TRABALHO DE CONCLUSÃO DE CURSO

IMPORTÂNCIA ESTRATÉGICA DOS SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO PARA A VALORIZAÇÃO DA CARREIRA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NO MINISTÉRIO PÚBLICO FEDERAL

DANIEL ARTUR SEELIG
Especialista em Segurança Cibernética
Técnico do MPU-TIC

JEYSONN ISAAC BALBINOT
Mestre em Ciência da Computação
Técnico do MPU-TIC

RENATO LUFT
Graduado em Engenharia Mecânica
Técnico do MPU-TIC

Orientador:
CLEBER DE ARAÚJO
Mestre em Gestão Pública
Técnico do MPU-TIC

RESUMO

O objetivo deste trabalho é compreender a relação entre os serviços de Segurança da Informação (SI) e a valorização da carreira de Tecnologia da Informação e Comunicação (TIC) no Ministério Público Federal (MPF). Para tanto, foram identificados e correlacionados os serviços prestados em SI com a carreira de tais profissionais. A pesquisa teve abordagem qualitativa e foi classificada como descritiva do tipo documental. O estudo foi realizado a partir de leitura e análise crítica de bibliografias relacionadas à força de trabalho, à valorização da carreira, à rotatividade de servidores nos cargos e aos benefícios e consequências da terceirização no serviço público e na SI. A coleta de dados foi feita a partir de consultas a sítios de transparência, relatórios gerenciais, sistemas internos e material divulgado publicamente a respeito do Planejamento Estratégico Institucional (PEI), do Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETI) e do Plano Diretor de Tecnologia da Informação e Comunicação do MPF (PDTIC). A interpretação e reflexão crítica dos resultados foi realizada a partir da análise dos dados, em que se pretendeu estudar a relação entre a valorização da carreira e os aspectos de SI na TIC. A análise considerou informações a respeito de pessoal, em especial a força de trabalho de TIC, envolvendo fatores como alocação, evasão, desvio de função etc. A pesquisa revelou que há um *déficit* no número desses servidores e que o processo da maturidade da SI poderia passar pelo fortalecimento de políticas, normas, ações, valorização das carreiras, transparência, gestão e governança.

ABSTRACT
The purpose of this work is to understand the relation between the Information Security (IS) services and the appreciation of the career of Information and Communication Technology (ICT) at the Ministério Público Federal - MPF (Federal Prosecution Office). Therefore, the services provided in IS were identified and correlated with the career of these professionals. The research had a qualitative approach and was classified as descriptive of the documental type. The study was developed from reading and critical analysis of bibliographies related to the workforce, the career appreciation, the employee turnover in positions, the benefits and the consequences of outsourcing in public service and IS. Data collection was based on searches on transparency websites, management reports, internal systems and publicly disclosed material regarding the Institutional Strategic Planning, the Information and Communication Technology Strategic Planning and the Information and Communication Technology Master Plan. The interpretation and the critical reflection of the results was performed from the data analysis, and was intended to study the relation between the career appreciation and the IS aspects in ICT. The analysis considered informations regarding the staff, in particular the ICT workforce in subjects such allocation, evasion, position deviation etc. The survey revealed that there is a shortage of ICT government employee and that the maturity of the IS could include policies strengthening, standards, actions, career appreciation, transparency, management and governance.

PALAVRAS-CHAVE:
Segurança da Informação, Valorização de Carreira, Tecnologia da Informação e Comunicação, Administração Pública Federal.

KEY-WORDS:
Information Security, Career Appreciation, Information and Communication Technology.

1 INTRODUÇÃO

Nos últimos cinquenta anos houve grande evolução na área de Tecnologia da Informação (TI). Computadores de grande porte (*mainframes*) foram substituídos por outros equipamentos, como servidores de dimensões menores e com maior capacidade de processamento. O armazenamento de informações passou de *MegaBytes* para *TeraBytes*, mesmo assim se adequando a espaços bem mais compactos, seja em Centros de Processamento de Dados nas empresas e instituições ou em "nuvem" (*cloud computing*). O uso da tecnologia, que era exclusivo em grandes empresas, passou também para o uso pessoal e está hoje nos bolsos, nos relógios de pulso, nos painéis de automóveis, nos televisores, na "Internet das Coisas" (*IoT – Internet of Things*). As instituições tiveram que se

adaptar à onda de modernização tecnológica, substituindo, por exemplo, equipamentos de telefonia (PABX) por computadores; contratação de serviços pela aquisição de *softwares* especializados; utilização de antigos equipamentos de comunicação (TELEX, FAX etc.) por modernos meios de comunicação (*smartphones*, *tablets* etc.), tudo isso para acompanhar a revolução gerada principalmente pela Internet. Com toda essa "explosão" de soluções tecnológicas, o portfólio de serviços prestados/suportados pelos profissionais da área de Tecnologia da Informação e Comunicação (TIC) também cresceu vertiginosamente e questões antes com pouca relevância para a maioria das pessoas, a exemplo da Segurança da Informação (SI), passaram a ser pautas essenciais dos gestores, tanto de empresas públicas quanto privadas.

Atualmente, pensar em segurança sem levar em consideração o fator humano é cometer falha primária, sendo relevante atentar-se a diversos fatores como, por exemplo, estímulos, valorização financeira e profissional, evasão, dentre outros, os quais merecem ser levantados e estudados com especial atenção.

Para melhor entendimento acerca do contexto do presente trabalho, foi necessário observar aspectos ligados ao profissional de TIC, relacionados à governança na Administração Pública Federal (APF), à terceirização de serviços e pessoas, às definições relacionadas à SI e às consequências que a falta de atratividade na carreira causa nas instituições. Ademais, e na medida em que esse trabalho teve como foco o ambiente do Ministério Público Federal (MPF), houve ainda a necessidade de analisar o projeto de modernização existente no órgão, com recorte nos tópicos que atuam diretamente no desenvolvimento do plano de carreira de TIC.

Nota-se que, nos últimos anos, a APF tem avançado nos processos de Governança de Tecnologia da Informação (GovTI), mas não tem dado a necessária atenção e relevância à SI, com ações meramente normativas, deixando o tratamento da informação, ativo de grande valia, relegado a segundo plano (ROCHA *et al.*, 2017). Nesse contexto, a Governança da SI (GovSI), tema multifacetado e estratégico para a organização, exerce seu papel trazendo o foco da discussão para a SI (LYRA, 2015), visando à proteção da instituição contra ameaças, vulnerabilidades e todo e qualquer incidente de segurança.

Nesse ponto, cabe destacar que a terceirização na área de TIC potencializa riscos e desafios associados à questão da SI, o que nem sempre é considerado na decisão pela contratação de terceirizados. Tais riscos estão diretamente relacionados ao fato de pessoas externas serem inseridas no negócio, passando a ter acesso a dados sensíveis da organização (CHEROBINI, 2017). A quebra de sigilo de informações e o vazamento de dados estão relacionados aos usuários internos na maioria dos casos, denominados de *insiders* (ALENCAR; QUEIROZ; QUEIROZ, 2013). Ocorre que pesquisas sugerem que os principais fatores estratégicos que influenciam determinada empresa na decisão pela terceirização de TIC se concentram em aspectos relacionados tão somente a custos, inovação tecnológica e melhoria em *performance*. No setor público, dentre os pontos comumente levantados, estão a redução de custos, melhoria na qualidade dos serviços prestados, rigidez na estrutura de cargos e salários e a impossibilidade de ajuste dos quadros, devido à estabilidade dos servidores (OLIVEIRA, 2006). No entanto, o processo de decisão acerca da terceirização de TIC deve abranger uma avaliação mais complexa. Afinal, é preciso considerar todos os impactos sensíveis da SI que a terceirização pode causar.

Dentre as definições e conceitos, de acordo com Sêmola (2003, p. 43), a SI "é a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Pesquisas demonstram que, há mais de dez anos, as normas ISO/IEC da família 27000 continuam sendo a base do modelo ou teoria mais utilizada quando se fala de SI (ALBUQUERQUE JUNIOR; SANTOS, 2014; ALENCAR *et al*., 2018). A norma 27002 define SI como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar os riscos ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio." (ABNT, 2005, p. 10).

Outro aspecto a ser analisado em relação à SI é aquele relativo à rotatividade de servidores de TIC e o fenômeno conhecido como *turn-away*, o qual é percebido tanto na esfera privada, quanto na pública. Trata-se de situação em que o profissional de TIC abandona a sua área para assumir função em outra distinta, dentro ou fora da instituição, muitas vezes evoluindo para uma posição gerencial.

Para assegurar a atratividade das carreiras, um dos objetivos do PEI 2011-2020 do MPF (BRASIL, 2011a), deve ser dada permanente atenção ao clima

organizacional, investindo em um ambiente que estimule o crescimento profissional e pessoal do servidor, seja por meio da capacitação deste servidor ou da valorização da carreira, seja pela via do envolvimento e da participação em projetos relacionados à sua área de atuação. Tal objetivo é relevante no contexto da SI pois servidores qualificados e motivados podem atuar com maior consciência e excelência a fim de reduzir vulnerabilidades e mitigar a ocorrência de incidentes de SI, como, por exemplo, o vazamento de dados pessoais e institucionais.

No Brasil, os incidentes de segurança em geral estão diretamente associados à atuação de *hackers* e a fontes internas, como terceiros - incluindo fornecedores, consultores e terceirizados - e colaboradores, onde o fator humano inevitavelmente está inserido, conforme apontam os estudos relacionados à SI (PRICEWATERHOUSECOOPERS, 2017). O PETI (BRASIL, 2013a) do MPF, um dos desdobramentos do PEI, será abordado no decorrer deste trabalho por conter informações e estudos importantes relacionados à SI.

Frente a esse cenário, a questão de investigação escolhida para o desenvolvimento deste trabalho foi: “Qual a relação entre os serviços de Segurança da Informação e a valorização da carreira de Tecnologia da Informação e Comunicação no Ministério Público Federal?”. O objetivo geral da pesquisa foi compreender essa relação e, para isso, foram traçados os seguintes objetivos específicos: 1. identificar os serviços de SI prestados no MPF; 2. descrever as atividades do profissional de TIC relativas à SI no MPF; 3. correlacionar os serviços de SI com os aspectos da valorização da carreira do profissional de TIC no MPF.

Para isso, o presente artigo foi estruturado em cinco seções, iniciando-se por esta introdução, que contextualiza a problemática. A seção dois apresenta a revisão da literatura baseada no levantamento bibliográfico com a fundamentação teórica em que está ancorado, partindo-se, então, para a seção três, a qual explica e descreve a estratégia metodológica adotada através da apresentação do método de operacionalização da investigação realizado. Na sequência, a seção quatro apresenta e discute os resultados obtidos e, por fim, a seção cinco apresenta as conclusões, sugestões e limitações da pesquisa, bem como uma recomendação de trabalhos futuros que podem ser desenvolvidos.

2 REVISÃO DE LITERATURA

Este capítulo contextualiza os principais termos e conceitos associados à SI, sendo eles a própria informação, a SI, a rotatividade de profissionais de TIC, a terceirização de TIC, a Política de Segurança da Informação (PSI) e a GovSI. Além da conceituação, com base na literatura nacional e internacional da área, serão mencionados os trabalhos mais relevantes relacionados a esses temas e ao presente artigo.

2.1 INFORMAÇÃO

Em um mundo interconectado, a informação, os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são ativos de valor para uma organização, sendo que a informação deve ser considerada nas suas diversas formas: impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos e apresentada em filmes ou falada em conversas (ABNT, 2005, p. 10). Para Sêmola (2003, p. 9), “toda informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade, além dos aspectos autenticidade e legalidade, que complementam essa influência”. A informação, por ser considerada um ativo essencial para os negócios de uma organização, necessita ser adequadamente protegida.

2.2 SEGURANÇA DA INFORMAÇÃO

O conceito de SI, segundo Sacramento (2007), é a aplicação de medidas de segurança para proteção da informação, seja ela processada, armazenada ou transmitida nos sistemas de informação e comunicações, ou qualquer outro sistema eletrônico, contra a perda de confidencialidade, integridade e disponibilidade. No contexto da norma ISO/IEC 27002 (ABNT, 2005, p. 10), SI “é a proteção da informação contra os vários tipos de ameaças, com o objetivo de manter a continuidade do negócio”. A norma afirma que, para alcançar a SI, é necessária a implementação de um conjunto de controles que inclui políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. A criação de políticas faz com que diversas práticas de segurança sejam implementadas. No entanto, se a cultura e a ética da organização e das pessoas

não forem apropriadas, os processos e os procedimentos de SI não serão efetivos (ISACA, 2012, p. 30).

Cabe destacar a abrangência do conceito de SI para o setor público, descrita no Decreto Nº 9.637, o qual instituiu a Política Nacional de Segurança da Informação (PNSI). O referido Decreto, em seu art. 2º, dispõe acerca do alcance da SI como sendo "a segurança cibernética; a defesa cibernética; a segurança física e a proteção de dados organizacionais; e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação" (BRASIL, 2018b).

Os modelos de SI, tanto para o setor público quanto para os setores corporativos e militares, possuem como princípios fundamentais a tríade confidencialidade, integridade e disponibilidade (CID). Esse conjunto é reconhecido como tripé da SI, internacionalmente denominado "*CIA-triad*" (MACHADO JUNIOR, p. 56, 2018). O autor, analisando os diferentes modelos de SI, afirma que "a *CIA-triad* levou praticamente 20 anos para ser cunhada (considerando o período entre o início do estudo em 1967 e o Pink Book)" e os modelos atuais, apesar de mais complexos, continuam mantendo-a como base.

Stallings e Brown (2014, p. 8) observaram que o padrão FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) do *National Institute of Standards and Technology* (NIST) (NIST, 2004) também considera a CID como sendo os três objetivos de SI para sistemas de informação e traz a descrição destes conceitos.

> **Confidencialidade:** Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias.
> **Integridade:** Defender contra a modificação ou destruição imprópria de informações, garantindo a irretratabilidade (ou não repúdio) e a autenticidade das informações.
> **Disponibilidade:** Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado.

Os autores complementam tais princípios, acrescentando a descrição de mais dois conceitos necessários, a autenticidade e a determinação de responsabilidade.

> **Autenticidade:** A propriedade de ser genuína e poder ser verificada e confiável; confiança na validade de uma transmissão, de uma mensagem ou do originador de uma mensagem.
> **Determinação de responsabilidade:** O objetivo de segurança que leva à exigência de que as ações de uma entidade sejam rastreadas e atribuídas

> unicamente àquela entidade. Isso dá suporte à irretratabilidade, à dissuasão, ao isolamento de falhas, à detecção e prevenção de intrusões, e à recuperação e à ação judicial após uma ação.

Uma vasta pesquisa de artigos sobre SI entre 2004 e 2013 foi realizada por Albuquerque Júnior e Santos (2014). Na sequência, Alencar e outros (2018) realizaram estudo similar no qual mostraram o resultado de um mapeamento sistemático da literatura sobre governança, gestão e maturidade de SI em periódicos e eventos nacionais de maior relevância entre os anos de 2008 e 2017. Esses trabalhos trazem o estado da arte das publicações sobre SI e demonstram que, há mais de dez anos, a norma técnica ISO/IEC 27002 é, além do modelo de análise mais utilizado, também o texto mais referenciado.

2.3 ROTATIVIDADE DE PROFISSIONAIS DE TIC

Com foco em servidores públicos de TIC, Soares, Capistrano e Barbosa (2015) analisaram a rotatividade desses profissionais dentro de suas carreiras. Os autores afirmaram que essa rotatividade, principalmente em órgãos públicos, pode significar descontinuidade de projetos, potenciais perdas de investimentos em capacitação, riscos de descontinuidade no atendimento de demandas, perda de base de conhecimento da instituição, entre outros problemas de ordem gerencial. Ou seja, conhecer e controlar essa rotatividade tem importância estratégica para a instituição. Além disso, a rotatividade pode ser um dos indícios da falta de valorização da carreira, um dos focos de estudo do presente artigo.

Ramos e Joia (2014) pesquisaram a percepção dos profissionais de TIC que saíram da área, fenômeno conhecido como *turn-away*. Os autores identificaram como características típicas dessa transição a necessidade de crescimento que, muitas vezes, a instituição ou a área técnica não são capazes de oferecer. Concluíram que, em geral, o desejo dos profissionais de TIC de mudar de área não está tanto relacionado a uma insatisfação com as suas atribuições, mas muito mais ligado à busca por atividades interessantes e diferentes e por novos desafios e experiências.

2.4 TERCEIRIZAÇÃO DE TIC

O conceito geral de terceirização foi definido por Marcelino e Cavalcante (2012) como sendo “todo processo de contratação de trabalhadores por empresa interposta, cujo objetivo último é a redução de custos com a força de

trabalho e (ou) a externalização dos conflitos trabalhistas". Na área de TIC, terceirização ou *outsourcing* é cada vez mais comum, especialmente no setor público. A estratégia de terceirizá-la tem sido adotada para permitir a concentração de esforços nas atividades-fim (GUARDA; OLIVEIRA; SOUZA JUNIOR, 2012). Contudo, cabe destacar que a terceirização na área de TIC pode potencializar os riscos e desafios associados à SI.

Nessa linha de preocupação, Cherobini (2017) fez um levantamento dos principais problemas associados à alocação de pessoas ou à terceirização na prestação de serviços de TIC e, levando em consideração normas, padrões e controles relativos à SI, sugeriu um conjunto de boas práticas como forma de mitigar tais riscos. Em áreas onde a informação manipulada é sensível e estratégica para a organização, a autora traz para os gestores um mínimo de subsídio para que possam balizar ações, contramedidas e analisar os riscos relacionados à SI.

Frente à tendência na terceirização de TIC, Scott (2010) aplicou no setor público da Irlanda um *framework* de análise de risco que originalmente havia sido desenvolvido para o setor privado. Segundo Scott, os fatores de risco mais importantes na estratégia de terceirização, quando aplicada ao setor público, são complexidade dos processos de compras, dificuldades na coleta de requisitos, custos extras no contrato e rigidez na estrutura dos postos de trabalho.

Gonzalez, Gasco e Llopis (2010) analisaram as principais razões e riscos que levam as empresas a terceirizar serviços. O estudo se baseou na perspectiva de 329 grandes empresas espanholas. Cabe destacar que a principal razão é a busca por serviços melhores e mais atualizados, ou seja, o foco está mais voltado a questões estratégicas do que mera economia de custos. Em contrapartida, o maior risco está relacionado ao fornecedor, mais precisamente à preocupação com a baixa qualificação ou falta de conformidade.

Para Schneier (2002), por sua vez, o principal argumento para a terceirização é a questão financeira. O autor afirma que, em geral, um serviço é terceirizado quando ele for muito complexo, muito importante ou muito desagradável. Segundo o autor, a SI reúne estas três características e poderia ser terceirizada, porém não aconselha a terceirização do gerenciamento da SI como um todo, mas apenas de serviços de assistências especializadas pontuais, como por

exemplo, rastreamento de vulnerabilidades, monitoramento, consultoria e análise forense.

Contudo, cabe destacar que a SI é o fator de risco mais crítico na terceirização de TIC no setor público, segundo pesquisa de Oliveira e Santos (2006) realizada com gerentes de nível estratégico e gerentes de nível tático de 14 das 27 Administrações Tributárias Estaduais do Brasil, o que representa 51,85% desse mercado. Porém, quando se considera o âmbito geral das instituições públicas federais, a análise de Rocha, Castro e Silva Júnior (2017), feita sobre os dados coletados pelo Tribunal de Contas da União (TCU) de 2007 a 2014, concluiu que é baixa a relevância que tais instituições têm dado à SI. O próprio TCU afirma, em seu relatório, que “o aspecto em que a situação da GovTI está mais crítica é no que diz respeito ao tratamento da SI” (BRASIL, 2008, p. 8). Além disso, diversos autores da área ressaltam que a SI está diretamente relacionada às pessoas e sua abordagem deve considerar aspectos culturais, educacionais e, principalmente, ações de treinamento e conscientização.

Quando se analisa SI e terceirização de TIC, o profissional de TIC figura como uma peça chave para o sucesso ou insucesso de sua aplicação. Dessa forma, é preciso analisar como esses fatores impactam em sua carreira.

2.5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para organizações que necessitam fazer a gestão de SI, a norma ISO/IEC 27002 (2013) fornece as principais diretrizes. A referida norma inclui a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco em SI da organização. Não se pode falar de SI sem mencionar também o conceito de PSI, que é um dos principais controles da norma. Este possui como objetivo prover orientação da direção e apoio para a SI de acordo com os requisitos de negócio e as leis e regulamentações relevantes.

PSI é um termo que pode possuir diferentes interpretações. Paananen, Lapke e Siponen (2019) analisaram diferentes definições sobre a perspectiva de diferentes autores e destacaram aquela que dispõe que PSI é a declaração da alta administração sobre as crenças, os objetivos e as razões e também as formas de alcançar a SI desejada. Com base na literatura internacional, os autores fizeram o levantamento do estado da arte sobre o desenvolvimento de

uma PSI, analisando 87 artigos publicados em bases de acesso aberto. O estudo revelou que o guia mais reconhecido para elaboração do seu conteúdo é a norma ISO/IEC 27002, sendo esse um importante mecanismo para facilitar a prevenção, a detecção e a resposta a incidentes de SI. Para os autores, o desenvolvimento da PSI, de maneira geral, deve considerar os requisitos específicos da organização, gerenciar o lado técnico e também os fatores humanos.

Em âmbito nacional, Simões (2014) analisou a PSI de dez órgãos da APF direta identificando que o nível de maturidade é bem diversificado e que apenas um previu todos os requisitos essenciais da norma ISO/IEC 27002. E, de acordo com o TCU (2008, p. 20), 64% das 255 das entidades/órgãos da APF pesquisadas declararam não possuir uma PSI.

2.6 GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

A SI e a PSI não são instrumentos de controle isolados ou específicos de TIC, muito pelo contrário, devem ser gerenciados e estar inseridos em todas as áreas da organização, da mesma forma que acontece, ou deveria acontecer, com a própria TIC. Assim, ao se pensar em SI, deve-se associá-la ao conceito de GovSI. Por sua vez, a GovSI também não deve estar isolada e deve estar alinhada a outros conceitos, como a Governança no Setor Público e a GovTI.

A definição de Governança no Setor Público, segundo o referencial básico de governança do TCU, “compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (BRASIL, 2014, p. 26). Já a GovTI, segundo a norma ISO/IEC 38500, é o sistema pelo qual o uso atual e futuro da TIC é dirigido e controlado (ABNT, 2018, p. 3), e tem como objetivo principal criar valor para a organização com base nas necessidades das partes interessadas (ISACA, 2012, p. 17). A GovSI, por sua vez, consiste em um conjunto de políticas e processos que permite que as instituições monitorem, avaliem e direcionem a gestão de seus ativos de informação, reduzindo os riscos à sua CID, de forma alinhada com as necessidades de negócio (GUIMARÃES; NETO; LYRA, 2018).

As orientações sobre os conceitos e princípios de GovSI para que as organizações possam avaliar, dirigir, monitorar e comunicar as atividades

relacionadas com a SI dentro da organização são definidas na norma ISO/IEC 27014 (ABNT, 2013). Segundo esta norma, GovSI engloba liderança, estruturas organizacionais, processos/procedimentos, aplicação da conformidade e mecanismos de monitoramento e tecnologias que garantem que a CID dos ativos (em meios) eletrônicos da organização (dados, informações, software etc.) estejam sempre disponíveis e íntegros. GovSI tem como foco alinhar os objetivos e estratégias de SI com os do negócio, sempre em conformidade com leis, regulamentos e contratos, adotando uma abordagem baseada em riscos para sua implementação e imputando ao corpo de governança da organização a responsabilidade pelas decisões e pelo desempenho.

Guimarães, Neto e Lyra (2018) analisaram vários modelos de GovSI e fizeram a proposição de um novo modelo conceitual específico para a APF, aderente às normas brasileiras e compatível com a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF 2015-2018 (CDN, 2015) do Departamento de Segurança da Informação e Comunicações (DSIC). Esse novo modelo proposto foi concebido a partir da análise de conteúdo, à luz de critérios específicos, do modelo do NIST 800-100 (NIST, 2007), por ser direcionado ao setor público, da norma ISO/IEC 27014, adotada como padrão estrutural referencial, por ser aceita no mercado nacional, e das normas de cumprimento obrigatório pela APF, publicadas pelo DSIC.

3 METODOLOGIA

A presente pesquisa possui abordagem qualitativa, que pressupõe uma análise e interpretação de aspectos mais profundos da complexidade do comportamento humano, uma vez que “fornece análise mais detalhada sobre investigações, hábitos, atitudes e tendências de comportamentos” (LAKATOS; MARCONI, 2005, p. 269).

Ela foi classificada como descritiva do tipo documental, que “exige do investigador uma série de informações sobre o que deseja pesquisar” e “pretende descrever os fatos e fenômenos de determinada realidade” (TRIVIÑOS, 1987, p. 110), sendo, segundo Gil (2008, p. 50), “desenvolvida a partir de material já elaborado”. A análise documental favorece a observação do processo de maturação

ou de evolução de indivíduos, grupos, conceitos, conhecimentos, comportamentos, mentalidades, práticas, entre outros (CELLARD, 2008).

Como estratégia de pesquisa para a revisão de literatura, foram utilizadas as bases de dados de acesso aberto Scielo, Google Scholar e Periódicos CAPES. Optou-se por priorizar a busca por trabalhos em língua portuguesa que refletissem estudos relacionados à realidade nacional, de preferência em órgãos públicos brasileiros. Adicionalmente, para a pesquisa também buscou-se por trabalhos internacionais. Os principais termos e palavras-chave pesquisados foram: “Segurança da Informação”, “Carreira de TI”, “Terceirização de TI”, “Governança”, “Política de Segurança da Informação”, “Governança da Segurança da Informação” e “Administração Pública Federal”. Esta fase teve por objetivo realizar o levantamento das principais definições sobre os principais termos da área, por meio de normas e regulamentos, artigos científicos e publicações de entidades e autores consagrados no assunto.

O estudo foi realizado a partir de leitura e análise crítica de bibliografia relacionada à força de trabalho, valorização da carreira e rotatividade de servidores nos cargos de TIC, benefícios e riscos da terceirização no serviço público e na SI. Buscou-se analisar possíveis relações entre os conceitos de SI e as atribuições dos profissionais de TIC do MPF.

A coleta de dados deste trabalho foi feita a partir de consulta de normativas, Portarias, documentos vigentes em sítios de transparência, relatórios gerenciais, materiais a respeito do PEI, PETI e PDTIC, a sistemas internos do MPF, como o Sistema Nacional de Pedidos (SNP), Sistema de Gestão de Pessoas (GPS) – nos aspectos de nomeações e exonerações – Portal de Informações Funcionais (PIN), Sistema Banco de Talentos e o correio eletrônico institucional.

A interpretação e reflexão crítica dos resultados foi realizada a partir da análise dos dados, quando se observou a relação entre a valorização da carreira e os aspectos de SI na TIC. A análise dos dados “é o momento de reunir todas as partes – elementos da problemática ou do quadro teórico, contexto, autores, interesses, confiabilidade, natureza do texto, conceitos-chave” (CELLARD, 2008, p. 303). May (2004) diz que os documentos não existem isoladamente, mas precisam estar situados em uma estrutura teórica para que o seu conteúdo seja entendido. A pesquisa considerou informações a respeito de pessoal, em especial a força de

trabalho de TIC (alocação, evasão, desvio de função etc.). O levantamento e o cruzamento dos dados foram organizados em tabelas e quadros, que serviram de base para a análise crítica das informações.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo, serão apresentados e discutidos os principais aspectos relacionados à SI, em relação às atribuições regimentais e aos controles que são de responsabilidade dos profissionais de TIC do MPF. O capítulo também analisa o índice de rotatividade, evasão e *déficit* no número desses profissionais dentro da instituição. O *déficit* somado à restrição orçamentária, que acaba por motivar iniciativas de terceirização, também serão discutidas neste capítulo. Por fim, será feita uma análise do clima organizacional entre os profissionais de TIC, relacionado ao tema SI, com base na seleção de algumas manifestações no correio eletrônico institucional.

4.1 ASPECTOS DE SI E ATRIBUIÇÕES DA CARREIRA.

A Portaria MPF/PGR Nº 83 (BRASIL, 2019c), que fixa as atribuições básicas e os requisitos de investidura nos cargos das carreiras de Analista e Técnico do MPU, apresenta para o cargo dos Técnicos do MPU/TIC a atribuição, relacionada à SI, de "contribuir para a implementação de processos de segurança da informação e comunicação". Ainda, atribui aos Analistas do MPU/Suporte e Infraestrutura o encargo de “estabelecer e monitorar processos, normas e padrões para a infraestrutura tecnológica, inclusive os relacionados à segurança da informação e comunicação”. E, por sua vez, aos Analistas do MPU/Desenvolvimento de Sistemas a atribuição de “estabelecer e monitorar processos, normas e padrões para o desenvolvimento de sistemas, inclusive o modelo corporativo de dados e os relacionados à segurança da informação”. Analisando-se o Regimento Interno Administrativo do MPF, estabelecido pela Portaria SG/MPF Nº 382 (BRASIL, 2015), percebeu-se que atribuições relativas à SI estão presentes em todos os níveis hierárquicos dos servidores de TIC do MPF, desde um Técnico de Informática em uma Procuradoria da República no Município (PRM), até o cargo mais alto de Secretário Nacional de TIC. Em relação aos servidores lotados nos diversos Núcleos e Seções da TIC, são atribuídas as obrigações de “supervisionar”, “executar”,

“fiscalizar”, acompanhar”, “estimular”, “zelar”, “administrar”, “atuar”, “planejar”, “organizar”, “gerenciar” e “monitorar”. E, com base no SNP e no Catálogo Nacional de Serviços de TIC (BRASIL, 2019d), verificou-se que a maioria dos serviços que se referem à SI estão sob responsabilidade da área de TIC nas unidades.

Nessa mesma linha de raciocínio, o Decreto Nº 9.637 (BRASIL, 2018b), que institui a Política Nacional de Segurança da Informação (PNSI) e dispõe sobre a GovSI, por sua vez, deixou clara a preocupação do Governo Federal com a SI e a profissionalização de recursos humanos para suprir essa área. Percebeu-se que essa iniciativa elevou a responsabilidade de todos os órgãos da APF em capacitar seus servidores. O próprio MPF promoveu a publicação de normas que mostram essa relação, como a Portaria PGR/MPF Nº 417 (BRASIL, 2013b), que dispõe sobre o Plano de SI do MPF. Este plano teve por finalidade orientar e desenvolver a atividade de segurança no âmbito do MPF, estabelecendo princípios e diretrizes complementares à Política de Segurança Institucional. Ainda, destacou que a segurança orgânica é composta por grupos de medidas, entre elas a SI, que se desdobra em SI nos meios de tecnologia da informação, nos recursos humanos, na documentação e nas áreas e instalações físicas. Dessas medidas, pode-se destacar práticas realizadas por servidores de TIC do MPF, como: (i) “os procedimentos de armazenamento de dados (*backup*), para promover a segurança e disponibilidade da informação”; (ii) “medidas relativas ao uso exclusivo de programas e sistemas homologados pela Secretaria de TIC (STIC), instalados de forma automática pelo sistema, por acesso remoto ou presencialmente por servidor qualificado da área de TIC de cada unidade do MPF”; (iii) “medidas de segurança no ato de produzir, classificar, tramitar, arquivar e destruir documentação ou informação”; (iv) “medidas voltadas a proteger informações sensíveis armazenadas ou em trânsito no espaço físico ou eletrônico sob a responsabilidade da Instituição”; (v) “medidas relativas ao acesso a dados e informações sigilosos nos recursos de TIC”; (vi) “medidas para que mídias e equipamentos que forem destinados à doação ou descarte tenham seus dados eliminados de forma segura pelas áreas de TIC das unidades” (BRASIL, 2013b). Demonstra-se, assim, a relação direta entre a carreira do servidor de TIC do MPF e suas responsabilidades quanto à SI, inclusive quanto à soberania nacional citada no Decreto 9.637 (BRASIL, 2018b).

Há evidências, nos dados desta pesquisa, que temas relacionados à SI passaram a ser tratados de maneira mais sistematizada no MPF somente a partir do PEI, PETI e PDTIC. Estes documentos impactaram na estrutura do MPF no âmbito jurídico e administrativo em geral e na TIC em especial.

Destaca-se aqui que, com relação à SI e conforme o Regimento Interno (BRASIL, 2015), os servidores de TIC passaram a ter que atuar no tratamento e na resposta a incidentes de segurança de redes de computadores, acompanhar e realizar testes de vulnerabilidade nos ambientes operacionais do MPF, manter os equipamentos e serviços sob sua responsabilidade atualizados e livres de vulnerabilidades conhecidas, promover a cultura da SI entre a equipe técnica e os usuários de recursos de TIC e zelar pela promoção e cumprimento das políticas e normas institucionais relativas à SI. Na STIC, por ocasião desta pesquisa, identificou-se a existência de uma Divisão de Segurança da Informação (DISEGI), subordinada à Subsecretaria de Infraestrutura de Tecnologia da Informação, que era responsável por essas atividades. E, nas unidades estaduais, observou-se que tal competência ficava a cargo dos Núcleos ou Seções de Infraestrutura de Tecnologia da Informação e Segurança da Informação.

Apesar das atribuições de SI terem sido destinadas à área de TIC, a responsabilidade sobre a Segurança Institucional (SIn) estava atrelada à Secretaria de Segurança Institucional (SSIn). No Plano de SIn, conforme já citado, a SI foi definida como uma subdivisão da SIn. Uma vez que a STIC e a SSIn tinham o mesmo *status* organizacional (ambas eram secretarias), existia um possível conflito de atribuições na área de SI, sendo que uma secretaria deveria se submeter à outra nesses assuntos, indicando talvez um conflito de competência na gestão e governança da SI.

4.2 CONTROLES DE SI

A norma ISO/IEC 27001 “elenca requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto de uma organização” (ABNT, 2013, p. 1). Esta norma traz 114 controles de SI organizados em 14 categorias. No Quadro 1, foram relacionados apenas alguns destes controles, que na prática são executados e são de responsabilidades específicas dos profissionais de TIC do

MPF, conforme evidências retiradas do sistema SNP.

Quadro 1: Controles de SI de responsabilidade dos servidores de TIC do MPF

Nº	Controle	Descrição do Controle
24	A.8.3.2	As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
27	A.9.1.2	Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
33	A.9.2.6	Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.
35	A.9.4.1	O acesso à informação e às funções dos sistemas de aplicações deve ser restrito de acordo com a política de controle de acesso.
37	A.9.4.3	Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade.
48	A.11.2.1	Os equipamentos devem ser protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
54	A.11.2.7	Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.
62	A.12.3.1	Cópias de segurança das informações, *softwares* e das imagens do sistema devem ser efetuadas e testadas regularmente contra *malware*, combinados com um adequado programa de conscientização do usuário.
76	A.13.2.3	As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
81	A.14.2.1	Regras para o desenvolvimento de sistemas e *software* devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.
93	A.15.1.3	Acordos com fornecedores devem incluir requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação.
100	A.16.1.5	Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados.
106	A.17.2.1	Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.
110	A.18.1.4	A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

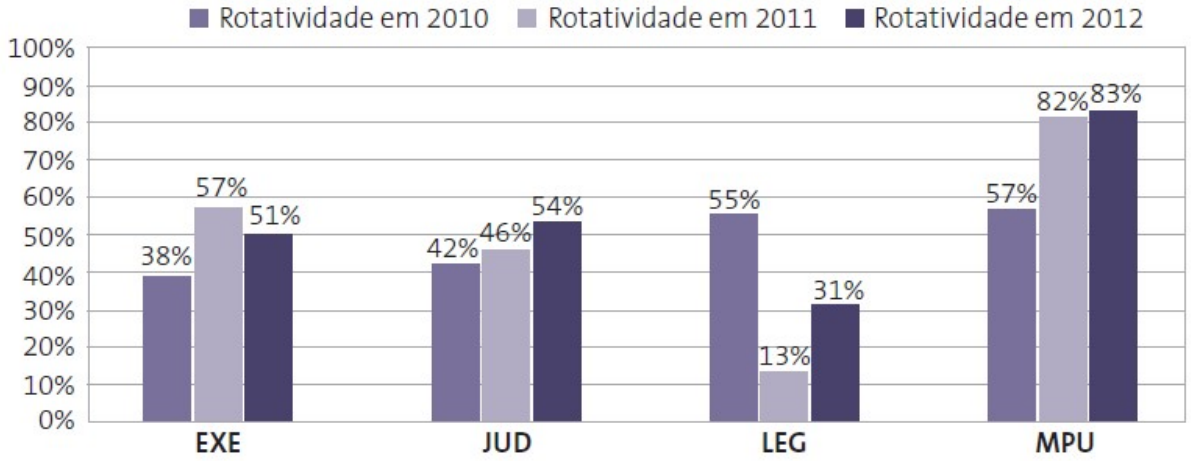
Fonte: Norma ISO/IEC 27001 (2013) adaptada pelos autores.

Observa-se que as atividades do Quadro 1 abordam diversos aspectos, sejam eles relacionados a fatores humanos, sejam relativos a equipamentos e mídias, sistemas, requisitos legais e contratuais, entre outros, reforçando a diversidade e importância da atuação do servidor de TIC em questões relacionadas à SI.

4.3 ROTATIVIDADE, EVASÃO E *DÉFICIT* DE SERVIDORES DE TIC

A pesquisa realizada pelo TCU (BRASIL, 2015), com 448 instituições federais dos três poderes (Executivo, Legislativo e Judiciário) e do Ministério Público da União (MPU), apontou uma retenção de pouco mais de 50% dos profissionais de TIC que ingressaram entre 2010 e 2012. O MPU foi o que apresentou o maior grau de rotatividade, como pode ser observado na Figura 1. O cálculo do percentual de rotatividade utilizado pelo TCU foi obtido a partir do resultado da relação entre a quantidade de entradas e saídas, computados todos os possíveis tipos, como aposentadorias, exonerações, falecimentos e posses em outros cargos. Além disso, a pesquisa apontou que a principal causa que poderia justificar as dificuldades encontradas para retenção de pessoal de TIC é a "remuneração inferior à de outras carreiras de TIC da APF".

Figura 1: Rotatividade de pessoal de TI (2010-2012) por poder



Fonte: TCU (2015, p. 20)

Foram coletados e sumarizados na Tabela 1 dados sobre os profissionais de TIC do MPF (técnicos e analistas) dos últimos 10 anos (de 2010 até dezembro de 2019). Levantou-se o quantitativo de cargos ativos (do início de cada ano), entradas, saídas e o índice de rotatividade anual. A coluna "Rotatividade" da Tabela 1 seguiu a mesma metodologia adotada pelo TCU, que correlaciona o total de entradas e saídas. Julgou-se pertinente analisar o percentual de saídas em relação ao total de ativos. A essa análise foi dado o nome de Índice de Rotatividade Relativa (IRR), que foi calculado pela divisão da quantidade total de saídas (desligamentos, falecimentos e aposentadorias) pelo total de ativos do início do ano. Por exemplo, 2010 iniciou com 607 cargos ativos de TIC. Naquele ano, houve 24

saídas (23 por desligamento e 1 por aposentadoria). Assim, o IRR de 2010 foi de 3,95% (24/607).

Tabela 1: Histórico de servidores de TI de 2010 a 2019.

Ano	Ativos	Entradas		Saídas			Rotatividade (método do TCU)	Índice de Rotatividade Relativa
		Nomeações	Transferências	Desligamentos	Falecimentos	Aposentadorias		
2010	607	51	1	23	1	0	46,15%	3,95%
2011	642	45	10	14	2	1	30,91%	2,65%
2012	604	18	44	86	3	3	148,39%	15,23%
2013	629	18	3	33	0	4	176,19%	5,55%
2014	596	59	28	49	0	4	60,92%	8,89%
2015	650	58	6	31	0	2	51,56%	5,08%
2016	698	15	14	14	0	1	51,72%	2,15%
2017	704	14	8	17	1	4	100,00%	3,12%
2018	717	1	3	6	0	4	250,00%	1,39%
2019	704	0	4	8	0	5	325,00%	1,85%
Total		279	121	278	7	28	---------	**Σ 50,20%**
		400		**316**			**79,00%**	

Fonte: Elaborada pelos autores.

A sumarização da Tabela 1 mostra que em 10 anos houve 400 entradas e 316 saídas, uma rotatividade de 79%. Já o somatório do IRR foi de 50,2%, ou seja, mais da metade do total de servidores de TIC deixaram a instituição nesse período. Além disso, do total de 316 desligamentos, apenas 35 foram involuntários (7 falecimentos e 28 aposentadorias). Esses índices podem ser considerados indícios de insatisfação ou evasão por conta de melhores oportunidades fora do MPF. E mais, tal rotatividade, como já constatado por Soares, Capistrano e Barbosa (2015), ainda pode significar para o MPF a descontinuidade em projetos, investimentos em capacitação potencialmente perdidos, dificuldades em continuidade no atendimento de demandas, perda de conhecimento da instituição, entre outros problemas de ordem gerencial.

A elaboração da Tabela 1 levou em consideração o total absoluto de servidores, mesmo os que não atuavam diretamente na TIC, com base na consulta

direta à base de dados do Sistema GPS do MPF. Um estudo preliminar da STIC, de março de 2019, revelou que há um desvio de função de aproximadamente 17% das suas vagas oficiais, ou seja, estes profissionais, ainda que servidores de TIC, não desempenhavam atividades para a STIC.

Os desligamentos somados aos desvios de função caracterizam o fenômeno conhecido como *turn-away*, conforme estudos de Ramos e Joia (2014). O *turn-away* na TIC do MPF pode ter sido motivado por diversos fatores, como oferta de gratificações em áreas distintas da TIC, descontentamento com a área técnica ou, simplesmente, a busca de novos desafios dentro da carreira pública.

Gartner (2016) fez um levantamento da quantidade de pessoas alocadas formalmente na área de TIC, criando a unidade de medida *Full-Time Equivalents* (FTE), que representa a equipe lógica para suportar funções executadas pela equipe física. Isso inclui todos os níveis de pessoal dentro da organização, desde gerentes e líderes de projeto até pessoal de operações diárias. Nessa pesquisa, realizada entre os anos de 2012 a 2016 com 3.172 empresas públicas e privadas de mais de 80 países, demonstrou-se que, para o segmento de órgãos públicos de natureza federal, o FTE de TIC é de 7,7%. Ou seja, para cada 1000 usuários, são necessários em média 77 servidores de TIC para atender as demandas. Esse valor foi obtido pela média dos valores de referência dos 5 anos do estudo (8,3% em 2012; 6,2% em 2013; 7,6% em 2014; 7,9% em 2015 e 8,5% em 2016) e observada uma pequena tendência de crescimento.

No cômputo dos FTEs foram excluídos os contratados que não estavam desempenhando suas atividades direta ou indiretamente sob a supervisão da gestão de TIC. Por exemplo, não foram levados em consideração aqueles que trabalhavam em provimento de serviços de comunicação de dados, telefonia ou impressão, visto que não trabalhavam de forma dedicada para a instituição, tampouco estão lotados em suas unidades. Já o universo de usuários atendidos foram todos aqueles que faziam uso de recursos de TIC na instituição, tais como membros, servidores, contratados, estagiários e voluntários. Usando esses parâmetros como referência, em dezembro de 2019 o total de usuários atendidos pela TIC no MPF era de 14.480 (1.150 membros, 9.049 servidores, 892 comissionados, 348 requisitados, 2.933 estagiários e 108 voluntários). Considerando o FTE de TIC médio de 7,7%, seriam idealmente necessários ao menos 1.115

servidores de TIC. Porém, o MPF contava nesta data com apenas 708 servidores de TIC. Ou seja, havia um *déficit* de 36,50%, cenário no qual seria necessário o aumento de 407 vagas.

No cálculo do *déficit*, não foram considerados os servidores que encontravam-se em desvio de função, que poderia chegar a 17%. Outro dado levantado no GPS foi a existência de 26 servidores de TIC lotados em Assessorias de Pesquisa e Análise Descentralizada (ASSPA), subordinados diretamente à Secretaria de Pesquisa, Análise e Perícia (SPPEA). Tais setores ofereciam uma Gratificação por Atividade de Segurança (GAS) por considerarem que esses servidores realizavam atividade de manipulação de dados sensíveis e/ou sigilosos.

Com base no PIN, cabe mencionar que 16,38% (116 servidores) do total de servidores de TIC estavam lotados em PRMs. Ou seja, vinculados às chefias administrativas e jurídicas locais e não diretamente à TIC, não havendo uma subordinação hierárquica no organograma que determinasse que esses deveriam seguir as orientações da Coordenadoria de TIC (CTIC) do estado, podendo, eventualmente, comprometer a SI. Observou-se servidores de TIC, principalmente de PRMs, lotados em gabinetes, setores jurídicos, de acompanhamento processual, de autuação e distribuição ou de pessoal. Essas foram possíveis evidências de que, por pressão local, por iniciativa própria ou mesmo por isolamento e distanciamento geográfico de equipes de TIC, os citados servidores acabavam atuando muito mais em atividades administrativas e jurídicas do que na própria TIC.

E nessa linha, em consulta à base de dados do Sistema de Banco de Talentos do MPF, foi possível observar servidores de TIC que, após o ingresso no MPF, capacitaram-se (cursos, graduação, especialização, entre outros) em outras áreas de atuação, principalmente na jurídica. Indícios fortes de que, com o tempo, poderiam vir a deixar a área de TIC (*turn-away*).

Todos esses fatos poderiam aumentar o *déficit* real no número de servidores de TIC do MPF e, possivelmente, tornar-se um sério obstáculo no cumprimento de prazos e de Acordos de Níveis de Serviços (ANS) estabelecidos junto aos clientes internos e parceiros, podendo comprometer inclusive os serviços de SI prestados. Esse *déficit* pode ter colaborado para a tendência à terceirização e para o aumento do número de vagas de estagiários, uma vez que as restrições orçamentárias dificultavam a reposição de pessoal concursado.

4.4 RAZÕES E RISCOS RELACIONADOS À TERCEIRIZAÇÃO DE TIC

A pesquisa do Gartner (2016) demonstrou em âmbito mundial que o segmento de órgãos federais foi o que mais investiu em terceirização e que a América Latina teve destaque nessa estratégia de aplicação de recursos.

A terceirização de TIC em órgãos públicos brasileiros tem se mostrado um caminho irreversível para suprir o *déficit* de pessoal em relação às crescentes demandas ou, e principalmente, para reduzir custos frente à escassez de recursos orçamentários e ao congelamento dos investimentos do setor, desde a Emenda Constitucional 95/2016 (BRASIL, 2016a). Porém, não se deve negligenciar os riscos desse processo, principalmente na área de SI. A análise de riscos é um dos pontos de destaque da IN MP/SLTI n° 01 de 2019 (BRASIL, 2019[a]), que em seu artigo 2°, incisos XII ao XVIII, demonstra a sua importância e necessidade. Esta IN também estabelece que gestão de SI não pode ser objeto de contratação, conforme consta no seu art. 3º, inciso II. Do que se conclui que cabe às instituições públicas investir na capacitação de suas equipes, eis que tais profissionais não poderão ser buscados no mercado.

Conforme (BRASIL, 2019b), o MPF já contratava alguns serviços de TIC terceirizados, como, por exemplo, segurança de perímetro (*firewall*), Internet e impressão/digitalização. Além destes, estava prevista no PETI (BRASIL, 2013a) a terceirização de uma Central Única de Serviços, sendo essa a última estrutura pendente para cumprir as orientações previstas na Resolução CNMP nº 171/2017 (BRASIL, 2017), que instituiu a Política Nacional de TI do Ministério Público.

Com o aumento do uso de TIC para as atividades-fim (eletronificação dos processos judiciais, por exemplo), o MPF necessitou de uma estrutura de atendimento cada vez mais robusta para satisfazer a crescente demanda. Somada a isso, a tendência de redução da reposição de servidores públicos, em função da suspensão de novos concursos, motivada pela Emenda Constitucional 95/2016 (BRASIL, 2016a), implicou a busca de soluções por meio da execução indireta de serviços, sempre que possível, a fim de desonerar os servidores de atividades acessórias, propiciando o seu direcionamento às atividades de planejamento, coordenação, supervisão e controle.

Essa tendência de solução, viabilizada pela terceirização, remete à análise de questões relacionadas à SI. O Quadro 2 resume os principais riscos e as possíveis consequências para as instituições.

Quadro 2: Principais Riscos de Terceirizar TIC e suas Consequências

	Risco:	Consequências:
1	Exposição de informações sigilosas sem restrição.	Vulnerabilidade do órgão.
2	Rotatividade de pessoal	Perda de conhecimento do negócio; Descontinuidade dos serviços prestados; Perda de identidade cultural da empresa.
3	Resistências e Conservadorismo.	Ausência de transferência ou troca de informações entre os servidores dos órgãos e os funcionários terceirizados dificultando o entendimento do negócio e integração entre as partes; Dificuldade de aproveitamento de servidores já capacitados como suporte a equipe terceirizada.
4	Ausência de Planejamento e Monitoramento.	Falta de controle de qualidade dos produtos ou serviços entregues; Não cumprimentos dos prazos; Maior volume de gastos do órgão com a empresa contratada.
5	Ausência de repasse de informações.	Dependência dos Terceirizados.
6	Ausência de controles de segurança.	Falta de esclarecimento para os terceirizados das suas responsabilidades contratuais.
7	Ausência de estimativa de gastos real por todo o período possível da vigência do contrato.	Aumento significativo do volume de gastos em relação aos valores estimados inicialmente; Necessidade de aprovação de Termos Aditivos em contratos.

Fonte: Guarda, Oliveira e Souza Junior (2012, p. 6).

Analisando o Quadro 2, observa-se que os itens apontados possuem relação com processos de trabalho, padronizações, controles, capacitações e cultura organizacional, todos relacionados à SI. Tais aspectos devem ser levados em consideração previamente ao processo de terceirização, visando mitigar os riscos inerentes.

4.5 CLIMA ORGANIZACIONAL ENTRE OS PROFISSIONAIS DE TIC DO MPF

A publicação da Portaria Nº 83 (BRASIL, 2019c), que atualizou as atribuições básicas e os requisitos de investidura nos cargos das Carreiras de Analista e Técnico do MPF, causou insatisfação a muitos servidores de TIC, pois apresentou superficialmente a sua atuação na área de SI. Isso foi constatado por manifestações no grupo de correio eletrônico institucional (rede@listas.mpf.mp.br), postadas por profissionais de todo o país.

Um dos pontos mais discutidos foi o fato de que a nova Portaria atribuiu aos servidores de TIC a função de “contribuir” para implementação de processos de SI e para os servidores da SIn a função de “executar” atividades relacionadas à SI. Na sequência, algumas dessas manifestações são apresentadas.

> [...] dentre as nossas atribuições, caberá: "contribuir para a implementação de processos de segurança da informação e comunicação." já para os técnicos em segurança institucional, que não possuem conhecimento algum na área, pasmem, caberá: "executar atividades relacionadas à segurança da informação e das comunicações;" quer dizer, nós só podemos contribuir, porque supostamente não somos capacitados, já os técn. em segurança institucional, tem condições e capacidade para executar atividades na área de segurança da informação e das comunicações, justificando assim, o recebimento da GAS, a qual não temos e nunca teremos direito.
>
> Em que pese a colaboração de outros setores do MPF que possuem conhecimento de segurança de forma geral, somente os profissionais de TI têm conhecimento técnico específico para atuar nas questões relativas à segurança da informação.

Como pôde ser observado, a preocupação dos servidores de TIC voltou-se para o fato de que a Portaria atribuiu a função de executar ações de SI a servidores que não eram de TIC e não possuíam conhecimento técnico específico para exercer tal atividade. Além disso, um dos manifestantes relatou a percepção de GAS como uma forma de valorização da carreira do profissional que atua em questões de SI, porém destacou a incoerência entre quem executava a função e quem estava capacitado a executá-la.

> Ficou claro que as atribuições desta portaria, ao invés de refletir a realidade, da forma que foram editadas pela administração, visa somente a não admissão e reconhecimento do nosso direito a GAS. Segurança da Informação é sim Segurança Institucional e essa administração, depois do "The Intercept Brasil", deveria ter aprendido isso.
>
> Sou responsável (legalmente) pela segurança? Então devo receber mais.... Se não sou então deixa quem faz fazer.

Nessas manifestações, outro posicionamento foi de que a alteração na Portaria veio para justificar a atribuição da GAS apenas para técnicos da SSIn, excluindo os servidores de TIC. A discussão envolveu o fato de que a SI é parte crucial da SIn e os servidores de TIC responsáveis pela SI deveriam ser reconhecidos.

> Não tenho nenhuma dúvida de que esse assunto precisa/deve ser melhor avaliado pela alta administração, dada a sua relevância. Entendo que as equipes de TIC devem ter conscientização de sua responsabilidade, intrínseca à profissão, entretanto pergunto: a Instituição MPF gratifica servidores que trabalham com segurança institucional? Se sim, que gratifiquem todos que trabalham com segurança institucional.

Observou-se que, na percepção do servidor, houve interpretação equivocada do MPF quanto a quem de fato deveria receber a valorização pelo desempenho das funções relativas à SI, deixando explícita a mensagem de que quem atuava em TIC atuava também em SIn. Portanto, se há remuneração diferenciada para o profissional que atuava na SIn, por analogia deveria haver também para o profissional de TIC.

5 CONCLUSÃO

Este trabalho teve o intuito de compreender a relação entre os serviços de SI e a valorização da carreira de TIC no MPF. Para tanto, foram identificados os serviços prestados em SI e correlacionados com a carreira desses profissionais, a partir da apresentação e discussão dos principais aspectos ligados à SI em relação às atribuições regimentais e aos controles; da análise de recursos humanos na instituição; de questões relacionadas aos riscos decorrentes da terceirização e, por fim; da análise do clima organizacional.

O estudo indicou que há significativa rotatividade, evasão e elevado *déficit* no número de servidores de TIC no MPF e que isso pode causar descontinuidade em projetos, perdas de recursos investidos em capacitação, descontinuidade no atendimento de demandas, dentre outros problemas de ordem gerencial. Observou-se ainda que o PETI (BRASIL, 2013a) destacou, em seu Objetivo Estratégico nº 15, a necessidade de "atrair, capacitar, motivar e reter talentos", com permanente atenção ao clima organizacional, mantendo um ambiente que estimule o crescimento profissional e pessoal, por meio de capacitações e da valorização da carreira de TIC. Diante disso, denota-se a necessidade de mudanças nas ações de Governança de TIC, visando a melhor alcançar tal objetivo.

No capítulo 4, foram apresentados indícios de insatisfação de servidores de TIC do MPF, a partir de mensagens do correio eletrônico institucional, tendo em vista que eles relataram exercer inúmeras atividades voltadas à SI, mas que aparentemente passaram despercebidas pela alta administração. Esse sentimento foi justificado em razão da Portaria MPF/PGR Nº 83 (BRASIL, 2019c), na qual servidores de outra área seriam responsáveis pelas atividades de SI que, na prática, são realizadas por servidores de TIC. Além disso, verificou-se que a Lei 13.316/2016 (BRASIL, 2016b), que dispõe sobre as carreiras dos servidores do

MPU, previa a percepção de gratificação para servidores que ocupavam cargos ou funções de segurança. Entretanto, não contemplava aqueles que exerciam tais atividades de SI, com exceção para os servidores lotados na SPPEA e nas ASSPAs. Concluiu-se que havia uma relativa desmotivação dos servidores de TIC, talvez em função da falta de algum tipo de compensação relativa aos serviços prestados em SI.

A SIn possui um grupo de medidas que inclui a SI, conforme constava na Portaria PGR/MPF Nº 417 (BRASIL, 2013b). A SSIn, por óbvio, é responsável pela SIn. Levando-se em conta que a STIC estava hierarquicamente no mesmo nível da SSIn, entendeu-se que a SI deveria estar sob responsabilidade da STIC, principalmente em função de que os servidores de TIC exerciam atividades de SI, conforme as atribuições dispostas no Regimento Interno Administrativo do MPF (BRASIL, 2015), e detinham conhecimento técnico específico para desempenhá-las.

Diante dos fatos apresentados no trabalho, observou-se que o fortalecimento de políticas, normas, ações, valorização das carreiras, transparência, gestão e governança seriam medidas que poderiam gerar aumento na maturidade da SIn do MPF.

Ações, como a criação de um comitê específico para analisar e estudar estratégias sobre SI no MPF, com a participação ativa do Secretário de TIC, de servidores da DISEGI e de servidores ligados à área de SI nos estados, poderiam aumentar o nível de comprometimento dos profissionais e evitar ou atenuar problemas relacionados à SI. Outra medida que poderia ser adotada, com objetivo de fortalecimento da atuação em SI, seria a sistematização e elaboração de um rol de treinamentos mínimos necessários para o credenciamento de servidores de TIC atuarem na área de SI em prol da SIn.

Este trabalho possui restrições, uma vez que contempla somente o ambiente do MPF, que apesar de possuir estruturação nacional, tem, como toda instituição, características próprias.

Como sugestões para trabalhos futuros, recomenda-se que novas pesquisas sejam realizadas em diferentes Ministérios Públicos brasileiros e em instituições públicas federais diversas, tanto de âmbito regional quanto nacional, visando a inferências e geração de teorias.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013.** Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2013. 30 p.

_____. **NBR ISO/IEC 27002:2005**. Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120 p. ISBN 987-85-07-00648-0.

_____. **NBR ISO/IEC 27014:2013**. Tecnologia da Informação – Técnicas de segurança – Governança de segurança da informação. Rio de Janeiro: ABNT, 2013. 12 p. ISBN 978-85-07-04333-1.

_____. **NBR ISO/IEC 38500:2018.** Tecnologia da informação - Governança da TI para a organização. Rio de Janeiro: ABNT, 2018. 13 p.

ALBUQUERQUE JUNIOR, Antônio Eduardo de; SANTOS, Ernani Marques dos. **Produção científica sobre segurança da informação em eventos científicos brasileiros**. *In*: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, 2014, São Paulo. *Proceedings of*… São Paulo: CONTECSI, 2014. p. 2085-2103. Disponível em: https://is.gd/eQp3JG. Acesso em: 30 ago. 2019.

ALENCAR, Gliner Dias *et al*. Governança, Gestão e Maturidade da Segurança da Informação: um mapeamento sistemático do cenário nacional. **Revista de Sistemas e Computação**, Salvador, v. 8, n. 1, p. 153-173, jan./jun. 2018. Disponível em: https://is.gd/aQmmUu. Acesso em: 30 ago. 2019.

ALENCAR, Gliner; QUEIROZ, Anderson; QUEIROZ, Ruy. **Insiders: Um Fator Ativo na Segurança da Informação.** *In:* SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 9. , 2013, João Pessoa. Anais do IX Simpósio Brasileiro de Sistemas de Informação. Porto Alegre: Sociedade Brasileira de Computação, 2013. p. 61-72. Disponível em: https://is.gd/STpFtB. Acesso em: 10 out. 2019.

BRASIL. Conselho Nacional do Ministério Público. **Resolução Nº 171, de 27 de junho de 2017.** Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP). Brasília, 2017. Disponível em: https://is.gd/K6qQTg. Acesso em: 10 dez. 2019.

_____. Ministério da Economia. **Instrução Normativa Nº 1, de 4 de abril de 2019.** Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP [...]. Brasília, 2019. Disponível em: https://is.gd/fxpdiT. Acesso em: 9 dez. 2019.

_____. Ministério Público Federal. **Planejamento Estratégico de Tecnologia da Informação (PETI) - 2012-2020.** Brasília: 2013. Disponível em: https://is.gd/bxpK0e. Acesso em: 22 jan. 2020.

_____. _____. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) - 2018-2020.** Brasília: Procuradoria Geral da República, 24 jan. 2018. Disponível em: https://is.gd/Pw9qZH. Acesso em: 9 dez. 2019.

_____. _____. **Portal da Transparência - Licitações, Contratos e Convênios - Contratos.** 2019. Disponível em: https://is.gd/u3ni9A. Acessado em: 27 dez. 2019.

_____. _____. **Portaria PGR/MPF Nº 417, de 5 de julho de 2013.** Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal. Brasília: PGR, 2013. Disponível em:https://is.gd/uhHJLu. Acesso em: 9 dez. 2019.

_____. _____. **Portaria PGR/MPF Nº 687, de 20 de dezembro de 2011.** Institui o

Planejamento Estratégico do Ministério Público Federal para o decênio 2011-2020. Publicada no BSMPF, Brasília, DF, p. 9, 2. quinzena dez. 2011. Disponível em: https://is.gd/f9tVDC. Acesso em: 21 ago. 2019.

_____. _____. **Portaria SG/MPF Nº 382, de 5 de maio de 2015.** Aprova o Regimento Interno Administrativo do Ministério Público Federal. Brasília: Procuradoria Geral da República, 2015. Disponível em:https://is.gd/GmUW6Y. Acesso em: 9 dez. 2019.

_____. _____. **Portaria PGR/MPU Nº 83, de 16 de setembro de 2019.** Fixa as atribuições básicas e os requisitos de investidura nos cargos das Carreiras de Analista e Técnico do Ministério Público da União e dá outras providências. Brasília: PGR, 2019. Disponível em: https://is.gd/c24PjM . Acesso em: 9 dez. 2019.

_____. _____. Secretaria de Tecnologia da Informação e Comunicação. **Catálogo nacional de serviços**: tecnologia da informação e comunicação – 2. ed. – Brasília: MPF, 2019. 62 p. Disponível em: https://is.gd/w4OuXw. Acesso em: 04 nov. 2019.

_____. _____. **Mapa estratégico do MPF**. Brasília: Procuradoria Geral da República, 2011. Disponível em: https://is.gd/iHGXio. Acesso em: 9 dez. 2019.

_____. Presidência da República. **Decreto Nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação [...]. Brasília: Secretaria-Geral, 2018. Disponível em: https://is.gd/LrNrEz. Acesso em: 10 dez. 2019.

_____. _____. **Emenda Constitucional Nº 95, de 15 de dezembro de 2016.** Altera o Ato das Disposições Constitucionais Transitórias, para instituir o Novo Regime Fiscal, e dá outras providências. Brasília: Casa Civil, 2016. Disponível em: https://is.gd/HMDx7C. Acesso em: 10 dez. 2019.

_____. _____. **Lei 13.316, de 20 de julho de 2016.** Dispõe sobre as carreiras dos servidores do Ministério Público da União e as carreiras dos servidores do Conselho Nacional do Ministério Público [...]. Brasília: Secretaria-Geral, 2016. Disponível em: https://is.gd/RjNNKD. Acesso em: 10 dez. 2019.

_____. Tribunal de Contas da União. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação (Sefti), 2008. 48 p. – (Sumário Executivo). Disponível em: https://is.gd/l8BxVY. Acesso em: 01 nov. 2019.

_____._____. **Levantamento de pessoal de TI** / Tribunal de Contas da União; Relator Ministro Raimundo Carreiro. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação (Sefti), 2015. 52 p. – (Sumário Executivo. Tecnologia da Informação). Disponível em: https://is.gd/xDHBXd. Acesso em: 29 ago. 2019.

_____._____. **Referencial básico de governança** Aplicável a Órgãos e Entidades da Administração Pública. Brasília: TCU, 2ª versão - Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014. 80 p. Disponível em: https://is.gd/U24GRl. Acesso em: 13 de nov. 2019.

CELLARD, André. **A análise documental.** *In:* POUPART, J. *et al*. A pesquisa qualitativa: enfoques epistemológicos e metodológicos. Petrópolis, Vozes, 2008.

CDN. **Portaria nº 14, de 11 de maio de 2015**, Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0" [...]. Disponível em: https://is.gd/zQbFvS. Acesso em: 25 Out. 2019.

CHEROBINI, Tatiana Minuzzi. **Terceirização de serviços de TI: aspectos de segurança.** Artigo do Trabalho de Conclusão do Curso de Especialização em Governança de Tecnologia da Informação, da Universidade do Sul de Santa

Catarina. 2017. Disponível em: https://is.gd/yxEO6j. Acesso em: 13 ago. 2019.
GARTNER. **IT Key Metrics Data 2017: Executive Summary**. 12 December 2016. Disponível em: https://is.gd/yURAnE. Acesso em: 03 dez. 2019.
GUARDA, Graziela Ferreira; OLIVEIRA, Edgard Costa; SOUZA JUNIOR, Rafael Timóteo de. **Análise de Contratos de Terceirização de TI na Administração Pública Federal sob a Ótica da Instrução Normativa N° 04**. IX SEGeT - Simpósio de Excelência em Gestão de Tecnologia. Resende, RJ, 2012. Disponível em: https://is.gd/afoyXw. Acesso em: 13 nov. 2019.
GONZALEZ, Reyes; GASCO, Jose; LLOPIS, Juan. **Information systems outsourcing reasons and risks**: A new assessment. Industrial Management and Data Systems. 110. 284-303. DOI: 10.1108/02635571011020359. 2010. Disponível em: https://is.gd/KMIOiE. Acesso em: 21 out. 2019.
GUIMARÃES, Rogério; NETO, João Souza; LYRA, Maurício Rocha. **Modelo de Governança de Segurança da Informação para a Administração Pública Federal**. Perspectivas em Gestão & Conhecimento, João Pessoa, v. 8, n. 3, p. 90-109, set./dez. 2018. DOI: http://dx.doi.org/10.21714/2236-417X2018v8n3p90. ISSN: 2236-417X. Disponível em: https://is.gd/mgZkey. Acesso em: 18 out. 2019.
GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2008.
ISACA (*Information Systems Audit and Control Association*). **COBIT 5 - *Controls Objectives for Information and related Technology*.** Modelo Corporativo para Governança e Gestão de TI da Organização. 2012. Disponível em: https://is.gd/hJIDDv. Acesso em: 31 out. 2019.
LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia Científica.** 5. ed. São Paulo: Atlas, 2008.
LYRA, Maurício Rocha. **Governança da Segurança da Informação.** 1. ed. Brasília, 2015. Disponível em: https://is.gd/BDeJau. Acesso em: 19 set. 2019.
MACHADO JUNIOR, Dorival Moreira. **Segurança da Informação: uma abordagem sobre a proteção da privacidade em internet das coisas.** Tese (Doutorado em Tecnologias da Inteligência e Design Digital) - PUC de São Paulo. São Paulo, p. 158. 2018. Disponível em: https://is.gd/QsWZuH. Acesso em: 31 out. 2019.
NIST, FIPS PUB 199. **Standards for Security Categorization of Federal Information.** 2004. Disponível em: https://is.gd/AgYHHt. Acesso em: 31 out. 2019.
NIST, Special Publication 800-100. **Information Security Handbook: a Guide for Managers.** 2007. Disponível em: https://is.gd/4MgMta. Acesso em 25 Out. 2019.
MARCELINO, Paula; CAVALCANTE, Sávio. **Por uma definição de terceirização.** Caderno CRH [online]. vol. 25, n. 65, p. 331-346, Salvador, Mai/Aug. 2012. ISSN 0103-4979. Disponível em: https://is.gd/DhCwp7. Acesso em: 13 nov. 2019.
MAY, Tim. **Pesquisa social: questões, métodos e processo.** Porto Alegre, 2004.
OLIVEIRA, Francisco Correia de; SANTOS, Joselias Lopes dos. **Fatores de riscos associados à terceirização de TI no setor público**. III SEGeT - Simpósio de Excelência em Gestão de Tecnologia. Fortaleza, 2006. Disponível em: https://is.gd/qMgk1B. Acesso em: 15 set. 2019.
PAANANEN, Hanna; LAPKE, Michael; SIPONEN, Mikko. **State of the art in information security policy development**. Computers & Security. Volume 88, January 2020, 101608. 2019. https://doi.org/10.1016/j.cose.2019.101608. Disponível em: https://is.gd/zQKNIk. Acesso em: 18 out. 2019.
PRICEWATERHOUSECOOPERS, **The Global State of Information Security® Survey 2018.** 2017. Disponível em: https://is.gd/AI7VJy. Acesso em: 29 ago. 2019.

RAMOS, Eduardo Augusto de Andrade; JOIA, Luiz Antonio. Uma investigação acerca do fenômeno do turn-away entre os profissionais de tecnologia da informação. RAM. **Revista de Administração Mackenzie**. 2014, vol. 15, n. 4, p. 75-109. Disponível em: https://is.gd/DETFuT. Acesso em: 29 ago. 2019.
ROCHA, Alexandre Pereira da; CASTRO, Carla Giovanna Costa de; SILVA JÚNIOR, Ivan Monteiro da. **Os desafios da Governança de Tecnologia da Informação na Administração Pública Federal: um enfoque na segurança da informação e nas pessoas.** Universidade Federal Fluminense, Niterói, dez. 2017. Disponível em: https://is.gd/1b8De3. Acesso em: 29 ago. 2019.
SACRAMENTO, António José Caessa Alves do. A. **Uma Reflexão Sobre a Segurança nas Comunicações**. Revista Militar Nº 2464. Maio de 2007. Portugal. Disponível em: https://is.gd/EGsnNs. Acesso em: 01 nov. 2019.
SCOTT, Murray. **Public sector IT outsourcing**: a framework for evaluating risk. IFIP e-Government Conference 2010. 2010. Disponível em: https://is.gd/krkCmH. Acesso em: 21 out. 2019.
SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva.** 1ª ed. Rio de Janeiro: Ed. Campus, 2003. p. 184. ISBN: 9788535211917.
SCHNEIER, Bruce. **The Case for Outsourcing Security**. Supl. to IEEE Computer Magazine, 2002. Disponível em: https://is.gd/FPcOPd. Acesso em: 21 out. 2019.
SIMÕES, José Carlos Ferrer. **Análise da maturidade da política de segurança da informação dos órgãos da Administração Pública Federal Direta.** Trabalho de Conclusão de Pós-graduação em Governança em TI (UniCEUB/ICPD). 2014. Disponível em: https://is.gd/IqXP7s. Acesso em: 8. out. 2019.
SOARES, Marison Luiz; CAPISTRANO, Alvaro Guilherme Ayres; BARBOSA, Mariana Biancucci Apolinário. **A rotatividade de servidores públicos na área de TI**: um estudo de caso sobre a ótica da gestão de pessoas. 2015. Disponível em: https://is.gd/hAJ6UD. Acesso em: 29 ago. 2019.
STALLINGS,William; BROWN, Lawrie. **Segurança de Computadores**, Elsevier Editora Ltda., 2014. p. 7-32, ISBN 9788535264494.
TRIVIÑOS, Augusto Nibaldo Silva. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação.** São Paulo: Atlas, 1987.