PROFNIT
Programa de Pós Graduação em Propriedade Intelectual
Transferência de Tecnologia para a Inovação

UnB

PAULO CESAR ANDRADE ARRUDA

UM PANORAMA DA ABORDAGEM DA SEGURANÇA DA INFORMAÇÃO NA PROPRIEDADE INTELECTUAL PELAS INSTITUIÇÕES DE CIÊNCIA E TECNOLOGIA

DEFESA DE MESTRADO

BRASÍLIA - DF
2019

PROFNIT
Programa de Pós Graduação em Propriedade Intelectual
Transferência de Tecnologia para a Inovação

PAULO CESAR ANDRADE ARRUDA

UM PANORAMA DA ABORDAGEM DA SEGURANÇA DA INFORMAÇÃO NA PROPRIEDADE INTELECTUAL PELAS INSTITUIÇÕES DE CIÊNCIA E TECNOLOGIA

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação, do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação (PROFNIT) – ponto focal Universidade de Brasília.

Orientador: Prof. Dr. Marcio Lima da Silva

Co-orientador: Prof. Dr. Edilson da Silva Pedro

BRASÍLIA - DF
2019

“Insanidade é continuar fazendo sempre a
mesma coisa e esperar resultados diferentes.”
(Albert Einstein)

DEDICATÓRIA

A Aline minha companheira de todas as horas e Isabel e Paulo Henrique, filhos amados, que me inspiram e me motivam.

AGRADECIMENTOS

Ao meu bom Deus, por ter me dado força, saúde e sabedoria para cumprir esta tarefa.

A minha esposa e filhos, pela paciência, compreensão e apoio nas horas em que necessitei de tempo para dedicar-me ao estudo.

A minha irmã que sempre me incentivou.

Ao meu orientador, Prof. Marcio Lima da Silva, meus sinceros agradecimentos pelo incentivo e dedicação durante todo este processo de pesquisa e troca de conhecimentos, sem o qual não teria concluído este trabalho.

A todos os professores do PROFNIT UnB pela dedicação, empenho e paciência com os alunos da primeira turma.

Aos meus companheiros de farda da seção de tecnologia da informação pela contribuição com importantes informações e sugestões.

Meu agradecimento pela ajuda que cada um prestou na construção deste trabalho.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CCUEC	Centro de Computação da Universidade Estadual de Campinas
CIO	*Chief Information Officer*
ConTIC	Conselho de Tecnologia da Informação e Comunicação
CTA	Centro de Telemática de Área
DSIC	Departamento de Segurança da Informação e Comunicações
GSIPR	Gabinete de Segurança Institucional da Presidência da República
ICT	Instituição de Ciência e Tecnologia
IG	Instrução Geral
MIT	Instituto de Tecnologia de Massachusetts
IN	Instrução Normativa
INPI	Instituto Nacional de Propriedade Industrial
IR	Instrução Reguladora
IEC	Comissão Eletrotécnica Internacional
ISO	Organização Internacional para Padronização
NIT	Núcleo de Inovação Tecnológica
NUPITEC	Núcleo de Propriedade Intelectual
OMPI	Organização Mundial de Propriedade Intelectual
PI	Propriedade Intelectual
SGSI	Sistema de Gestão de Segurança da Informação
SIAFI	Sistema Integrado de Administração Financeira do Governo Federal
SIC	Segurança da Informação e Comunicações
SPED	Sistema de Protocolo Eletrônico de Documentos
SISCOFIS	Sistema de Controle Físico
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
Unicamp	Universidade de Campinas
UFRJ	Universidade Federal do Rio de Janeiro
UFSC	Universidade Federal de Santa Catarina
UnB	Universidade de Brasília

RESUMO

O presente estudo apresenta um panorama nacional e internacional dos controles relacionados à segurança da informação, utilizados pelas Instituições de Ciência e Tecnologia (ICT) em suas atividades relacionadas à Propriedade Intelectual. Para esta análise foram selecionadas Instituições de renome internacional, divididas em três estrangeiras (Harvard, MIT e Oxford) e quatro nacionais (UFSC, UFRJ, UnB e Unicamp). A metodologia utilizada usou como referencial as recomendações das normas ABNT NBR ISO/IEC 27001 e 27002, e permitiu mapear os principais controles adotados pelas ICT, 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, tais como a proteção de ativos intangíveis e a transferência de tecnologias. Observou-se que, comparando-se as ICT nacionais com as estrangeiras, estas apresentam um Sistema de Gestão de Segurança da Informação mais abrangente, em relação à PI. Destacou-se ainda, que as normas e as diretrizes das ICT nacionais, para segurança da informação, são direcionadas para TI, não abordando aspectos importantes para PI. Neste sentido, foi apresentado uma proposta de *check-list* de protocolo de segurança da informação para ser implementado nas ICT.

Palavras-chave: segurança da informação. propriedade intelectual.

ABSTRACT

The present study presents a national and international panorama of the information security controls used by Science and Technology Institutions (STI) in their activities related to Intellectual Property. For this analysis, internationally renowned institutions were selected, divided into three foreign universities (Harvard, MIT and Oxford) and four Brazilian universities (UFSC, UFRJ, UnB and Unicamp). The methodology used used as a reference the recommendations of ABNT NBR ISO / IEC 27001 and 27002, and allowed mapping the main controls adopted by the ICTs, besides indicating the Institutions that have a more complete and comprehensive Information Security Management System (ISMS). From this mapping, the impact of the main controls on the institutional activities involving Intellectual Property was analyzed. It was concluded that the adoption of an ISMS is crucial for the development of activities related to Intellectual Property, such as the protection of intangible assets and the transfer of technologies. It was observed that, comparing national and foreign ICT, they present a more comprehensive Information Security Management System in relation to IP. It was also pointed out that the norms and guidelines of national ICT for information security are directed to IT, not addressing important aspects of IP. It was also pointed out that the norms and guidelines of national ICT for information security are directed to IT, not addressing important aspects of IP. In this sense, a proposal was proposed to check-list the information security protocol to be implemented in the ICT.

Keywords: information security. intellectual property.

SUMÁRIO

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 revistas especializadas em segurança da informação, reforçaram a necessidade das instituições em adotarem sistemas que reduzam os riscos de comprometimento dos seus bancos de dados (DHILLON e TORKZADEH, 2006). O investimento em sistemas para proteção de dados também aumentou, 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 et al., 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 e LUTHANS, 2003).

A segurança da informação depende de um conjunto de processos bem executados com políticas e regulamentos bem fundamentados. Neste cenário são definidos os níveis de proteção que devem ser implementados na segurança envolvendo a área jurídica, os recursos humanos, a administração, bem como, 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 utilizada para difusão da informação e possibilita a conexão entre todos os usuários. Neste sentido, essas estruturas devem primar pela segurança da informação, principalmente no que tange a confiabilidade, integridade e 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, pela perda de receita e produtividade (AHMAD et al., 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 desta questão, uma vez que ela 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 como um todo, visto que neste ambiente são produzidas novas tecnologias, tais como produtos e processos, ou seja, um ambiente onde a inovação faz-se presente (YILMAZ e YALMAN, 2016).

Em pesquisa recente realizada por YILMAZ e YALMAN, em 2016, nas universidades da Índia foi objeto de estudo a importância dada à segurança da informação dentro dessas instituições de ensino. Dentre as universidades pesquisadas por YILMAZ e YALMAN, verificou-se que aquelas universidades que utilizavam de 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 segurança da informação (YILMAZ e 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 e YALMAN, 2016).

Segundo Lyra (2016), durante o tempo 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 por meio da 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 tratam-se de informações tecnológicas, como é o caso de pesquisa e desenvolvimento. A própria Organização Mundial de 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 visem proteger o patrimônio informacional das instituições, a fim de garantir sua integridade e disponibilidade.

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 do mesmo nas organizações contribui para a preservação da confidencialidade, integridade e 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 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 nº 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 neste contexto, pois tratam de informações sensíveis, que requerem cuidados especiais, tais 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, implementados 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, onde se observa a importância da adoção de medidas que visem 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 estas políticas, na Propriedade Intelectual, e, consequentemente, o nível de sensibilização destas Instituições em relação à segurança da informação e as estratégias escolhidas por elas adotadas para tratar esse tema.

De acordo com o parágrafo 2º inciso VI, artigo 17 do decreto nº 9.283 de 07 de fevereiro 18 de 2018, a ICT pública deverá publicar em seu sítio eletrônico as informações encaminhadas ao MCTIC, sob a forma de base de dados abertos, ressalvadas as informações sigilosas. No entanto, esse mesmo decreto, estabelece em seu artigo 68, que as informações sobre projetos de pesquisa e desenvolvimento poderão ser classificadas como sigilosas e ter a sua divulgação restringida quando imprescindível à segurança da sociedade ou do Estado (BRASIL, 2018). Neste sentido, ficam resguardadas as condições de manutenção de sigilo e segurança das informações de pesquisa que são tramitadas nos NITs e ICTs e que necessitem da devida proteção do seu conteúdo.

O artigo 8º da Instrução Normativa nº 24, de 29 de julho de 2013, do Instituto Nacional de Propriedade Industrial (INPI) estabelece que toda informação criada, adquirida ou custodiada pelo usuário interno, no exercício de suas atividades no INPI, é considerada um bem e propriedade do Instituto e deve ser protegida, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor (INPI, 2013)

As universidades são alvos preferenciais de ataques cibernéticos, que visam comprometer a integridade de informações relacionadas a pesquisas científicas nessas instituições (MIT, 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, 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 epidêmicas por natureza (MIT, 2018).

Algumas informações consideradas confidenciais necessitam de cuidados e manuseios especiais. A manipulação inadequada dos dados pode trazer sérias consequências para o indivíduo e para a instituição, como: penalidades, roubo de identidade, perda financeira, invasão de privacidade ou acesso não autorizado por um ou por vários indivíduos. Os dados também podem estar sujeitos a regulamentação por leis estaduais ou federais e, nesses casos há necessidade que seja realizada a notificação no caso de uma divulgação (MIT, 2018).

A divulgação indevida de informações confidenciais ou restritas pode prejudicar a imagem e a reputação da Instituição, causar perda de recurso e constrangimento a alunos, professores e funcionários, além de incorrer em obrigações legais e custos financeiros relacionados à notificação dos indivíduos afetados pela divulgação (MIT, 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 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, 2013).

Atualmente, diversas ICTs nacionais e estrangeiras utilizam-se de uma política de segurança da informação para proteger seus dados e informações sensíveis, principalmente, aqueles relacionados à Pesquisa e à Propriedade Intelectual. No trabalho publicado em 2016, por YILMAZ, foi realizada uma análise comparativa dos sistemas de informação em uso nas universidades da Turquia e os riscos associados à segurança da informação. Neste estudo observou-se que os sistemas institucionais de gerenciamento de segurança da informação são cruciais para a proteção das propriedades da informação; e que as universidades que planejaram ou conduziram esforços para obter uma certificação ISO/IEC 27001 diminuíram os riscos de segurança da informação, aplicando os procedimentos da ISO/IEC 27001 (YILMAZ e YALMAN, 2016).

2 OBJETIVOS

2.1 OBJETIVO GERAL

- O objetivo geral do presente trabalho foi apresentar um panorama nacional e internacional dos controles relacionados à segurança da informação, utilizados pelas Instituições de Ciência e Tecnologia em suas atividades relacionadas à Propriedade Intelectual.

2.2 OBJETIVOS ESPECÍFICOS

A fim de atender o objetivo geral, o presente estudo tem os seguintes objetivos específicos:

- Verificar a existência de um SGSI, que atende às demandas de segurança da informação em todas as fases do processo de proteção de uma tecnologia;

- Verificar a aderência dos domínios de segurança da informação das normas ABNT NBR ISO/IEC 27001 e 27002, no contexto das ICTs de renome internacional, selecionadas para o presente estudo;

- Comparar as ICTs selecionadas, em relação à utilização dos principais domínios da norma ISO 27001;

- Apresentar um panorama comparativo, em relação à segurança da informação, nas ICTs selecionadas, a fim de servir de subsídios para melhorias no sistema de gestão de segurança da informação dessas instituições;

- Propor um *check-list* de protocolos de controles de segurança da informação a serem adotados pelas ICTs e NITs nas atividades relacionadas à Propriedade Intelectual no âmbito da Instituição (Anexo C).

2.3 JUSTIFICATIVA

Os NITs possuem um papel relevante e estratégico para as atividades de proteção das tecnologias que são desenvolvidas dentro das ICT.Sendo os seus colaboradores responsáveis por cuidar da gestão de todo o processo de proteção e transferência de tecnologias inovadoras com potencial de inserção na indústria e no comércio. Essas informações são importantes e muitas devem ser mantidas em sigilo em função das questões de propriedade intelectual das tecnologias. Nesse sentido faz-se necessário que os dados e informações, que são tramitadas dentro dos NITs, sejam protegidos por um eficiente sistema de gestão de tecnologia da informação. Esse sistema deve colaborar para que a credibilidade e eficiência dos NITs sejam asseguradas em todas as fases do processo de proteção e transferência de tecnologia.

A implementação de um SGSI nas ICTs busca aperfeiçoar as questões de controle de acesso, segurança física e ambiental, conformidade, gestão de ativos e segurança de recursos humanos nos NITs.

Diante do explicitado, o presente estudo justifica-se pela importância da implementação de um SGSI nas ICTs para o estabelecimento de um correto gerenciamento, fiscalização e controle das informações.

O levantamento dos problemas existentes, concomitante com a apresentação de propostas mais adequadas a gestão de segurança da informação e comunicações, pode auxiliar para um melhor desempenho dos NITs e também sua adequação a legislação vigente, relacionada com a segurança da informação. Além disso, pode contribuir para uma significativa melhoria do SGSI dos NITs e, consequentemente, fortalecer a credibilidade dos trabalhos desenvolvidos.

3 REVISÃO DA LITERATURA

3.1 INFORMAÇÃO

Conhecimento é um termo multifacetado cuja definição varia de disciplina para disciplina e até mesmo entre domínios individuais (MAIER, 2007). As ciências computacionais distinguem entre dados, informação e conhecimento (ALAVI e

LEIDNER, 2001), com dados considerados consistindo de elementos brutos e não analisados como símbolos e que necessitam de entrada em um processo de interpretação, enquanto informação está relacionada ao significado e resulta da agregação de dados (TRKMAN e DE SOUZA, 2012).

Informação não é um conceito, cuja definição agregue uniformidade pesquisadores, estudantes e demais profissionais. No entanto, duas perspectivas da informação se apresentam igualmente importantes para o praticante da área (FERNANDES, 2011).

A primeira é concernente à informação como estrutura, Bastos (2008) sinaliza que, para as áreas da comunicação e da biblioteconomia, a informação seria “uma cadeia de símbolos que possui significado”, ou, de outra forma, “o registro de um conhecimento que pode ser necessário a uma decisão”. Neste caso a informação fica associada a uma decisão ou significado.

Numa segunda perspectiva vemos a informação como resultado de uma transformação. A natureza transformadora da informação fica clara na definição de Shannon, que indica a informação como “aquilo que reduz a incerteza”, bem como em Baterson (apud ROBREDO, 2005), que indica que informação é “aquilo que nos muda”. É ainda digno de nota o emprego original do termo informação, do latim *informatio*, conforme indica Robredo (2005): “o ato de dar ou mudar a forma de uma peça particular de matéria”.

Desse modo, a informação somente é criada quando há indivíduos com capacidade de interpretar e decidir, o que envolve atualização do modelo mental do agente. Isso gera uma dinâmica transformadora que pode ser posteriormente codificada e registrada, criando nova informação em estado de estrutura (FERNANDES, 2011).

Segundo Veneziano (2011), a informação (*informare* = dar forma) é um conjunto de dados organizados de tal forma que faz sentido ou possui utilidade para alguém. É imprescindível que uma informação sempre seja precisa, completa, econômica, flexível, confiável, relevante, simples, pontual, verificável, acessível e segura.

Para Foina (2013), a informação pode ser definida como um dado (valor) associado a um conceito claro, não ambíguo e de conhecimento de todos os

interessados, que seja acompanhado de uma referência para efeito de comparação e possa trazer vantagens competitivas para a organização. Normalmente, a conceituação e as referências não acompanham o dado correspondente, mas deve-se garantir que todos os interessados naquela informação tenham os mesmos conceitos e referências sobre ela. Dados que não tenham utilidade, para uma pessoa ou para uma organização, não são considerados uma informação e podem ser descartados.

Uma informação usada para realizar intervenções na realidade de forma produtiva e vantajosa é uma informação útil para garantir o sucesso da organização e oferecer diferenciais competitivos importantes. Para que a informação possa ter esse papel, é importante que a própria organização esteja preparada e estruturada para captar e aproveitar essas características da informação (URDANETA, 1992).

De acordo com o inciso I, artigo 3º da lei 12.527 de 18 de novembro de 2011, informação são “dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”.

As teorias do conhecimento também diferenciam conhecimento tácito de explícito (NONAKA, 1994). O conhecimento tácito é altamente pessoal e enraizado em ações; consiste em modelos mentais, crenças e perspectivas individuais que dificultam a articulação da pessoa. Isso contrasta com o conhecimento explícito, como um documento, por exemplo, que, por ser formalizado e sistemático, pode ser facilmente comunicado e compartilhado dentro das comunidades (OLANDER et al., 2011). É esse conhecimento explícito que converge a informação e que precisa ser protegida e cuidada que iremos abordar ao longo deste trabalho.

3.2 SEGURANÇA DA INFORMAÇÃO

Na vasta literatura que trata de SIC existem várias definições sobre segurança da informação. No entanto, de acordo com a norma ABNT NBR ISO/IEC 17799 (ABNT, 2005, p.ix) a Segurança da Informação envolve a proteção contra um grande número de ameaças às informações. Neste sentido, busca assegurar a continuidade do negócio, agindo sobre os danos comerciais e privilegiando o retorno de investimentos.

A segurança da informação é alcançada através da implementação de um conjunto eficiente de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais, além de funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, a fim de assegurar que os objetivos específicos de segurança e do negócio da organização sejam alcançados. É muito importante que essa ação seja realizada em conjunto com outros processos de gerenciamento de negócio (SMULDERS e BAARS, 2018)

Ainda conforme a norma ABNT NBR ISO/IEC 17799 (ABNT, 2005, p.ix), “a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade”.

Dentro deste contexto enquadra-se o controle de acesso que busca impor barreiras de proteção nas organizações. Estas barreiras podem ser de natureza física ou lógica e visam proteger os ativos organizacionais de acessos indevidos, bem como permitir o acesso de usuários autorizados. Conforme está explicitado no DSIC/GSIPR (2010, p.3), controle de acessos é “o conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear acesso”. Ainda tomando por base o DSIC/GSIPR (2010, p.2), o objetivo do controle de acessos é “sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações”.

O controle de acesso é parte importante dentro do contexto da segurança da informação e comunicações e está relacionado e depende, prioritariamente, da cultura de segurança observada pelas pessoas.

A norma ABNT NBR ISO/IEC 17799:2005 que posteriormente foi modificada pela norma ABNT NBR ISO/IEC 27002:2013 agrega as orientações e informações mais importantes referentes ao controle de acesso e ao controle de segurança física e ambiental. A Norma ABNT NBR ISO/IEC 27002:2013 cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações, das áreas físicas e do ambiente de uma empresa/instituição. A Norma ABNT NBR ISO/IEC 27002:2013 pode ser considerada a norma mais importante para a gestão da segurança da informação que já foi elaborada. A implantação dessa norma

deverá tornar-se uma ferramenta essencial para empresas de qualquer tipo ou tamanho. (VIDAL, 2010, p.28)

A existência de sistemas de segurança da informação eficazes possibilita a redução de riscos, colabora com a proteção de organizações de ameaças e vulnerabilidades. Além disso, para que a segurança da informação seja alcançada são necessárias à implementação de controles adequados, como políticas, processos, estruturas (Norma ABNT NBR ISO/IEC 27002, 2013).

Ainda segundo a mesma norma, “a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade”, **Figura 1**.

Figura 1: Política de Segurança da Informação – PSI.

Fonte: https://periciacomputacional.com/psi-politica-de-seguranca-da-informacao/

Uma das dificuldades que existe em relação a muitos sistemas de informação que são implementados é que os mesmos não foram projetados levando em consideração a segurança e para suprir tal deficiência são empregados recursos técnicos para minimizar os riscos do uso destes sistemas. Importante ressaltar que para que um sistema de gestão de segurança da informação possa obter êxito é fundamental a participação de todos, incluindo funcionários, patrões e agentes externos (ABNT, 2013b)

Dentro das organizações faz-se necessária a adoção de medidas e procedimentos inseridos em normas e políticas que visem contribuir para um ambiente de segurança. Dentro do contexto da segurança da informação estão incluídos procedimentos, políticas, controle dos usuários e a proteção de dados,

sendo necessário o constante monitoramento dos sistemas e a evolução do nível de segurança. Além disso, deve-se ser dada atenção especial as ações de hackers contra organizações (NAKAMURA, 2007)

Outros autores, como Fontes, 2008 também ressalta a necessidade de execução de processos formalizados em normas e políticas atualizadas que possam definir e direcionar as práticas de segurança da informação e comunicações.

Existem várias formas de operacionalizar o controle de acesso dos usuários às áreas ou instalações pertencentes aos órgãos da APF. De acordo com as Diretrizes para Controle de Acesso Físico constante da 07/IN01/DSIC/GSIPR (2010, p.5), “os Órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas” (crachá, botom, cartões, selos, etc.), que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades. Além disso, a norma ressalta que se deve “intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente”

3.3 PROPRIEDADE INTELECTUAL

O conhecimento, no mundo atual, tem papel fundamental na área econômica para valoração de um negócio ou empreendimento. Ele tem grande poder de influenciar as transações comerciais nas relações internacionais. Diversas empresas já começaram a colocar a propriedade intelectual no ponto central de suas estratégias de negócios (GHESTI et al., 2016).

A difusão da Propriedade Intelectual abre novas possibilidades de negócios inovadores, além de gerar novas oportunidades. Importante também salientar o aspecto motivacional que isso gera no indivíduo, com a possibilidade de novas criações, a valorização do seu trabalho e o retorno financeiro advindo desse trabalho (GHESTI et al., 2016).

A Organização Mundial de Propriedade Intelectual (OMPI), que tem por propósito a promoção da proteção da propriedade intelectual ao redor do mundo através da cooperação entre Estado também tem uma grande preocupação com a segurança da informação. Essa instituição é uma das 16 agências especializadas da ONU, criada em 1967, com sede em Genebra. Ela possui uma Divisão de Segurança e Garantia da Informação (SIAD) com a responsabilidade de gerenciar todos os aspectos da segurança da informação, segurança física e segurança da OMPI (WIPO, 2002).

A Convenção da Organização Mundial da Propriedade Intelectual - OMPI coloca no bojo da Propriedade Intelectual o conjunto dos direitos relativos às diversas obras, interpretações artísticas, invenções do domínio humano, os desenhos industriais, marcas de serviços, industriais e comerciais e a proteção contra a concorrência desleal (WIPO, 2002).

4 METODOLOGIA

Quanto aos objetivos, a pesquisa foi classificada como exploratória, pois o objeto de pesquisa é pouco conhecido e recente no ambiente das ICTs e dos NIT, sendo necessário que se busquem mais informações sobre o sistema de gestão da segurança da informação específico para a proteção das informações tramitadas nas ICT. Nesse sentido, serão utilizadas como fontes de pesquisa, normas e artigos científicos, além de consulta aos sites das principais ICTs e órgãos internacionais e nacionais que trabalham com a propriedade intelectual.

Quanto à abordagem do problema, a pesquisa foi classificada como quantitativa e qualitativa. A pesquisa é quantitativa, pois apresenta dados quantificáveis oriundo das pesquisas aos documentos e artigos referentes à temática de SGSI nos NIT e a sua adoção nesses ambientes. A pesquisa também é qualitativa, pois se busca explicar o porquê das coisas, exprimindo o que convém ser feito. As características da pesquisa qualitativa são: objetivação do fenômeno; hierarquização das ações de descrever, compreender, explicar, precisão das relações entre o global e o local em determinado fenômeno; observância das diferenças entre o mundo social e o mundo natural; respeito ao caráter interativo entre os objetivos buscados pelos investigadores, suas orientações teóricas e seus dados empíricos; busca de resultados os mais fidedignos possíveis; oposição ao pressuposto que defende um modelo único de pesquisa para todas as ciências.

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 utilizar a técnica de análise por amostragem, onde, inicialmente, foi definido o universo de estudo, a partir da seleção de Instituições de renome nacional e internacional, considerando entidades estrangeiras e nacionais. 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 estas ICTs, tendo como referencial o previsto na norma ABNT NBR ISO/IEC 27002 (ABNT, 2013), 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, 2018); Política de Informação do MIT (MIT, 2018); Política de Segurança da Informação da Universidade de Oxford (OXFORD, 2018); 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, foi adotado, 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, por se tratar 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 na Normas ABNT NBR ISO/IEC 27001 e 27002. Nesta 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, gerenciamento das operações e comunicações, gestão de ativos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, criptografia, 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, apresentados em Publicação em Propriedade Intelectual do NUPITEC (GHESTI, 2016).

5 RESULTADOS E DISCUSSÃO

5.1 GENERALIDADES

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, 2013), utilizados pelo grupo de ICTs estudadas, foi possível identificar as Instituições que possuem um SGSI mais abrangente e quais controles são 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 de Instituições, que os incluíram em suas legislações internas de segurança da informação. A compilação dos controles por ICT é apresentada na

Tabela 1.

Inicialmente, pode-se observar que, dentre 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 10 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 13 pontos, situação na qual todos os treze 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, onde 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.

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

Controle/Domínio (Norma ISO 27002 e 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 Operações e 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	-	-	-	-	-	-	-	-
Relacionamento na Cadeia de Suprimento	-	-	-	-	-	-	-	-
Segurança da Informação na Gestão da Continuidade do Negócio	1	1	-	-	-	-	-	2
Abrangência da Política	**11**	**11**	**8**	**5**	**5**	**1**	**8**	**-**

Fonte: Autoria própria (2018).

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 operações e comunicações. A partir deste resultado para os controles utilizados mais comumente pelas ICTs, foi realizada uma análise da influência destes principais controles na Propriedade Intelectual.

5.1.1 Controle de Acesso

Na Norma ABNT NBR ISO/IEC 27001 (ABNT, 2013) 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, 2013). 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.

Na Universidade de Harvard existe uma política de segurança da informação onde o controle de acesso é aplicado. O controle de acesso da Universidade de Harvard aborda efetivamente a necessidade de proteger e controlar o acesso às informações confidenciais e sensíveis que são mantidas nas várias esferas da administração da Universidade.

Muitos membros do corpo docente, funcionários e alunos de Harvard participam de pesquisas que envolvem a coleta ou uso de informações confidenciais identificáveis. A lei federal e a política da Universidade de Harvard fornecem orientação específica ou protegem informações de pesquisa identificáveis.

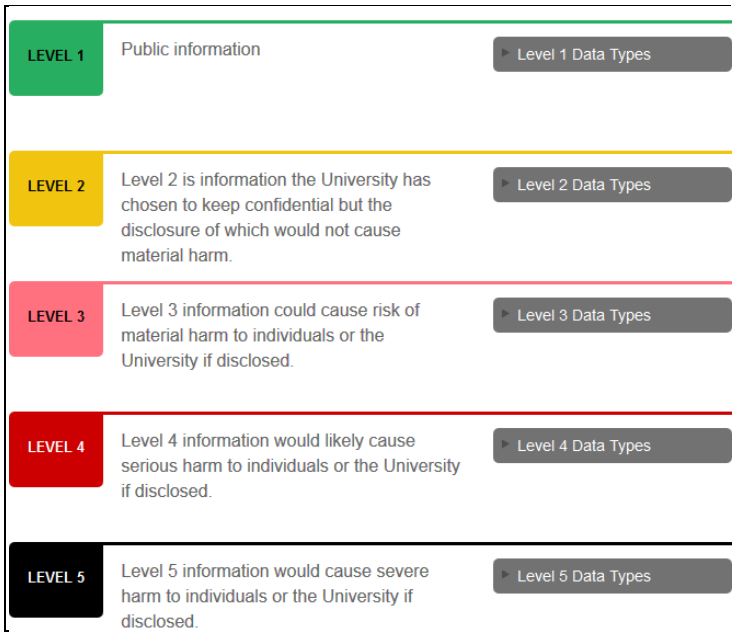
Para proteger os dados de pesquisa de forma adequada e eficaz, os pesquisadores da Universidade, os órgãos de supervisão de pesquisa e os Oficiais de Segurança da Informação devem entender e cumprir suas responsabilidades relacionadas à segurança de dados. Os níveis de segurança a seguir, descritos na **Tabela 2**, refletem o princípio básico de que requisitos de segurança mais exigentes devem ser implementados à medida que aumenta o risco associado aos dados da pesquisa:

O Nível 1 (*Level 1*) da **Tabela 2** são as Informações de pesquisa não confidenciais ou públicas. Nesta classificação estão enquadrados os dados de pesquisa que foram identificados de acordo com as regras aplicáveis, pesquisa publicada, informação pública sobre a Universidade, catálogos de cursos e informação do diretório de professores e funcionários (HARVARD, 2018).

O Nível 2 (*Level 2*) são as informações que a universidade decidiu manter de forma confidencial, mas cuja divulgação não causaria danos materiais. Nela estão incluídos os trabalhos de pesquisa não publicados e propriedade intelectual não constantes do Nível 3 ou 4, informações de pesquisa classificadas como Nível 2, pedidos de patentes e documentos de trabalho e rascunhos de documentos de pesquisa (HARVARD, 2018).

No Nível 3 (*Level 3*) são caracterizadas as Informações confidenciais e que podem causar risco de danos materiais a indivíduos ou à universidade, se divulgadas. Neste nível fazem parte as informações de pesquisa classificadas como Nível 3, informações protegidas pela Lei de Direitos e Privacidade Educacional da Família, registros do pessoal da Universidade de Harvard, registros financeiros institucionais e outras informações pessoais protegidas por leis de privacidade estaduais, federais e estrangeiras não classificadas como Nível 4 ou 5 (HARVARD, 2018).

Tabela 2: Nível de Classificação dos Dados



Fonte: https://policy.security.harvard.edu/

No Nível 4 (*Level 4*) estão as Informações caracterizadas como muito sensíveis e que provavelmente causariam sérios danos a indivíduos ou à Universidade, se divulgadas. Neste conjunto estão enquadradas as informações confidenciais de alto risco e informações de pesquisa classificadas como Nível 4, informações financeiras ou médicas pessoalmente identificáveis, informações normalmente usadas para estabelecer identidade protegida por leis de privacidade estaduais, federais ou estrangeiras e regulamentos, Informações genéticas individualmente identificáveis que não são do Nível 5, informações de segurança nacional (sujeitas a requisitos governamentais específicos), senhas e PINs de

Harvard que podem ser usados para acessar informações confidenciais (HARVARD, 2018).

Por fim, verifica-se na Universidade de Harvard o Nível 5 (*Level* 5) onde constam as informações extremamente sensíveis e que causariam danos graves a indivíduos ou à universidade, se divulgadas. Neste último nível estão enquadradas as informações de pesquisa classificadas como Nível 5 e que são obrigadas a serem armazenadas ou processadas em locais com alta segurança, os ambientes computadorizados não conectado às redes de dados da Universidade de Harvard e certos registros médicos individualmente identificáveis e informações genéticas, categorizados como extremamente sensíveis (HARVARD, 2018).

Este controle se aplica a todos os dados de pesquisa, independentemente da mídia de armazenamento (por exemplo, unidade de disco, fita eletrônica, cartucho, disco, CD, DVD, unidade externa, papel, ficha, etc.) e independentemente da forma (por exemplo, texto, gráfico, vídeo, áudio, etc.), fisicamente abrigado na Universidade de Harvard ou armazenado remotamente sob a gestão dos seus pesquisadores.

Os pesquisadores de Harvard geralmente lidam com informações confidenciais que não estão relacionadas a assuntos administrativos. Os exemplos podem incluir informações proprietárias sujeitas a requisitos de confidencialidade e informações com implicações na segurança nacional. A maioria desses tipos de informação será categorizada como informação de Nível 3 sob as categorias descritas na Política de Segurança da Informação de Dados de Pesquisa da Harvard (HRDSP). No entanto, as informações com implicações de segurança nacional geralmente serão categorizadas como informações de Nível 4. Os pesquisadores devem consultar o CIO (*Chief Information Officer)* da escola ou o diretor de TI para determinar o nível adequado para esses tipos de informações, caso não tenham certeza de qual categoria é apropriada (HARVARD, 2018).

Na *Massachusetts Institute of Technology* (MIT) a norma ABNT NBR ISO/IEC 27001 não é utilizada oficialmente, mas o controle de acesso é empregado por todos os membros da comunidade do MIT e são responsáveis por garantir que o tratamento das informações sobre os indivíduos seja consistente com a política do Instituto sobre privacidade de informações. Além disso, outros registros do Instituto

(isto é, registros que não contenham informações pessoais) devem ser tratados com a devida consideração e com ações visando à privacidade e confidencialidade.

A Política praticada no MIT se aplica a pesquisadores e membros da equipe de pesquisa que obtêm, acessam ou geram dados de pesquisa, em particular informações confidenciais. A política se aplica independentemente da fonte de financiamento para a pesquisa.

A Política também se aplica aos órgãos de supervisão de pesquisa que trabalham com o Gabinete do Vice-Reitor de Pesquisa, auxiliando os pesquisadores na identificação e avaliação de riscos de confidencialidade de dados; e Agentes de Segurança da Informação que trabalham com pesquisadores e membros da equipe de pesquisa para garantir a implementação dos controles de segurança para os requisitos do nível de segurança designado para informações de pesquisa.

Os Pesquisadores têm estas responsabilidades de identificar obrigações de confidencialidade e segurança de dados, com base em leis, regulamentos, políticas e compromissos vinculantes, como contratos de uso de dados e contratos de consentimento de participantes. Exceto nos casos em que é de responsabilidade de um órgão de supervisão de pesquisa, é responsabilidade dos pesquisadores identificar o nível apropriado de segurança de dados para dados de pesquisa. Quando o nível de segurança de dados for estabelecido, os pesquisadores são responsáveis pela criação e manutenção da documentação de dados, implementando os controles de segurança correspondentes aos requisitos da segurança de dados. Devem também desenvolver e seguir um plano e procedimentos de segurança de dados ao longo de seus projetos.

O MIT tem a obrigação de fornecer informações precisas e confiáveis aos destinatários autorizados e de preservar registros vitais. O MIT está cada vez mais dependente da precisão, disponibilidade e acessibilidade das informações armazenadas eletronicamente e dos recursos de computação e de rede que armazenam, processam e transmitem essas informações. Registros criados e mantidos em formato eletrônico estão incluídos na definição de materiais arquivados do Instituto. Além disso, sob orientação do Escritório do Conselho Geral, os registros devem, às vezes, ser preservados por períodos prescritos de tempo para litígios ou outros fins legais.

A Universidade de Oxford está empenhada em manter um ambiente aberto, mas seguro, onde a segurança de todos os seus alunos, funcionários e visitantes é equilibrada com os direitos e liberdades indivíduos.

A Universidade de Oxford espera que todos os membros da comunidade universitária assumam o seu papel individual e responsabilidades coletivas para tornar a Universidade um lugar livre de crime, medo e desordem, e para proporcionar um ambiente civil e aberto que promova a aprendizagem. A informação sustenta todas as atividades da Universidade e é essencial para sua pesquisa, ensino e funções administrativas. A Universidade reconhece o papel da segurança da informação para garantir que os utilizadores têm acesso às informações de que necessitam para realizar o seu trabalho, evitando acesso não autorizado. Esta política fornece uma estrutura para o gerenciamento da segurança da informação em toda a Universidade.

Na Universidade de Oxford, a norma ISO 27001 é utilizada como uma das principais referências para a estrutura normativa do sistema de segurança da informação da instituição. As informações são críticas para as operações da Universidade e a falha em proteger as informações aumenta o risco de perdas financeiras e de reputação. A Universidade está empenhada em proteger a informação, em todas as suas formas, incluindo a perda de confidencialidade, integridade e disponibilidade.

No que se refere ao controle de acesso, um dos objetivos da universidade é de que usuários autorizados possam acessar, com segurança, informações para desempenhar suas funções e os controles de segurança implementados sejam pragmáticos, eficazes e mensuráveis. Os controles de segurança da informação apropriados devem ser implementados para proteger todas as instalações, tecnologias e serviços usados para acessar, processar e armazenar informações.

A universidade de Oxford dispõe em sua estrutura de um Conselho que tem responsabilidade executiva pela segurança da informação dentro da Universidade. O Conselho especificamente é responsável por determinar o sistema de controles internos operados pela Universidade e por monitorar a adequação e eficácia do ambiente de controle. O Subcomitê de Segurança do Comitê de Fins Gerais tem a responsabilidade de supervisionar o gerenciamento dos riscos de segurança para os

funcionários da Universidade e seus estudantes, sua infraestrutura e suas informações.

Cada vez mais, a pesquisa é realizada por equipes interdisciplinares, muitas vezes distribuídas entre instituições ou países. 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, compartilhamento e comunicação de material didático, entrega de palestras e tutoriais e o apoio às atividades de aprendizagem é essencial para garantir que os funcionários tenham confiança nas tecnologias utilizadas.

A UFRJ trata o controle de acesso de forma muito genérica em sua documentação disponibilizada no seu site. O único documento que trata sobre segurança da informação é a portaria 4579 de 15 de junho de 2012. Este documento reproduz a publicação da Política de Segurança da Informação da UFRJ. O documento se preocupa mais em relação ao controle de acesso relacionado aos recursos de tecnologia da informação (UFRJ, 2012).

Importante salientar que a UFRJ é uma das melhores universidades do Brasil e que possui grandes pesquisadores, além de uma agência de inovação responsável por tratar das questões relacionadas com a propriedade intelectual e a transferência de tecnologia. Uma política de controle de acesso mais específica e detalhada ajudaria a minimizar os riscos de vazamento de pesquisas e outras informações importantes e estratégicas relacionadas com a propriedade intelectual.

A UFSC também, na esteira do que foi verificado na UFRJ adota uma política de controle de acesso bem enxuta, apenas dando direcionamentos muito gerais e atribuindo e delegando aos demais setores e departamentos o aprofundamento destas questões. Assim como a UFRJ, a UFSC também possui uma gama de pesquisadores e agência de inovação vocacionada para a propriedade intelectual, além de ser responsável por articular as questões de transferência de tecnologia.

Na Unicamp foi possível verificar um conjunto de normas e políticas mais abrangente, principalmente no que tange ao controle de acesso. Neste aspecto, merece destaque, as orientações e normas de acesso em relação ao uso de recursos computacionais interno ao campus, sejam eles particulares ou

pertencentes à própria universidade. Há também uma preocupação com acesso aos meios de comunicações e ao conteúdo trafegado ou hospedado em máquinas ou dispositivos magnéticos sob a forma de arquivos eletrônicos. A universidade estabelece critérios de privacidade de determinados tipos de informações e as respectivas punições no cometimento de falta desta natureza. Há também uma preocupação em deixar claro nas normas as definições, principalmente às relacionadas a dados, informação, características e tipos de dados, acesso e demais conceitos importantes.

A Unicamp delega ao Conselho de Tecnologia da Informação e Comunicações (ConTIC) a função de rever, recomendar e aprovar políticas e procedimentos relacionadas ao uso e acesso a Dados Corporativos, bem como resolver conflitos e disputas que ocorram em função da implementação ou administração destas políticas e procedimentos. O acesso aos meios de TI é controlado e monitorado de forma a prover segurança aos dados trafegados pelos meios de TI.

A Unicamp também possui uma gama de estudantes, professores e pesquisadores envolvidos com pesquisas, projetos inovadores, muitas vezes financiados pela iniciativa privada e que necessitam de uma base sólida de segurança em relação às informações que são tramitadas. Atualmente as normas e políticas internas de controle de acesso da Unicamp são bem rígidas e detalhadas possibilitando e favorecendo um ambiente mais seguro onde o controle de acesso a determinado tipo de informação colabora para um ambiente de maior confiança e credibilidade em relação aos dados de pesquisa utilizados.

Importante ressaltar que tanto a UFRJ, Unicamp e UFSC têm normas e políticas de segurança da informação relacionadas com controle de acesso baseadas nas normas ABNT NBR ISO/IEC 27001 e 27002. Além disso, as instruções normativas do Gabinete de Segurança Institucional também são utilizadas como referências para a normatização do controle de acesso.

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, tais como no caso do inventor ter protegido a sua tecnologia, como, 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 deve ficar restrito ao período em que não houve a sua divulgação oficial. Nesse contexto, faz-se necessária a restrição de acesso às informações referentes a essas tecnologias, por meio de normas e 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 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.

5.1.2 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 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 a 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 anteriormente, 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 normalmente as normas de segurança não são bem conhecidas pelos usuários. Para um inventor, bem como 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 NITs, no intuito de propiciar maior segurança nas ações a serem desenvolvidas, bem como 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.

Todas as ICTs pesquisadas sejam elas nacionais ou estrangeiras apresentam em seus sites uma Política de Segurança da Informação devidamente publicado. No entanto, somente as universidades de Oxford, MIT, Harvard e Unicamp apresentam orientações específicas para a segurança da informação envolvendo a PI. Há de se destacar também a preocupação dessas políticas de segurança em abordar questões relacionadas com a segurança dos meios de TI, nos seus mais variados ramos.

Nas normas de Segurança da Informação e Comunicação (SIC) publicado pela Unicamp há um capítulo específico voltado para a proteção de software proprietário e sua gestão, inclusive mencionando a Lei n.º 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e a Lei n.º 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais (Unicamp, 2012).

Nas políticas de segurança da informação das universidades estrangeiras são abordas as questões de PI, principalmente no que concerne a pesquisa científica e inovação, onde é dado atenção às regulamentações, legislações e contratos; ambiente de ameaça da segurança da informação, atual e futuro; atribuições de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos. Estas ações estão diretamente relacionadas com os requisitos constantes da ISO 27002.

No MIT a política de segurança da informação é denominada de Política de Informação onde constam dentro de seu bojo como capítulos principais as questões sobre: propriedade intelectual, política de uso de recursos de TI, política de

arquivamento, programa de gerenciamento de registros e reprodução de material protegido por direitos autorais. Fica evidenciada a importância dessa política para o desenvolvimento das atividades principais do MIT e sua relação intrínseca com a propriedade intelectual.

A Política de Segurança da Informação da Universidade de Harvard aborda efetivamente a necessidade de proteger informações confidenciais e sensíveis que são mantidas nas várias esferas da administração da Universidade. De acordo o preconizado pela Universidade de Harvard o cenário de pesquisa apresenta riscos e desafios específicos de segurança da informação, incluindo restrições regulatórias e contratuais que exigem provisões adicionais de políticas e medidas de proteção. Essa política fornece orientação específica para o gerenciamento de dados de pesquisa incluindo neste escopo as questões de patentes.

Essa política é particularmente focada na proteção de dados de pesquisa que são confidenciais em razão de leis e regulamentos aplicáveis, acordos cobrindo a aquisição e uso dos dados e políticas da Universidade. A Política de Segurança da Informação de Harvard é denominada de Política de Segurança de Dados e juntamente com a Política de Propriedade Intelectual fazem parte das Políticas e orientações de pesquisa de Harvard, logo se verifica que estas políticas são aplicadas de forma complementar e não excludentes.

O escopo da política de segurança da informação de Oxford é abrangido em toda a Universidade e aplica-se individualmente a:

- Todos os indivíduos que têm acesso a informações e tecnologias da Universidade;
- Todas as instalações, tecnologias e serviços usados para processar informações da Universidade;
- Informações processadas, em qualquer formato, pela Universidade, de acordo com suas atividades;
- Processos internos e externos usados para processar informações da Universidade; e
- Partes externas que fornecem serviços de processamento de informações para a Universidade (Oxford, 2018).

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, compartilhamento e comunicação de material didático, entrega de palestras e tutoriais e o apoio às atividades de aprendizagem é essencial para garantir que os funcionários tenham confiança nas tecnologias utilizadas.

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, compartilhamento e comunicação de material didático, 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 como um todo, 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 nestes processos saibam como tratar de forma segura determinadas informações e como agir em relação aos contratos e convênios estabelecidos com outros órgãos públicos ou privados.

5.1.3 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 operação da segurança da informação, dentro das Instituições. Para que este controle cumpra o seu papel, estas normas orientam que sejam levados em consideração alguns aspectos, tais como responsabilidades e papéis pela segurança da informação, a segregação de funções, 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 deste 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.

A Universidade de Oxford possui dois órgãos responsáveis pela organização da segurança da informação: o Conselho de Segurança da Universidade e o Grupo Consultivo Conjunto de Segurança da Informação. O Conselho de segurança tem responsabilidade executiva pela segurança da informação dentro da Universidade. O Conselho especificamente é responsável por determinar o sistema de controles internos operados pela Universidade e por monitorar a adequação e eficácia do ambiente de controle. O Subcomitê de Segurança do Comitê de Fins Gerais tem a responsabilidade de supervisionar o gerenciamento dos riscos de segurança para os funcionários da Universidade e seus estudantes, sua infraestrutura e suas informações. Já o Grupo Consultivo Conjunto de Segurança da Informação (JISAG) tem a responsabilidade de desenvolver e manter a estrutura de políticas de segurança da informação, revisar relatórios sobre conformidade, fornecer apoio e orientação, escalar riscos e problemas e fornecer recomendações à Universidade (OXFORD, 2018).

Na Universidade de Harvard, os próprios pesquisadores são responsáveis por identificar as obrigações de confidencialidade e segurança de dados, com base em leis, regulamentos, políticas e compromissos vinculantes, como contratos de uso de dados e contratos de consentimento dos participantes. Exceto nos casos em que é de responsabilidade de um órgão de supervisão de pesquisa é responsabilidade dos pesquisadores identificar o nível apropriado de segurança para dados de pesquisa. Quando o nível de segurança de dados foi estabelecido, os pesquisadores são responsáveis pela criação e manutenção da documentação de dados, implementando os controles de segurança correspondentes aos requisitos da segurança de dados e desenvolver e seguir um plano e procedimentos de segurança de dados ao longo de seus projetos. Os agentes de segurança da

informação são responsáveis pela Segurança da Informação Local ou Escolar e são responsáveis por auxiliar os pesquisadores na implementação de controles de segurança apropriados, de acordo com o nível designado pelo Órgão de Supervisão da Pesquisa ou controles específicos especificados. Ainda existem na universidade os órgãos de supervisão de pesquisa que são responsáveis por: avaliar os riscos de segurança de dados associados à pesquisa dentro de sua área de atuação e atribuindo níveis de segurança de dados para a pesquisa, estabelecer procedimentos para definir níveis de segurança, seja projeto a projeto ou por categoria de dados de pesquisa, e informar os pesquisadores sobre riscos de segurança de dados e trabalhar com eles para definir níveis apropriados de segurança de dados (HARVARD, 2018).

Nas ICTs nacionais a organização da segurança da informação está normalmente vinculada àquela estabelecida pelas universidades. Além disso, há uma clara associação desta organização com as questões de TI das ICTs. Na Unicamp a Coordenadoria de Tecnologia de Informação e Comunicação (CTIC) é o Órgão executivo da Reitoria que traça as políticas e programas da Unicamp nas áreas de tecnologia da informação e comunicação e que, uma vez aprovados pelo ConTIC – Conselho de Tecnologia da Informação e Comunicação, coordena a sua execução com o apoio do Centro de Computação da Universidade Estadual de Campinas (CCUEC). O Conselho de Tecnologia da Informação e Comunicação – ConTIC, nos termos da Resolução GR-021/2006, é o Órgão deliberativo da Reitoria que estabelece políticas e programas nas áreas de tecnologia da informação e comunicação.

Na UnB não foi possível identificar esta estrutura de forma clara, uma vez que não foi encontrado um documento que formaliza esta questão. A ferramenta SEI que é utilizada pela UnB não se constitui em um instrumento capaz de deixar claro a organização da segurança da informação e no site da UnB foi verificado que o CPD (Centro de Processamento de Dados) administra e orienta em relação a questões de TI no âmbito da universidade.

Da análise deste controle, pode-se concluir, que a sua adoção é muito importante para as ICTs, pois deixa claro aos usuários, pesquisadores e profissionais de PI quem são os responsáveis pela segurança da informação e quais

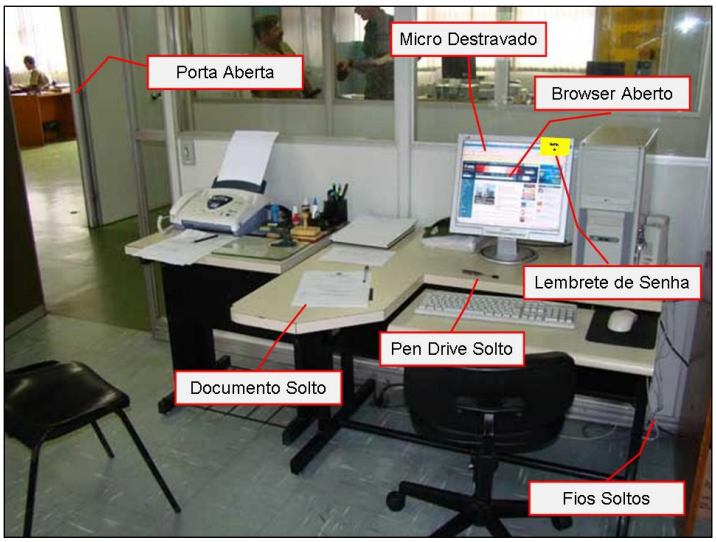
são as penalidades advindas do descumprimento de normas de segurança envolvendo os processos de PI.

5.1.4 Segurança Física e do Ambiente

A segurança física e do ambiente visa prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização, bem como impedir perdas, danos, roubo ou comprometimento de ativos e interrupção das operações (ABNT, 2013a). A norma ABNT ISO/IEC 27001 estabelece que este controle, quando aplicado, deve dar atenção às áreas consideradas seguras, principalmente às 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 podem evitar a exposição e acesso indevido às informações tramitadas nesses ambientes, conforme ilustrado na

Figura 2.

Figura 2: Ambiente de trabalho com falhas de segurança.



Fonte: 3º CTA (2011, p. 9).

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 que a documentação tramitada, seja em mídia digital ou física, contém informações relevantes sobre os processos de proteção e transferência de tecnologia. A aplicação deste 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.

Na universidade de Harvard, todos os dispositivos devem ser configurados para armazenamento seguro, transporte e descarte de informações confidenciais. Todos os dispositivos do usuário devem ser configurados para operação segura. O dispositivo deve ser configurado para limitar o acesso à pessoa específica ou pessoas autorizadas a usar o dispositivo. A informação armazenada no dispositivo deve ser protegida contra o acesso se o dispositivo for perdido ou roubado. Todos os dispositivos móveis (laptops, celulares, etc.) que podem ser usados para armazenar ou acessar informações de Harvard, incluindo o acesso ao e-mail de Harvard, devem ser configurados com segurança, incluindo criptografia. Sistema operacional e correções de aplicativos devem ser aplicados imediatamente. As informações armazenadas no dispositivo devem estar protegidas contra o acesso quando o dispositivo for descartado. Qualquer perda real ou suspeita, roubo ou uso indevido de um dispositivo que armazene informações confidenciais deve ser relatado imediatamente (HARVARD, 2018).

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

5.1.5 Segurança em Recursos Humanos

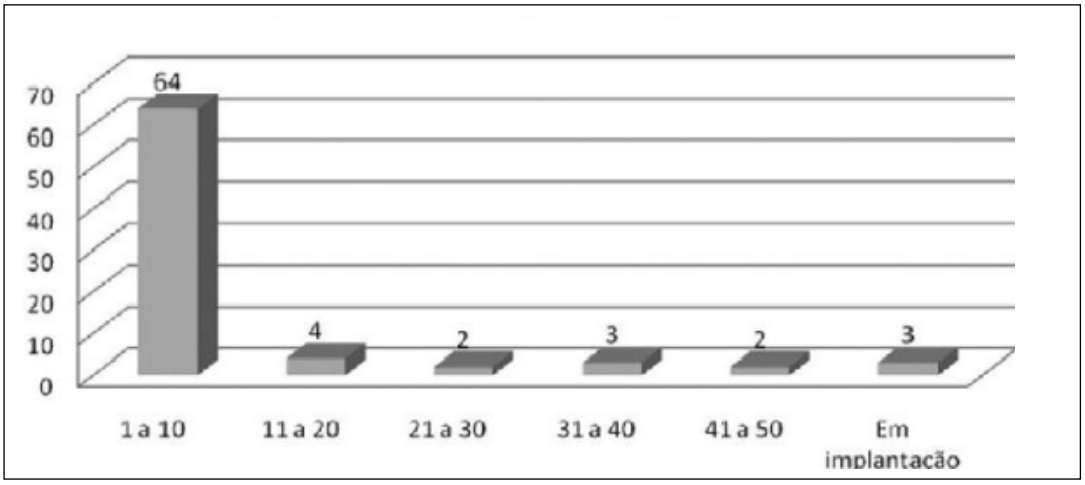
A segurança em recursos humanos, conforme consta da norma ABNT NBR ISO 27002 (ABNT, 2013b), deve ser aplicada antes, durante e no encerramento e na mudança da contratação dos colaboradores. Esse controle tem por objetivo

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 por 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, termos e condições de contratação, conscientização, educação e treinamento em segurança da informação, 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, operações e 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 estas informações. Atualmente, muitos dos profissionais que trabalham nos NITs, encarregados dos processos de proteção de tecnologias e nas atividades de transferências de tecnologia, são temporários o que ocasiona uma rotatividade muito grande, oferecendo vulnerabilidade aos sistemas de proteção como um todo. A implementação desse controle nas ICTs pode contribuir para uma 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.

A contratação e capacitação de pessoal foram consideradas as principais deficiências e apontados como partes mais importantes por 77% dos NITs. Isso pode ser observado uma vez que a 82% apontaram não possuir mais de 10 pessoas trabalhando na sua estrutura, conforme apresenta a **Figura** . Em segundo lugar, a falta de competências e habilidades em transferência de tecnologia foram citadas por 68%. Além disso, a falta 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% deles como muito importantes (TORKOMIAN, 2009).

Figura 3: Quantidade de pessoas por NIT.



Fonte: Torkomian (2009).

Na Universidade de Oxford há uma preocupação muito grande com este controle onde há grande apoio no compartilhamento e disseminação de conhecimento e boas práticas de segurança da informação em toda a comunidade de segurança da informação. Verificou-se que essa universidade tem desenvolvido relacionamentos sólidos e colaboração com outras equipes de segurança da informação no ensino superior e setores mais amplos de segurança da informação.

São introduzidos aprendizados de segurança da informação para fornecer empregos e treinamento e garantir o desenvolvimento contínuo de recursos de segurança da informação para a Universidade e para a comunidade em geral. Dentre os objetivos da Universidade de Oxford relacionados a esse controle estão: desenvolver uma forte cultura de segurança da informação em toda a Universidade, através da educação, conscientização e colaboração; estabelecer uma equipe de segurança da informação altamente capacitada que seja reconhecida como um centro de excelência dentro da Universidade e que ofereça serviços de segurança de informações responsivos e recrutar e reter a segurança de informação técnica e não técnica especializada e construir e desenvolver capacidade de gestão e liderança (OXFORD, 2018).

O inciso IV, § 1º, Art. 38. do Decreto nº 9.283, de 7 de fevereiro de 2018 estabelece que o convênio para pesquisa, desenvolvimento e inovação é o instrumento jurídico celebrado entre os órgãos e as entidades da União, as agências

de fomento e as ICT públicas e privadas para execução de projetos de pesquisa, desenvolvimento e inovação, com transferência de recursos financeiros públicos e que os projetos de pesquisa, desenvolvimento e inovação poderão contemplar, entre outras finalidades: a capacitação, a formação e o aperfeiçoamento de recursos humanos para atuação em pesquisa, desenvolvimento e inovação, inclusive no âmbito de programas de pós-graduação.

Conclui-se que a adoção desse controle, nos processos de PI contribui diretamente para a melhoria da segurança da informação, uma vez que a presença de profissionais cada vez 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.

5.1.6 Segurança nas Operações e Comunicações

A segurança nas operações e comunicações visa assegurar a proteção das informações, em redes e dos recursos de processamento da informação, que as apoiam, bem como a manutenção da segurança da informação transferida dentro da organização ou com as entidades externas (ABNT, 2013b). 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 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 que as redes de dados sejam 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.

No MIT todos os membros dessa comunidade são obrigados a usar os recursos de TI do MIT de acordo com as leis aplicáveis, com as políticas do Instituto (incluindo sua política contra assédio e seus padrões de honestidade e conduta pessoal) e de maneiras responsáveis, éticas e profissionais. O uso dos recursos de TI do MIT é restrito aos negócios do Instituto. O uso pessoal não pode interferir no trabalho do MIT, nem pode resultar em custos diretos adicionais para o MIT. Os computadores do MIT e outros recursos de TI devem ser usados de maneira consistente com o status do MIT como uma organização sem fins lucrativos e, por exemplo, não podem ser usados para o benefício de negócios pessoais ou outras organizações. Os membros da comunidade do Instituto não devem tomar ações não autorizadas para interferir, perturbar ou alterar a integridade dos recursos de TI do MIT. Os esforços para restringir ou negar o acesso de usuários legítimos dos recursos de TI do Instituto são inaceitáveis. Os indivíduos não devem usar as instalações do MIT para interferir ou alterar a integridade de quaisquer recursos de TI, independentemente de sua localização.

Restrições especiais são frequentemente colocadas no uso de recursos de TI, como hardware, software, bancos de dados e documentação, principalmente quando adquiridos de fontes externas. O uso de tais recursos de TI pode ser ainda mais restrito pela lei de patentes, como um segredo comercial ou por contrato na forma de uma licença ou outro contrato. Os membros da comunidade do MIT são obrigados a respeitar as restrições impostas por lei ou por contrato sobre os recursos de TI adquiridos para uso no Instituto. Qualquer indivíduo que organize a distribuição autorizada de produtos e serviços de tecnologia da informação de fontes externas deve informar às pessoas que têm acesso aos produtos e serviços de todas as restrições de uso associadas (MIT, 2018).

A Agência Inova Unicamp é o órgão responsável pela gestão da propriedade intelectual gerada na Unicamp. Dessa maneira, o pesquisador da Unicamp conta com a Agência para proteger suas invenções. Conforme descrito no site da Inova Unicamp, o caso da patente, o procedimento começa com o envio das informações mais relevantes sobre sua invenção por meio do Sistema de Comunicação de Invenção. O Sistema de Comunicação de Invenção foi desenvolvido para facilitar a interação com o inventor da Unicamp. Nesta nova interface basta preencher o formulário online e fazer o envio das informações pelo próprio sistema, que também

permite o salvamento temporário das informações, antes do envio definitivo. Esse sistema deve ser seguro o suficiente que inviabilize o acesso ao banco de dados por pessoas não autorizadas, contribuindo assim para o controle de acesso aos meios de TI utilizados no processo de proteção de invenções.

Após o recebimento das informações referentes à Comunicação de Invenção, analistas de Propriedade Intelectual (PI) da Inova Unicamp entram em contato com os pesquisadores para esclarecer possíveis dúvidas sobre a tecnologia desenvolvida. Também deve haver uma série de procedimentos de controle de acesso envolvendo o analista de PI da Inova Unicamp e o pesquisador, no intuito de proteger os dados da invenção enquanto a mesma não é registrada, por meio dos canais legais.

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.

5.1.7 Demais controles das normas ABNT ISO/IEC 27001 e 27002

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

6 CONSIDERAÇÕES FINAIS

O presente estudo permitiu verificar que a adoção de um SGSI é crucial para o desenvolvimento de atividades relacionadas à Propriedade Intelectual, tais 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 respeito, que

parceiros e sociedade possuem dessas Instituições. O estudo demonstrou que a família de normas ISO 27000, em especial as normas ISO 27001 e 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 as 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 estas Instituições. Outro ponto que se destacou, foi que as políticas de gestão de PI nessas Instituições, faz 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. Destacou-se a estrutura e a gama de informações disponibilizada 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 visam 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, implementado em Harvard e no MIT pode servir de modelo para as ICTs nacionais. Este 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 onde 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 direcionada às questões de TI.

A UnB não apresenta normativos específicos para a segurança da informação relacionados a assuntos relacionados à Propriedade Intelectual. Apesar disso, a ferramenta SEI, utilizada no gerenciamento eletrônico de processos, associado às informações disponibilizadas no site da instituição, que poderiam permitir a implementação de um SGSI amplo e eficiente dentro da Instituição, não atendem, atualmente, a todos os requisitos de um SGSI relacionados à PI. A plataforma SEI atende 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 relacionadas à segurança de informações para PI. Nesse contexto, tem-se como perspectivas para futuros trabalhos, 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.

Com a implementação de um SGSI específico para uma instituição de pesquisa busca-se o aperfeiçoamento das questões de controle de acesso, segurança física e ambiental, conformidade, gestão de ativos e segurança de recursos humanos.

O levantamento dos problemas existentes, concomitante com a apresentação de propostas mais adequadas à gestão de segurança da informação e comunicações, pode contribuir para um melhor desempenho das ICTs e a sua adequação a legislação vigente, relacionada com a segurança da informação. Além disso, pode favorecer para uma significativa melhoria do SGSI dos NIT e, consequentemente fortalecerá a credibilidade dos trabalhos desenvolvidos.

7 REFERÊNCIAS BIBLIOGRÁFICAS

3º Centro de telemática de Área (CTA). **Apostila de Segurança Aplicada à Segurança da Informação**. São Paulo, 2011.

ABNT. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 17799:2005**. 2a. ed. Rio de Janeiro, 2005.

ABNT. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2013**. 2a. ed. Rio de Janeiro, 2013a.

ABNT. **Tecnologia da informação - Técnicas de segurança – Gestão de riscos de segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013b.

AHMAD, A., Bosua, R. and Scheepers, R. (2014), "**Protecting organizational competitive advantage: a knowledge leakage perspective**", Computers & Security, Vol. 42, pp. 27-39.

ALAVI, M. and Leidner, D.E. (2001), "**Review: knowledge management and knowledge management systems: conceptual foundations and research issues**", MISQ, Vol. 25 No. 1, pp. 107-136.

ASLLANI, A. and Luthans, F. (2003), "**What knowledge managers really do: an empirical and comparative analysis**", Journal of Knowledge Management, Vol. 7 No. 3, pp. 53-66.

BACHLECHNER, D., Thalmann, S. and Manhart, M. (2014), "**Auditing service providers: supporting auditors in cross-organizational settings**", Managerial Auditing Journal, Vol. 29 No. 4, pp. 286-303.

BRASIL. Presidência da República. **Decreto nº 9.283, de 7 de fevereiro de 2018**. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 13.243, de 11 de janeiro de 2016, o art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666, de 21 de junho de 1993, o art. 1º da Lei nº 8.010, de 29 de março de 1990, e o art. 2º, caput, inciso I, alínea "g", da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional. Disponível em: <http:// http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm>. Acesso em: 01 mar. 2019.

DHILLON, G. and TORKZADEH, G. (2006), **Value-focused assessment of information system security in organizations**, Information Systems Journal, Vol. 16 No. 3, pp. 293-314.

DSIC/ GSIPR. **Norma Complementar 07/IN01/DSIC/GSIPR, de 06 de maio de 2010 : Diretrizes para implementação de controles de acesso relativos á segurança da informação e comunicações**. Brasília, maio 2010. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 10 out. 2018.

DSIC/ GSIPR. **Norma Complementar 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. Norma Complementar nº 20/IN01/DSIC/GSIPR de 15 de dezembro de 2014

FERNANDES, Jorge Henrique Cabral. **Controle de Acessos: GSIC211 (Notas de Aula)**. Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 32 p.

FOINA, P. R. **Tecnologia de informação: planejamento e gestão**. 3a. ed. São Paulo: Atlas, 2013.

FONTES, E. **Praticando a segurança da informação**. 1ª ed. Rio de Janeiro: Brasport, 2008.

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**. Disponível em:< https://vpr.harvard.edu/pages/research-data-security-and-management>. Acesso: em 10 out.2018.

INSTITUTO NACIONAL DE PROPRIEDADE INDUSTRIAL. **Instrução Normativa nº 24, de 29 de julho de 2013**. Institui a Política de Segurança da Informação e Comunicações no âmbito do Instituto Nacional da Propriedade Industrial. (INPI, 2013). Disponível em:< http://www.inpi.gov.br/legislacao-arquivo/docs/instrucao-normativa-no-24-13-posic.pdf>. Acesso: em 11 mar.2019.

LEE, S.C., Chang, S.N., Liu, C.Y. and Yang, J. (2007), "**The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance**", Knowledge and Process Management, Vol. 14 No. 1, pp. 58-69.

LYRA, Maurício Rocha. Segurança do Patrimônio Intangível. In: FOINA, P. R (Org). **Planejamento Estratégico para Empresas de Base Tecnológica**. 1ª ed. Brasília: Instituto CEUB de Pesquisa e Desenvolvimento - ICPD, 2016.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT). **MIT Policies**. 13.0 Informatiom Policies. Massachusetts: Cambridge, [20--]. Disponível em:< https://policies.mit.edu/policies-procedures/130-information-policies>. Acesso em: 17 out. 2018.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT). **Information Protect @ MIT**. Massachusetts: Cambridge, [20--]. Disponível em:< https://infoprotect.mit.edu/>. Acesso em: 17 out. 2018.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES - MCTI. Secretaria de Desenvolvimento Tecnológico e Inovação. **Política de Propriedade Intelectual das Instituições Científicas, Tecnológicas e de Inovação do Brasil: relatório FORMICT 2016**. Brasília, DF: MCTIC, 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.

NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambientes Cooperativos**. 1ª ed. São Paulo: Novatec Editora, 2007.

NONAKA, I. (1994), "**A dynamic theory of organizational knowledge creation**", Organization Science, Vol. 5 No. 1, pp. 14-37.

NORMAN, P.M. (2002), "**Protecting knowledge in strategic alliances: resource and relational characteristics**", The Journal of High Technology Management Research, Vol. 13 No. 2, pp. 177-202.

OLANDER, H., Hurmelinna-Laukkanen, P. and Heilmann, P. (2011), "**Do SMEs benefit from HRM-related knowledge protection in innovation management?**" International Journal of Innovation Management, Vol. 15 No. 3, pp. 593-616.

ROBREDO, Jaime. **Da Ciência da Informação aos Sistemas Humanos de Informação**. Brasília: Thesauros. 2005.

YILMAZ, R. and YALMAN Y. **A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks**. TEM Journal, Vol 5, Iss 2, Pp 180-191 (2016), [s. l.], n. 2, p. 180, 2016. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.71d180d6b918456ea51fb766196d292d&lang=pt-br&site=eds-live&authtype=ip,uid>. Acesso em: 19 set. 2018.

TORKOMIAN, Ana Lúcia Vitale. Panorama dos Núcleos de Inovação Tecnológica no Brasil. In: T**ransferência de Tecnologia: Estratégias para estruturação e gestão de Núcleos de Inovação Tecnológica**. Campinas, SP: Komedi, 2009.

TRKMAN, P. and DeSouza, K.C. (2012), "**Knowledge risks in organizational networks: an exploratory framework**", Journal of Strategic Information Systems, Vol. 21 No. 1, pp. 1-17.

UNIVERSIDADE DE BRASÍLIA (UnB). **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.

UNIVERSIDADE ESTADUAL DE CAMPINAS (Unicamp). **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.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). **Portaria nº 4579, 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.

UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). **Portaria nº 1754/2015/GR, de 09 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 (1) to No 5140, 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.

VENEZIANO, Wilson Henrique. Organizações e **Sistemas de Informação: GSIC051 (Notas de Aula)**. Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. Brasília, DF, 2010. 21 p

VIDAL, Flávio de Barros. **Controles de Segurança Física e Ambiental: GSIC202** (Notas de Aula). Curso de Especialização em Gestão da Segurança da Informação e Comunicações: 2009/2011. Departamento de Ciências da Computação da Universidade de Brasília. 2010. 29 p.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **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

8 ANEXO A

PRODUTO TECNOLÓGICO – Artigo submetido para publicação no periódico Cadernos de Prospecção submissão realizada em 11 de fevereiro de 2019.

UM PANORAMA DA ABORDAGEM DA SEGURANÇA DA INFORMAÇÃO NA PROPRIEDADE INTELECTUAL PELAS INSTITUIÇÕES DE CIÊNCIA E TECNOLOGIA

Autores: Paulo Cesar Andrade Arruda
Marcio Lima da Silva
Edilson da Silva Pedro

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 relacionadas à Propriedade Intelectual. Para esta análise foram selecionadas Instituições de renome internacional, divididas em três estrangeiras (Harvard, MIT e Oxford) e quatro nacionais (UFSC, UFRJ, UnB e Unicamp). A metodologia utilizada usou 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 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, tais como a proteção de ativos intangíveis e a transferência de tecnologias. Observou-se que, comparando-se as ICTs nacionais com as estrangeiras, estas apresentam um Sistema de Gestão de Segurança da Informação mais abrangente, em relação à PI. Destacou-se ainda, que as normas e as diretrizes das ICTs nacionais, para segurança da informação, são direcionadas para TI, não abordando aspectos importantes para PI.

Palavras-chave: segurança da informação. propriedade intelectual.

A PANORAMA OF THE INFORMATION SECURITY APPROACH ON INTELLECTUAL PROPERTY BY THE SCIENCE AND TECHNOLOGY INSTITUTIONS

ABSTRACT

The present study presents a national and international panorama of the information security controls used by Science and Technology Institutions (STIs) in their activities related to Intellectual Property. For this analysis, internationally renowned institutions were selected, divided into three foreign universities (Harvard, MIT and Oxford) and four Brazilian universities (UFSC, UFRJ, UnB and Unicamp). The methodology used used as a reference the recommendations of ABNT NBR ISO / IEC 27001 and 27002, and allowed mapping the main controls adopted by the ICTs, besides indicating the Institutions that have a more complete and comprehensive Information Security System (ISMS). From this mapping, the impact of the main controls on the institutional activities involving Intellectual Property was analyzed. It was concluded that the adoption of an ISMS is crucial for the development of activities related to Intellectual Property, such as the protection of intangible assets and the transfer of technologies. It was observed that, comparing national and foreign ICTs, they present a more comprehensive Information Security Management System in relation to IP. It was also pointed out that the norms and guidelines of national ICTs for information security are directed to IT, not addressing important aspects of IP.

Keywords: information security. intellectual property.

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 revistas especializadas em segurança da informação, reforçaram a necessidade das instituições em adotarem sistemas que reduzam os riscos de comprometimento dos seus bancos de dados (DHILLON e TORKZADEH, 2006). O investimento em sistemas para proteção de dados também aumentou, 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 et al., 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 e LUTHANS, 2003).

A segurança da informação depende de um conjunto de processos bem executados com políticas e regulamentos bem fundamentados. Neste cenário são definidos os níveis de proteção que devem ser implementados na segurança envolvendo a área jurídica, os recursos humanos, a administração, bem como, 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 utilizada para difusão da informação e possibilita a conexão entre todos os usuários. Neste sentido, essas estruturas devem primar pela segurança da informação, principalmente no que tange a confiabilidade, integridade e 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, pela perda de receita e produtividade (AHMAD et al., 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 desta questão, uma vez que ela 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 como um todo, visto que neste ambiente são produzidas novas tecnologias, tais como produtos e processos, ou seja, um ambiente onde a inovação faz-se presente (YILMAZ e YALMAN , 2016).

Em pesquisa recente realizada por YILMAZ e YALMAN, em 2016, nas universidades da Índia foi objeto de estudo a importância dada à segurança da informação dentro dessas instituições de ensino. Dentre as universidades pesquisadas por YILMAZ e YALMAN, verificou-se que aquelas universidades que utilizavam de 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 segurança da informação (YILMAZ e 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 e YALMAN, 2016).

Segundo Lyra (2016), durante o tempo 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 por meio da 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 tratam-se de informações tecnológicas, como é o caso de pesquisa e desenvolvimento. A própria Organização Mundial de 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 visem proteger o patrimônio informacional das instituições, a fim de garantir sua integridade e disponibilidade.

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 do mesmo nas organizações contribui para a preservação da confidencialidade, integridade e 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 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 nº 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 neste contexto, pois tratam de informações sensíveis, que requerem cuidados especiais, tais 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, implementados 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, onde se observa a importância da adoção de medidas que visem 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 estas políticas, na Propriedade Intelectual, e, consequentemente, o nível de sensibilização destas Instituições em relação à segurança da informação e as estratégias escolhidas por elas adotadas para tratar esse tema.

As universidades são alvos preferenciais de ataques cibernéticos, que visam comprometer a integridade de informações relacionadas a pesquisas científicas nessas instituições (MIT, 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, 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 epidêmicas por natureza (MIT, 2018).

Algumas informações consideradas confidenciais necessitam de cuidados e manuseios especiais. A manipulação inadequada dos dados pode trazer sérias consequências para o indivíduo e para a instituição, como: penalidades, roubo de identidade, perda financeira, invasão de privacidade ou acesso não autorizado por um ou por vários indivíduos. Os dados também podem estar sujeitos a regulamentação por leis estaduais ou federais e, nesses casos há necessidade que seja realizada a notificação no caso de uma divulgação (MIT, 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 (MIT, 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 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, 2013).

Atualmente, diversas ICTs nacionais e estrangeiras utilizam-se de uma política de segurança da informação para proteger seus dados e informações sensíveis, principalmente, aqueles relacionados à Pesquisa e à Propriedade Intelectual. No trabalho publicado em 2016, por YILMAZ, foi realizada uma análise comparativa dos sistemas de informação em uso nas universidades da Turquia e os riscos associados à segurança da informação. Neste estudo observou-se que os sistemas institucionais de gerenciamento de segurança da informação são cruciais para a proteção das propriedades da informação; e que as universidades que planejaram ou conduziram esforços para obter uma certificação ISO/IEC 27001 diminuíram os riscos de segurança da informação, aplicando os procedimentos da ISO/IEC 27001 (YILMAZ e YALMAN, 2016).

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 utilizar a técnica de análise por amostragem, onde, inicialmente, foi definido o universo de estudo, a partir da seleção de Instituições de renome nacional e internacional, considerando entidades estrangeiras e nacionais. As Instituições estrangeiras escolhidas foram a Universidade de Harvard, o Instituto de Tecnologia de Masschusetts - 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 estas ICTs, tendo como referencial o previsto na norma ABNT NBR ISO/IEC 27002 (ABNT, 2013), 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, 2018); Política de Informação do MIT (MIT, 2018); Política de Segurança da Informação da Universidade de Oxford (OXFORD, 2018); 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, foi adotado, 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, por se tratar 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. Nesta 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, gerenciamento das operações e comunicações, gestão de ativos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, criptografia, 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, apresentados em Publicação em Propriedade Intelectual do NUPITEC (GHESTI, 2016).

RESULTADOS E DISCUSSÃO

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, 2013), utilizados pelo grupo de ICTs estudadas, foi possível identificar as Instituições que possuem um SGSI mais abrangente e quais controles são 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 de Instituições, que os incluíram em suas legislações internas de segurança da informação. A compilação dos controles por ICT é apresentada na Tabela 1.

Inicialmente, pode-se observar que, dentre 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 10 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 13 pontos, situação na qual todos os treze 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, onde 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.

Tabela1: Mapeamento de controles, previstos na Norma ISO 27002, por Instituições de Ciência e Tecnologia – ICTs.

Controle/Domínio (Norma ISO 27002 e 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 Operações e 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	-	-	-	-	-	-	-	-
Relacionamento na Cadeia de Suprimento	-	-	-	-	-	-	-	-
Segurança da Informação na Gestão da Continuidade do Negócio	1	1	-	-	-	-	-	2
Abrangência da Política	**10**	**10**	**8**	**5**	**5**	**1**	**8**	**-**

Fonte: Autoria própria (2018).

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 operações e comunicações. A partir deste resultado para os controles utilizados mais comumente pelas ICTs, foi realizada uma análise da influência destes principais controles na Propriedade Intelectual.

Controle de Acesso

Na Norma ABNT NBR ISO/IEC 27001 (ABNT, 2013) 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, 2013). 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, tais como no caso do inventor ter protegido a sua tecnologia, como, 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 deve ficar restrito ao período em que não houve a sua divulgação oficial. Nesse contexto, faz-se necessária a restrição de acesso às informações referentes a essas tecnologias, por meio de normas e 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 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.

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 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 a 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 anteriormente, 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 normalmente as normas de segurança não são bem conhecidas pelos usuários. Para um inventor, bem como 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 NITs, no intuito de propiciar maior segurança nas ações a serem desenvolvidas, bem como 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, compartilhamento e comunicação de material didático, 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 como um todo, 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 nestes processos saibam como tratar de forma segura determinadas informações e como agir em relação aos contratos e convênios estabelecidos com outros órgãos públicos ou privados.

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 operação da segurança da informação, dentro das Instituições. Para que este controle cumpra o seu papel, estas normas orientam que sejam levados em consideração alguns aspectos, tais como responsabilidades e papéis pela segurança da informação, a segregação de funções, 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 deste 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.

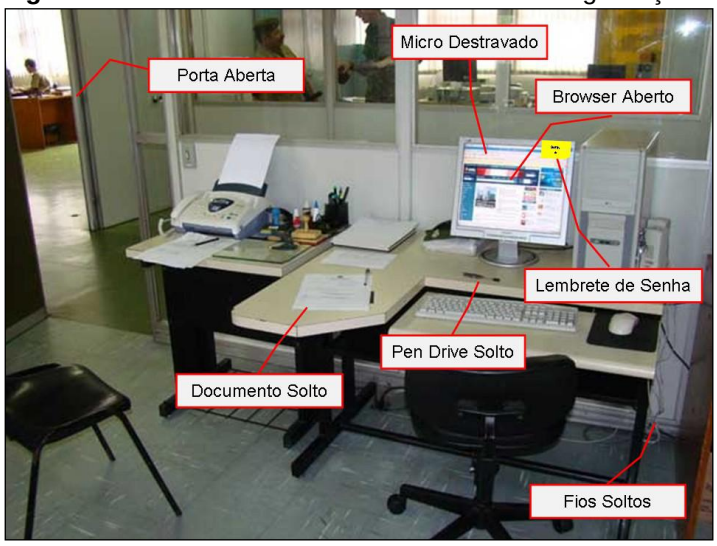
Da análise deste controle, pode-se concluir, que a sua adoção é muito importante para as ICTs, pois deixa claro aos usuários, pesquisadores e profissionais de PI quem são os responsáveis pela segurança da informação e quais são as penalidades advindas do descumprimento de normas de segurança envolvendo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

Segurança Física e do Ambiente

A segurança física e do ambiente visa prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização, bem como impedir perdas, danos, roubo ou comprometimento de ativos e interrupção das operações (Norma ISO 27001). A norma ISO 27001 estabelece que este controle, quando aplicado, deve dar atenção às áreas consideradas seguras, principalmente às 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 podem evitar a exposição e acesso indevido às informações tramitadas nesses ambientes, conforme ilustrado na **Figura** .

Figura 1: Ambiente de trabalho com falhas de segurança.



Fonte: 3º CTA (2011, p. 9).

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 que a documentação tramitada, seja em mídia digital ou física, contém informações relevantes sobre os processos de proteção e transferência de tecnologia. A aplicação deste 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 onde são processadas as informações de PI, principalmente, os ambientes de NITs e escritórios de inovação onde são tratados assuntos de acesso restrito e cuja área necessita de ser controlada.

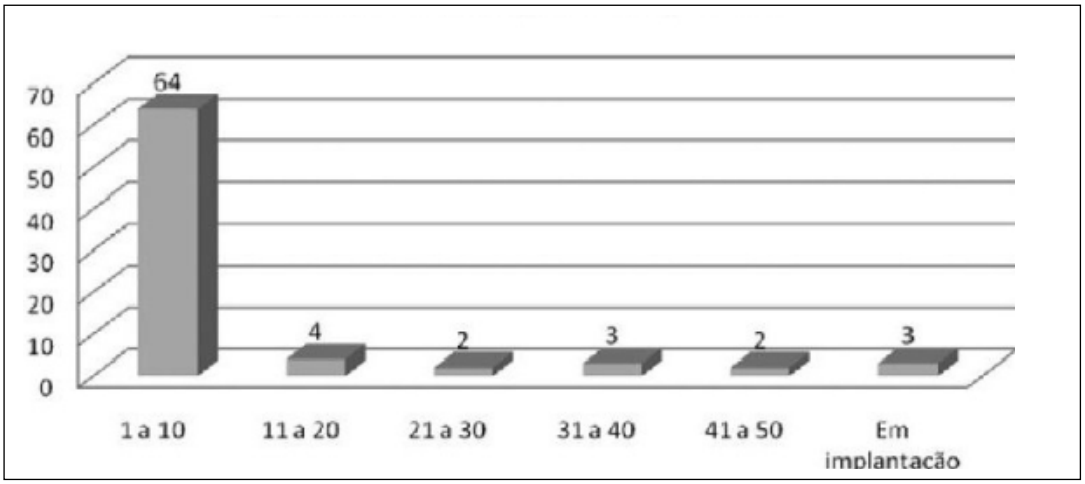
Segurança em Recursos Humanos

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 por 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, termos e condições de contratação, conscientização, educação e treinamento em segurança da informação, 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, operações e 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 estas informações. Atualmente, muitos dos profissionais que trabalham nos NITs, encarregados dos processos de proteção de tecnologias e nas atividades de transferências de tecnologia, são temporários o que ocasiona uma rotatividade muito grande, oferecendo vulnerabilidade aos sistemas de proteção como um todo. A implementação desse controle nas ICTs pode contribuir para uma 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.

A contratação e capacitação de pessoal foram consideradas as principais deficiências e apontados como partes mais importantes por 77% dos NITs. Isso pode ser observado uma vez que a 82% apontaram não possuir mais de 10 pessoas trabalhando na sua estrutura, conforme apresenta o **Gráfico 1**. Em segundo lugar, a falta de competências e habilidades em transferência de tecnologia foram citadas por 68%. Além disso, a falta 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% deles como muito importantes (TORKOMIAN, 2009).

Gráfico 1: Quantidade de pessoas por NIT.



Fonte: Torkomian (2009).

Conclui-se que a adoção desse controle, nos processos de PI contribui diretamente para a melhoria da segurança da informação, uma vez que a presença de profissionais cada vez 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.

Segurança nas Operações e Comunicações

A segurança nas operações e comunicações visa assegurar a proteção das informações, em redes e dos recursos de processamento da informação, que as apoiam, bem como a manutenção da segurança da informação transferida dentro da

organização ou com as entidades externas (ABNT, 2013b). 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 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 que as redes de dados sejam 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.

Demais controles das normas ABNT ISO/IEC 27001 e 27002

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

CONCLUSÃO

O presente estudo permitiu verificar que a adoção de um SGSI é crucial para o desenvolvimento de atividades relacionadas à Propriedade Intelectual, tais 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 respeito, que parceiros e sociedade possuem dessas Instituições. O estudo demonstrou que a família de normas ISO 27000, em especial as normas ISO 27001 e 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 as 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 estas Instituições. Outro ponto que se destacou, foi que as políticas de gestão de PI nessas Instituições, faz 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. Destacou-se a estrutura e a gama de informações disponibilizada 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 visam 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, implementado em Harvard e no MIT pode servir de modelo para as ICTs nacionais. Este 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 onde 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 direcionada às questões de TI.

A UnB não apresenta normativos específicos para a segurança da informação relacionados a assuntos relacionados à Propriedade Intelectual. Apesar disso, a ferramenta SEI, utilizada no gerenciamento eletrônico de processos, associado às informações disponibilizadas no site da instituição, que poderiam permitir a implementação de um SGSI amplo e eficiente dentro da Instituição, não atendem, atualmente, a todos os requisitos de um SGSI relacionados à PI. A plataforma SEI atende 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 relacionadas à segurança de informações para PI. Nesse contexto, tem-se como perspectivas para futuros trabalhos, 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

3º Centro de telemática de Área (CTA). **Apostila de Segurança Aplicada à Segurança da Informação**. São Paulo, 2011.

ABNT. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2013**. 2a. ed. Rio de Janeiro, 2013a.

ABNT. **Tecnologia da informação - Técnicas de segurança – Gestão de riscos de segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013b.

AHMAD, A., Bosua, R. and Scheepers, R. (2014), "**Protecting organizational competitive advantage: a knowledge leakage perspective**", Computers & Security, Vol. 42, pp. 27-39.

ASLLANI, A. and Luthans, F. (2003), "**What knowledge managers really do: an empirical and comparative analysis**", Journal of Knowledge Management, Vol. 7 No. 3, pp. 53-66.

BACHLECHNER, D., Thalmann, S. and Manhart, M. (2014), "**Auditing service providers: supporting auditors in cross-organizational settings**", Managerial Auditing Journal, Vol. 29 No. 4, pp. 286-303.

DHILLON, G. and TORKZADEH, G. (2006), **Value-focused assessment of information system security in organizations**, Information Systems Journal, Vol. 16 No. 3, pp. 293-314.

DSIC/ GSIPR. **Norma Complementar 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. Norma Complementar nº 20/IN01/DSIC/GSIPR de 15 de dezembro de 2014

FONTES, E. **Praticando a segurança da informação**. 1ª ed. Rio de Janeiro: Brasport, 2008.

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**. Disponível em:< https://vpr.harvard.edu/pages/research-data-security-and-management>. Acesso: em 10 out.2018.

LEE, S.C., Chang, S.N., Liu, C.Y. and Yang, J. (2007), "**The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance**", Knowledge and Process Management, Vol. 14 No. 1, pp. 58-69.

LYRA, Maurício Rocha. Segurança do Patrimônio Intangível. In: FOINA, P. R (Org). **Planejamento Estratégico para Empresas de Base Tecnológica**. 1ª ed. Brasília: Instituto CEUB de Pesquisa e Desenvolvimento - ICPD, 2016.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT). **MIT Policies**. 13.0 Information Policies. Massachusetts: Cambridge, [20--]. Disponível em:<

https://policies.mit.edu/policies-procedures/130-information-policies>. Acesso em: 17 out. 2018.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT). **Information Protect @ MIT**. Massachusetts: Cambridge, [20--]. Disponível em:< https://infoprotect.mit.edu/>. Acesso em: 17 out. 2018.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES - MCTI. Secretaria de Desenvolvimento Tecnológico e Inovação. **Política de Propriedade Intelectual das Instituições Científicas, Tecnológicas e de Inovação do Brasil: relatório FORMICT 2016**. Brasília, DF: MCTIC, 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.

NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambientes Cooperativos**. 1ª ed. São Paulo: Novatec Editora, 2007.

NORMAN, P.M. (2002), "**Protecting knowledge in strategic alliances: resource and relational characteristics**", The Journal of High Technology Management Research, Vol. 13 No. 2, pp. 177-202.

YILMAZ, R. and YALMAN Y. **A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks**. TEM Journal, Vol 5, Iss 2, Pp 180-191 (2016), [s. l.], n. 2, p. 180, 2016. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.71d180d6b918456ea51fb766196d292d&lang=pt-br&site=eds-live&authtype=ip,uid>. Acesso em: 19 set. 2018.

TORKOMIAN, Ana Lúcia Vitale. Panorama dos Núcleos de Inovação Tecnológica no Brasil.
In: T**ransferência de Tecnologia: Estratégias para estruturação e gestão de Núcleos de Inovação Tecnológica**. Campinas, SP: Komedi, 2009.

UNIVERSIDADE DE BRASÍLIA (UnB). **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.

UNIVERSIDADE ESTADUAL DE CAMPINAS (Unicamp). **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.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ). **Portaria nº 4579, 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.

UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). **Portaria nº 1754/2015/GR, de 09 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 (1) to No 5140, 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.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **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

9 ANEXO B

Relatório Final de Oficina Profissional

Em atendimento (NIT50) Oficina Profissional do Projeto Pedagógico do PROFNIT (6 créditos)

Dados do aluno			
Ponto Focal	UNIVERSIDADE DE BRASÍLIA	**Ano de ingresso**	2017
Nome do aluno	PAULO CESAR ANDRADE ARRUDA		
Semestre em que cursa a disciplina	1ºSEMESTRE/2018	**Período da Oficina Profissional**	1ºSEMESTRE/2018
Dados da Oficina Profissional			
Organização	CENTRO DE APOIO AO DESENVOLVIMENTO		
Setor da organização			
Marcar todos os setores da sociedade em que se insere a organização	(X) Setor Acadêmico; ☐ Setor empresarial: (X)Setor Governamental;	☐ Sociedade Organizada Não-Governamental; ☐ Outro	
Nome Supervisor	SÔNIA MARISE SALLES CARVALHO		
CPF Supervisor	437.645.096-00	**Celular do Supervisor**	(61) 99263-0196
Email do Supervisor	Smarises1960@gmail.com	**Telefone Supervisor**	(61) 3107-4120
Houve alteração do que foi aprovado? **Se sim, explique e justifique**	NÃO.		
Título	ESTUDOS DE INOVAÇÃO ENTRE AMBIENTES DE INOVAÇÃO		
Marcar todas as atividades em que atuou	(x) Legislação e políticas públicas referentes a propriedade intelectual e transferência de tecnologia para inovação tecnológica; ( ) Políticas de estímulo à proteção das criações; ( ) Avaliação da conveniência da proteção das criações e sua divulgação; (X) Processamento de pedidos e de manutenção dos títulos de propriedade intelectual; (X) Licenciamento, inovação e outras formas de transferência de tecnologia; (X) Estudos de prospecção tecnológica e de inteligência competitiva no campo da propriedade intelectual, de forma a orientar as ações de inovação; (X) Estudos e estratégias para a transferência de inovação; (X) Promoção e acompanhamento de relacionamento academia-empresa; ( ) Negociação e gestão de acordos de transferência de tecnologia; (X) Atividades rotineiras de diálogo e de ações academia-empresa, interagindo propositivamente com os diversos setores.		

Resumo das atividades realizadas (até 150 palavras)	As atividades foram realizadas na Agência de Gestão e Inovação Tecnológica do Exército (AGITEC) e no Centro de Apoio ao Desenvolvimento e Tecnológico (CDT). Neste período foram realizadas visitas, entrevistas, leitura de documentação relacionada aos processos e atividades, acompanhamento das atividades desenvolvidas pela Multincubadora e NUPITEC do CDT e visita com mapeamento dos processos da AGITEC. Nesta oportunidade foram gerados relatórios com o objetivo de servir de subsídios para a melhoria das atividades desenvolvidas nestes órgãos.

Atividades desenvolvidas (até 1.000 palavras)	As atividades foram desenvolvidas no Centro de Apoio ao Desenvolvimento Tecnológico (CDT) todas as sextas-feiras e em outros dias da semana de forma inopinada, sempre no período da tarde durante o primeiro semestre de 2018. Também foi realizado o monitoramento das atividades desenvolvidas pela Agência de Gestão e Inovação Tecnológica do Exército (AGITEC), situada no Rio de Janeiro no mês de março de 2018 e posterior videoconferências com a equipe da AGITEC para dar continuidade aos trabalhos iniciados. Durante o período de permanência no CDT foi realizado o acompanhamento dos trabalhos desenvolvidos na Multincubadora de Empresas e no Núcleo de Propriedade Intelectual - Nupitec. O objetivo da oficina foi conhecer os processos em andamento e propor algumas sugestões de melhorias para cada setor e divisão integrante da Multincubadora e do Nupitec do CDT. Durante este processo foram realizadas coletas de dados para levantamento dos pontos fortes, as fraquezas, ameaças e oportunidades de melhoria para cada área percorrida e, ao final, gerado um relatório da Multincubadora e outro do Nupitec. O objetivos desses relatórios foi apresentar uma visão com olhar externo sobre o funcionamento dos processos internos para que os mesmos possam ser aperfeiçoados. Na AGITEC foi realizada uma visita e reuniões por videoconferência com o objetivo de mapear os principais processos executados pela AGITEC. Nesta ocasião também foram apresentadas oportunidades de melhoria para a estruturação da AGITEC baseado nas melhores práticas desenvolvidas pelo CDT, em especial no NUPITEC, na Multincubadora e em outros órgãos. Foi possível verificar a estrutura da AGITEC e os seus macroprocessos: Inteligência e Prospecção Tecnológica, Gestão da Propriedade Intelectual e Gestão do Conhecimento. Pelo que se pode observar, o resultado do macroprocesso de inteligência e prospecção tecnológica indica no curto prazo, quais as linhas de pesquisa devem ser incentivadas para desenvolvimento de inovações. O macroprocesso de gestão do conhecimento registra os conhecimentos de como são desenvolvidas as inovações para divulgação, capacitação e promoção da cultura inovadora. Assim, os processos inovativos seguintes são executados com base em experiências pregressas. Importante se faz ressaltar que os conhecimentos aplicados ficam sob a gestão da Seção de Inteligência e Prospecção Tecnológicas, enquanto os conhecimentos de uso, especialmente as metodologias utilizadas, ficam a cargo da Seção de Gestão do Conhecimento. O macroprocesso de Gestão da Propriedade Intelectual tem a finalidade de apropriar as inovações desenvolvidas, registrando-as junto aos órgãos de registro de propriedade intelectual. Também tem a missão de pesquisar a existência de registros das inovações já existentes com vistas a encontrar neles as lacunas que permitam o desenvolvimento de outras inovações. Nas reuniões com a equipe da AGITEC foram realizadas consultorias para aquisição de um sistema de Tecnologia da Informação para auxiliar na gestão dos processos já mencionados. Como instrumento de coleta de dados foram analisadas as fontes secundárias, composta de documentos e relatórios do CDT e da AGITEC e as fontes primárias, compostas por entrevistas com os integrantes de cada setor, bem como a aplicação da análise SWOT para as equipes. Dentro da carga horária destinada à Oficina Profissional foram gastos cerca de 40 horas nas atividades da AGITEC e 60 horas no CDT. Todo o processo desenvolvido na Oficina profissional foi coordenado pela Professora Sônia Marise Salles Carvalho, no CDT e contou com a colaboração dos integrantes das diversas seções do CDT.

Houve geração de produtos de sua autoria? **Se sim, marque todos os que se apliquem**	( ) a) Elaboração e encaminhamento de pedidos de registros de propriedade intelectual, bem como depósito de software livre em repositório reconhecido ou obtenção de licenças alternativas ou flexíveis para produção intelectual, desde que demonstrado o uso pela comunidade acadêmica ou pelo setor produtivo; ( ) b) Construção de base de dados técnico-científicas; ( ) c) Desenvolvimento de aplicativos e materiais didáticos e instrucionais e de produtos, processos e técnicas; ( ) d) Desenvolvimento de tecnologias sociais; ( ) e) Produção de programas de mídia; (X) f) Elaboração de relatórios técnicos com regras de sigilo; (X) g) Elaboração de relatório relativo à proposição ou a avaliação de programas, projetos e políticas institucionais ou públicas; ( ) h) Elaboração de manuais de operação técnica, protocolo experimental ou de aplicação ou adequação tecnológica; ( ) i) Elaboração de projetos de inovação tecnológica; projeto de aplicação ou adequação tecnológica; ( ) j) Elaboração de processos de gestão de inovação; ( ) k) Curadoria de coleções biológicas; ( ) l) Editoria; ( ) m) Elaboração de artigos originais e publicações tecnológicas.
Se gerou produtos, descrevê-los (até 150 palavras) **Anexar comprovantes desses produtos**	Foram gerados relatórios referentes aos processos da AGITEC (sob sigilo) e os processos do NUPITEC do CDT. O relatório do NUPITEC descreve as principais atividades desenvolvidas por esse setor e ainda realiza uma análise SWOT, no intuito de apresentar as principais ameaças, pontos fortes, oportunidades e fraquezas desse setor. Os dados levantados, com posterior análise visam apontar algumas soluções e alertar sobre as prioridades que devem ser dadas a esses problemas.
Vai utilizar no seu TCC?	( ) Sim (X) Parcialmente ( ) Não
Assinatura do Supervisor	
Assinatura do Coordenador do Setor	
Assinatura do aluno	
Assinatura docente Responsável Institucional pela disciplina	

Curso: Mestrado Profissional em Propriedade Intelectual e Transferência de Tecnologia para Inovação
Disciplina: Oficina Profissional
Professora: SÔNIA MARISE SALLES CARVALHO
Aluno: PAULO CESAR ANDRADE ARRUDA

ANEXO AO RELATÓRIO DA OFICINA PROFISSIONAL
RELATÓRIO NUPITEC

1. OBJETIVO DO TRABALHO

Este trabalho tem por objetivo apresentar uma visão geral do NUPITEC, com foco nos processos e realizar uma análise SWOT, com vistas a possibilitar a identificação de pontos fortes, fraquezas, oportunidades de melhoria e ameaças, no intuito de dar um diagnóstico do trabalho desenvolvido nesse setor do Centro de Apoio ao Desenvolvimento Tecnológico (CDT).

2. INTRODUÇÃO

O CDT atua oficialmente como o Núcleo de Inovação Tecnológica (NIT) da Universidade de Brasília, conforme previsto na Lei de Inovação (10.973/2004). Essa designação foi formalizada por meio do Ato da Reitoria nº 882/2007.

O Núcleo de Propriedade Intelectual (Nupitec), que faz parte do NIT da UnB, atua de acordo com a Resolução do CAD nº 005/98, que dispõe sobre a proteção e alocação de direitos de propriedade intelectual, e é responsável pela proteção das tecnologias desenvolvidas pela comunidade acadêmica. Estas tecnologias podem ser pesquisas ou projetos passíveis de proteção por patente, além de programas de computador, marcas, cultivares, desenhos industriais e outras modalidades de proteção. Este Núcleo atende a comunidade acadêmica da UnB, empresas interessadas em parcerias e também inventores independentes, como previsto na Lei de Inovação.

O Nupitec apoia o pesquisador nos procedimentos relacionados à proteção, entre eles, a análise da invenção, a elaboração da redação de patente, o depósito e o acompanhamento dos pedidos de proteção junto ao Instituto Nacional da

Propriedade Industrial (INPI), órgão do governo responsável por este tipo de proteção. O Nupitec é também responsável pela formalização de parcerias (casos de cotitularidade, cooperação técnica, desenvolvimento de tecnologias e confidencialidade) que envolvem Propriedade Intelectual.

Dentro desse contexto foi realizada uma visita e entrevista com integrantes do NUPITEC com o objetivo de colher o maior número possível de dados para servir de subsídios para geração de um relatório que pudesse dar um diagnóstico e apontar caminhos para a solução de alguns dos problemas relacionados com a proteção das tecnologias. Dessa forma, também, indicar soluções para melhorar a produtividade e qualidade dos processos finalísticos realizados nesse setor.

3. DESENVOLVIMENTO

3.1 RECURSOS HUMANOS

Atualmente a equipe responsável pelos trabalhos de proteção do NUPITEC é formada por sete redatores, sendo dois da área de biologia, dois da área de química, dois da área de engenharia e a professora Grace que atua como supervisora dos trabalhos. Este número de redatores já chegou a 13 (treze) em outros momentos. Todos os redatores são capacitados para a função e a maioria tem curso de mestrado e alguns de doutorado. Esta mesma equipe é responsável por realizar todos os trabalhos de proteção envolvendo: marcas, patentes, desenho industrial e etc. Todos os redatores, com exceção da Profª. Grace são bolsistas da FUB. Há uma grande rotatividade dos integrantes da equipe uma vez que o salário não é tão atrativo e tendo em vista a forma de contratação por meio de bolsa de pesquisa. A equipe, no entanto, apresenta um alto padrão de qualidade dos trabalhos realizados.

Normalmente procura-se dividir os trabalhos entre os redatores em função da característica da tecnologia e afinidade e especialização dos redatores. No entanto, todos os integrantes da equipe do são treinados em todas as funções e tipos de proteção, de forma que não haja solução de continuidade das atividades que estão sendo desenvolvidas, mesmo quando há falta de algum dos integrantes da equipe.

3.2 ATIVIDADES DESENVOLVIDAS

O NUPITEC é responsável por realizar todo o trabalho de proteção das inovações junto aos professores e pesquisadores da FUB. Importante ressaltar que

por força de legislação o NUPITEC fica restrito a realizar as atividades de proteção de integrantes da FUB. Dessa forma, os pedidos de proteção oriundo de outros setores, ou mesmo externos ao CDT não são permitidos. O máximo que ainda é realizado, mas de forma bem simples é uma consultoria não formalizada para alguns atores do CDT que não se enquadram na situação de funcionários da FUB. Todavia esse assessoramento tende a ser extinto em função do grande volume de trabalho em comparação com o reduzido número de pessoas do NUPITEC.

A realização de um processo de proteção é demorada, principalmente em se tratando de patentes. Normalmente leva-se cerca de dois meses para se realizar uma busca exaustiva de anterioridade e mais cerca de oito meses para se realizar uma redação de patente. A média é de 12 (doze) redações de patentes anuais no NUPITEC. Muitas vezes o trabalho tende a ser elevado em função da necessidade da presença do inventor para acompanhar e aprovar o processo de redação de patentes e também os prazos impostos pelo INPI. O total de proteções realizadas chega a 90 (noventa) por ano. Nesse número são contabilizadas as proteções por: marcas, desenho industrial, registro de software. A meta de pedidos de patentes estipulada pela chefia do CDT é de 15 (quinze) redações de patentes anuais para cada redator.

Tabela 1: Resultados dos trabalhos de proteção do NUPITEC
Dados atualizados a partir de junho de 1999 até a presente data.

Ativos Intangíveis Protegidos	Quantidade
Depósitos de Patentes	99
Depósitos de Patentes Cotitulares	84
Depósitos de Patentes Internacional	52
Programa de Computador	113
Desenho Industrial	28
Marcas	70
Cultivares	16
Direito Autoral	4
Total de Patentes Nacionais Concedidas	17
Total de Patentes Internacionais Concedidas	21
Total de Depósitos de Patentes	235

Total de Ativos Protegidos	466

Fonte:http://www.cdt.unb.br/programaseprojetos/nupitec/resultados/?menu-principal=programas-e-projetos&menu-action=resultados

O processo de proteção junto aos inventores envolve:

1) Receber o inventor da tecnologia e ouvir o relato da sua invenção;
2) Selecionar a tecnologia que tem possibilidade de proteção;
3) Realizar o enquadramento do tipo de proteção ou proteções;
4) Realizar a redação da patente ou outro tipo de proteção;
5) Realizar o acompanhamento administrativo de proteção junto ao INPI, inclusive com o cálculo e pagamento das taxas referentes aos depósitos;
6) Manutenção de sigilo de todo o processo de gestão da proteção.
7) Encaminhamento do pedido de proteção finalizado ao setor de transferência de tecnologia do CDT para fins de comercialização da tecnologia.

O próprio site do CDT indica a forma como é realizado o atendimento à Comunidade Acadêmica pelo NUPITEC. A informação é de que o atendimento é feito por uma equipe de prospecção de tecnologias, vinculada ao NIT da UnB, que tem por objetivo visitar laboratórios nas Unidades Acadêmicas a fim de entrevistar pesquisadores (grupos de pesquisa) para identificar tecnologias passíveis de proteção. Caso o pesquisador tenha desenvolvido uma pesquisa ou projeto passível de proteção e ainda não recebeu a visita da equipe de prospecção, pode entrar em contato direto com o Nupitec. Cabe ressaltar, que em função do número reduzido de redatores no NUPITEC, atualmente não tem ocorrido essa visita de prospecção tecnológica. Na seção que trata de divulgação será abordado com mais propriedade essa questão.

De acordo com as orientações contidas no site do CDT são realizados alguns procedimentos pela equipe do NUPITEC junto aos inventores:

1) Entrevista - receber o inventor da tecnologia e ouvir o relato da sua invenção. São realizadas algumas perguntas a fim de esclarecer também questões sobre a viabilidade ou não de proteção do invento.
2) Preenchimento de formulário de invenção - enquadramento quanto ao tipo de proteção e abertura de atendimento em um formulário.
3) Busca de Anterioridade – é neste momento que é realizada a busca em bases de patentes tanto nacionais como internacionais, com o objetivo de

saber se existe alguma invenção similar, patente desse invento ou mesmo saber o estado da técnica da invenção.

4) Redação da Patente – uma serie de documentos que compõem esse pedido serão preenchidos no intuito de dar entrada no pedido de patente. Esses documentos são preenchidos pelo pesquisador em conjunto com o redator do NUPITEC.
5) Encaminhamento do Pedido ao INPI - Realizar o acompanhamento administrativo de proteção junto ao INPI, inclusive com o cálculo e pagamento das taxas referentes aos depósitos.
6) Acompanhamento do pedido nos trâmites do INPI – esse acompanhamento em todas as fases do processo é realizado junto ao INPI por meio de software específico e pela Revista de Propriedade Industrial (RPI).
7) Transferência de Tecnologia – com a possibilidade de comercialização dessa tecnologia por meio de licenciamento ou outra forma, a mesma é encaminhada à Agência de Comercialização de tecnologia (ACT) do CDT que passará a conduzir esse processo, desvinculando do NUPITEC.

Importante ressaltar que em função da grande quantidade de trabalho realizada no NUPITEC, fica inviável a realização da atividade de prospecção tecnológica nesse setor do CDT. Atualmente existem cerca de 100 (cem) tipos de tecnologia na fila de espera do NUPITEC para serem redigidas e encaminhadas ao INPI. Há certa resistência de alguns professores em realizar a proteção de software, em função das questões de direito autoral.

A realização dos trabalhos de redação, principalmente de patentes, requer além de conhecimento técnico especializado o conhecimento da metodologia utilizada pelo INPI. Nesse sentido, todos os redatores devem dominar o conteúdo das Instruções normativas do INPI e demais recomendações para fazer a redação de patente. Importante ressaltar que essas instruções são bem detalhadas e extensas e requer estudo e dedicação para a realização das redações.

3.3 INFRAESTRUTURA

Atualmente o NUPITEC ocupa uma sala de escritório de tamanho modesto para o número de pessoas que ali trabalha, tendo em vista a necessidade de receber os inventores para as entrevistas e acompanhamentos das redações. Todos os redatores possuem desktop para realização do trabalho com acesso à internet e material de escritório.

As bases de dados de patentes consultadas para fins de busca de anterioridade são livres, como: INPI, USPTO, Google Patents, Espacenet, etc. O CDT não dispõe de bases pagas para a realização desse trabalho. Há também uma ferramenta utilizada para gerenciamento das patentes e demais proteções disponibilizada pelo CDT, sendo que este instrumento é pago com recursos do centro. A maioria dos redatores utiliza essa ferramenta para realizar o backup, mas também mantém os dados em planilhas do Excel arquivados no próprio desktop de trabalho.

Os serviços de acesso e uso de ferramentas é compartilhado com outros usuários do CDT, ou seja, não há um servidor exclusivo para as atividades do NUPITEC.

Não é permitida a entrada de pessoas não autorizadas na sala do NUPITEC, mesmo que sejam integrantes do CDT. O objetivo é manter sigilo e segurança para as tecnologias que estão sendo avaliadas e protegidas. Esse controle é rigoroso e com avisos sobre a restrição de acesso.

3.4 DIVULGAÇÃO

A divulgação das atividades do NUPITEC em termos de proteção é realizada por meio de eventos, sendo o principal o “INOVATECH”, que acontece 02 (duas) vezes por ano. Há também a divulgação e orientação ao público interno por meio de palestras agendadas e sob a demanda dos setores da UnB. Importante destacar que a divulgação realizada nesses eventos normalmente tende a surtir o efeito desejado após dois ou três anos, quando o pesquisador vai necessitar efetivamente dos trabalhos do NUPITEC.

O NUPITEC não oferece cursos específicos, em função da grande demanda de trabalho diária e o número limitado de redatores. O INPI também não tem oferecido esses tipos de cursos em função da quantidade de pedidos de patentes aguardando solução.

3.5 ANÁLISE SWOT

Baseado nas entrevistas realizadas, leitura de documentação e relatórios realizados foi elaborada a análise SWOT abaixo:

	Fatores Internos	Fatores Externos
FATORES POSITIVOS	**Forças** - Equipe qualificada - Equipe Motivada - Sigilo das informações - Qualidade da redação de Patentes - Controle da documentação - Seleção das tecnologias - Proximidade dos pesquisadores	**Oportunidades** - Divulgação dos trabalhos por outros setores do CDT - Recebimento de outras fontes de recursos orçamentários - Capacitação da equipe de forma contínua - Contratação de bases pagas pelo CDT - Contratação de mais redatores - Mudança na forma de contratação de redatores
FATORES NEGATIOS	**Fraquezas** - Efetivo pequeno de redatores em comparação com a demanda - Rotatividade dos redatores - Local de trabalho pequeno - Recursos financeiros insuficientes - Baixo número de depósitos em relação à demanda - Divulgação insuficiente do NUPITEC - Impossibilidade de realizar prospecção em função dos trabalhos internos	**Ameaças** - Corte de recurso orçamentário - Mudanças na legislação de concessão de bolsas - Aumento no número de pedidos de proteção - Impossibilidade de renovação de bolsas dos redatores do NUPITEC

4. CONCLUSÃO

Após analise e acompanhamento das atividades desenvolvidas pelo NUPITEC fica claro que o trabalho realizado por esse setor é de alto nível, principalmente pela qualidade profissional e da equipe de trabalho. No entanto, algumas ações devem ser tomadas no intuito de aumentar a capacidade de

processamento das redações de patentes e de reter, na função, o profissional qualificado. Nesse sentido, ações no intuito de melhorar as relações de trabalho (tipo de contratação) e o valor pago ao profissional devem ser buscados, sob pena de reduzir ainda mais o efetivo de profissionais ou, até mesmo, inviabilizar as atividades desenvolvidas nesse setor.

10 ANEXO C

CHECK-LIST DE PROTOCOLO DE SEGURANÇA DA INFORMAÇÃO PARA INSTITUIÇÕES DE CIÊNCIA E TECNOLOGIA (baseado na Norma NBR ISO/IEC 27001 e 17799)

Checklist	Seção	Questão de auditoria	Sim	Não	Não se Aplica
1	***Política de Segurança da Informação***				
1.1	***Política de segurança da informação***				
1.1.1	Documento da política de segurança da informação	Se existe alguma política de segurança da informação, que seja aprovado pela direção, publicado e comunicado, de forma adequada, para todos os funcionários e alunos da ICT.			
		Se está expressa as preocupações da direção e estabelece as linhas-mestras para a gestão da segurança da informação relacionados com a propriedade intelectual.			
1.1.2	Análise crítica das políticas para segurança da informação	Se a política de segurança da ICT tem um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo de análise crítica definido.			
		Se as políticas de segurança da informação das ICts são analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem.			
2	***Organização da Segurança da Informação***				
2.1	***Organização Interna***				
2.1.1	Segregação de funções	Se as funções conflitantes e áreas de responsabilidade envolvendo propriedade intelectual são segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional.			
2.1.2	Coordenação de segurança da informação	Se existe um órgão interno com representantes da direção de áreas relevantes da ICT para coordenar a implementação de controles de segurança da informação envolvendo a propriedade intelectual.			
2.1.3	Responsabilidades e papéis da segurança da informação	Se as responsabilidades pela proteção de cada ativo relacionado com a propriedade intelectual e pelo cumprimento de processos de segurança específicos são claramente definidos na ICT.			
2.1.4	Processo de autorização para as instalações de processamento da informação	Se na ICT foi implantado um processo de gestão de autorização para novos recursos de processamento da informação. Isto deve incluir todos os novos recursos, como hardware e software aplicados nos processos de propriedade intelectual..			
2.1.5	Cooperação entre ICTs	Se são mantidos contatos apropriados com autoridades legais, organismos regulamentadores, provedores de serviço de informação e operadores de telecomunicações, para garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança envolvendo propriedade intelectual na ICT.			
2.1.5	Segurança da Informação no gerenciamento de projetos	Se a segurança da informação é considerada no gerenciamento de projetos envolvendo propriedade intelectual nas ICT e nos NIT.			
2.2	***Segurança no acesso de prestadores de serviço***				

2.2.1	Identificação no acesso de prestadores de serviço	Se os riscos do acesso de prestadores de serviço são identificados e controles de segurança apropriados foram implementados na ICT. Se os tipos de acesso são identificados, classificados e as razões para o acesso são justificadas nas ICT. Se os riscos de segurança com prestadores de serviço trabalhando no ambiente da ICT foram identificados e controles apropriados são identificados.			
2.2.2	Requisitos de segurança nos contratos com prestadores de serviço.	Se existe um contrato formal contendo ou referenciando todos os requisitos de segurança para assegurar a conformidade com as normas e políticas de segurança da informação.			
2.3	***Terceirização***				
2.3.1	Requisitos de segurança dos contratos da terceirização	Se os requisitos de segurança são definidos no contrato com prestadores de serviços, quando a ICT tiver terceirizado o gerenciamento e controle de todos ou alguns dos sistemas de informação, redes e/ ou estações de trabalho vinculados as atividades de propriedade intelectual.			
		O contrato deve definir como os requisitos legais são referenciados, como a segurança dos ativos é mantida e testada, e o direito de auditoria, características de segurança física e como a disponibilidade dos serviços é mantida em um evento de desastre.			
3	***Segurança em Recursos Humanos***				
3.1	***Antes da Contratação***				
3.1.1	Seleção e política de pessoal	Se verificações sobre a equipe de trabalho permanente são conduzidas no momento da seleção de candidatos para trabalhar com propriedade intelectual na ICT e no NIT.			
		Isto deve incluir referências de caráter, confirmação das qualificações acadêmicas e profissionais, e verificação da identidade.			
3.1.2	Termos e Condições de contratação	Se os funcionários são questionados a assinarem acordos de confidencialidade ou não divulgação como parte dos termos e condições iniciais de contratação.			
		Se estes acordos cobrem a segurança dos recursos de processamento de informação e os ativos da organização.			
		Se os termos e condições de trabalho determinam as responsabilidades dos funcionários pela segurança da informação. Quando apropriado, estas responsabilidades devem continuar por um período de tempo definido, após o término do contrato de trabalho na ICT.			
3.2	***Durante a contratação***				
3.2.1	Conscientização, educação e treinamento em segurança da informação	Se todos os funcionários da organização e, onde for relevante, prestadores de serviços recebem treinamento apropriado e atualizações regulares sobre as políticas e procedimentos organizacionais da ICT.			
3.2.2	Responsabilidades da Direção	Se regras e responsabilidades de segurança envolvendo propriedade intelectual são documentadas onde for apropriado, de acordo com a política de segurança da informação da ICT.			
		Isto deve incluir responsabilidades gerais pela implementação ou manutenção da política de segurança assim como quaisquer responsabilidades específicas para a proteção de determinados ativos ou pela execução de processos ou atividades de segurança envolvendo propriedade intelectual.			

3.2.3	Processo Disciplinar	Na ICT existe um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.			
3.3	***Encerramento e mudança da contratação***				
3.3.1	Responsabilidades pelo encerramento ou mudança da contratação	Se as responsabilidades e obrigações pela segurança da informação envolvendo processos de propriedade intelectual permanecem válidas após um encerramento ou mudança da contratação e se são definidas, comunicadas aos funcionários ou partes externas e as mesmas são cumpridas.			
4	***Segurança física e do ambiente***				
4.1	***Áreas de segurança***				
4.1.1	Perímetro da segurança física	Se barreiras físicas, como recursos de segurança, foram implementadas para proteger o serviço de processamento da informação nas ICT envolvendo propriedade intelectual. Alguns exemplos de tais recursos de segurança são o controle por cartão do portão de entrada, muros, presença de um funcionário na recepção, etc.			
4.1.2	Controles de entrada física	Se existem controles de entrada para permitir somente a entrada do pessoal autorizado dentro de várias áreas da ICT.			
4.1.3	Segurança em escritórios, salas e instalações de processamento	Se as salas, que possuem o serviço de processamento de informação envolvendo propriedade intelectual contêm armários fechados ou cofres, são trancadas.			
		Se o serviço de processamento de informação envolvendo propriedade intelectual é protegido contra desastres naturais ou causados pelo homem.			
4.1.4	Trabalhando em áreas de segurança	Se existe algum controle de segurança para prestadores de serviço ou funcionários trabalhando em área de segurança envolvendo propriedade intelectual. A informação só deve ser fornecida quando necessário.			
4.2	***Equipamentos***				
4.2.1	Instalação e proteção de equipamentos	Se o equipamento foi instalado em local apropriado para minimizar acesso não autorizado à área de trabalho.			
		Se os itens que requerem proteção especial foram isolados para reduzir o nível geral de proteção exigida.			
		Se controles foram adotados para minimizar o risco de ameaças potenciais, como roubo, fogo, explosão, fumaça, água, poeira, vibração, efeitos químicos, interferência no fornecimento elétrico, radiação eletromagnética, inundação.			
		Se existe uma política especial para alimentação, bebida e fumo nas proximidades das instalações de processamento da informação de propriedade intelectual.			
		Se os aspectos ambientais são monitorados para evitar condições que possam afetar de maneira adversa a operação das instalações de processamento da informação de propriedade intelectual.			
4.2.2	Segurança do cabeamento	Se o cabeamento elétrico e de telecomunicações que transmitem dados ou suporta os serviços de informação nas ICT e nos NIT são protegidos contra interceptação ou dano.			
		Se existe algum controle de segurança adicional para informações sensíveis ou críticas envolvendo propriedade intelectual.			
4.2.3	Manutenção de equipamentos	Se os equipamentos têm manutenção de acordo com intervalos e especificações do fabricante.			
		Se a manutenção é realizada apenas pelo pessoal autorizado.			
		Se são mantidos registros com todas as falhas suspeitas ou ocorridas e de toda a manutenção corretiva e preventiva.			
		Se os controles apropriados são utilizados quando do envio de equipamentos para manutenção fora da instalação física.			

		Se todos os requisitos impostos pelas apólices de seguro são atendidos.			
4.2.4	Segurança de equipamentos fora das instalações	Se um equipamento é autorizado pela direção quando necessitar ser utilizado fora das instalações da ICT.			
4.2.5	Reutilização e descarte seguro de equipamentos	Se dispositivos de armazenamento contendo informações sensíveis de propriedade intelectual são fisicamente destruídos ou sobrescritos de maneira segura.			
4.2.6	Política de mesa limpa e tela limpa	Se um serviço de bloqueio automático de tela de computador está ativo. Isso irá travar o computador sempre que for deixado ocioso por um determinado tempo.			
		Se os empregados são avisados para deixar qualquer material confidencial de forma segura e trancada.			
4.2.7	Remoção de propriedade	Se equipamentos, informações ou software podem ser retirados em adequada autorização das ICT.			
		Se inspeções regulares são realizadas para detectar remoção de propriedade não autorizada.			
		Se as pessoas estão cientes que estas inspeções regulares estão realizadas.			
5	***Segurança nas Operações e Comunicações***				
5.1	***Responsabilidades e procedimentos operacionais***				
5.1.1	Documentação dos procedimentos de operação	Se uma política de segurança identifica qualquer procedimento operacional como backup, manutenção de equipamentos, etc.			
		Se estes procedimentos estão documentados e são utilizados nas ICT.			
5.1.2	Gestão das Mudanças	Se todos os programas executados no sistema de produção são submetidos ao controle estrito de mudanças. Qualquer mudança nesses programas de produção deve ser autorizada pelo controle de mudanças.			
		Se registros são mantidos para qualquer modificação nos programas de produção envolvendo propriedade intelectual.			
5.1.3	Procedimentos para o gerenciamento de incidentes	Se existe um procedimento de gerenciamento de incidente definido para uma resposta a incidentes de segurança.			
		Se o procedimento define as responsabilidades de gerenciamento de incidente, de maneira organizada e rápida em resposta a incidentes de segurança.			
		Se o procedimento define diferentes tipos de incidentes, desde Negação de Serviço (DoS) até quebra de confidencialidade, assim como modos de gerencia-los.			
		Se registros e evidências relacionadas aos incidentes são mantidos, e ações proativas são realizadas de maneira que os incidentes não mais ocorram.			
5.1.4	Segregação de funções	Se tarefas e áreas de responsabilidades são separadas para reduzir a possibilidade de modificação não autorizada ou mal uso de informação ou serviços envolvendo propriedade intelectual.			
5.1.5	Separação de ambientes de desenvolvimento e de produção	Se os ambientes de desenvolvimento e de teste são isolados do ambiente de produção. Por exemplo, software em desenvolvimento deve ser executado em um computador diferente do computador com software de produção. Quando necessário, as redes de desenvolvimento e produção devem ser separadas uma da outra.			
5.1.6	Gestão de recursos terceirizados	Se algum recurso de processamento de Informação envolvendo propriedade intelectual é gerenciado por terceiros.			
		Se os riscos associados a tal gerenciamento são detalhadamente identificados, discutidos com a terceira parte, e controles apropriados			

		foram incorporados no contrato.			
		Se aprovação necessária foi obtida dos empresários e donos de aplicações.			
6	***Controle de acesso***				
6.1	***Requisitos do negócio para controle de acesso***				
6.1.1	Política de controle de acesso	Se os requisitos do negócio para controle de acesso foram definidos e documentados.			
		Se a política de controle de acesso define as regras e direitos para cada usuário ou um grupo de usuários.			
		Se os usuários ou provedores de serviço receberam um documento contendo claramente os controles de acesso que satisfaçam os requisitos do negócio.			
6.2	***Gerenciamento de acesso do usuário***				
6.2.1	Registro e cancelamento de usuário	Se existe algum procedimento formal de registro e cancelamento de registro para garantir o acesso a todos os sistemas de informação e serviços multiusuários nas ICT.			
6.2.2	Gerenciamento de direitos de acesso privilégiado	Se a concessão e o uso de quaisquer privilégios de um sistema de informação multiusuário é restrito e controlado, por exemplo, se privilégios são concedidos pela necessidade do usuário, e somente depois de um processo de autorização formal nas ICT.			
6.2.3	Gerenciamento de senha dos usuários	Se os usuários são solicitados a assinar uma declaração a fim de manter a confidencialidade de sua senha pessoal. A concessão e alteração de senhas devem ser controladas por um processo de gerenciamento formal.			
6.2.4	Análise crítica dos direitos de acesso do usuário	Se existe um processo de revisão dos direitos de acesso do usuário em intervalos regulares aos processos de propriedade intelectual.			
6.3	***Responsabilidades dos usuários***				
6.3.1	Uso de senhas	Se existe alguma diretriz para guiar usuários na escolha e manutenção segura de senhas.			
6.3.2	Uso de informação de autenticação secreta	Se os usuários são orientados a seguir as praticas da ICT quanto ao uso da informação de autenticação secreta envolvendo propriedade intelectual.			
6.4	***Controle de acesso ao sistema e á aplicação***				
6.4.1	Procedimentos de entrada no sistema (*logon*)	Se o acesso ao sistema de informação é realizado através de um processo seguro de entrada no sistema. Convém que o procedimento de entrada no sistema de computador seja projetado para minimizar a oportunidade de acessos não autorizados.			
6.4.2	Identificação e autenticação de usuário	Se todos os usuários (incluindo o pessoal de suporte técnico, como operadores, administradores de redes, programadores de sistema e administradores de rede) tenham um identificador único. As contas genéricas de usuário devem somente ser fornecidas sobre circunstâncias excepcionais no qual há um benefício de negócio claro. Controles adicionais devem ser necessários para gerenciar as contas.			
		Se o método de autenticação utilizado confirma a identidade alegada pelo usuário. Método comumente utilizado: Senhas somente conhecidas pelos usuários.			
6.4.3	Sistema de gerenciamento de senhas	Se existe um sistema de gerenciamento de senhas que reforça vários controles de senhas, como: Senha individual reforça alterações de senha, gravar senha de forma criptografada, não mostrar senhas na tela, etc.			
6.4.4	Uso de programas	Se programas utilitários do sistema que vêm junto com as instalações do computador, que podem sobrepor os controles do sistema e			

	utilitários privilegiados	aplicações, são estritamente controlados.			
6.4.5	Restrição de acesso à informação	Se o acesso à aplicação por vários grupos ou pessoal dentro da ICT é definido na política de controle de acesso como requisito de aplicação de negócio individual e é consistente com a política de acesso a Informação da ICT.			
6.4.6	Isolamento de sistemas sensíveis	Se sistemas sensíveis utilizados nos processos de propriedade intelectual são isolados do ambiente de computação, como sendo executados em computadores dedicados, recursos compartilhados somente com sistemas de informações confiáveis, etc.			
6.5	***Monitoração do uso e acesso ao sistema***				
6.5.1	Monitoração do uso do sistema	Se foram estabelecidos procedimentos para a monitoração do uso dos recursos de processamento da informação. Os procedimentos devem assegurar que os usuários estão executando apenas as atividades para as quais eles foram explicitamente autorizados.			
		Se os resultados do monitoramento das atividades são revisados regularmente.			
6.6	***Computação móvel e trabalho remoto***				
6.6.1	Computação móvel	Se uma política formal foi adotada levando em conta os riscos de trabalhar com recursos de computação móvel, como notebooks, tablets, etc., especialmente em ambientes desprotegidos das ICT e dos NIT.			
6.6.2	Trabalho remoto	Se existe alguma política, procedimento e/ou padrão para controlar as atividades do trabalho remoto. Isto deve ser consistente com a política de segurança da informação da ICT.			
		Se a proteção apropriada para o local do trabalho remoto foi implantada, para evitar o roubo de equipamentos e de informações ou o uso impróprio destes recursos.			