-se pouco comprometimento com o tema. O controle registros e monitoramento da norma ABNT ISO/IEC 27002/2013 pois, além de eventos de segurança da informação ele pode ser usado para registrar atividades do usuário, exceções e falhas do sistema. A análise desses registros pode ser usada para direcionar companhas mais objetivas em temas deficientes no tocante a segurança da informação. Tal indagação objetivou a análise de comprometimento dos servidores com o assunto pois, a varredura é obrigatória de acordo com as políticas de segurança da informação do órgão e realizada de forma transparente para qualquer tipo de mídia inserida no computador do usuário.

4.2.2.3 Análise sobre comprometimento

Nota-se que o empenho dos funcionários é muito bom, pois a grande maioria segue as boas práticas de segurança da informação que o órgão preconiza. Infelizmente, o seguimento das boas práticas não impede que exista violações de segurança. Seu intuito é mitigar ao máximo a ocorrência e a probabilidade de invasões

de usuários não autorizados. Como mencionado pelo gestor de TI entrevistado, o corpo funcional heterogêneo do órgão e seus diversos níveis apresentados na resposta do gestor mostra-se o desafio enfrentado pelo departamento de TI do órgão que tenta através das campanhas de conscientização nivelar o conhecimento dos funcionários. Tais campanhas estão em acordo com o controle de conscientização, educação e treinamento em segurança da informação da norma ABNT ISO/IEC 27002/2013 citado anteriormente.

4.2.3 Violações de segurança e seus impactos

O grande objetivo de um SGSI é reduzir a possibilidade ou o risco de uma violação de segurança dos sistemas de TI da organização. As interrupções dos serviços TI podem causar enormes prejuízos para qualquer instituição, principalmente aquelas que utilizam a TI para a realização de tarefas essenciais para o seu funcionamento e armazenamento de informações sigilosas e sensíveis.

As violações de segurança não se limitam apenas a parte virtual das organizações. Prova disto é o caso ocorrido em 27 de dezembro de 2005, onde um incêndio destruiu seis dos dez andares do edifício do Instituto Nacional de Seguro Social (INSS), no Setor de Autarquias Sul, em Brasília (LAUDO, 2006). Estima-se que o prejuízo causado pelo incêndio tenha sido da ordem de bilhões de reais, pois muitos processos contra devedores da Previdência Social foram destruídos na ocasião (FUTEMA, 2005).

4.2.3.1 Violações de segurança da informação por vírus de computador

O assunto, vírus, voltou a ser alvo de consulta na pesquisa e por isso, os participantes foram indagados sobre a violação da segurança por algum tipo de vírus de computador. As respostas foram variadas: 42,6% nunca tiveram seus computadores infectados por vírus, 19,1% uma ou duas vezes, 2,9% entre três e cinco vezes, 4,4% mais de cinco vezes e 30,9% não se lembraram. Vale lembrar que, as capacidades de proliferação e replicação dos vírus de computador são os principais obstáculos enfrentados em seu combate.

Além disto, os vírus criam brechas no sistema que podem ser exploradas futuramente pelo invasor e podem ser imperceptíveis para usuários sem experiência na

análise dos impactos causados pela infecção por algum tipo de vírus. Essas características dificultam o trabalho dos administradores de rede, pois um simples computador infectado pode comprometer toda a rede de uma determinada organização e a rastreabilidade muito difícil. Por serem difíceis de rastrear, um controle que registra eventos e gera evidências (log) de eventos de segurança da informação deve existir e ser mantido e analisado criticamente a intervalos regulares como dispõe o controle registros e monitoramento da norma

4.2.3.2 Acesso não autorizado por terceiros, dado extraviado, excluído ou alterado

O acesso ao computador pessoal deve ser uma preocupação recorrente e este tópico é exclusivamente dependente do usuário final. Não divulgar as senhas de acesso pessoal a serviços é uma das várias recomendações que são dadas para diminuir o risco de acesso não autorizado. Na instituição estudada, 55,9% nunca tiveram seu computador acesso por terceiros sem autorização, 7,4% tiveram seus computadores acessados sem autorização uma ou duas vezes, 1,5% entre três e cinco vezes, 4,4% mais de cinco vezes e 30,9% não tem conhecimento. Esse último dado demonstra que a possibilidade de acesso não autorizado pode ter ocorrido, porém, não foi percebida.

O grande número de pessoas que nunca tiveram seu computador acessado sem autorização corrobora e pode ter relação com outra questão. Na instituição, 48,5% nunca tiveram algum dado extraviado, excluído ou alterado, parcial ou integralmente em seu computador de trabalho, seguido de 32,4% tiveram informações comprometidas uma ou duas vezes, 7,4% entre três e cinco vezes, 4,4% mais de cinco vezes e, por fim, 7,4% não tem conhecimento.

Aqueles que tiveram alguma informação perdida, excluída ou alterada relataram que em dezenove oportunidades o comprometimento da informação ocorreu devido a falhas nas conexões de rede, treze por motivo de queda de energia, cinco por causa de vírus de computador, três provocado por dano físico em algum componente do computador e dois foram originados por queima do dispositivo de armazenamento externo. Para seis perguntados, o motivo associado ao comprometimento da informação fora outro que não os enunciados anteriormente.

Conforme aconselhado pela norma ABNT NBR ISO/IEC 27002/2013, uma forma de proteger as informações de acesso não autorizado é a utilização de uma política de mesa limpa e tela protegida. Ela reduz o risco de não só de acesso não autorizado, a perda ou dano da informação. Essa política tenta cercar ações não autorizadas durante ou fora do expediente normal de trabalho.

Uma solução possível é a utilização de outros mecanismos de controle de acesso, conforme incentiva o manual de boas práticas do TCU. Recomenda-se a desativação da sessão após a inatividade por período de tempo determinado. Este recurso está disponível em alguns sistemas operacionais e o próprio usuário pode configurá-lo. Outro mecanismo, é a limitação de quantidade de sessões concorrentes impede a conexão de um usuário em terminais distintos. Isto reduz o risco de acesso de um invasor caso o usuário esteja conectado.

4.2.3.3 Impactos das violações de segurança

Os impactos oriundos das violações de segurança são os mais variados. Eles podem causar desde prejuízos financeiros até ativos intangíveis como a imagem da organização, mas o prejuízo mais evidente é sem dúvida, a perda financeira. Ela pode ser desmembrada em diversas variantes como por exemplo: interrupção dos serviços.

Por isso, fora perguntado quantas vezes que problema ocasionado por falhas de segurança comprometera a realização dos trabalhos funcionais nos últimos seis meses. Pelo menos, 50% - 48,5% uma ou duas vezes e 1,5% entre três e cinco vezes - respondeu que ao menos uma vez teve seus trabalhos interrompidos. Do restante, 33,8% nunca tiveram seu trabalho comprometido e 18,2% não se lembraram. Esse mostra como as violações impactam o cotidiano de uma organização.

O tempo perdido, aproximadamente em horas, pelos funcionários com relação a essas falhas de segurança da informação gerou interrupções de trabalho que foram: menos duas para 32,4% deles, 13,2% entre duas e seis, 5,9% entre seis e dez, 4,4% entre dez e dezesseis e 8,8% mais de quatorze. Dentre os respondentes, 35,3% informaram que não se lembravam do tempo perdido. Tais dados demonstram o impacto causado pelas falhas de segurança podem ocasionar na continuidade dos negócios da organização.

5 CONSIDERAÇÕES FINAIS

A instituição objeto do estudo é uma instituição muito importante pois é possível observar a variedade e abrangência dos serviços prestados em apoio ao Sistema Único de Saúde do estado de Minas Gerais. Conforme mostrado no estudo, a instituição apoia grande parte dos seus negócios sobre os serviços de TIC e a falta de um sistema especifico de segurança da informação é um fator negativo, pois compromete a continuidade dos negócios da organização.

A análise das metas da presidência para o ano corrente na instituição estudada demonstra que a TI ainda é tratada como uma área sem a devida importância para a alta direção. Em períodos de crise como o vivido atualmente, a destinação de recursos exclusivos para a melhoria da segurança da instituição pode enfrentar obstáculos por causa do seu valor financeiro diante da escassez de recursos vivida pela instituição.

Como mostrado nas normas[2] estudadas, a escolha de um SGSI é uma decisão estratégica e necessita do apoio da alta direção. Infelizmente, como respondido na entrevista com o gestor de TI, a alta rotatividade dos gestores dificulta a implementação de tal sistema. A implementação de um SGSI não deve ser uma decisão, tampouco, o objetivo da gestão de TI. A metodologia de atendimento às demandas de segurança da informação de acordo com o seu surgimento não é uma forma correta e se mostra uma maneira reativa de tratativa do assunto.

Porém por necessidade de atendimento às normas de negócio e *compliances,* a instituição possui um nível de segurança bem definido em outras áreas, o que pode corroborar para o pequeno número de incidentes registrados no período de seis meses. Os controles de segurança da informação juntamente com os controles de outras normas demonstraram, até o momento, um ótimo nível de efetividade. Somado a isso, as campanhas sistemáticas de conscientização demonstraram estar surtindo efeitos positivos junto aos funcionários da organização.

A escolha de normas orientadoras no assunto segurança da informação, como por exemplo ABNT NBR ISO/IEC 27002/2013, responsável pela seleção dos

controles de segurança da informação, poderia facilitar a administração do assunto, pois a norma (ISO 9001) utilizada na instituição que não é focada na segurança da informação.

Outro fato observado foi a ausência de uma gestão de riscos de segurança da informação. Como respondido na entrevista realizado com o gestor de TI, a norma ISO 9001 utilizada para o tratamento de riscos não é focada especialmente no assunto segurança da informação. Uma recomendação seria a utilização da norma ABNT NBR ISO/IEC 27005/2011 que possui o propósito de fornecer diretrizes para o processo de Gestão de Riscos da Segurança da Informação de uma organização. Outro fator que corrobora para a escolha da norma é que ela está intimamente relacionada com a norma ABNT NBR ISO/IEC 27001/2013 que dispõe sobre os requisitos necessários para a implementação de um SGSI.

As aspirações de qualquer órgão da Administração Pública durante o uso da TI é prover serviços públicos eficientes e eficazes para a Sociedade. A utilização adequada da TI, no serviço público, automatiza os processos administrativos, tornando-os mais transparentes o que melhora o exercício do controle social e a participação social. Um exemplo claro disto é a Lei 10.520/2002, comumente conhecida como a lei do pregão. Devido a isso, o maior desafio encontrado é o aprimoramento do uso da TI em organizações públicas.

Para a transposição de tal desafio, a utilização das normas citadas durante o transcuro do estudo seria uma ótima escolha para o gerenciamento de todo o ciclo de vida de um SGSI na instituição estudada. Todas as normas da família ABNT NBR ISO/IEC 27000 atuam de maneira conjunta e complementar. Além disto, outras fontes complementares especialistas podem ser usadas como o *framework*[1] COBIT que foca em prover um modelo para uma governança e gestão de TI eficaz e eficiente.

Em suma, os pontos negativos identificados na organização são: a) a não adoção ou alinhamento a uma norma orientadora específica de segurança da informação para tratar o assunto, pois, a instituição orienta-se pela ISO 9001; b) a utilização de boas práticas de segurança da informação ante a utilização de um sistema de gestão de segurança da informação; c) a falta de alinhamento dos controles de segurança da

informação com a norma ABNT ISO/IEC 27002/2013; d) a inexistência de uma gestão de riscos de segurança da informação; e) falta de comprometimento da alta direção como dispõe a norma ABNT ISO/IEC 27001/2013; f) a inexistência de uma central de serviços para a gestão de incidentes conforme estimula a ITIL.

Após a análise dos programas e ações promovidas pela SEPLAG foi constatado que ainda não existe nenhum programa focado exclusivamente em segurança da informação. Entretanto, ficou evidente que a SEPLAG está preocupada em aperfeiçoar diversos serviços prestados através de uma melhora da TIC em órgãos do estado através de determinados programas. O programa Governança Eletrônica pode ser citado como exemplo. Ele objetiva melhorar a prestação de serviços através de canais eletrônicos de atendimento, promover a gestão de documentos através de ferramentas virtuais e disponibilizar mecanismos de padronização para a gestão de TIC e seus processos.

As descobertas feitas na análise da segurança da informação do órgão possibilitaram sugestões de trabalhos futuros na própria instituição. Entre elas, pode-se citar: a implementação de um Sistema de Gestão de Segurança da Informação de acordo com as normas referência no assunto, a adequação dos controles implementados e criação de novos sob a orientação da norma ABNT ISO/IEC 27002/2013, implementação de uma gestão de riscos de segurança da informação na organização, a análise de um número maior de controles de segurança da informação na organização. Outros trabalhos futuros focando a área acadêmica podem ser desenvolvidos como: análise da gestão de riscos da segurança da informação no serviço público ou estudo sobre os investimentos em segurança da informação no serviço público.

O estudo fora limitado por alguns aspectos inerentes a sua própria natureza. A segurança da informação é um assunto sensível e estratégico para qualquer instituição e trata-lo com atores externos à organização limitam o aprofundamento em assuntos específicos do tema. Outro aspecto limitador foi o público alvo do estudo ante o número expressivo de funcionários do órgão. A organização possui mais de mil funcionários e apenas sessenta e oito responderam ao questionário.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Código de Prática para controles de segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:** Gestão de riscos de segurança da informação. Rio de Janeiro, 2011.

BOGDAN, R.; BIKLEN, S. **Características da investigação qualitativa. In: Investigação qualitativa em educação: uma introdução à teoria e aos métodos.** Porto, Porto Editora, 1994. p.47- 51.

BRASIL. Tribunal de Contas da União. **Boas práticas em Segurança da Informação.** 4 ed. Brasília, 2012.

BRASIL. Tribunal de Contas da União. **Guia de boas práticas em contratação de soluções de tecnologia da informação:** riscos e controles para o planejamento da contratação**.** Versão 1.0. Brasília, 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Planejamento Estratégico da Secretaria de Tecnologia da Informação 2016-2019.** Brasília: MP, 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet.** Versão 3.1. São Paulo, 2006.

COSTA, Regivaldo Gomes. **Terceirização de serviços de TI:** aspectos de segurança. 2010. Artigo (Programa de Pós-Graduação *lato sensu* em MBA – Governança em Tecnologia da Informação) – Universidade Católica de Brasília/Fundação Universa, Brasília, 2010.

DANTAS, Marco Leal. **Segurança da Informação:** Uma Abordagem Focada em Gestão de Riscos. Olinda, PE 2011.

FERNANDES, Jorge Henrique Cabral (Org.). **Gestão da Segurança da Informação e Comunicação**. (Segurança da Informação, v. I). Brasília: Faculdade da Ciência da Informação, 2010.

FLICK, UWE. **Introdução à pesquisa qualitativa.** Tradução Joice Elias Costa. 3ed. Porto Alegre: Artmed, 2009.

FUTEMA, Fabiana. Incêndio destruiu processos administrativos e logísticos do INSS, diz deputado. Da Folha Online, São Paulo, 29 de dezembro. 2005. Disponível em:< http://www1.folha.uol.com.br/folha/cotidiano/ult95u116752.shtml>. Acesso em: 13 abril de 2017.

GIL, A.C. **Como elaborar projetos de pesquisa**.5ª ed. São Paulo: Atlas, 2010.121p.

INTERNATIONAL STANDARD (ISO/IEC). **ISO/IEC 27000** – Information technology — Security techniques — Information security management systems — Overview and vocabulary. Suíça, 2014.

ISACA. **COBIT 5 – Modelo Corporativo para Governança e Gestão de TI na Organização.** São Paulo, 2012**.**

LAUDO aponta que incêndio no prédio do INSS foi acidental. Folha de São Paulo com Agência Brasil, São Paulo, 14 de janeiro. 2006

MARCIANO, João Luiz Pereira. **Segurança da Informação – uma abordagem social.** Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2006.

*OFFICE FOR GOVERNMENT COMMERCE (*OGC). ***Information Technology Infrastructure Library* (ITIL).** Versão 3. 2011.

PMG ACADEMY. **ITIL: Ciclo de Deming ou PDCA.** Disponível em <http://www.pmgacademy.com/pt/blog/artigos/itil-ciclo-de-deming-ou-pdca>. Acesso em: 10 de abril de 2017.

SOUSA, Evaldo Silva de. **A gestão da TI dentro do serviço público.** In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA. 2013, Rio de Janeiro. [s.n.]

SOUZA, Jackson Gomes Soares, *et al* **Gestão de riscos de segurança da informação e sua apresentação na governança de TI da administração pública.** In: X WORKSHOP DE PÓS-GRADUAÇÃO E PESQUISA DO CENTRO PAULO SOUZA. 2015, São Paulo. [s.n.]

VIEIRA, Flávia Monaco, SANTOS, Vando Vieira Batista dos. **Governo Eletrônico: A busca por um governo mais transparente e democrático.** In: III Congresso Consad de Gestão Pública. 2010, Brasília.

APÊNDICE 1 – Questionário

Especialização em Administração Pública, Planejamento e Gestão Governamental
Informações para o(a) participante voluntário(a):

Você está convidado(a) a responder este questionário anônimo que faz parte da coleta de dados da pesquisa sobre a Gestão da Segurança da Informação na Fundação Ezequiel Dias, sob responsabilidade do(a) pesquisador(a) Eduardo de Oliveira Vasconcelos, Max Melquiades da Silva e a Fundação João Pinheiro.
Caso você concorde em participar da pesquisa, leia com atenção os seguintes pontos: a) você é livre para, a qualquer momento, recusar-se a responder às perguntas que lhe ocasionem constrangimento de qualquer natureza; b) você pode deixar de participar da pesquisa e não precisa apresentar justificativas para isso; c) sua identidade será mantida em sigilo; d) caso você queira, poderá ser informado(a) de todos os resultados obtidos com a pesquisa, independentemente do fato de mudar seu consentimento em participar da pesquisa.

QUESTIONÁRIO:

1. Você utiliza algum sistema informatizado (*softwares*) para realizar seu trabalho?

	Sim
	Não

2. Com qual frequência?

	Todos os dias
	3 ou 4 vezes na semana
	2 vezes na semana
	1 vez na semana
	Raramente
	Não utiliza.

3. Você conhece as políticas de segurança da informação existentes em seu órgão?

	Conhece totalmente
	Conhece a maior parte
	Neutro
	Conhece pouco
	Desconhece

4. A escolha das suas senhas seguiu alguma política de segurança da informação do órgão?

	Sim
	Não
	Não tenho conhecimento

5. Você possui backup dos arquivos necessários para a realização do seu trabalho?

	Sim
	Não
	Não tenho conhecimento

6. Seu computador possui proteção (antivírus) contra códigos maliciosos?

	Sim
	Não
	Não tenho conhecimento

7. Você executa o antivírus antes de executar algum arquivo presente em alguma mídia móvel (*pendrives*, HD, DVD, CD-ROM)?

	Sempre
	Maioria das vezes
	Ocasionalmente
	Raramente
	Nunca

8. Você já sofreu algum tipo de invasão em seu computador de trabalho?

	Mais de 5 vezes
	Entre 3 e 5 vezes
	Neutro
	Entre 1 e 2 vezes
	Nunca

9. Você já perdeu de dados, parcialmente ou integralmente, ou teve algum dado corrompido em seu computador do trabalho?

	Mais de 5 vezes
	Entre 3 e 5 vezes
	Neutro
	Entre 1 e 2 vezes
	Nunca

10. Você já foi infectado por algum vírus em seu computador do trabalho?

	Mais de 5 vezes
	Entre 3 e 5 vezes
	Neutro
	Entre 1 e 2 vezes
	Nunca

11. Quantas vezes algum problema ocasionado por falhas de segurança comprometeu a realização de seu trabalho nos últimos 6 meses?

	Mais de 5 vezes
	Entre 3 e 5 vezes
	Não me lembro
	Entre 1 e 2 vezes
	Nunca

12. Quanto tempo aproximadamente você calcula ter perdido nos últimos 6 meses, decorrentes de impossibilidade de trabalho ou retrabalho relacionado às falhas de segurança da informação mencionadas acima?

	Mais de 24 horas
	Entre 12 horas e 23 horas
	Neutro
	Entre 6 horas e 11 horas
	Entre 3 e 5 horas
	Entre 1 e 2 horas
	Menos de 1 hora

13. Qual o nível de importância a respeito da segurança da informação, você considera?

	Muito importante
	Importante
	Neutro
	Pouco importante
	Sem importância

14. Como você julga o nível de importância do seu trabalho para a organização?

	Muito importante
	Importante
	Neutro
	Pouco importante
	Sem importância

APÊNDICE 2 – Roteiro de entrevista semiestruturada
Especialização em Administração Pública, Planejamento e Gestão Governamental
Entrevista semiestruturada

1. A instituição possui um sistema de gestão de segurança da informação (SGSI)?

2. Os requisitos de sua implementação, manutenção ou melhoria seguem alguma norma?

3. Os controles selecionados para o SGSI seguiram alguma norma?

4. Os controles são validados, atualizados ou melhorados durante algum intervalo de tempo?

5. Existe gestão de riscos de TI na instituição? Ela está alinhada com alguma norma?

6. Como é feita a gestão e governança da TI? Existe a separação entre os assuntos? A governança e gestão de TI seguem alguma norma, política, *framework*?

7. Como tem sido o comprometimento e a visão da alta direção com relação a um Sistema de Gestão de Segurança da Informação?

8. Como são tratados os incidentes de segurança da informação? A instituição segue alguma prática, framework ou biblioteca para gerenciá-los?

9. A instituição possui um plano de continuidade de negócios? Ele foi confeccionado de acordo com alguma diretiva ou norma?

10. A instituição utiliza boas práticas em Segurança da Informação?

11. Existe algum controle de inventário de software na organização?

12. Política de segurança da informação para mídias móveis?

13. É feito treinamento dos funcionários relacionados à segurança da informação? Como são difundidas as políticas de segurança da informação?

14. Quais os processos de segurança da informação são transparentes aos usuários?

15. Que aspectos da segurança da informação dependem fundamentalmente do usuário?

16. Como você vê a aderência/comprometimento dos servidores (funcionários) às políticas e práticas de segurança da informação?

17. Como você avalia a efetividade do SGSI? Foram registrados incidentes nos últimos 6 meses?

18. Existe uma central de serviços que classifica e prioriza os incidentes?

19. A organização possui um *software* que registre os incidentes e controle todo seu ciclo de vida?

20. Existe uma base de registros de erros conhecidos para que os funcionários responsáveis pela resolução dos incidentes possam consultar e tentar associar o erro com algum erro conhecido?

21. Os erros têm a relação de resolução de acordo com a prioridade? Existe um tempo limite definido e relacionado com a classificação do incidente?

APÊNDICE 3 – Termo de consentimento livre e esclarecido

Especialização em Administração Pública, Planejamento e Gestão Governamental

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

PESQUISA: Gestão da Segurança da Informação
As informações contidas nesta folha, fornecidas por Eduardo de Oliveira Vasconcelos têm por objetivo firmar acordo escrito com o(a) voluntária(o) para participação da pesquisa acima referida, autorizando sua participação com pleno conhecimento da natureza dos procedimentos a que ela(e) será submetida(o).

1) Natureza da pesquisa: Esta pesquisa tem como finalidades: verificar a segurança da informação na organização.

2) Participantes da pesquisa: (colocar o número de participantes, especificando qual será a população alvo da pesquisa).

3) Envolvimento na pesquisa: Ao participar deste estudo você DESCREVER. Você tem liberdade de se recusar a participar e ainda de se recusar a continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo para você. Sempre que quiser poderá pedir mais informações sobre a pesquisa através do telefone do coordenador do projeto e, se necessário, por meio do telefone do Comitê de Ética em Pesquisa.

4)Sobre as coletas ou entrevistas: As (se houver, especificar como serão realizadas).DESCREVER O LOCAL.

5) Sobre as entrevistas e questionários: DESCREVER os procedimentos que serão adotados

6) Confidencialidade: Todas as informações coletadas neste estudo são estritamente confidenciais. Os dados da(o) voluntária(o) serão identificados com um código, e não com o nome. Apenas os membros da pesquisa terão conhecimento dos dados, assegurando assim sua privacidade.

7) Benefícios: Ao participar desta pesquisa você não terá nenhum benefício direto. Entretanto, esperamos que este estudo contribua com informações importantes que deve acrescentar elementos importantes à literatura, onde o pesquisador se compromete a divulgar os resultados obtidos.

8) Pagamento: Você não terá nenhum tipo de despesa ao autorizar sua participação nesta pesquisa, bem como nada será pago pela participação.

9) Liberdade de recusar ou retirar o consentimento: Você tem a liberdade de retirar seu consentimento a qualquer momento e deixar de participar do estudo sem penalizastes.

Após estes esclarecimentos, solicitamos o seu consentimento de forma livre para permitir sua participação nesta pesquisa. Portanto, preencha os itens que seguem:
CONSENTIMENTO LIVRE E ESCLARECIDO

Eu, _____,
RG_____ após a leitura e compreensão destas informações, entendo que a participação de (escrever o nome do menor), sob minha responsabilidade, é voluntária, e que ele(a) pode sair a qualquer momento do estudo, sem prejuízo algum. Confiro que

recebi cópia deste termo de consentimento, e autorizo a execução do trabalho de pesquisa e a divulgação dos dados obtidos neste estudo.
Obs: Não assine esse termo se ainda tiver dúvida a respeito.
Belo Horizonte, _____/_____/_____
Telefone para contato:_____
Nome do Voluntário :_____
Assinatura do Responsável: _____
Assinatura do Pesquisador: _____
Contatos: NOME E TELEFONE DOS PESQUISADORES: