DOI: http://dx.doi.org/10.9771/cp.v13i4.29512

Um Estudo da Segurança da Informação na Propriedade Intelectual nas ICTs

A Study of the Information Security on Intellectual Property in Science and Technology Institutions

Paulo Cesar Andrade Arruda[1]
Marcio Lima da Silva[1]
Edilson da Silva Pedro[1]
[1]Universidade de Brasília, Brasília, DF, Brasil

Resumo

O presente estudo apresenta um panorama nacional e internacional dos controles relacionados à segurança da informação utilizados pelas Instituições de Ciência e Tecnologia (ICTs) em suas atividades sobre a Propriedade Intelectual. Para esta análise foram selecionadas Instituições de renome nacional e internacional. A metodologia utilizada tem como referencial as recomendações das normas ABNT NBR ISO/IEC 27001 e 27002 e permitiu mapear os principais controles adotados pelas ICTs, além de indicar as Instituições que possuem um Sistema de Gestão de Segurança da Informação (SGSI) mais completo e abrangente. A partir desse mapeamento, analisou-se o impacto dos principais controles nas atividades institucionais que envolvem Propriedade Intelectual. Concluiu-se que a adoção de um SGSI é crucial para o desenvolvimento de atividades relacionadas à Propriedade Intelectual, como a proteção de ativos intangíveis e a transferência de tecnologias. Observou-se que, comparando as ICTs nacionais com as estrangeiras, estas apresentam um Sistema de Gestão de Segurança da Informação mais abrangente em relação à PI.

Palavras-chave: Segurança da Informação. Propriedade Intelectual.

Abstract

This study presents a national and international overview of the controls related to the security of information used by the Institutions of Science and Technology (ICTs) in activities related to Intellectual Property. For this analysis, Institutions of national and international renown were selected. The methodology used is based on the ABNT NBR ISO / IEC 27001 and 27002 standards and allows mapping the main controls adopted by ICTs, in addition to indicating as Institutions that use the most complete and comprehensive Information Security Management System (ISMS). From this mapping, analysis or impact of the main controls in the institutional activities that involve Intellectual Property. It was concluded that the adoption of an ISMS is crucial for the development of activities related to Intellectual Property, such as protection of intangible assets and technology transfer. It can be seen that, comparing national and foreign ICTs, they present a more comprehensive Information Security Management System in relation to IP.

Keywords: Information Security. Intellectual Property.

Área Tecnológica: Propriedade Intelectual. Segurança da Informação.

Artigo recebido em: 11/02/2019
Revisado em: 18/02/2020
Aprovado em: 17/03/2020

1 Introdução

As organizações dependem fortemente de Sistemas de Informação (SI) eficientes e seguros. As violações de segurança, amplamente divulgadas por vários canais de comunicação, principalmente em *sites* e em revistas especializadas em segurança da informação, reforçam a necessidade de as instituições adotarem sistemas que reduzam os riscos de comprometimento dos seus bancos de dados (DHILLON; TORKZADEH, 2006). O investimento em sistemas para proteção de dados também se elevou devido ao aumento dos gastos e de alocação de recursos pelas empresas na implementação de estruturas e ferramentas para a governança de Tecnologia de Informação (TI) (BACHLECHNER; THALMANN; MANHART, 2014). No entanto, enquanto a informação, em si, é considerada um ativo organizacional que deve ser protegido e apesar de pesquisas empíricas mostrarem que o êxito na proteção do conhecimento aumenta significativamente o desempenho organizacional (LEE *et al*., 2007), observa-se, em alguns casos, que os responsáveis pelo controle e tramitação das informações não dedicam a devida importância às questões ligadas à segurança da informação em suas atividades institucionais (ASLLANI; LUTHANS, 2003). A segurança da informação depende de um conjunto de processos executados com políticas e regulamentos bem fundamentados. Nesse cenário, são definidos os níveis de proteção que devem ser implementados na segurança envolvendo a área jurídica, os recursos humanos, a administração e as demais áreas julgadas necessárias. Quanto maior o número de atores envolvidos, melhor e mais amplas serão as áreas protegidas, independentemente do tempo de formulação desses instrumentos (FONTES, 2008).

A rede de dados é uma das principais estruturas utilizadas para difusão da informação e possibilita a conexão entre todos os usuários. Nesse sentido, essas estruturas devem primar pela segurança da informação, principalmente no que tange à confiabilidade, à integridade e à disponibilidade dos sistemas estabelecidos (NAKAMURA, 2007).

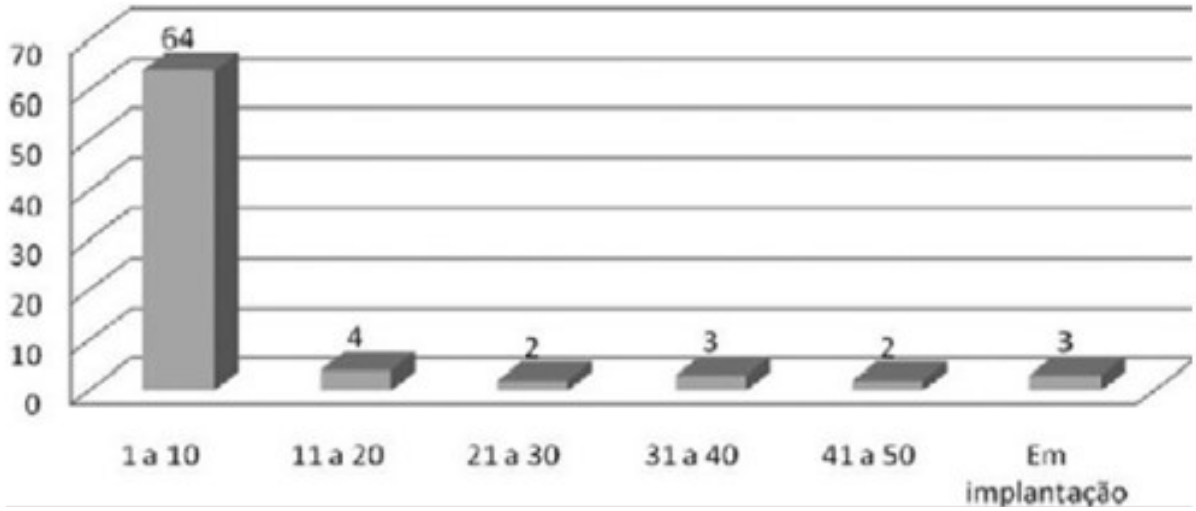
É importante salientar que a preocupação com a segurança da informação extrapola as fronteiras físicas, os tipos de instituições e as atividades desenvolvidas. O vazamento de dados também é conhecido por causar danos à reputação e pela perda de receita e de produtividade (AHMAD; BOSUA; SCHEEPERS, 2014). Portanto, encontrar um equilíbrio entre proteger e compartilhar informações é crucial para resolver o paradoxo da fronteira (NORMAN, 2002). Nesse contexto, a comunidade acadêmica não poderia estar de fora dessa questão, uma vez que lida com pesquisas importantes, que, muitas vezes, apresentam resultados sensíveis. Esse é um dos motivos pelos quais a preocupação com a gestão da segurança da informação envolve a comunidade acadêmica, visto que nesse ambiente são produzidas novas tecnologias, como produtos e processos, ou seja, um ambiente em que a inovação se faz presente (YILMAZ; YALMAN, 2016).

Em pesquisa recente realizada por Yilmaz e Yalman (2016) foi objeto de estudo a importância da segurança da informação dentro das universidades indianas. Entre as universidades pesquisadas por esses autores, verificou-se que aquelas universidades que utilizavam um sistema de gestão de segurança da informação, baseado na norma NBR ISO/IEC 27001, aplicando, principalmente, os procedimentos relativos à conscientização e ao treinamento de pessoal, apresentaram uma melhor gestão, em termos de controle e de segurança da informação (YILMAZ; YALMAN, 2016). As universidades que buscam a certificação na norma NBR ISO/IEC 27001 apresentam um maior índice de maturidade em relação à gestão de riscos e à própria

segurança da informação, sem, no entanto, afetar a usabilidade e a flexibilidade de sistemas informatizados (YILMAZ; YALMAN, 2016).

Segundo Torkomian (2009), a contratação e a capacitação de pessoal foram consideradas as principais deficiências e são apontadas como partes mais importantes por 77% dos Núcleos de Inovação Tecnológicos (NITs). Isso pode ser observado, uma vez que 82% apontaram não possuir mais de 10 pessoas trabalhando na sua estrutura, conforme mostra o Gráfico 1. Em segundo lugar, a falta de competências e de habilidades em transferência de tecnologia foi citada por 68%. Além disso, a ausência de uma cultura de proteção da Propriedade Intelectual foi citada como muito importante por 64% dos NITs, e os problemas relativos à sustentabilidade foram apontados por 58% como muito importantes (TORKOMIAN, 2009).

Gráfico 1 – Quantidade de pessoas por NIT



Fonte: Torkomian (2009)

Segundo Lyra (2016), durante o tempo compreendido entre o início desses processos de desenvolvimento de uma nova tecnologia e a proteção efetiva desse produto, a melhor maneira de proteger os investimentos alocados e a propriedade intelectual da empresa é utilizando a Segurança da Informação. Nesse contexto, e ainda segundo Lyra (2016), percebe-se que a segurança da informação é importante em diversos setores da indústria, especialmente quando se trata de informações tecnológicas, como é o caso de pesquisa e desenvolvimento. A própria Organização Mundial da Propriedade Intelectual (OMPI) possui uma Divisão de Segurança e Garantia da Informação (SIAD) que tem a responsabilidade de gerenciar todos os aspectos da segurança da informação e física da OMPI (WIPO, 2002).

Todos esses elementos mostram, portanto, a importância de serem implementadas ações que pretendam proteger o patrimônio informacional das instituições, a fim de garantir sua integridade e disponibilidade. No entanto, apesar da importância desse tema, não foram encontrados estudos que tratassem da segurança da informação no contexto da Propriedade Intelectual nas instituições de ensino nacionais.

A fim de atender a essa realidade, o Sistema de Gestão de Segurança da Informação e Comunicações (SGSI), mencionado na norma ABNT NBR ISO/IEC 27001: 2013 (Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação –

Requisitos) e na norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação), se reveste de grande importância estratégica, pois a adoção desse sistema nas organizações contribui para a preservação da confidencialidade, da integridade e da disponibilidade da informação (ABNT, 2013a). Essas normas auxiliam na preparação dos requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI (ABNT, 2013b).

O Departamento de Segurança da Informação e Comunicação (DSIC), órgão diretamente ligado ao Gabinete Institucional da Presidência da República, tem publicado atos normativos e orientações, relacionados com a segurança da informação, para serem seguidos pelos Órgãos da Administração Pública, incluindo as Instituições de Ciência e Tecnologia (ICT). Destaca-se entre os documentos publicados pelo DSIC a Norma Complementar n. 20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014. Essa norma estabelece as Diretrizes de Segurança da Informação e Comunicações para Implementação do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta (DSIC/GSIPR, 2014).

Os Núcleos de Inovação Tecnológica (NITs) estão inseridos nesse contexto, pois tratam de informações sensíveis, que requerem cuidados especiais, como restrição e classificação do nível de acesso da informação. Segundo dados do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), em 2016, existiam 208 NITs, implementadas em ICTs públicas e privadas (MCTIC, 2016). Além do grande número de informações tramitadas, a preocupação com o tratamento dado a essas informações dentro dos NITs é pertinente, em razão das suas atividades consistirem na condução de processos de proteção e de comercialização de tecnologias inovadoras, desenvolvidas nas ICTs.

Nesse contexto, no qual se observa a importância da adoção de medidas que visem a garantir a segurança da informação nas ICTs, em especial dentro dos NITs, o presente estudo tem como objetivo apresentar um panorama das políticas de segurança da informação, implementadas pelas Instituições de Ciência e Tecnologia, indicando a aderência dos pontos abordados por essas políticas na Propriedade Intelectual, e, consequentemente, o nível de sensibilização dessas Instituições em relação à segurança da informação e às estratégias escolhidas por elas e adotadas para tratar esse tema.

As universidades são alvos preferenciais de ataques cibernéticos que pretendem comprometer a integridade de informações relacionadas a pesquisas científicas nessas instituições (MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2018). Em agosto de 2014, a Cronologia de Violações de Dados da PRC (Privacy Privacy Clearing House) relatou 742 violações na educação desde 2005, envolvendo mais de 14 milhões de registros violados (MIT, 2014).

As Instituições de Ciência e Tecnologia têm a tendência de empregar protocolos de segurança de dados menos rigorosos, o que aumenta o potencial de perda e exposição acidental de dados. A amplitude e o volume de dados pessoais coletados pelas universidades, dados estes aliados à alta rotatividade de pessoal e a uma população tecnicamente pouco experiente em geral, tornam o problema da perda de dados em instituições quase uma situação epidêmica por natureza (MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2018).

Algumas informações consideradas confidenciais precisam de cuidados e de manuseios especiais. A manipulação inadequada dos dados pode trazer sérias consequências para o indivíduo e para a instituição, como: roubo de identidade, perda financeira, invasão de privacidade ou acesso não autorizado por um ou por vários indivíduos. Os dados também podem estar

sujeitos à regulamentação por leis estaduais ou federais e, nesses casos, há necessidade de que seja realizada a notificação no caso de uma divulgação (MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2018).

A divulgação indevida de informações confidenciais ou restritas pode prejudicar a imagem e a reputação da Instituição, causar perda financeira e constrangimento a alunos, professores e funcionários, além de incorrer em obrigações legais e custos financeiros relacionados à notificação dos indivíduos afetados pela divulgação (MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2018).

A Norma ABNT NBR ISO/IEC 27001 é um padrão que pode ser aplicado por todas as organizações sem considerar o tipo de indústria, instituição de ensino, empresa, tamanho ou número de funcionários. O objetivo principal da norma é fornecer segurança da informação e preservar os ativos de informação de um estabelecimento (ABNT, 2013a). A Norma ABNT NBR ISO/IEC 27002 fornece as diretrizes para práticas de gestão de segurança da informação para as organizações, incluindo aspectos de seleção, implementação e o gerenciamento de controles, levando em consideração os riscos da segurança da informação da organização. Eles fornecem às organizações os meios para gerenciar ameaças à segurança das informações, obter informações confiáveis e auxiliar na continuidade dos negócios (ABNT, 2013b).

Percebe-se que os sistemas institucionais de gerenciamento de segurança da informação são cruciais para a proteção das propriedades da informação; portanto, as ICTs que estão planejando ou não estão fazendo nenhum esforço para obter uma ISO/IEC 27001 diminuirão os riscos de segurança da informação aplicando os procedimentos da ISO/IEC 27001, caso tentem usar sistemas institucionais de gestão de segurança da informação.

A norma ISO 27001 é a única passível de certificação. A Norma ISO 27002:2013 possui um sistema de gestão de segurança da informação (Information Security Management System – ISMS) que é a parte do sistema de gestão global, baseado na abordagem de riscos de negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação (ABNT, 2013b).

2 Metodologia

A metodologia adotada no presente estudo tem o objetivo de identificar os controles de segurança da informação estabelecidos pelas Normas ABNT NBR ISO/IEC 27001 e 27002, que são utilizados nas ICTs e, também, de avaliá-los em relação à importância que eles apresentam dentro do domínio da Propriedade Intelectual. Para tanto, optou-se por selecionar três universidades estrangeiras e quatro nacionais, que aplicam a segurança da informação na propriedade intelectual, seja por meio de uma política ou de plataformas de gerenciamento de documentos. Por se tratar de um estudo inicial, optou-se por estudar instituições de ensino norte-americanas e sul-americanas. As instituições estrangeiras escolhidas foram a Universidade de Harvard, o Instituto de Tecnologia de Massachusetts (MIT) e a Universidade de Oxford; e as nacionais foram a Universidade Federal de Santa Catarina (UFSC), a Universidade Federal do Rio de Janeiro (UFRJ), a Universidade de Brasília (UnB) e a Universidade de Campinas (Unicamp).

A identificação dos controles de segurança da informação, adotados por essas ICTs, tendo como referencial o previsto na norma ABNT NBR ISO/IEC 27002 (ABNT, 2013b), foi realizada

a partir das Políticas de Segurança da Informação, publicadas por cada uma delas ou de documentação correlata referente ao SGSI da instituição, como: Política de Segurança de Dados da Universidade de Harvard (HARVARD UNIVERSITY, 2018); Política de Informação do MIT (MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 2018); Política de Segurança da Informação da Universidade de Oxford (UNIVERSITY OF OXFORD, 2016); Política de Segurança da Informação e Comunicações da USFC (UFSC, 2015), Política de Segurança da Informação e Comunicações para UFRJ (UFRJ, 2012) e Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação para a Unicamp (UNICAMP, 2012) e normas de segurança disponibilizadas no site da UnB e o próprio SEI da UnB (UnB, 2017).

No caso da Universidade de Brasília, que não apresentou nas pesquisas realizadas uma compilação das Políticas em Segurança da Informação e normas de segurança da informação, tal como disponibilizada pelas demais ICTs, foram adotadas, por analogia, as informações de segurança da informação disponibilizadas no *site* do Centro de Informática da Instituição e no Guia Prático do Serviço Eletrônico de Informações (SEI) da UnB.

O Serviço Eletrônico de Informações (SEI) trata-se de um sistema de tramitação de processos *on-line*, utilizado por várias Universidades e Órgãos Públicos da Administração Federal, Estadual e Distrital. Esse sistema possui incorporado, em si, alguns dos controles previstos nas Normas ABNT NBR ISO/IEC 27001 e 27002. Nessa etapa foi verificada a presença dos seguintes controles: controle de acessos, política de segurança, organização da segurança da informação, segurança em recursos humanos, segurança física e do ambiente, segurança nas comunicações, gestão de ativos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, criptografia, segurança nas operações, relacionamento na cadeia de suprimento, gestão da continuidade do negócio e conformidade.

A fase de avaliação da relevância dos controles identificados, no âmbito da Propriedade Intelectual, utilizou-se de uma análise comparativa das definições dos controles, fornecida pelas normas ABNT NBR ISO/IEC 27001 e 27002, com os conceitos de Propriedade Intelectual (GHESTI *et al*., 2016).

A partir da metodologia desenvolvida para o presente estudo, que consiste em um mapeamento dos controles de segurança da informação previstos na Norma ABNT NBR ISO/IEC 27002 (ABNT, 2013b) e utilizados pelo grupo de ICTs estudado, foi possível identificar quais as instituições que possuem um SGSI mais abrangente e quais são os controles mais recorrentes. Também foi analisada qual a contribuição dos controles mais recorrentes no contexto da Propriedade Intelectual. Em relação ao nível de abrangência dos SGSI, esse indicador foi obtido a partir da quantidade de controles adotados por cada uma das Instituições. A recorrência de cada controle foi mensurada a partir do número das Instituições que os incluíram em suas legislações internas de segurança da informação. A compilação dos controles por ICT é apresentada na Tabela 1.

Tabela 1 – Mapeamento de controles, previstos na Norma ISO 27002, por Instituições de Ciência e Tecnologia – ICTs

Controle/Domínio (Normas ISO 27002 e ISO 27001)	Instituições de Ciência e Tecnologia (ICTs)							Principais controles
	Harvard	**MIT**	**Oxford**	**UFSC**	**UFRJ**	**UnB**	**Unicamp**	
Controle de Acesso	1	1	1	1	1	1	1	7
Política de Segurança da Informação	1	1	1	1	1	-	1	6
Organização da Segurança da Informação	1	1	1	1	1	-	1	6
Segurança Física e do Ambiente	1	1	1	1	1	-	1	6
Segurança em Recursos Humanos	1	1	1	-	-	-	1	4
Segurança nas Comunicações	1	1	-	1	1	-	1	5
Gestão de Ativos	1	1	1	-	-	-	1	4
Conformidade	1	1	1	-	-	-	1	4
Gestão de incidentes de Segurança da Informação	1	1	1	-	-	-	-	3
Aquisição, Desenvolvimento e Manutenção de Sistemas	1	1	-	-	-	-	-	2
Criptografia	-	-	-	-	-	-	-	-
Segurança nas Operações	1	1	-	-	-	-	-	2
Relacionamento na Cadeia de Suprimento	-	-	-	-	-	-	-	-
Segurança da Informação na Gestão da Continuidade do Negócio	1	1	-	-	-	-	-	2
Abrangência da Política	**12**	**12**	**8**	**5**	**5**	**1**	**8**	**-**

Fonte: Elaborada pelos autores deste artigo (2018)

3 Resultados e Discussão

Inicialmente, pode-se observar que, entre as Instituições selecionadas, a Universidade de Harvard, o Instituto de Tecnologia de Massachusetts (MIT) e a Universidade de Campinas (Unicamp) foram as que apresentaram as pontuações mais elevadas para o indicador "Abrangência da Política", com a Universidade de Harvard e o MIT empatados com 12 pontos e a Unicamp e a Universidade de Oxford com 8 pontos. No entanto, observou-se que nenhuma das ICTs atingiu a pontuação máxima de 14 pontos, situação na qual todos os catorze controles estariam presentes no SGSI da ICT. Há casos em que alguns dos controles foram encontrados dentro da Política de Segurança da Informação da instituição. Nesses casos, em que um determinado

controle estaria sendo contemplado dentro de outro controle da Norma NBR ISO/IEC 27001, foi considerado como atendido a sua aderência à norma referenciada.

Em relação aos controles mais recorrentes, destacaram-se o controle de acesso, a política de segurança da informação, a organização da segurança da informação, a segurança física e do ambiente, segurança em recursos humanos e segurança nas comunicações. A partir desse resultado para os controles utilizados mais comumente pelas ICTs, foi realizada uma análise da influência desses principais controles na Propriedade Intelectual.

3.1 Controle de Acesso

Na Norma ABNT NBR ISO/IEC 27001 (ABNT, 2013a), o controle de acesso tem por objetivo limitar o acesso à informação e aos recursos de processamento da informação. Ela estabelece a necessidade de que seja implementada uma política de controle de acesso, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios (ABNT, 2013a). O controle de acesso é um dos domínios presentes na norma ISO 27001 que é utilizado por várias ICTs na formulação de sistemas de gestão de segurança da informação, relacionados com a Propriedade Intelectual.

O uso do controle de acesso é extremamente importante quando se trabalha com o ramo da Propriedade Industrial, principalmente em cenários nos quais o sigilo é fundamental, como no caso de o inventor ter protegido a sua tecnologia, por exemplo, por meio de pedido de patente ou registro de programa de computador, ou faz uso da modalidade de segredo industrial. Na Propriedade Industrial, o sigilo e, consequentemente, o maior controle de acesso às informações de patentes, programas de computador ou desenhos industriais devem ficar restritos ao período em que não houve divulgação oficial. Nesse contexto, faz-se necessária a restrição de acesso às informações referentes a essas tecnologias, por meio de normas e de controles eficientes que impeçam a divulgação não autorizada dessas informações.

As ICTs, por meio dos seus NITs, devem propiciar um ambiente favorável para que inventores e profissionais, envolvidos diretamente com o processo de proteção das tecnologias, conheçam as regras existentes relacionadas. Nesse sentido, as normas ISO 27001 e ISO 27002 podem ser de grande utilidade para as ICTs, orientando em relação aos processos de controle de acesso mais adequados a serem implementados em seus NITs.

3.2 Política de Segurança da Informação

As normas ABNT NBR ISO/IEC 27001 (ABNT, 2013a) e ABNT NBR ISO/IEC 27002 (ABNT, 2013b) estabelecem que o objetivo da Política de Segurança da Informação é prover orientação da Direção da Instituição e apoio para a segurança da informação, de acordo com os requisitos da atividade e com as leis e as regulamentações relevantes. As normas 27001 e 27002 estabelecem que o conjunto de políticas de segurança da informação seja definido, aprovado pela Direção, publicado e comunicado para todos os colaboradores internos e externos relevantes.

A utilização de políticas de segurança da informação é essencial para as atividades de PI desenvolvidas pelas ICTs, principalmente nos processos envolvendo a propriedade industrial, pois essas políticas irão orientar a direção para apoiar a segurança da informação. A existência de uma política de segurança da informação que atenda à demanda de proteção dos processos de

propriedade intelectual serve de orientação para que os profissionais envolvidos nesses processos saibam com clareza aquilo que é permitido e as ações que devem ser evitadas quando se trata das informações de PI. Dessa forma, como já foi dito, os ambientes de pesquisa envolvendo instituições de ensino se caracterizam pela proliferação de inovações e descobertas, todavia não se caracterizam por ser um ambiente muito seguro e principalmente as normas de segurança não são bem conhecidas pelos usuários. Para um inventor, assim como para os profissionais envolvidos nos processos de proteção de tecnologias, é muito importante que as políticas de segurança da informação englobem as ações desenvolvidas pelas ICTs e pelos NITs no intuito de propiciar maior segurança nas ações a serem desenvolvidas e definir as responsabilidades de cada um dos atores, além das penalidades, quando houver descumprimento das normas existentes. Para as empresas, sejam elas públicas ou privadas, que participam do processo de transferência de tecnologia ou financiam o desenvolvimento de tecnologias, a implementação de Políticas de Segurança da Informação eficientes é uma garantia de que as ICTs apresentam um sistema de governança institucional, que define as responsabilidades e os cuidados que devem ser tomados com os dados e as informações sigilosas ou de acesso restrito.

As informações, em qualquer formato, usadas ou produzidas como parte da atividade de pesquisa, podem incluir dados confidenciais ou propriedade intelectual que devem ser armazenados, processados e transferidos com segurança. A segurança das tecnologias digitais utilizadas para o planejamento, o compartilhamento e comunicação de material didático, a entrega de palestras e tutoriais e o apoio às atividades de aprendizagem é essencial para garantir que os funcionários tenham confiança nas tecnologias utilizadas.

Pode-se concluir, a respeito do domínio "Política de Segurança da Informação", que ele é importante dentro do contexto de segurança em relação à PI, não se restringindo somente as questões de propriedade industrial, mas avançando para as demais áreas da PI. Uma Política de Segurança da Informação específica para a PI ou que aborde essas questões é a garantia de que os envolvidos nesses processos saibam como tratar de forma segura determinadas informações e como agir em relação aos contratos e aos convênios estabelecidos com outros órgãos públicos ou privados.

3.3 Organização da Segurança da Informação

A organização da segurança da informação é um dos controles previstos nas normas ABNT NBR ISO/IEC 27001 (ABNT, 2013a) e 27002 (ABNT, 2013b) e tem por objetivo estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e a operação da segurança da informação dentro das Instituições. Para que esse controle cumpra o seu papel, essas normas orientam que sejam levados em consideração alguns aspectos, como responsabilidades e papéis pela segurança da informação, a segregação de funções, o contato com autoridades ou com grupos especiais (associações profissionais ou outros fóruns), a segurança no gerenciamento de projetos e as questões relacionadas com dispositivos móveis e com o trabalho remoto.

Dentro das ICTs, a presença desse controle contribui consideravelmente para a segurança das atividades desenvolvidas envolvendo a PI. Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas e que as pessoas que trabalham com PI, dentro das ICTs, mais especificamente, em seus NITs, estejam envolvidas, uma vez que o ativo informacional que é administrado por esses profissionais é extremamente valioso e necessita ser

controlado e fiscalizado. Além disso, é importante que os pesquisadores e os agentes de PI das ICTs saibam identificar como está organizada a segurança da informação, no intuito de buscar referências e de alinhar as suas atividades e estruturas internas com o sistema de segurança da informação.

Da análise desse controle, pode-se concluir que a sua adoção é muito importante para as ICTs, pois deixa claro aos usuários, aos pesquisadores e aos profissionais de PI quem são os responsáveis pela segurança da informação e quais são as penalidades advindas do descumprimento de normas de segurança envolvendo os processos de PI.

3.4 Segurança Física e do Ambiente

A segurança física e do ambiente tem o intuito de prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização, além de impedir perdas, danos, roubo ou comprometimento de ativos e interrupção das operações (Norma ISO 27001). A norma ISO 27001 estabelece que esse controle, quando aplicado, deve dar atenção às áreas consideradas seguras, principalmente aquelas relacionadas com as questões de perímetro de segurança física, controles de entrada física, segurança em escritórios, salas e instalações. Deve ser dada também atenção aos equipamentos, em relação à sua localização e proteção, ao seu cabeamento e manutenção, à sua reutilização ou descarte seguro aos equipamentos que não estejam sendo monitorados, que não possuem conexão física com rede local, e às questões de política de mesa limpa e tela limpa. É muito importante que haja uma preocupação constante do público interno das ICTs em relação à segurança física e do ambiente nos locais de trabalho. Na maioria das vezes, a utilização de alguns procedimentos simples de segurança pode evitar a exposição e o acesso indevido às informações tramitadas nesses ambientes.

Dentro das ICTs, as atividades de proteção de tecnologias são normalmente realizadas nos NITs. É importante que o acesso a esses locais seja controlado e fiscalizado, uma vez que os assuntos tratados nesses ambientes possuem certo grau de sigilo e a documentação tramitada, seja em mídia digital ou física, contém informações relevantes sobre os processos de proteção e transferência de tecnologia. A aplicação desse controle contribui para que os ambientes de inovação e de proteção de tecnologias sejam protegidos contra ações de divulgações não autorizadas de informações, além de propiciarem aos inventores e aos profissionais da área de PI uma maior segurança em relação ao ambiente de trabalho e aos equipamentos utilizados para suas atividades, principalmente os equipamentos de TI.

Conclui-se que esse controle, quando implementado, possibilita melhor segurança dos ambientes nos quais são processadas as informações de PI, principalmente os ambientes de NITs e escritórios de inovação em que são tratados assuntos de acesso restrito e cuja área precisa de controle.

3.5 Segurança em Recursos Humanos

A segurança em recursos humanos, conforme consta da norma ABNT NBR ISO 27002 (ABNT, 2013b), deve ser aplicada antes, durante e no encerramento e na mudança da contratação dos colaboradores. Esse controle tem por objetivo assegurar que colaboradores e partes

externas entendam as suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados. É importante que a organização faça verificações mais detalhadas, tanto na contratação como na promoção, em locais de trabalho envolvendo pessoal, que tenha acesso aos recursos de processamento da informação, em particular aqueles que tratam de informações financeiras ou informações altamente confidenciais. A segurança em recursos humanos deve se preocupar com a seleção dos profissionais, os termos e condições de contratação, a conscientização, a educação e o treinamento em segurança da informação, o processo disciplinar e as responsabilidades pelo encerramento ou mudança da contratação.

No estudo foi verificado que a segurança em recursos humanos deve estar presente e alinhada com as contratações, as operações e com o posterior desligamento dos profissionais que trabalham com PI dentro das ICTs. As informações tramitadas pelos pesquisadores e profissionais de PI são altamente valiosas, e a área de Segurança deve estar preocupada com os colaboradores que manipulam essas informações. Atualmente, muitos dos profissionais que trabalham nos NITs, encarregados dos processos de proteção de tecnologias e nas atividades de transferências de tecnologia, são prestadores de serviços temporários, o que ocasiona uma rotatividade muito grande, oferecendo vulnerabilidade aos sistemas de proteção. A implementação desse controle nas ICTs pode contribuir para a melhor seleção, acompanhamento e desligamento desses profissionais, uma vez que estaria com um viés mais voltado para questões relacionadas com seu histórico profissional, moral e ético e a sua atuação no desenvolvimento das atividades em relação à segurança das informações.

Conclui-se que a adoção desse controle, nos processos de PI, contribui diretamente para a melhoria da segurança da informação, já que a presença de profissionais preparados nessa área minimiza os riscos de segurança envolvendo os recursos humanos. Além disso, a necessária fiscalização da atividade desses profissionais no desenvolvimento de suas atividades, em relação às práticas de segurança em PI, colabora para o aumento do nível de segurança da informação nas ICTs.

3.6 Segurança nas Comunicações

A segurança nas comunicações tem como objetivo proporcionar a proteção das informações que trafegam em redes e dos recursos de processamento da informação que as apoiam, além de ser responsável por manter o sigilo da informação tramitada dentro da organização ou com as entidades externas (ABNT, 2013a). De acordo com a norma citada, na implementação desse controle deve haver atenção em relação aos elementos de controles, segurança dos serviços e segregação das redes, às políticas, procedimentos e acordos para a transferência de informações, bem como das mensagens eletrônicas e os acordos de confidencialidade e de não divulgação.

Atualmente, os ambientes de trabalho e de processamento de informações estão baseados e dependentes cada vez mais das estruturas de TI existentes. Nesse sentido, os ambientes das ICTs, principalmente os NITs, devem ser dotados de equipamentos de TI e precisam de procedimentos que assegurem o máximo de segurança nas comunicações estabelecidas, principalmente no que se refere aos dados trafegados na rede de dados e os relacionados aos acordos firmados entre as partes durante o processo de proteção das tecnologias e, também, durante os processos de transferência de tecnologia. Ressalta-se a importância de as redes de dados serem constantemente auditadas e aperfeiçoadas, a fim de manter um ambiente seguro.

Algumas organizações adotam a prática de utilizar redes segregadas da internet como forma de ampliar o escopo de segurança.

Pode-se concluir que, nesse aspecto, as ICTs que adotam esse controle diminuem os riscos de que seus meios de comunicações, como redes, sistemas e equipamentos de TI, nos quais trafegam dados de PI venham a ser explorados por pessoas não autorizadas.

3.7 Demais Controles das Normas ABNT ISO/IEC 27001 e 27002

As normas ABNT NBR ISO/IEC 27001 e 27002 estabelecem mais oito controles, que são: a) gestão de ativos, b) criptografia, c) segurança nas operações, d) aquisição, e) desenvolvimento e manutenção de sistemas, f) relacionamento na cadeia de suprimento, g) gestão de incidentes em segurança da informação; e h) conformidade. Esses controles são muito importantes e podem ser implementados com seus processos nas organizações para o estabelecimento de um SGSI. No entanto, na realização do estudo das normas ABNT NBR ISO/IEC 27001 e 27002 e na aplicação desses controles nos processos envolvendo PI, verificou-se que eles tinham pouca aderência e eram raramente utilizados pelas ICTs pesquisadas nas atividades de proteção e segurança envolvendo PI.

4 Considerações Finais

O presente estudo permitiu verificar que a adoção de um SGSI é crucial para o desenvolvimento de atividades relacionadas à Propriedade Intelectual, como a proteção de ativos intangíveis e a transferência de tecnologias. A adoção de um SGSI pelas ICTs não se restringe a proporcionar uma maior segurança às atividades de PI, mas também influencia na percepção da credibilidade e do respeito que os parceiros e a sociedade possuem dessas Instituições. O estudo demonstrou que a família de normas ISO 27000, em especial as normas ISO 27001 e ISO 27002, por se tratarem de normas reconhecidas pela sua eficiência e capilaridade, no que se refere à implantação de um SGSI, apresentam controles que podem ser aplicados em ICTs, a fim de proporcionar a implantação de SGSIs eficientes, que atendam às demandas de segurança das Instituições.

Da análise dos resultados, pode-se afirmar que as ICTs estrangeiras pesquisadas apresentam Políticas de Segurança da Informação mais abrangentes, em relação às atividades que envolvem PI. Isso ficou evidenciado pela quantidade de controles, associados à família de norma ISO 27000, que são aplicados por essas Instituições. Outro ponto que se destacou foi que as políticas de gestão de PI nessas Instituições fazem parte de um Planejamento ou de Políticas de Informação, que também incluíram a Segurança da Informação.

Nesse contexto, verificou-se a estreita relação entre os processos de PI e o SGSI, implantados nessas Instituições. Destacam-se a estrutura e a gama de informações disponibilizadas pelas universidades de Harvard e MIT e, também, o nível de detalhamento de informações relacionadas com segurança da informação envolvendo PI, disponibilizado em seus *sites*. Tais informações têm como propósito proteger usuários, pesquisadores, empresas e as próprias Instituições de possíveis danos à sua imagem e às suas atividades em PI.

O processo de classificação das informações, por nível e cores, implementados em Harvard e MIT pode servir de modelo para as ICTs nacionais. Esse tipo de classificação, além de ser simples e objetivo, facilita a identificação da informação dentro das categorias existentes e contribui para uma melhor gestão, segurança e controle das informações tramitadas nas ICTs e nos NITs. Além disso, faz o enquadramento da PI dentro do contexto da segurança da informação nas ICTs.

Em relação às ICTs nacionais, observou-se a existência de políticas, normas e orientações voltadas para a segurança dos processos de PI menos abrangentes, em comparação às Instituições estrangeiras, sendo a Unicamp a ICT nacional na qual se constatou um normativo mais completo, relacionado com a adoção de um SGSI. No entanto, além de questões relacionadas com direito de propriedade de *software*, não foi possível verificar algo específico relacionado com a segurança dos processos de PI. As normas internas da Unicamp encontram-se muito direcionadas para as questões de TI.

A UnB não apresenta normativos específicos para a segurança da informação de assuntos relacionados à Propriedade Intelectual. Apesar disso, a ferramenta SEI, utilizada no gerenciamento eletrônico de processos, associada às informações disponibilizadas no *site* da instituição, que poderiam permitir a implementação de um SGSI amplo e eficiente dentro da Instituição, não atende, atualmente, a todos os requisitos de um SGSI relacionados à PI. A plataforma SEI atende a alguns dos requisitos necessários a um SGSI, em especial, o controle de acesso.

Observou-se claramente, em relação às ICTs nacionais, que suas normativas para segurança da informação são direcionadas para as atividades de Tecnologia da Informação, não abordando de forma mais objetiva e abrangente as questões referentes à segurança de informações para PI. Nesse contexto, como perspectivas para futuros trabalhos, tem-se a realização de estudos de casos das atividades realizadas dentro dos NITs, tendo como objetivo a proposição de normas e/ou diretrizes relacionadas à segurança da informação a serem empregadas dentro dos NITs.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos:** ABNT NBR ISO/IEC 27001:2013. 2. ed. Rio de Janeiro: ABNT, 2013a.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação:** ABNT NBR ISO/IEC 27002:2013. 2. ed. Rio de Janeiro: ABNT, 2013b.

AHMAD, A.; BOSUA, R.; SCHEEPERS, R. Protecting organizational competitive advantage: a knowledge leakage perspective. **Computers & Security**, [*S.l.*], v. 42, p. 27-39, maio 2014. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404814000054. Acesso em: 13 out. 2018.

ASLLANI, A.; LUTHANS, F. What knowledge managers really do: an empirical and comparative analysis. **Journal of Knowledge Management**, [*S.l.*], v. 7, n. 3, p. 53-66, agosto, 2003. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/13673270310485622/full/html?journalCode=jkm. Acesso em: 12 out. 2018.

BACHLECHNER, D.; THALMANN, S.; MANHART, M. Auditing service providers: supporting auditors in cross-organizational settings. **Managerial Auditing Journal**, [*S.l.*], v. 29, n. 4, p. 286-303, abril, 2014. Disponível em: https://www.researchgate.net/publication/263764469_Auditing_service_providers_Supporting_auditors_in_cross-organizational_settings. Acesso em: 12 out. 2018.

DHILLON, G.; TORKZADEH, G. Value-focused assessment of information system security in organizations. **Information Systems Journal**, [*S.l.*], v. 16, n. 3, p. 293-314, maio, 2006. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2575.2006.00219.x. Acesso em: 15 out. 2018.

DSIC/GSIPR. **Norma Complementar n. 20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014.** Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal. Brasília, dezembro 2014. Disponível em: http://dsic.planalto.gov.br. Acesso em: 10 out. 2018.

GHESTI, G. F. *et al*. **Conhecimentos Básicos sobre Propriedade Intelectual**. Centro de Apoio ao Desenvolvimento Tecnológico, CDT/UnB, 2016. Disponível em: http://www.cdt.unb.br/pdf/programaseprojetos/nupitec/PROPRIEDADE%20INTELECTUAL.compressed.pdf. Acesso em: 10 set. 2018.

HARVARD UNIVERSITY. **Research Data Security & Management**. [2018]. Disponível em: https://vpr.harvard.edu/pages/research-data-security-and-management. Acesso: em 10 out. 2018.

LEE, S. C. *et al*. The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance. **Knowledge and Process Management**, [*S.l.*], v. 14, n. 1, p. 58-69, janeiro, 2007. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/kpm.270. Acesso em: 12 set. 2018.

LYRA, M. R. Segurança do Patrimônio Intangível. *In*: FOINA, P. R (org.). **Planejamento Estratégico para Empresas de Base Tecnológica**. 1. ed. Brasília: Instituto CEUB de Pesquisa e Desenvolvimento, 2016. p. 43-49.

MCTI – MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Secretaria de Desenvolvimento Tecnológico e Inovação. **Política de Propriedade Intelectual das Instituições Científicas, Tecnológicas e de Inovação do Brasil:** relatório FORMICT 2016. Brasília, DF: MCTI, 2016. 56p. Disponível em: https://www.mctic.gov.br/mctic/export/sites/institucional/tecnologia/propriedade_intelectual/arquivos/Relatorio-Formict-Ano-Base-2016.pdf. Acesso em: 10 nov. 2018.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **MIT Policies**. 13.0 Information Policies. Massachusetts: Cambridge, [2018]. Disponível em: https://policies.mit.edu/policies-procedures/130-information-policies. Acesso em: 17 out. 2018.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Information Protect @ MIT**. Massachusetts: Cambridge, [2018]. Disponível em: https://infoprotect.mit.edu/. Acesso em: 17 out. 2018.

NAKAMURA, E. T. **Segurança de Redes em Ambientes Cooperativos**. 1. ed. São Paulo: Novatec Editora, 2007.

NORMAN, P. M. Protecting knowledge in strategic alliances: resource and relational characteristics. **The Journal of High Technology Management Research**, [*S.l.*], v. 13, n. 2, p. 177-202, outubro, 2002. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1047831002000500. Acesso em: 15 out. 2018.

TORKOMIAN, A. L. V. Panorama dos Núcleos de Inovação Tecnológica no Brasil. *In*: SANTOS, M. E. R. *et al*. (org.). T**ransferência de Tecnologia:** estratégias para estruturação e gestão de Núcleos de Inovação Tecnológica. Campinas, SP: Komedi, 2009. p. 21-37.

UnB – UNIVERSIDADE DE BRASÍLIA. **Guia Prático do SEI na UnB – Sistema Eletrônico de Informações – Usuário Básico UnB**. Versão 3.0 Brasília, 2017. Disponível em: http://www.portalsei.unb.br/images/documentos_sei/Guia_v3_0_Atualizado_10_7_17.pdf. Acesso em: 10 dez. 2018.

UNICAMPI – UMIVERSIDADE ESTADUAL DE CAMPINAS. **Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação na Universidade Estadual de Campinas:** Resolução GR-052/2012. Campinas-SP 21 de dezembro de 2012. Disponível em: https://www.pg.unicamp.br/mostra_norma.php?id_norma=3256. Acesso em: 10 nov. 2018.

UFRJ – UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Portaria n. 4.579, de 15 de junho de 2012:** Política de Segurança da Informação da UFRJ. Rio de Janeiro, junho de 2012. Disponível em: https://www.security.ufrj.br/wp-content/uploads/2013/09/Portaria_4579_Pol%C3%ADtica_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_da_UFRJ.pdf. Acesso em: 12 nov. 2018.

UFSC – UNIVERSIDADE FEDERAL DE SANTA CATARINA. **Portaria n. 1754/2015/GR, de 9 de outubro de 2015:** Política de Segurança da Informação e Comunicações da UFSC. Santa Catarina, outubro de 2015. Disponível em: http://cotic.paginas.ufsc.br/files/2014/04/UFSC-POSIC-Politica-de-Seguran%C3%A7a-da-Informa%C3%A7%C3%A3o-e-Comunica%C3%A7%C3%B5es-v1.0.pdf. Acesso em: 12 nov. 2018.

UNIVERSITY OF OXFORD. University of Oxford Gazette. **Supplement**, Oxford, v. 1, n. 5.140, 20 July 2016. Disponível em: https://www.ox.ac.uk/media/global/wwwoxacuk/localsites/gazette/documents/supplements2015-16/Information_Security_-_%281%29_to_No_5140.pdf. Acesso em: 29 out. 2018.

WIPO – WORLD INTELLECTUAL PROPERTY ORGANIZATION. **Standing Committee on Information Technologies**. Geneva, April, 2002. Disponível em: http://www.wipo.int/edocs/mdocs/scit/en/scit_7/scit_7_12.pdf. Acesso em: 10 out. 2018.

YILMAZ, R.; YALMAN, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. **TEM Journal**, [*S.l.*], v. 5, n. 2, Iss 2, p 180-191, 2016 2016. Disponível em: https://pdfs.semanticscholar.org/ce5e/947228017401ca18a9e7070ec0cfafc581fc.pdf. Acesso em: 19 set. 2018.

Sobre os Autores

Paulo Cesar Andrade Arruda

E-mail: pcandrad3@gmail.com
Mestrado em Propriedade Intelectual e Transferência de Tecnologia para Inovação. Grande Área: Ciências Sociais Aplicadas/Área: Administração pela Universidade de Brasília em 2019.
Endereço profissional: Gabinete de Segurança Institucional da Presidência da República, GSI/PR, Praça dos Três Poderes, s/n, Palácio do Planalto, Plano Piloto, Brasília, DF. CEP: 70150-900.

Marcio Lima da Silva

E-mail: dasilva.marciolima@gmail.com
Doutor em Mecânica dos Fluidos, Processos e Energia. Grande Área: Engenharias/Área: Engenharia Mecânica pela Université de Grenoble, Grenoble-Univ, França em 2014.
Endereço profissional: Centro de Apoio ao Desenvolvimento Tecnológico, Universidade de Brasília, Campus Darcy Ribeiro, Asa Norte, Brasília, DF. CEP: 70904-970.

Edilson da Silva Pedro

E-mail: edipedro@gmail.com
Doutorado em Política Científica e Tecnológica. Grande Área: Ciências Sociais Aplicadas/Área: Administração pela Universidade Estadual de Campinas em 2008.
Endereço profissional: Ministério da Ciência Tecnologia Inovação e Comunicação, Bloco E, sala T 98, Esplanada dos Ministérios, Brasília, DF. CEP: 70067-900.