DOI: 10.5748/9788599693124-13CONTECSI/PS-3929

MODEL FOR INFORMATION SECURITY ASSESSMENT IN SELECTION PROCESS

Stellio Matos Mineiro (Universidade Estadual de Goiás, Goiás, Brasil) – stellio.matos@outlook.com
Prof. Dr. Francisco Ramos de Melo(Universidade Estadual de Goiás, Goiás, Brasil) – francisco.melo@ueg.br

People selection processes, such as public contests and university entrance exams, require information security to ensure fair, isonomic and quality results. Organizations that provide selection services without appropriate information security may be affected by security incidents that will bring false results, cost increases and tarnish the image of the organization. This study analyzed information security controls used in selection processes in order to demonstrate the application of an assessment model. Methodologically, the study was distinguished as an exploratory and descriptive research, considering the perception of respondents in 136 issues related to the proposed theme, divided into physical, logical and administrative aspects, identifying critical points of failure and risks related to the information environment. Thus, with the outcomes it was possible to propose improvements to operational processes and changes in organizational cultures to minimize operational risks, reduce costs and increase the credibility of organizations.

Keywords: Information security,security in publiccontest, security protocol in university admission test, ISO/IEC 27002:2013.

MODELAGEM DE AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO EM PROCESSOS DE SELEÇÃO

Processos de seleção de pessoas, como concursos e vestibulares, requerem segurança da informação para garantir resultados com qualidade, lisura e isonomia. Organizações que realizam serviços de seleção sem se preocuparem com a segurança da informação podem sofrer incidentes de segurança, acarretandoem falsos resultados, aumentos de custos e comprometimento da imagem da organização. Este trabalho analisou controles de segurança da informação utilizados em processos de seleção com o objetivo de demonstrar a aplicação de um modelo de avaliação desta segurança. Metodologicamente, o trabalho se distinguiu como uma pesquisa exploratória e descritiva, considerando a percepção de respondentes em 136 questões relacionadas ao tema proposto, divididos em aspectos físicos, lógicos e administrativos, para identificar pontos críticos de falhas e riscos relacionados ao ambiente da informação. Desta forma, com os resultados obtidos, foi possível propor melhorias aos processos operacionais e mudanças nas culturas organizacionais, visando minimizar riscos operacionais, reduzir custos e aumentar a credibilidade das organizações.

Palavras-chave:Segurança da informação, segurança em vestibular, segurança em concurso público, ABNT NBR ISO/IEC 27002:2013.

1. INTRODUÇÃO

O avanço da tecnologia da informação e da comunicação proporcionou uma crescente preocupação com a segurança da informação, tendo esta como um ativo de grande valor para qualquer organização pública ou privada. Incidentes de segurança da informação são cada vez mais comuns e não se limitam apenas a roubo de dados pessoais ou espionagem industrial, mas a ataques e monitoramento a governos e países. Em 2015, foram reportados ao CERT.br[1] mais de 70 mil incidentes de segurança da informação ocorridos no país.

Para instituições que realizam processos de seleção (concursos/vestibulares) a segurança da informação é fator chave para garantir o sucesso do negócio com lisura e isonomia para com todos os candidatos. Com a criação de novos órgãos públicos e com a abertura de faculdades particulares houve um aumento no número de processos de seleção, destinados ao preenchimento destas novas vagas. Este aumento resultou em uma oportunidade de negócio, fazendo surgir novas empresas e instituições que realizam este tipo de trabalho.

A maioria destas empresas não possui uma estrutura básica mínima, com requisitos de segurança bem estabelecidos e atendidos, que permita a execução dos processos de seleção com a garantia da segurança da informação, segurança esta que se faz necessária pela própria natureza dos serviços de seleção. O que ocorre, então, são processos de seleção realizados precariamente e com grande possibilidade de ocorrência de falhas, como pode ser observado nas provas do Exame Nacional do Ensino Médio (ENEM) de 2009, 2010 e 2011 (COM 5,7, 2012). Em 2009, ocorreu a subtração de uma prova da gráfica. Um ano depois, provas apresentaram problemas de impressão e em 2011 alguns candidatos tiveram prévios acessos a algumas questões da prova.

Diante disto, se faz necessário a elaboração de modelos para identificação e análise de requisitos de segurança da informação que possibilitem a avaliação de organizações que realizam processos de seleção, quanto à segurança da informação e da comunicação, proporcionando mecanismos para melhoria da estrutura e dos procedimentos organizacionais, para fundamentação de requisitos para licitação/contratação, bem como, para fiscalização destas organizações.

A proposta deste artigo é o estudo e levantamento do cenário atual de uma organização que realiza processos de seleção por meio da criação e aplicação de um modelo de avaliação da segurança da informação, possibilitando a identificação e a classificação do nível de existência de estrutura básica para realização dos processos de forma segura, que minimize as falhas e diminua os riscos que possam comprometer os resultados, onerar os custos de execução e fragilizar a credibilidade da organização. Para isto será utilizada, como padrão orientador, a norma ABNT NBR ISO/IEC 27002:2013 - Código de prática para a gestão de segurança da informação.

2. INFORMAÇÃO E SUA SEGURANÇA

A história da informação está incorporada na história da escrita e da fala. Civilizações antigas, como os sumérios e os egípcios, desenvolveram tipos de escritas utilizadas para proteger e perpetuar suas informações e os conhecimentos relacionados às mesmas (QUEIROZ, 2005, p.4-5).

[1] CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

No decorrer da história muitas tecnologias da informação e da comunicação foram criadas. Tais tecnologias provocaram mudanças culturais e deram novos sentidos aos panoramas sociais, econômicos, científicos e políticos. A exemplo disto pode-se destacar a prensa para impressão tipográfica do alemão Johannes Gutenberg (ca. 1398-1468), que principiou o processo de disseminação de informações e publicação de conhecimento (CAPOBIANCO & CURY, 2011, p.3).

O tema da segurança da informação surgiu bem depois, porém a preocupação com a proteção da informação também remonta aos tempos antigos. Esta preocupação foi percebida principalmente em momentos de guerras, nas quais a grande necessidade era a troca de mensagens codificadas de forma a escondê-las dos inimigos, mesmo se fossem apossadas por estes (COHEN, 1995).

Ainda quanto à informação, a preocupação em entender o que ela é de fato iniciou-se na década de 1940, com a publicação do artigo "*The mathematic Theory of communication urban*", de Shannon e Weaver, dando origem a ciência da informação. A partir de 1960, o termo "ciência da informação" foi amplamente utilizado (SIEWERT, 2006, p.2).

Então, na mesma década, surgem os primeiros computadores. São grandes equipamentos eletromagnéticos, constituídos principalmente por relês ou válvulas. O foco da segurança no controle de acesso físico e na manutenção do ambiente de operação possibilitava a percepção e monitoramento mais ágil de problemas eventuais de segurança (CÔRTE, 2014, p.65).

Já na década de 1960, com a disseminação da ciência da informação, surgem as primeiras pesquisas sobre redes de comutação de pacotes e a criação de protocolos de trabalhos em redes conectadas (TANENBAUM, 2003, p.54-58). Tem-se início a Internet, e com ela as questões de segurança da informação são focadas nos aspectos lógicos e tecnológicos. (STALLINGS, 2007, p.702-703).

Consequentemente, com o avanço das tecnologias que permitiram a criação de computadores cada vez menores, mais rápidos e mais acessíveis e com a expansão da Internet, das redes locais, das trocas e compartilhamentos de informações, surgem também, de forma acelerada, novas ameaças e com estas a crescente preocupação com a segurança da informação. Côrte (2014, p.66) afirma que a interconexão de microcomputadores e a expansão das redes possibilitou a interação de qualquer lugar físico. Isto fez surgir novas vulnerabilidades e ameaças, alterando o foco da segurança. Este passa a enfatizar os controles de acesso lógico, preocupados com o acesso indevido da informação por usuários não autorizados ou sistemas não autenticados, e com a continuidade dos serviços, buscando o desenvolvimento de planos de contingência e de recuperação de desastres, pois a indisponibilidade dos mesmos poderia causar impactos negativos aos negócios das organizações.

Para Siewert (2006, p.1), o crescimento sucessivo das correspondências e transações eletrônicas particulares, comerciais e bancárias, entre outras, evidenciou o problema da gestão da informação. Esta se empenhava em gerenciar as informações que trafegavam nas redes de computadores e na segurança das informações trocadas entre usuários e sistemas. É fundamental destacar que a percepção da importância da informação evoluiu juntamente com o progresso tecnológico. O entendimento desta importância se faz necessário para compreender a necessidade da segurança da informação. Assim sendo, é importante saber o que é e quanto vale a informação para entender o porquê de protegê-la.

2.1. Informação

O conceito de informação é muito diversificado, conforme seu uso e contexto. Para a ciência da informação seu significado tem base definida a partir da separação dos conceitos distintos de dados e informação.

Dados podem ser definidos como sendo fatos brutos sobre eventos que não possuem significado, porém, estes dados podem ser organizados de maneira a obterem significado, transformando-se em informação (MOSCOVE, SIMKIN & BAGRANOFF, 2002, como citado em SILVA, 2011, p.22).

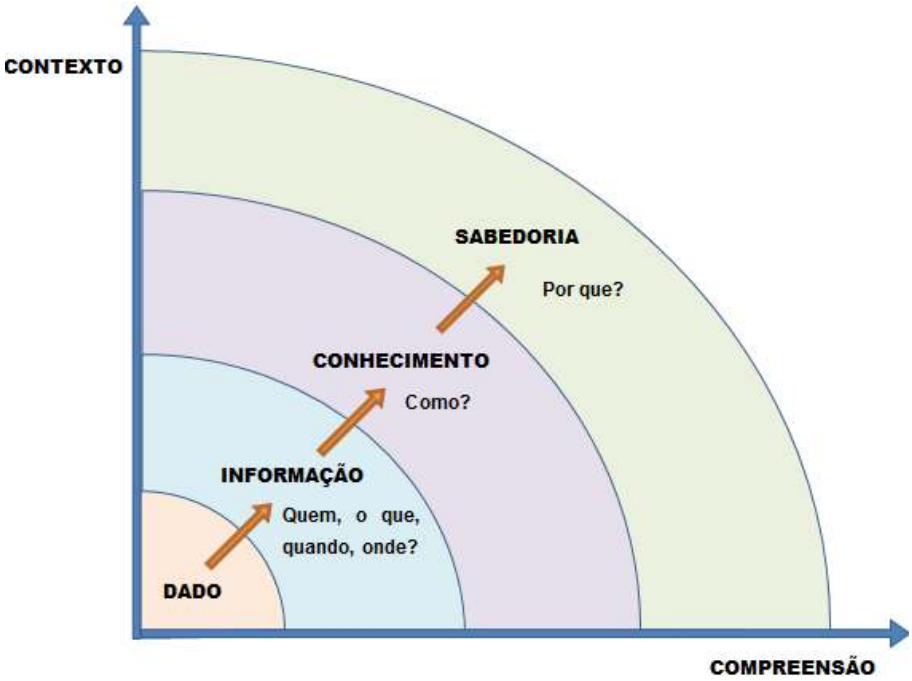
Tarapanoff (2006, p.21-23) conceitua informação sob duas perspectivas: a primeira, ciência da informação, a informação é o conhecimento comunicado, portanto, dados contextualizados e transmitidos. A segunda, gestão da informação, a informação é todos os tipos de informação de valor, tanto de origem interna quanto externa à organização.

Já para Sêmola (2014, p.43), informação é o conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais.

Com o rápido progresso tecnológico, à estas definições foram agregadas outras e a informação ganhou novas distinções e pesos. Surgem os conceitos de conhecimento e sabedoria, demonstrando um escalonamento dependente da informação, conforme apresentado na hierarquia da informação ou pirâmide do conhecimento, também conhecido como modelo DIKW (do inglês, *Data/Information/Knowledge/Wisdom*) ou modelo DICS (Dado/Informação/Conhecimento/Sabedoria).

Nesta abordagem, a informação tem sua origem nos dados, acrescentados de contexto, significados, estrutura e organização. Esta informação, processada e compreendida, gera conhecimento. Ao conhecimento gerado pode-se agregar o entendimento de quando e o porquê empregá-lo, o que define a sabedoria (DROGSETH & TURBITT, 2008, p.2). A Figura 1 ilustra este relacionamento.

Figura 1 – Modelo DIKW



Fonte: Adaptada de DROGSETH e TURBITT (2008, p.2)

2.2. Valor da informação

Ao longo do tempo o valor da informação foi ganhando peso e a percepção da sua importância foi ressaltada como papel da transformação da sociedade. Lesca e Almeida (1994, p.66) já destacavam esta transformação devido ao intenso envolvimento da informação e de seus fluxos. Para eles, naquele momento a informação permitiu uma grande mudança na economia global, pois sua utilização, como fator de produção, possibilitou a agregação de valor aos produtos e serviços desde sua elaboração até sua entrega aos clientes. Desta forma era necessária uma administração estratégica da informação, ou seja, um gerenciamento organizado da informação para fins estratégicos, objetivando a obtenção de vantagens competitivas (LESCA & ALMEIDA, 1994, p.66-67). Lesca e Almeida (1994, p.67-68), então, destacam a importância da informação como fator de apoio à decisão, de produção, de sinergia e determinante de comportamento.

Choo (2003, p.27-29) percebe a inerência da informação em quase todas as atividades das organizações. A teoria de administração daquela época enfatizou o valor da geração e utilização da informação no papel de dar sentido às mudanças do ambiente externo, na geração de novos conhecimentos por meio do aprendizado e como fator de suporte a decisões.

Observam-se, ao computar os aspectos apresentados pelos autores, que a informação possui diferentes papéis e utilidades perante sua criação e utilização nas organizações e na sociedade, mas percebe-se um ponto em comum: o papel estratégico no apoio às decisões.

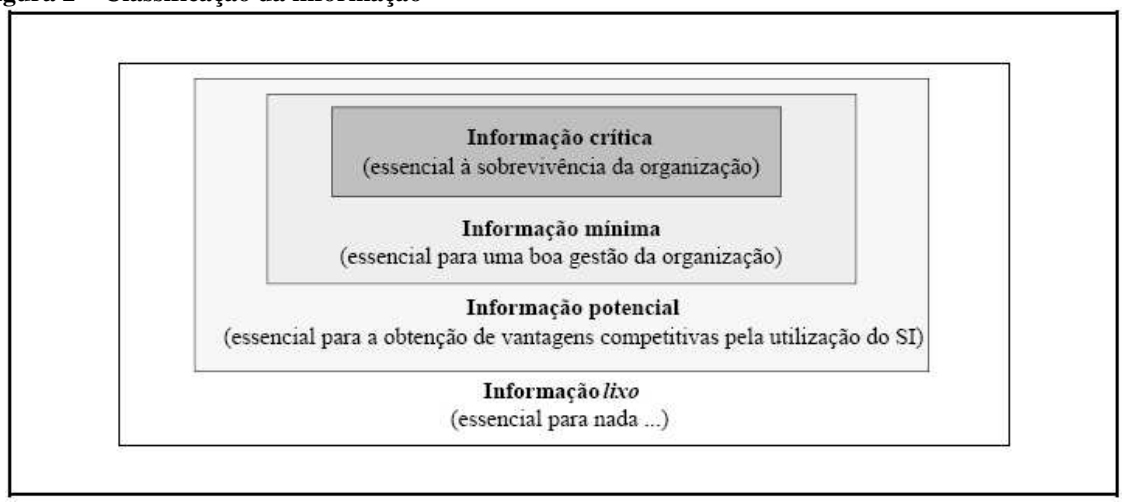
Outro ponto a destacar é o relacionamento do valor da informação com sua potencialidade de uso e com sua utilidade. Por este raciocínio, a informação é valorizada pelo contexto da sua serventia para aqueles que a usam. Ou seja, o usuário da informação é quem percebe e define o valor da mesma, conforme suas experiências e os momentos e contextos em que a informação é utilizada (CÔRTE, 2014, p.58).

A informação passa a ser tratada com um ativo, e como tal, representa algo que tem valor para a organização. A norma ABNT NBR ISO/IEC 17799:2005 define a informação como um importante ativo e essencial para os negócios da organização, e sua proteção assegura a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado (ABNT, 2007, p.X).

A atribuição de valor à informação é determinante para a definição da sua segurança. Efetivamente os custos de proteção são definidos pelo valor do objeto a ser protegido, de forma que este custo não seja maior que o valor do objeto alvo da proteção. A partir da correta atribuição de valor à informação é possível dimensionar a segurança necessária para protegê-la.

Outro aspecto importante para definição de valor e dimensionamento da segurança da informação é a classificação da informação. O processo de classificação da informação possibilita a categorização da sua proteção, definindo-se custos e recursos conforme o grau de importância da informação. Amaral (1994, p.28-29) apresentou uma estrutura de classificação definida em função das atribuições que a informação pode exercer nas atividades da organização, ilustrada na Figura 2. Conforme Amaral (1994, p.28-29), quanto mais crítica a informação, mais recursos são necessários para sua proteção.

Figura 2 – Classificação da informação



Fonte: Amaral (1994, p.29)

2.3. Segurança da informação

2.3.1. Definições

Cepik (2003, p.138) define segurança como uma condição relativa de proteção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa.

Este conceito, quanto à informação, ainda não foi totalmente consolidado, tendo muitas definições que abordam diferenciados contextos e focos.

Em 2004, Peltier, em seu livro "*Information Security Policies and Procedures"* define a segurança da informação como "a prevenção e recuperação de destruição, modificação, divulgação, não autorizada ou indesejável, ou uso de informação e recursos de informação, sendo acidental ou intencional" (PELTIER, 2004, p.257, tradução nossa) [2].

Marciano e Lima-Marques (2006, p.95) sugerem uma nova definição para segurança da informação que englobe os agentes humanos e ambientais envolvidos na sistemática da segurança da informação. Para eles, segurança da informação era a somatória do sistema social no qual se encontra, abrangendo usuários, sistemas e suas interações, e do complexo tecnológico que sustentava estas interações.

Sêmola (2014, p.41) define segurança da informação como sendo uma área de conhecimento destinada ao resguardo da informação como ativo, contra acessos desautorizados, indevidas alterações e sua indisponibilidade.

Outra possível definição é que a segurança da informação é o estudo sistemático de metodologias que visam garantir o estado ou qualidade de seguro da informação, mitigando ameaças e minimizando riscos e danos.

A norma ABNT NBR ISO/IEC 17799:2005 descreve segurança da informação como a proteção da informação de diversas ameaças para assegurar a continuidade do negócio, atenuar riscos e maximizar lucros (ABNT, 2007, p.X).

Desta certa forma, considerando-se estas e outras definições, percebe-se uma complementaridade de suas abordagens. Isto direciona a visão da segurança da informação

[2] "Information security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional."

como responsabilidade mais abrangente da organização como um todo, e não exclusivamente da área de tecnologia.

2.3.2. Princípios da segurança da informação

Qualquer informação pode ser influenciada por três princípios básicos: confidencialidade, integridade e disponibilidade. A garantia destes princípios é o objetivo principal da segurança da informação (BRASIL, 2012, p.9-10).

Segundo Vidal (2010, p.6) estes princípios norteiam a análise, planejamento e implementação da segurança de um determinado grupo de informações as quais precisam de proteção. Ele descreve estes princípios como:

- Confidencialidade: garantia de que a informação só pode ser acessada e manipulada por pessoas autorizadas, ou seja, ela é restrita a um conjunto de entidades, que podem ser pessoas ou um sistema eletrônico;
- Integridade: garantia de que, toda vez que uma informação é manipulada, ela está consistente, ou seja, que não foi alterada ou adulterada por um acesso legal ou ilegal; e
- Disponibilidade: garantia de que uma informação sempre poderá ser acessada, por pessoas e processos autorizados, independentemente do momento em que ela é requisitada e do local no qual está armazenada.

Para Sêmola (2014, p.43) confidencialidade representa a proteção da informação conforme o grau de sigilo de seu conteúdo, objetivando a restrição de acesso e de utilização por apenas pessoas a quem se destina; integridade é a conservação da informação na mesma conjuntura em que foi disponibilizada pelo proprietário, objetivando proteção contra modificações indevidas, intencionais ou não; e disponibilidade é a acessibilidade da informação produzida ou obtida por um indivíduo ou organização, devendo estar disponível aos seus usuários no instante em que eles necessitem delas para qualquer propósito.

Apesar de não constituírem os princípios básicos da segurança da informação, outros atributos são relacionados por diversos autores com sendo importantes para garantia da proteção do ativo de informação, a exemplo de:

- Autenticidade: garantia de que as entidades fontes da informação são verdadeiras e que a informação não sofreu alterações ao longo do processo de comunicação. A autenticidade visa assegurar a validação da identificação da entidade que presta a informação (BRASIL, 2012, p.9);
- Legalidade: propriedade de que a informação está de acordo com as cláusulas contratuais pactuadas e com a legislação vigente, ratificando o valor legal da informação dentro do processo de comunicação. Atualmente é definida como conformidade, tendo o papel de garantir o cumprimento das obrigações organizacionais, englobando compromissos com *stakholders* a aspectos legais e regulatórios relacionados à administração das empresas (SÊMOLA, 2014, p.42);
- Não-repúdio: também chamada de irretratabilidade, atributo da informação que garante a impossibilidade de negar a autoria em relação a uma transação realizada. Para a norma ISO/IEC 27000:2014 (referência para termos e vocabulários de segurança da informação), é a capacidade de provar a ocorrência de um alegado evento ou ação, bem como a sua entidade originária (ABNT, 2014, p.7).

2.3.3. Ciclo de vida da informação

A informação possui um ciclo de vida. Neste contexto, a informação pode ser criada, recebida, tratada, organizada, armazenada, utilizada, disseminada e descartada.

De acordo com Beal (2008, como citado em SILVA, 2010, p.28-29) o ciclo de vida da informação dentro das organizações apresenta sete etapas: identificação de necessidades e requisitos, obtenção, tratamento, armazenamento, distribuição, uso e descarte.

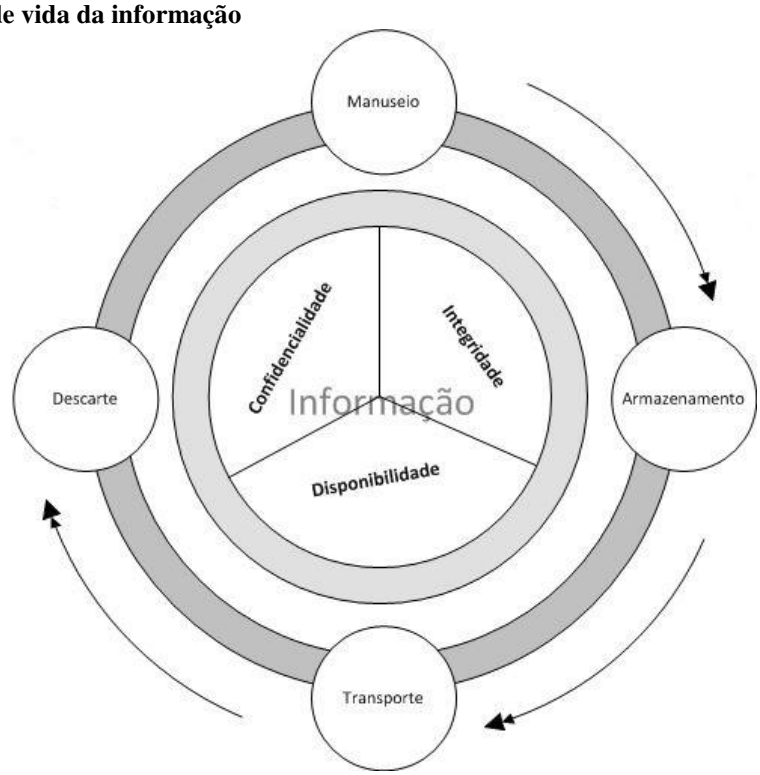
Já Sêmola (2014, p.10) apresenta o seguinte ciclo de vida para a informação: manuseio, armazenamento, transporte e descarte.

- Manuseio: momento em que a informação surge e é manipulada. É a fase onde a informação é criada e passa a ser manuseada;
- Armazenamento: momento de arquivamento da informação (seja meio físico ou digital);
- Transporte: momento em que a informação é conduzida, encaminhada ou compartilhada;
- Descarte: momento em que a informação perde sua serventia e é inutilizada ou descartada.

Este ciclo de vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Estes momentos são justamente vivenciados quando os ativos humanos, tecnológicos e físicos manuseiam a informação para dar suporte aos processos que mantêm a organização. Independentemente do formato de representação da informação, todos estes momentos se aplicam (SÊMOLA, 2014, p.9-10).

Sêmola ainda associa o ciclo de vida da informação aos princípios da segurança da informação, destacando a importância da garantia destes princípios durante todos os momentos ao longo do ciclo de vida, como ilustra a Figura 3.

Figura 3 – Ciclo de vida da informação



Fonte: Sêmola (2014, p.11)

2.3.4. Risco e seus conceitos associados

Como descrito anteriormente, a informação é colocada em risco durante os momentos vivenciados em seu ciclo de vida. Este risco implica na possibilidade do não atendimento de um ou mais princípios da segurança das informações e demais aspectos que a influenciam.

O risco compreende as possíveis oportunidades e condições que possibilitam a criação de eventos ou ampliação do seu potencial de danos e perdas (DANTAS, 2011, p.41). Já a norma ISO/IEC 27000:2014 adota o conceito de risco estabelecido na ISO GUIA 73:2009: "Risco é o efeito da incerteza sobre os objetivos" (ABNT, 2014, p.8).

Sêmola (2014, p.48) descreve risco como a possibilidade de **ameaças** explorarem **vulnerabilidades**, incorrendo em **incidentes** que provocam a quebra de sigilo, adulteração e indisponibilidade, causando, possivelmente, **impactos** nos negócios. Sob esta perspectiva, ele define os termos em destaque como:

- Ameaças: condições ou agentes que causam incidentes de segurança, pondo em risco as informações e seus ativos por meio da exploração de vulnerabilidades, ocasionando perdas de confidencialidade, integridade e disponibilidade;
- Vulnerabilidades: fraquezas presentes ou associadas a ativos que processam e/ou manipulam informações que possibilitam a ocorrência de incidentes de segurança. São elementos passivos, sendo exploradas pelas ameaças;
- Incidentes: eventos decorrentes da ação de uma ameaça ao explorar uma ou mais vulnerabilidades, conduzindo à perda de princípios da segurança da informação e, consequentemente, à impactos aos processos de negócio;
- Impactos: consequências e efeitos de danos ocasionados por um incidente de segurança sobre os processos de negócio.

Sêmola (2014, p.53) ainda destaca a importância do mapeamento e identificação da situação atual da organização, suas ameaças, vulnerabilidades, riscos, sensibilidades e impactos, a fim de possibilitar uma apropriada modelagem e dimensionamento da solução de segurança.

2.3.5. Norma ABNT NBR ISO/IEC 27002:2013

A ABNT é o Foro Nacional de Normalização, confirmado pelo governo federal, responsável pela publicação das Normas Brasileiras (ABNT NBR). Estas normas são elaboradas por seus Comitês Brasileiros (ABNT/CB), Organismos de Normalização Setorial (ABNT/ONS) e Comissões de Estudo Especiais (ABNT/CEE) (ABNT, 2015).

A norma ABNT NBR ISO/IEC 27002:2013, elaborada pelo Comitê ABNT/CB-021 Computadores e Processamento de Dados, tem sua origem na norma ISO/IEC 17799:2005. Ela é o modelo/padrão que fornece orientações para as normas de segurança da informação organizacionais e diretrizes para práticas de gestão de segurança da informação, incluindo seleção, implementação e gestão de controles considerando os ambientes de riscos de segurança da informação da organização (ABNT, 2013a). Conforme seu próprio título (Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação), a norma ABNT NBR ISO/IEC 27002:2013 é um documento genérico, consultivo, e não uma especificação formal. Ela recomenda controles de segurança da informação com seus respectivos

objetivos de segurança da informação, que atendam aos requisitos decorrentes de riscos para a confidencialidade, integridade e disponibilidade da informação (ISECT, 2015).

Para Sêmola (2014, p.139) a norma ABNT NBR ISO/IEC 27002:2013 é uma compilação específica de orientações e padronizações comuns voltadas para a gestão da segurança da informação. Sua elaboração foi motivada pelo nível de automação, de compartilhamento e de dependência da informação atingido pelo mercado. Como norma técnica, apresenta exemplos de critérios, padrões e instrumentos de controle, aplicáveis de forma parcial ou total conforme a natureza e porte de cada organização.

A norma ABNT NBR ISO/IEC 27002:2013 está logicamente estruturada em 14 grupos de controle de segurança relacionados. Estes grupos são denominados seções (ou domínios) e apresentam um agrupamento de 35 categorias com seus respectivos objetivos de controles. Os objetivos de controle, por sua vez, totalizam 114 controles (ABNT, 2013b, p.7). As 14 seções são:

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

3. PROCESSO DE SELEÇÃO

3.1. Conceitos

Processo de seleção de pessoas são mecanismos adotados para, de forma fundamentada, filtrar e definir as pessoas mais capacitadas para ocupar uma determinada vaga seja de emprego, estágio ou para cursos. Como exemplos destacam-se os concursos públicos e os vestibulares.

Estes dois tipos de processos de seleção, apesar de possuírem aspectos legais distintos, são norteados pelos Princípios da Administração Pública, conforme estabelece o caput do art. 37 da Constituição Federal de 1988:

Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...] (BRASIL, 2015, p.13).

Além destes princípios, os concursos públicos e os vestibulares obedecem ao princípio da isonomia ou igualdade. Este, assegurado como princípio constitucional, garante que todos são iguais perante a lei e possui ligação com o princípio da impessoalidade. Vieira (2013) descreve o princípio da impessoalidade como o objetivo de impossibilitar que um agente público aja com simpatia ou antipatia, vingança ou

favorecimento, na realização de seus atos administrativos, não tendo como finalidade o interesse público. Para ele o princípio da impessoalidade se traduz na busca do tratamento isonômico a ser dado a todos os administrados que se encontrem em idêntica situação jurídica.

A segurança da informação, apoiada em seus próprios princípios, vem sustentar esta necessária condição para garantir tratamento igualitário a todos os candidatos em concursos públicos ou vestibulares.

3.1.1. Vestibular ou processo seletivo

O vestibular, ou processo seletivo, é o processo de seleção para admissão aos cursos de graduação das instituições de educação superior.

Quanto aos aspectos legais, o Decreto n. 99.490, de 30 de agosto de 1990, em seu art. 1°, determina que as instituições de ensino superior devam realizar seus processos seletivos nos termos da lei, de seus estatutos e regimentos. Já a Lei n. 9.394, de 20 de dezembro de 1996, define o processo seletivo como meio de acesso aos cursos de graduação da educação superior (BRASIL, 1996).

Em 1998, O Ministério da Educação criou o Exame Nacional do Ensino Médio (ENEM) visando avaliar o desempenho dos estudantes ao fim da educação básica. A partir de 2009, o ENEM foi adotado, por algumas instituições, como mecanismo de seleção para o ingresso no ensino superior, seja complementando ou substituindo o vestibular. Respeitando a autonomia das universidades, a utilização dos resultados do Enem para acesso ao ensino superior pode ocorrer como fase única de seleção ou combinado com seus processos seletivos próprios (SOBRE O ENEM, 2011).

Apesar de ser um processo diferenciado, o ENEM segue o modelo de qualquer vestibular ou concurso, com provas objetivas e/ou discursivas (redação).

3.1.2. Concurso público

O concurso público é o processo de seleção para preenchimento de vagas de emprego ou cargo público. Para Carvalho Filho (2014, p. 632), concurso público é o procedimento administrativo que visa aferir as aptidões pessoais e selecionar os melhores candidatos ao provimento de vagas para cargos e funções públicas, por meio da verificação da capacidade intelectual, física e psíquica de interessados em ocupar estas vagas.

No que se refere a concursos públicos, o artigo 37, inciso II, da Constituição Federal (BRASIL, 2015, p.13) estabelece: “a investidura em cargo ou emprego público depende de aprovação prévia em concurso público de provas ou de provas e títulos, [...]”. Existe, ainda em tramitação, o Projeto de Lei n. 74, de 2010, que regulamenta o artigo 37, inciso II, da Constituição Federal, criando regras para a aplicação de concursos para a investidura em cargos e empregos públicos no âmbito da União, dos Estados, dos Municípios e do Distrito Federal. Neste projeto de lei, a preocupação quanto à segurança da informação pode ser percebida apenas no parágrafo 4, do artigo 16: “A inscrição pela internet impõe a adoção de processos de controle, segurança do procedimento e proteção contra fraude.” (BRASIL, 2013, p.6).

3.2. Estrutura e organização

Os concursos e processos seletivos seguem, normalmente, uma organização padrão quanto suas etapas de execução: inscrição, elaboração, impressão e armazenamento

de provas, aplicação de provas, correção de provas e apuração de resultados e divulgação de resultados. Estas etapas se aplicam a provas de conhecimentos, podendo variar para outros tipos de provas, como prova de aptidão física, de avaliação psicológica, de habilidade prática ou avaliação de títulos.

A etapa de inscrição é a porta de entrada do certame, caracterizada pelo registro da intenção de participar do processo e pela captação e armazenamento dos dados correlatos dos candidatos. Nesta etapa destaca-se a necessidade da garantia da integridade dos dados dos mesmos.

A elaboração, impressão e armazenamento de provas é a principal etapa de cada certame. Esta etapa é marcada pela criação e preparação das questões, a montagem da prova, impressão dos cadernos de prova e pelo acondicionamento seguro das provas até sua utilização. Neste momento é importante a garantia da confidencialidade das provas, de suas questões, bem como de seus gabaritos.

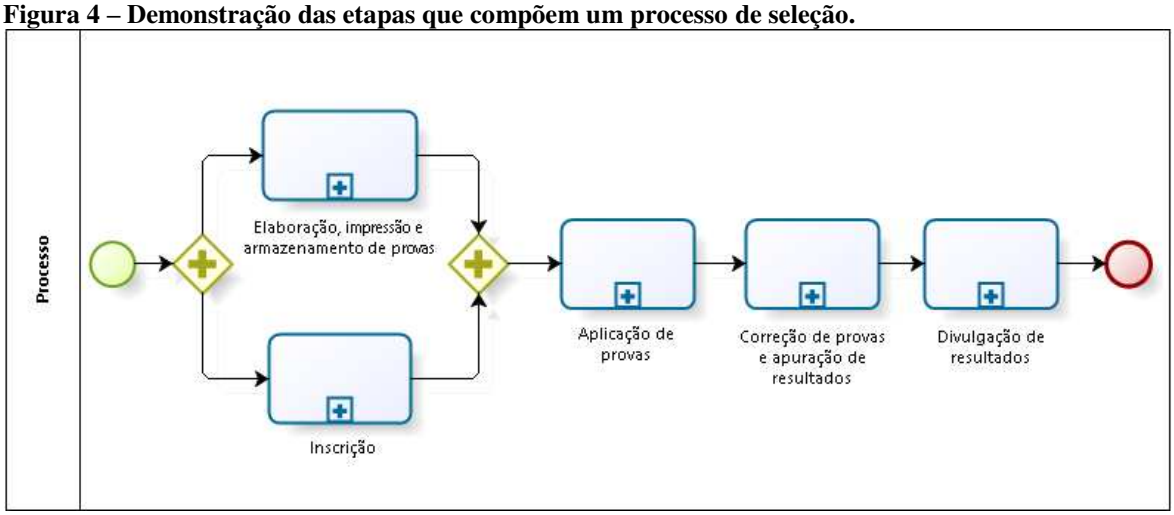
A aplicação da prova é o momento de utilização das mesmas onde os candidatos deverão responder as questões e registrar suas repostas em documento específico, que será utilizado como objeto de correção. Nesta etapa, os candidatos podem responder provas de questões objetivas, discursivas ou de redação. Destaca-se a importância da garantia de confidencialidade da prova e da integridade das respostas dos candidatos.

A etapa de correção de provas e apuração de resultados visa a aferição da capacidade técnica-teórica dos candidatos, conforme os pré-requisitos demandados da opção pretendida. Esta aferição é realizada por meio da comparação das respostas registradas pelos candidatos com os respectivos gabaritos ou respostas esperadas, sendo ests definidas previamente pelas bancas elaboradoras das questões aplicadas. Nesta etapa o foco da segurança é a confidencialidade e a integridade da apuração e dos seus resultados.

Na última etapa, divulgação de resultados, o importante é a disponibilidade dos resultados apurados das provas e a garantia da integridade das mesmas. Nesta etapa os resultados são dispostos para os candidatos da forma mais clara e objetiva possível.

Estas etapas são apenas macro momentos, que englobam outras atividades menores para sua realização e obtenção de seus respectivos resultados, conforme ilustra a Figura 4.

Figura 4 – Demonstração das etapas que compõem um processo de seleção.



Fonte: Elaborado pelo autor

3.3. Segurança da informação em processos de seleção

A segurança da informação é um pilar fundamental para o sucesso na realização de um certame. A garantia da disponibilidade, integridade e confidencialidade estão envolvidas em todas as etapas de execução de um concurso ou processo seletivo, e visam sustentar os preceitos de isonomia e transparência que norteiam qualquer processo de seleção.

O Quadro 1 demonstra o mapeamento do princípios da segurança da informação com relação as etapas de execução de um processo. Para cada etapa são identificados os princípios primários (P), foco da preocupação da segurança da informação naquele momento, e os princípios secundários (S), menos importantes, mas com forte relação com a segurança da informação da etapa.

Quadro 1 – Mapeamento dos princípios da segurança nas etapas do processo de seleção

	Inscrição	Elaboração, impressão e armazenamento de provas	Aplicação de provas	Correção de provas e apuração de resultados	Divulgação de resultados
Integridade	**P**	**S**	**P**	**P**	**S**
Disponibilidade	**S**	**S**			**P**
Confidencialidade	**S**	**P**	**S**	**S**	**S**

Legenda:
P =Primário
S =Secundário

Fonte: Elaborado pelo autor

4. METODOLOGIA

Esta pesquisa é exploratória e descritiva, apresentando um estudo de caso único de natureza aplicada, com abordagem qualitativa e quantitativa. Seu objetivo é identificar controles de segurança da informação em processos de seleção de pessoas (concurso/vestibular) e demostrar a aplicabilidade de um modelo de avaliação junto a uma instituição que desenvolve este tipo de serviço.

As instituições localizadas no Estado de Goiás que realizam processos de seleção (concurso/vestibular) foram identificadas como notáveis laboratórios para a pesquisa de campo, pelo fato de suas proximidades e pela abrangência de seus serviços exercidos nas esferas municipais, estaduais e federais.

Neste trabalho a organização adotada como objeto de estudo de caso é identificada, por questão de segurança, como organização G. Esta organização promove serviços de seleção de pessoas, tanto como concursos como vestibulares, em âmbito municipal e estadual.

A organização G é uma instituição que desenvolve diversas atividades/serviços de seleção de pessoas, atuando dentro do Estado de Goiás. Desde sua criação, em 1999, até ao final do ano de 2014, a organização G realizou mais de 160 (cento e sessenta) processos de seleção entre concursos e vestibulares. Em seu portifólio constam atividades como

assessoria acadêmica, técnica e jurídica na elaboração de editais e provas, comunicação e divulgação de processos e resultados, elaboração de formulários e captação de dados de inscrição, elaboração, impressão, armazenamento, transporte aplicação e correção de provas, exames, testes e avaliações. Sua estrutura está dividida em direção e seis coordenações (administrativa, técnica, acadêmica, tecnologia da informação, pessoas e logística) comportando mais de 30 colaboradores com vínculos diretos e indiretos.

Como principal ferramenta de coleta de dados foi utilizado o questionário. Conforme Gil (2008, p.121), o questionário é uma técnica de investigação composta por uma coleção de questões, apresentadas por escrito aos respondentes, com objetivo de obter informações sobre conhecimento de suas opiniões, sentimentos, interesses, expectativas e experiências. Além do questionário, revisões bibliográficas, entrevistas, observações participativas e levantamentos e estudos documentais auxiliaram na pesquisa como instrumentos complementares.

Foram elaborados três questionários, aqui denominados *check-lists*, com questionamentos sobre a presença de controles básicos de segurança da informação, baseados em experiência própria, em entrevistas e observações, e levando em consideração a norma ABNT NBR ISO/IEC 27002:2013. Estes *check-lists* foram organizados conforme a classificação proposta por Silva Netto e Silveira (2007, p.379-380): controles da camada física , controles da camada lógica e controles da camada humana (administrativa). Cada *check-list* abrange controles dentro de cada uma das etapas de um processo (Quadro 1): inscrição; elaboração, impressão e armazenamento de provas; aplicação de provas; correção de provas e apuração de resultados; e divulgação de resultados.

Os controles de segurança, que compõem os *check-lists*, foram definidos por meio de conhecimentos técnicos próprios, adquiridos com a experiência de mais dez anos de serviços realizados na seleção de pessoas em concursos e vestibulares, em observações participantes e na coleta de dados junto a outras instituições que realizam este tipo de serviço por meio de e-mails.

A camada física engloba o ambiente onde se encontra fisicamente os equipamentos (computadores, servidores, meio de comunicação), bem como a infraestrutura necessária para manter o bom funcionamento dos mesmos, como energia, climatização e cabeamentos (SILVA NETTO & SILVEIRA, 2007, p.379). O *check-list* da camada física possui 53 controles.

A camada lógica se qualifica pela utilização de *softwares* (programas ou sistemas computacionais) responsáveis pela funcionalidade do hardware e gestão das informações, como criptografia, transações, troca de mensagens e etc. (SILVA NETTO & SILVEIRA, 2007, p.379-380). O *check-list* da camada lógica é composto por 41 controles.

A camada administrativa é constituída pelos recursos humanos/administrativos presentes na organização, sendo a camada mais difícil de avaliação e gerenciamento da segurança, pois envolve o fator humano, como características psicológicas, socioculturais e emocionais (SILVA NETTO & SILVEIRA, 2007, p.380). O *check-list* camada humana possui 42 controles.

Estes controles, organizados e convertidos em questionamentos associados a uma escala Likert. A escala Likert (CÔRTE, 2014, p.112) é uma escala de resposta utilizada para captar o nível de concordância da opinião do respondente com a questão ou afirmativa. Para tanto, a questão ou afirmativa possui um intervalo de níveis de respostas possíveis, previamente determinado, dentro dos limites propostos. Optou-se, nesta pesquisa, por utilizar uma escala Likert de 4 (quatro) níveis: 1-Totalmente não aplicado, 2-Minimamente aplicado, 3-Razoavelmente aplicado e 4-Totalmente aplicado.

Após a criação dos *check-lists*, os mesmos foram submetidos a uma apreciação por parte da direção da instituição a ser avaliada com o intuito de esclarecimento e delineação da abrangência dos dados, visto que o tema trata de um assunto delicado quanto à exposição de informações.

Com a conclusão definitiva dos *check-lists*, estes foram aplicados e respondidos por colaboradores da organização G, indicados pela direção da mesma. Os *check-lists* foram respondidos por assessores e coordenadores que possuem maior familiaridade ou responsabilidade sobre determinado aspecto (camada). Cada respondente preencheu os três *check-lists*, o que possibilitou avaliar, além da sua camada de domínio, sua perspectiva sobre as demais camadas. Também foi solicitado o preenchimento dos *check-lists* a um assessor da direção, detentor de conhecimento e experiência mais ampla do negócio como um todo.

Por se tratar da instituição selecionada como objeto de estudo da pesquisa de campo o ambiente de trabalho do autor deste trabalho, optou-se por aplicar os *check-lists* de forma mais simplificada, a partir da disponibilização dos mesmos em formulários impressos.

5. ANÁLISE DE RESULTADOS

Após a aplicação dos *check-lists* e a captação dos dados em arquivo digital, no formato de planilha eletrônica, os mesmos foram tabulados e analisados com auxílio do *software* de planilha eletrônica LibreOffice Calc, em sua versão 5.0.1.2.

Para análise dos resultados, nesta pesquisa foram contabilizadas as respostas, de todos os respondentes, por nível, por etapa do processo de seleção e por dimensão (camada) que compõem a segurança da informação.

Os níveis adotados foram: 1-Totalmente não aplicado; 2-Minimamente aplicado; 3-Razoavelmente aplicado; e 4-Totalmente aplicado. As etapas do processo seleção são: inscrição (INS), elaboração, impressão e armazenamento de provas (EIA), aplicação de provas (APL), correção de provas e apuração de resultados (CAR) e divulgação de resultados (DIV).

Foi calculada, então, a média percentual do grau de aplicação dos controles de segurança em cada etapa para cada camada. As respostas também foram totalizadas, em cada nível, por cada camada, demonstrando um aspecto mais geral destas para cada etapa do processo de seleção. Esta totalização é percebida na apresentação da média geral (GER) de cada camada. Com isto, foram elaborados gráficos que permitiram uma melhor visualização das análises e, consequentemente, uma maior facilidade na descrição dos resultados.

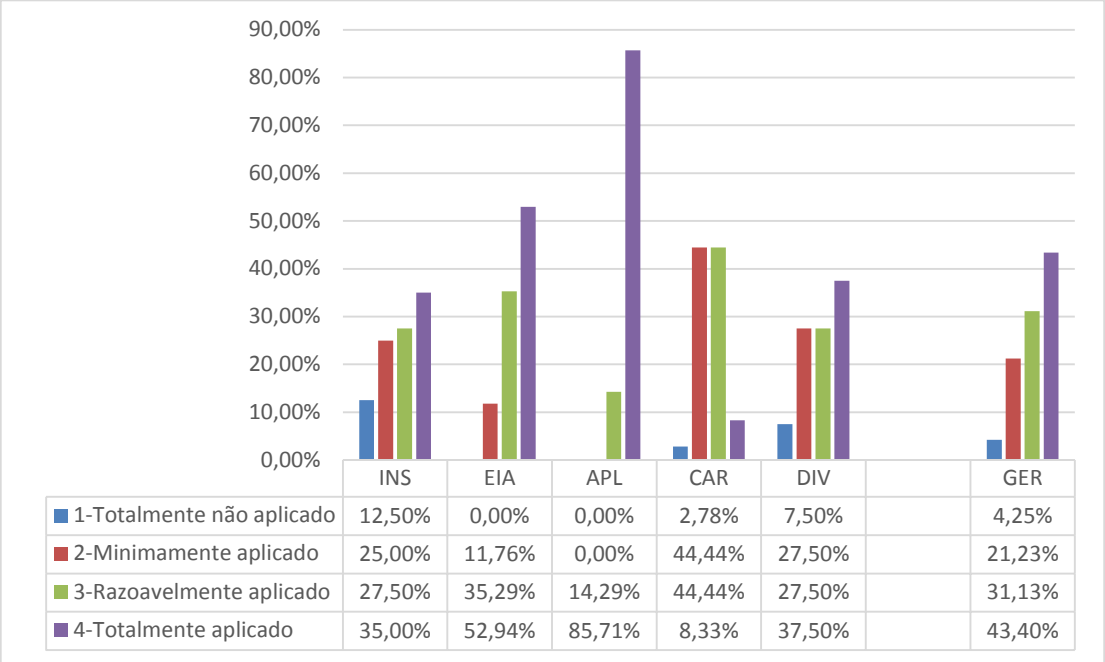
5.1. Resultados por camada

5.1.1. Camada física

Na camada física foram avaliados, principalmente, a segurança física de ambientes, o controle de acesso físico a estes ambientes e a infraestrutura fornecida para a manutenção dos mesmos.

O Gráfico 1 apresenta a avaliação do nível de aplicação dos controles de segurança da informação adotados para a camada física.

Gráfico 1 – Nível de aplicação dos controles de segurança – média da camada física



	INS	EIA	APL	CAR	DIV		GER
1-Totalmente não aplicado	12,50%	0,00%	0,00%	2,78%	7,50%		4,25%
2-Minimamente aplicado	25,00%	11,76%	0,00%	44,44%	27,50%		21,23%
3-Razoavelmente aplicado	27,50%	35,29%	14,29%	44,44%	27,50%		31,13%
4-Totalmente aplicado	35,00%	52,94%	85,71%	8,33%	37,50%		43,40%

Fonte: Elaborado pelo autor

O Gráfico 1 evidencia a avaliação do nível de aplicação, da organização G, dos controles de segurança da informação adotados para a camada física. Percebe-se que há uma maior preocupação com a segurança da informação nas etapas de elaboração, impressão e armazenamento de provas (EIA), com 52,94% dos controles aplicados em totalidade e na aplicação de provas (APL), com 85,71% dos controles totalmente aplicados.

Estas etapas são vistas como mais críticas, pois são fases anteriores a publicação das provas aplicadas e dos gabaritos, ou seja, são fases em que já se tem o conhecimento das questões das provas e que devem garantir a proteção da confidencialidade das mesmas.

As etapas de inscrição (INS), correção de provas e apuração de resultados (CAR) e divulgação de resultados (DIV) apresentaram uma maior fragilidade quanto a segurança física, com 37,50%, 47,22% e 35% dos seus controles de minimamente aplicados a totalmente não aplicados, respectivamente. Apesar de demonstrarem certa fragilidade, a pesquisa não identificou ocorrência de alguma falha de segurança nestas etapas, no histórico de serviços realizados pela organização G, quanto à segurança física. Mesmo assim, é importante destacar que estas fragilidades podem gerar riscos as informações e aos processos, como a perda de disponibilidade e da integridade da informação.

Após verificação dos *check-lists* de avaliação preenchidos e da identificação dos controles menos aplicados, foram propostas ações para aprimorar a segurança física como:

- Melhoria da proteção contra incêndio com adoção de mais extintores para diversos tipos de materiais;
- Adoção de equipamentos de controle e registro do acesso de pessoal a ambientes críticos, com uso de leitores biométricos, cartão RFID, botoeiras de acionamento, catracas e etc.;

- Adoção de mais um sistema de ar condicionado, com religamento automático após queda de energia elétrica, na sala dos servidores;
- Isolamento do ambiente de correção de provas e apuração de resultados;
- Uso de equipamentos ligados a *no-breaks* para a correção de provas e apuração de resultados;

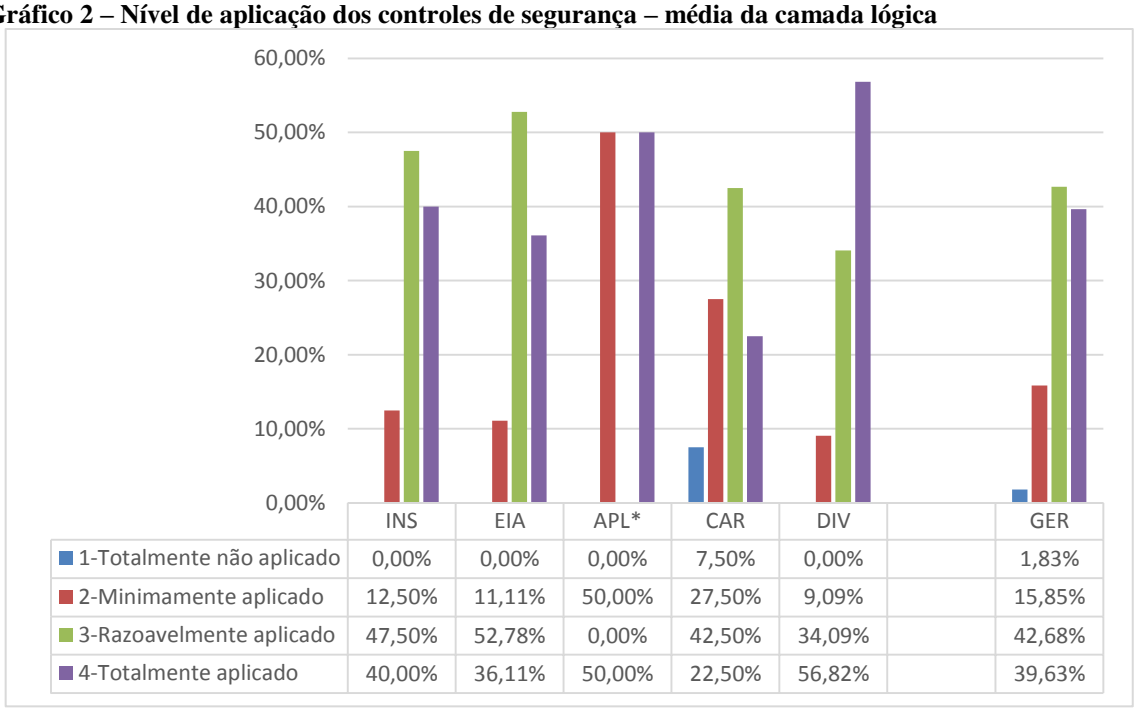
De modo geral, a camada física encontra-se em um grau satisfatório de segurança, apresentando mais de 74% de seus controles em razoavelmente aplicados e totalmente aplicados, conforme demostrado na média geral (GER).

5.1.2. Camada lógica

O *check-list* da camada lógica avaliou, principalmente, a segregação lógica de ambientes, o controle de acesso lógico a estes ambientes e o uso de *softwares* aplicativos e sistemas de segurança.

A avaliação do nível de aplicação dos controles de segurança da informação adotados para camada lógica é apresentada no Gráfico 2.

Gráfico 2 – Nível de aplicação dos controles de segurança – média da camada lógica



	INS	EIA	APL*	CAR	DIV		GER
1-Totalmente não aplicado	0,00%	0,00%	0,00%	7,50%	0,00%		1,83%
2-Minimamente aplicado	12,50%	11,11%	50,00%	27,50%	9,09%		15,85%
3-Razoavelmente aplicado	47,50%	52,78%	0,00%	42,50%	34,09%		42,68%
4-Totalmente aplicado	40,00%	36,11%	50,00%	22,50%	56,82%		39,63%

Fonte: Elaborado pelo autor

No Gráfico 2 pode ser observada a avaliação do nível de aplicação dos controles de segurança da informação adotados para a camada lógica. Para esta camada, foi identificada uma maior preocupação com a segurança das informações nas etapas de elaboração, impressão e armazenamento de provas (EIA) e na divulgação de resultados (DIV). A primeira detêm 52,78% de seus controles aplicados razoavelmente e 36,11% aplicados totalmente. A segunda tem 56,82% de seus controles aplicados totalmente.

A etapa de aplicação de prova se apresentou em uma situação interessante, pois é apenas um controle de segurança, sendo este considerado 50% minimamente aplicado e 50% totalmente aplicado pelos respondentes. Após algumas entrevistas com os mesmos, foi identificado o motivo de tal disparidade: alguns respondentes levaram em consideração a adoção, por parte da organização G, dos controles de segurança no seu rol de serviços e

outros consideraram a aplicação dos controles nos últimos processos. Isto ocorre pelo fato de que alguns controles estarem disponíveis, mas somente são aplicados conforme a disponibilidade de agentes externos e de acordo com a definição orçamentária contratual assinada pelo cliente.

A etapa EIA é considerada como uma das mais críticas, tal como na camada física. Já a etapa DIV apresentou-se como uma mais preocupante para esta camada, pois as publicações de divulgação são realizadas de forma eletrônica, por meio do sítio *on-line* da organização. Neste caso, há uma preocupação com a disponibilidade e confidencialidade das publicações.

A etapa de correção de provas e apuração de resultados (CAR) apresentou-se como a mais frágil, com relação à segurança desta camada, com 42,50% dos controles razoavelmente aplicados e 27,50% em minimamente aplicado. No entanto, os índices desta camada foram melhores do que da camada física.

Foi identificado um acontecimento de falha de segurança, no histórico de serviços realizados pela organização G, quanto à segurança lógica. Em 2007, durante as inscrições para um concurso público, após uma queda no fornecimento de energia elétrica, o sistema de banco de dados utilizado foi corrompido e apresentou perda de integridade, infringindo as regras de validação do número de inscrição e permitindo que mais de um candidato possuísse o mesmo número de inscrição. Para evitar novas ocorrências, a organização G passou a utilizar *software* aplicativo específico de banco de dados, mais robusto, e que apresenta mais qualidade e segurança, além de suportar as demandas necessárias.

Assim, para a camada lógica, após a verificação e identificação dos controles menos aplicados, por meio da averiguação do *check-list* de avaliação preenchido, ações foram propostas para aperfeiçoar mais a segurança, como:

- Melhoria da política de identificação (*login* e senha), administração e monitoramento de privilégios e acessos de usuários aos sistemas operacionais;
- Adoção de procedimentos e rotinas para análise e avaliação periódica do *firewall*;
- Adoção de procedimentos e rotinas para geração, testes e armazenamento de cópias de segurança (*backup*);
- Adoção de sistema de registro de atividades/tarefas executadas (*log*) em ambientes críticos;
- Segregação/isolamento dos ambientes de correção de provas e apuração de resultados.

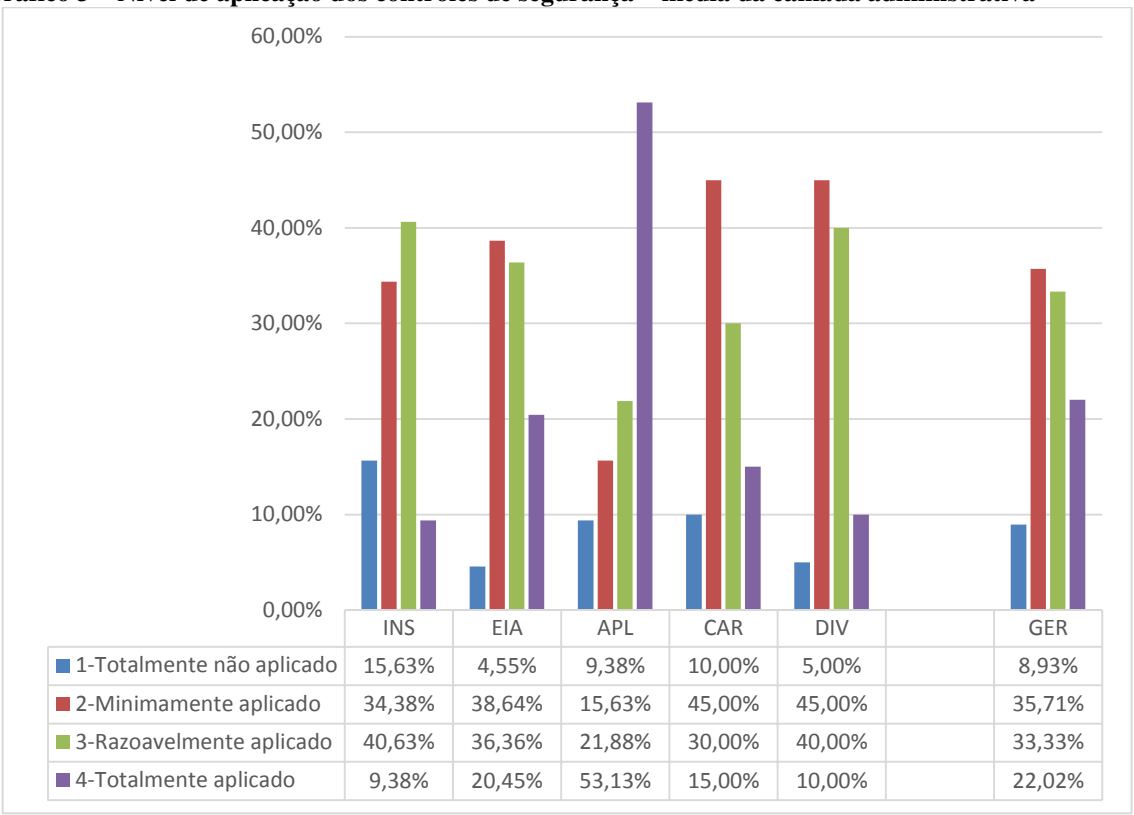
A camada lógica, de forma geral, apresenta-se com grau muito satisfatório de segurança, detendo mais de 80% de seus controles em razoavelmente aplicados e totalmente aplicados, conforme demostrado na média geral (GER).

5.1.3. Camada Administrativa (Humana)

Na avaliação da camada administrativa foram avaliados, principalmente, as políticas e conformidades legais, a segurança em recursos humanos e as rotinas e procedimentos adotados para garantia da segurança da informação.

A avaliação do nível de aplicação dos controles de segurança da informação adotados para esta camada é apresentada no Gráfico 3.

Gráfico 3 – Nível de aplicação dos controles de segurança – média da camada administrativa



	INS	EIA	APL	CAR	DIV		GER
1-Totalmente não aplicado	15,63%	4,55%	9,38%	10,00%	5,00%		8,93%
2-Minimamente aplicado	34,38%	38,64%	15,63%	45,00%	45,00%		35,71%
3-Razoavelmente aplicado	40,63%	36,36%	21,88%	30,00%	40,00%		33,33%
4-Totalmente aplicado	9,38%	20,45%	53,13%	15,00%	10,00%		22,02%

Fonte: Elaborado pelo autor

A avaliação do nível de aplicação dos controles de segurança da informação adotados para a camada administrativa pode ser observada no Gráfico 3. Nota-se que a etapa de aplicação de provas (APL) foi a que mais demonstrou totalidade da aplicação de seus controles, ou seja, foi a etapa que apresentou maior receio quanto a segurança administrativa. Esta possui 53,13% de seus controles totalmente aplicados e 21,88% aplicados razoavelmente.

Esta etapa é considerada como a mais crítica, com relação à camada administrativa de segurança, pois é a que envolve mais pessoas. Nesta etapa são utilizados coordenadores, auxiliares de coordenação e fiscais, dentre outras funções, para garantir a aplicação segura das provas. Estas são, em sua maioria, pessoas externas a organização, que não participam das demais etapas e não conhecem todos os procedimentos e rotinas já definidos. Para sanar esta fragilidade e evitar riscos são utilizadas ferramentas como treinamentos, reuniões e manuais para divulgar e reforçar as orientações, procedimentos e regulamentos utilizados na aplicação de provas de forma segura.

As demais etapas se apresentaram com alto grau de fragilidade, principalmente as etapas CAR e DIV, com 45,00% dos controles minimamente aplicados, e EIA, com 38,64% minimamente aplicados. Estas etapas pecam pela falta de orientações e treinamentos específicos e pela ausência de procedimentos bem definidos e documentos para as principais atividades correlatas.

De modo geral, a camada administrativa apresenta-se com grau insatisfatório de segurança, com mais quase 50% de seus controles em minimamente aplicados a totalmente não aplicados, conforme demostrado na média geral (GER).

Quanto a ocorrências de falhas, foi identificado um evento no histórico de serviços realizados. Na realização de alguns concursos públicos, em 2012, foram utilizados

gabaritos padronizados, com uma mesma sequencia repetitiva de alternativas. Isto conduziu a suspeitas de fraudes com possível perda de confidencialidade dos gabaritos. Este tipo de ocorrência pode ser evitado com a adoção de boas práticas de montagem de gabaritos de forma aleatória, definindo-se e documentando-se as rotinas e procedimentos. Qualquer alteração nos métodos adotados deverá ser analisada e discutida junto à direção da organização.

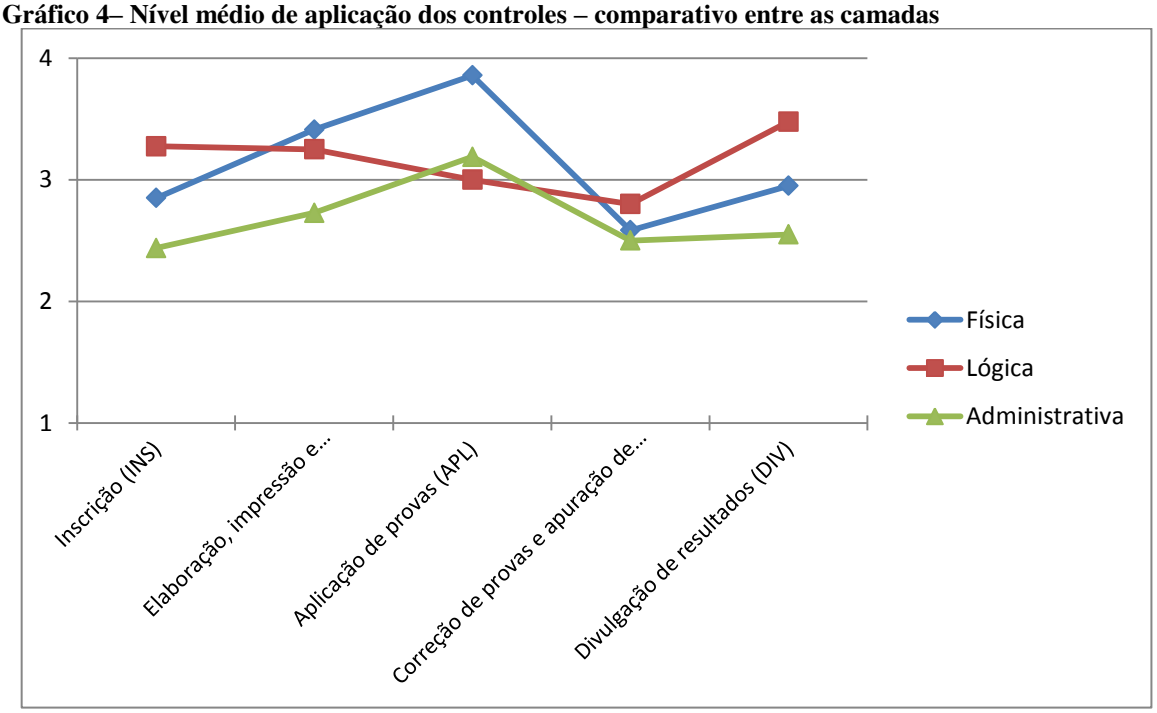
Como principais ações de melhoria da segurança para a camada administrativa, foram propostas as seguintes ações:

- Criação de um comitê de segurança da informação, com membros de cada coordenação;
- Melhoria da política da segurança, com participação efetiva da direção, sendo esta avaliada e adaptada constantemente;
- Adoção de técnicas e procedimentos para disseminação das orientações, políticas, normas e regulamentos quanto à segurança da informação, tanto para os colaboradores internos quanto para os externos;
- Adoção de políticas específicas para classificação da informação e para execução de tarefas/atividades em ambientes críticos.

5.2. Comparando as camadas

Após a avaliação individual das camadas foi realizada uma análise comparativa entre as mesmas. Para tal fim, foi calculado o nível de resposta médio, conforme a escola adota, para cada controle. Após, foram calculados o nível médio por etapa para cada camada. Estes dados foram utilizados para elaboração do gráfico comparativo das camadas, por etapa, conforme Gráfico 4.

Gráfico 4– Nível médio de aplicação dos controles – comparativo entre as camadas



Fonte: Elaborado pelo autor

Pelo Gráfico 4 é possível perceber a grande preocupação com a segurança da informação na etapa de aplicação de provas (APL). Esta etapa apresentou índices médios maiores na camada física e administrativa.

Quanto à camada lógica, seus índices são melhores nas etapas INS e DIV. Estas etapas demandam mais atenção quanto à segurança lógica, pois são quase totalmente realizadas e dependentes de ambientes lógicos e virtuais, como sítios e sistemas *on-line*, banco de dados, arquivos digitais,etc.

A camada administrativa foi a que se apresentou mais preocupante. Nota-se que a mesma só superou as demais na etapa APL, sendo um pouco melhor apenas que a camada lógica para esta etapa. Apesar de adotar muitas rotinas, procedimentos e mecanismos de segurança nesta camada, estes não são documentados e padronizados. Muitas rotinas são realizadas de forma cultural e mecanicamente, sem qualquer base formal documentada. Estes e outros procedimentos, não são analisados e reavaliados periodicamente para melhor adaptação e melhoria constante.

O ponto chave da fragilidade da camada administrativa, identificado por meio do *check-list*, é a falta de uma política de segurança bem elaborada. Esta deveria ser desenvolvida por um comitê gestor e apoiada pela direção da organização G, sendo documentada, distribuída a todos os colaboradores e periodicamente analisada, reavaliada e readaptada de forma a acompanhar as mudanças que ocorrem dentro e fora da organização. Esta política de segurança deverá ser um norte para qualquer tomada de decisão e para adoção de outras medidas e procedimentos de segurança da informação. Importante salientar que a organização G já possui uma política de segurança, mas a mesma está muito defasada.

6. CONCLUSÕES

Este trabalho objetivou identificar e estudar controles de segurança da informação adotados como boas práticas em organizações que executam serviços de seleção de pessoas (concursos/vestibulares). Com isto, demonstrar uma avaliação da segurança da informação, como estudo de caso, de uma destas organizações, por meio da aplicação de *check-lists*, que possibilitassem a identificação das competências de segurança e dos pontos críticos de falhas. Entrevistas e observações participativas também foram utilizadas para identificação de outros fatores correlatos e de possível impacto na avaliação da segurança da informação.

Quanto à norma ABNT NBR ISO/IEC 27002:2013, foram identificadas conformidades mínimas das organizações que prestam serviços de seleção. Isto se deve ao fato do pouco ou nenhum conhecimento da referida norma e/ou pela adoção parcial de seus controles. Deve-se levar em consideração, também, que a norma sugere 114 controles, não sendo obrigatória e viável sua total adoção para todos os tipos e portes de organizações.

A pesquisa evidenciou a importância de controles de segurança na etapa de aplicação de provas. Esta etapa é considerada como a mais crítica, pois é o momento de exposição da prova aos candidatos e envolve a grande maioria de pessoas, fragilizando o processo. O foco, neste momento, é na integridade das respostas dos candidatos e na confidencialidade das questões e gabaritos das provas. Nota-se que na etapa posterior (correção de provas e apuração de resultados) há um declínio da preocupação quanto à segurança da informação, possivelmente pelo uso de procedimentos e rotinas mais frágeis e de uma cultura organizacional que não apresentou quaisquer indícios de falhas até o presente momento.

Outros fatores importantes que influenciaram nos resultados foram identificados na pesquisa, como a falta de alinhamento da percepção quanto aos controles de segurança da informação, a influência da definição contratual junto ao cliente e a dependência de agentes externos/terceirizados. Houve uma discrepância entre as respostas dos entrevistados quanto à adoção de certos controles. Isto se justificou pelas diferentes visões sobre o tema relacionado e os diferentes níveis de saber sobre a existência, ou não, dos controles citados, por parte dos respondentes. Outras diferenças detectadas foram justificadas pelos fatores de contrato com o cliente e pela dependência de agentes externos/terceiros. Muitos controles foram avaliados não pela adoção dos mesmos no rol de serviços da organização avaliada, mas pela sua aplicação nos últimos processos realizados. Esta aplicação é determinada pelo contrato de serviço junto ao cliente, que visando um custo mais baixo, pode não optar pelo uso de certos controles. Além disto, existem controles que dependem de agentes externos/terceiros, como o procedimento de identificação humana por meio de impressões digitais, da camada administrativa, que depende exclusivamente da Polícia Técnico-científica.

Como descrito anteriormente, a camada administrativa é a que demanda maiores cuidados dentro das organizações. O que ocorre é que as organizações se preocupam em investir em controles tecnológicos e estruturais, a fim de minimizar os riscos de incidentes de segurança da informação, contudo desprezam o fator humano, que responde pela grande maioria das ocorrências de falhas na segurança. A fragilidade desta camada apontou para a necessidade da elaboração, aprovação e publicação de políticas mais consistentes de classificação e segurança da informação. Estas políticas estão diretamente relacionadas com diversos outros controles e são determinantes para orientar os níveis estratégicos e táticos das organizações quanto à adoção de boas práticas de segurança da informação.

Importante relatar que este trabalho teve como limitador o número baixo de organizações para estudo e avaliação, devido ao receio de exposição das mesmas. Entretanto, os resultados apresentados no estudo possibilitou a análise das competências de segurança da informação em processos de seleção, evidenciando possíveis riscos e possibilitando a melhoria dos processos operacionais.

Deve ser considerado, também, que sobre o tema proposto não há legislação pertinente e tampouco órgãos reguladores. Desta forma, a adoção de controles e mecanismos de segurança da informação não são exigências legais, mas apenas diferencial de mercado que pode impactar diretamente nos resultados dos processos, no retorno de investimentos e na imagem da organização.

Como trabalhos futuros, sugere-se a avaliação da percepção quanto à segurança da informação nos diferentes níveis organizacionais com o objetivo do alinhamento e integração das áreas envolvidas. Assim, a criação, adoção, prática e avaliação de controles, mecanismos e procedimentos de segurança da informação compartilhariam de perpectivas integradas e adotadas por todas as áreas envolvidas.

Assim, concluindo, através destes *check-lists*, e se baseando na ABNT NBR ISO/IEC 27002:2013, pode-se mensurar, classificar e avaliar o nível de segurança da informação de uma organização que realiza processos de seleção, possibilitando a identificação de pontos críticos passíveis de correção. Esta metodologia pode auxiliar na melhoria da estrutura e dos processos organizacionais, na fundamentação de requisitos para licitação/contratação por empresas privadas ou órgãos governamentais, bem como, na fiscalização de organizações contratadas. Para as organizações que realizam este tipo de serviço, isto pode representar uma consolidação da imagem e uma maior valorização diante do mercado.

7. REFERÊNCIAS

AMARAL, Luis Alfredo Martins do (1994). **Praxis**: um referencial para o Planejamento de Sistemas de Informação. Tese (Doutorado) - Departamento de Sistemas de Informação, Universidade do Minho, Guimarães (Portugal). Recuperado em 11 maio, 2015, de https://repositorium.sdum.uminho.pt/retrieve/301/PRAXIS_Amaral.pdf

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT) (2013a.). **ABNT Catálogo**: Segurança, Qualidade, Padrão e Confiança. Recuperado em 30 maio, 2015, de http://www.abntcatalogo.com.br/norma.aspx?ID=306582

_____ (2015). **Conheça a ABNT**. Recuperado em 30 maio, 2015, de http://www.abnt.org.br/abnt/conheca-a-abnt

_____ (2014). **ISO/IEC 27000:2014** – Information technology — Security techniques — Information security management systems — Overview and vocabulary. Third edition. Switzerland: International Organization for Standardization.

_____ (2007). **NBR ISO/IEC 17799:2005** - Tecnologia da informação – código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT.

_____ (2013b). **NBR ISO/IEC 27002:2013** - Tecnologia da informação – código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT.

BRASIL (2015). **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Secretaria Especial de Informática. Recuperado em 06 abril, 2015, de http://www.senado.gov.br/legislacao/const/con1988/CON1988_07.05.2015/CON1988.pdf

BRASIL (1996). **Lei nº 9.394, de 20 de dezembro de 1996**. Recuperado em 12 maio, 2015, de http://www.planalto.gov.br/CCIVIL_03/leis/L9394.htm

BRASIL (2013). Senado Federal. **Projeto de Lei do Senado PLS n. 74/2010**. Cria regras para a aplicação de concursos para a investidura em cargos e empregos públicos no âmbito da União, dos Estados, dos Municípios e do Distrito Federal. Recuperado em 07 abril, 2015, de http://legis.senado.leg.br/mateweb/arquivos/mate-pdf/132436.pdf

BRASIL (2012). Tribunal de Contas da União. **Boas práticas em segurança da informação/Tribunal de Contas da União**. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação.

CAPOBIANCO, Ligia & CURY, Lucilene (2011). **Princípios da História das Tecnologias de Informação e Comunicação – Grandes Invenções**. In: VIII Encontro Nacional de História da Mídia, Guarapuava. Anais do VIII Encontro Nacional de História da Mídia. Recuperado em 13 maio, 2015, de http://goo.gl/eE946T

CARVALHO FILHO, José dos Santos (2014). **Manual de direito**. 27. ed. São Paulo: Atlas.

CEPIK, Marco (2003). **Espionagem e Democracia**. Fundação Getúlio Vargas. Recuperado em 12 maio, 2015, de https://books.google.com.br/books?id=xERuDA-Ra8wC

CHOO, Chun Wei (2003). **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. 2. ed. São Paulo: SENAC.

COHEN, Fred (1995). **Introductory Information Protection** - Chapter 2.1 - A Short History of Cryptography. Recuperado em 01 maio, 2015, de http://all.net/edu/curr/ip/Chap2-1.html

COM 5,7 mi de inscritos, enem tem desafio: evitar falhas (2012). **Veja on-line**, São Paulo. Recuperado em 02 abril, 2015, de http://veja.abril.com.br/noticia/educacao/com-5-7-mi-de-inscritos-enem-tem-desafio-evitar-falhas/

CÔRTE, Kelson (2014). **Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos**. 212 f., il. Tese (Doutorado em Ciência da Informação)—Universidade de Brasília, Brasília. Recuperado em 05 maio, 2015, de http://hdl.handle.net/10482/16748

DANTAS, Marcus Leal (2011). **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido.

DROGSETH, Dennis & TURBITT, Ken (2008). **Gleaning Wisdom from Data** - The role of service knowledge management in IT decision-making and ITIL® V3. BMC Software and Enterprise Management Associates. Recuperado em 02 maio, 2015, de http://documents.bmc.com/products/documents/12/90/91290/91290.pdf

GIL, Antônio Carlos (2008). **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas.

ISECT (2015). **ISO/IEC 27002**. Nova Zêlandia. Recuperado em 30 maio, 2015, de http://www.iso27001security.com/html/27002.html

LESCA, Humbert & ALMEIDA, Fernando C. De (1994). **Administração estratégica da informação**. RAUSP. São Paulo, v.29, n.03, p.66-75, jul./set.

MARCIANO, João Luiz & LIMA-MARQUES, Mamede (2006). **O enfoque social da segurança da informação**. Ci. Inf. [online]. Recuperado em 05 maio, 2015, de http://hdl.handle.net/10482/939

PELTIER, Thomas R (2004). **Information security risk analysis**. 2. ed. Boca Raton: Auerbach Publications.

QUEIROZ, Rita de C. R (2005). **Informação Escrita**: Do manuscrito ao texto virtual. VI Encontro Nacional de Ciência da Informação – Informação, Conhecimento e Sociedade Digital. Salvador, BA. Recuperado em 01 maio, 2015, de http://www.cinform-anteriores.ufba.br/vi_anais/docs/RitaQueiroz.pdf

SÊMOLA, Marcos (2014). **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier.

SIEWERT, Vanderson C (2006). **A Constante Evolução da Segurança da Informação**. Recuperado em 02 maio, 2015, de http://pt.scribd.com/doc/109157762/Yasser-Baio-A-Constante-Evolucao-Da-Seguranca-Da-Informacao

SILVA NETTO, Abner da & SILVEIRA, Marco Antonio Pinheiro (2007). **Gestão da Segurança da Informação**: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. JISTEM, v.4, n.3, p.375-397.

SILVA, Luiz Fernando Costa Pereira da (2010). **Gestão de riscos em tecnologia da informação como fator crítico de sucesso na gestão da segurança da informação dos órgãos da administração pública federal**: estudo de caso da Empresa Brasileira de Correios e Telégrafos - ECT. Dissertação (Mestrado em Ciência da Informação e Documentação)-Universidade de Brasília, Brasília. Recuperado em 10 maio, 2015, de http://hdl.handle.net/10482/7473

SILVA, Wagner Lima da (2011). **Segurança da Informação**: Um Estudo Sobre a Percepção do Usuário da Informação Contábil. Dissertação (Pós-graduação em Ciências Contábeis). Universidade Presbiteriana Mackenzie, São Paulo. Recuperado em 05 maio, 2015, de http://up.mackenzie.br/fileadmin/user_upload/_imported/fileadmin/PUBLIC/UP_MACKENZIE/servicos_educacionais/stricto_sensu/Ciencias_Contabeis/Dissertacoes/Wagner_Lima_da_Silva.pdf

SOBRE O ENEM (2011). **INEP** - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Recuperado em 14 maio, 2015, de http://portal.inep.gov.br/web/enem/sobre-o-enem

STALLINGS, William (2007). **Data and Computer Communications**. 8. ed. Upper Saddle River: Pearson Prentice Hall.

TANENBAUM, A. S (2003). **Redes de computadores**, Tradução da 4a Edição, Rio de Janeiro: Campus.

TARAPANOFF, Kira (2006). **Inteligência, informação e conhecimento em corporações**. Brasília: IBICT, UNESCO. Recuperado em 11 maio, 2015, de http://livroaberto.ibict.br/bitstream/1/465/1/Inteligencia,%20informa%C3%A7%C3%A3o%20e%20conhecimento.pdf

VIDAL, Flávio de Barros (2010). **Controles de Segurança Física e Ambiental**: GSIC202. Curso de Especialização em Gestão da Segurança da Informação e comunicações. Departamento de Ciências da Computação da Universidade de Brasília.

VIEIRA, Walber Siqueira (2013). **O princípio da isonomia e sua aplicabilidade no acesso aos cargos públicos efetivos no ordenamento jurídico brasileiro**. Recuperado em 12 maio, 2015, de http://www.egov.ufsc.br/portal/conteudo/o-princ%C3%ADpio-da-isonomia-e-sua-aplicabilidade-no-acesso-aos-cargos-p%C3%BAblicos-efetivos-no-orde