Segurança da Informação em um Instituto de Pesquisa: Uma Análise Utilizando a Norma ISO/IEC 27002:2005

Antonio Eduardo de Albuquerque Junior *[eduardo.albuquerque@bahia.fiocruz.br]*,
Ernani Marques dos Santos *[ernanims@ufba.br]* e Elaine Santos de Albuquerque *[soselaine@gmail.com]*

Resumo

A dependência que as organizações tem da infraestrutura de TI junto com a crescente facilidade de acesso à tecnologia elevaram a importância das informações, um ativo intangível importante para a tomada de decisões nas organizações. A norma NBR ISO/IEC 27002:2005 traz uma série de controles e objetivos de controle para segurança dos seus ativos de processamento de informações, recursos humanos, ambientes e contratos de maneira que promovam a segurança das suas informações. Este trabalho é um estudo de caso único, de abordagem qualitativa e caráter exploratório e descritivo, que tem como objetivo identificar quais categorias de controles de segurança da informação tem seus objetivos de controle alcançados e quais mecanismos e processos de segurança da informação são utilizados em um instituto de pesquisa público federal, com base nos controles e objetivos de controle presentes na norma NBR ISO/IEC 27002:2005. A pesquisa utilizou como procedimentos técnicos a entrevista estruturada, a pesquisa bibliográfica e a análise documental. Os controles recomendados pela norma foram utilizados para elaboração das perguntas utilizadas na entrevista. Os entrevistados são os profissionais e o coordenador de TI do instituto pesquisado. O trabalho está dividido em sete seções: Introdução; Segurança da Informação e Política de Segurança da Informação na Administração Pública Federal; Metodologia; Estudo de Caso; Resultados; Considerações Finais; e Referências Bibliográficas.

Palavras-chave: Segurança da informação. Instituto de pesquisa. Organização pública.

1 Introdução

A dependência de uma infraestrutura de TI cada vez mais complexa tem elevado a prioridade de questões relacionadas à administração de pessoas, políticas e programas para assegurar a continuidade das operações nas organizações (HERATH; HERATH; BREMSER, 2010). Essa dependência e a crescente facilidade de acesso à tecnologia fizeram com que a TI ficasse sujeita a ameaças físicas ou virtuais que comprometem a segurança de pessoas, transações e informações (MARCIANO, 2006).

As informações estiveram presentes em todas as fases do processo evolutivo das empresas (DONNER; OLIVEIRA, 2008), e as transações eletrônicas, a velocidade de transmissão e a facilidade de disseminação de dados fizeram com que as informações ganhassem importância e permitiram sua disponibilização para diversas organizações, em um contexto que Sêmola (2014) chamou de Sociedade do Conhecimento. Mello et al. (2010) afirmam que a chamada nova economia, que tem base na informação e no conhecimento, surgiu acompanhada de mudanças na forma de gestão e atuação das organizações. Considerando que as informações são ativos intangíveis e que podem estar entre os bens mais valiosos em uma organização (NOBRE; RAMOS; NASCIMENTO, 2010), e que o valor

econômico de uma organização é resultado da soma dos seus ativos tangíveis e intangíveis (KAYO et al., 2006), e considerando que a informação é importante para a tomada de decisões, há o risco de divulgação de informações estratégicas por vias não autorizadas, ampliado pelas facilidades de conexão com redes e pela portabilidade dos equipamentos (FACHINI, 2009), há a necessidade de protegê-las e aos equipamentos que as processam, armazenam e transmitem dos riscos associados.

Nesse contexto, a Associação Brasileira de Normas Técnicas (ABNT) (2005) considera ativos organizacionais tanto as informações, em meio digital ou não, quanto computadores, impressoras, discos rígidos, fitas magnéticas, discos óticos, aparelhos de fax e qualquer outro equipamento ou objeto que processe, contenha, armazene, receba, envie ou imprima informações sensíveis, bem como serviços de computação, comunicação, refrigeração e fornecimento de energia, entre outros, além da reputação, da imagem da organização, do seu nome e sua marca, classificando-os como: ativos de informação; ativos de software; ativos físicos; serviços; pessoas e suas qualificações, habilidades e experiências; e intangíveis. Silva (2009) afirma que o entendimento do ambiente é importante, uma vez que existem diferentes mecanismos de proteção para proteger as informações. Nobre, Ramos e Nascimento (2010) afirmam que a segurança da informação inclui também a integridade dos equipamentos que armazenam informações e que falhas nessa estrutura podem expor as informações a acessos não autorizados, a alterações indevidas ou a indisponibilidade para as pessoas que precisam acessá-las, concordando com Moreira (2001) e Sêmola (2014).

A justificativa para este trabalho reside no fato de que, em organizações que tem como atividade principal a pesquisa científica, é preciso proteger não só a informação, mas também o conhecimento produzido, como segredos industriais e a propriedade intelectual (ALEXANDRIA, 2009). Assim, o estudo visa aumentar a compreensão sobre segurança da informação em organizações de pesquisa.

Este trabalho é um estudo de caso único de natureza aplicada, abordagem qualitativa, de caráter exploratório e descritivo, que utilizou como procedimentos técnicos a entrevista estruturada, a pesquisa bibliográfica e a análise documental, e que é parte de uma pesquisa maior. Os entrevistados são profissionais de TI de um instituto de pesquisa, unidade descentralizada de uma instituição pública de pesquisa. O objetivo da pesquisa é identificar, com base na norma NBR ISO/IEC 27002:2005, quais categorias de controles de segurança da informação tem seus objetivos de controle alcançados na organização pesquisada e quais mecanismos e processos de segurança da informação são utilizados. Após a realização do diagnóstico, pretende-se identificar quais objetivos de controle são considerados mais importantes para o instituto e, em seguida, propor ações para atender às necessidades de segurança da informação. O trabalho está dividido em cinco seções, além desta introdução e das referências bibliográficas: a seção seguinte trata da teoria sobre segurança da informação e Política de Segurança da Informação, bem como da norma NBR ISO/IEC 27002:2005; a seção 3 trata da metodologia utilizada na pesquisa; a seção 4 apresenta a instituição pesquisada; a seção 6 apresenta os resultados da pesquisa; e a seção 7 mostra as considerações finais do trabalho.

2 Segurança da Informação na Administração Pública Federal e em Ambiente de Pesquisa Científica

Sêmola (2014) argumenta que segurança da informação é uma área de conhecimento dedicada a proteger ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade, e Mandarini (2004) diz que sua finalidade é proteger as informações contra ameaças para garantir a continuidade do negócio, minimizar as perdas e maximizar o retorno sobre os investimentos. Donner e Oliveira (2008) conceituam segurança da informação como o processo de proteção das informações de ameaças para assegurar sua integridade, disponibilidade e confidencialidade. Muito já foi feito no sentido de aprimorar a segurança da informação, apesar de não ser possível erradicar completamente o risco de seu uso indevido, como observam Silva e Stein (2007, p.48). As autoras confirmam que a segurança da informação não deve ficar restrita aos aspectos tecnológicos, devendo proteger a informação em qualquer forma que se encontre. Afirmam ainda que a segurança da informação cobre também "toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros", e a proteção deve ser correspondente ao seu valor para a organização e aos prejuízos que sua perda ou acesso indevido podem provocar. Isso é confirmado por Marciano (2006), que afirma que a TI não é suficiente para garantir a proteção das informações, e vai além ao afirmar que a tecnologia pode tanto ajudar quanto agravar os problemas relacionados à segurança da informação.

Considerando que muitas organizações tem a informação como um importante insumo ou produto, há a necessidade estratégica de proteger essas informações sensíveis para garantir a continuidade do seu funcionamento. Há a necessidade de proteger também propriedade intelectual em organizações que desenvolvem tecnologia. Diversas instituições públicas ou privadas Brasileiras desenvolvem tecnologia e, por isso, tem a informação como parte importante do seu processo de inovação. Muitas delas atuam em áreas em que o Brasil tem uma posição de destaque internacional e muitas são instituições públicas ou de capital misto, que precisam proteger não só por seus interesses comerciais relacionados às informações ou os interesses de cidadãos cujas informações estão sob seu poder, mas também por obrigação legal, graças a atos normativos que visam proteger informações com as quais lidam.

A preocupação com segurança da informação na Administração Pública Federal vem sendo demonstrada através de diferentes instrumentos normativos. A Lei nº 8.159/1991 diz que é "dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação". Já a Lei nº 9.983/2000 altera o Código Penal, incluindo uma preocupação com a integridade e confiabilidade das informações armazenadas em sistemas computacionais ao tipificar a alteração desses dados. O Decreto nº 3.505/2000 institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, dizendo que um dos pressupostos básicos para essa Política de Segurança da Informação é a conscientização dos órgãos e entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco de suas vulnerabilidades. Já o

Decreto nº 4.553/2002 trata da "salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal". A segurança da informação em instituições públicas foi também, segundo Cepik, Canabarro e Possamai (2010, p.61), um dos objetivos do levantamento realizado em 2007 pela Secretaria de Fiscalização de Tecnologia da Informação (SEFTI) do Tribunal de Contas da União (TCU), que identificou "ausência de política de segurança da informação" na Administração Pública Federal.

Em organizações que desenvolvem pesquisa científica, o acesso à Internet, o acesso remoto a recursos computacionais e a serviços potencializam os riscos à segurança da informação, segundo Bernaschi, d'Aiutolo e Ruguetti (1999). Para Alexandria (2009), em ambiente de pesquisa, a segurança da informação visa a proteção das informações e do conhecimento científico, que se traduzem em propriedade intelectual e segredos industriais. Caminha et al. (2006) dizem que a informação é um dos ativos mais valiosos para os institutos de pesquisa, e citam como exemplos de informações importantes para essas organizações as técnicas de gestão, as análises de dados, os projetos e as patentes. Já Pimenta e Sousa Neto (2010) afirmam que a informação em institutos de pesquisa tecnológica é um diferencial competitivo, o que fortalece a necessidade de protegê-la. Diante desse cenário, a pesquisa que resultou neste trabalho estudou um dos institutos de pesquisa regionais vinculados a uma fundação pública de pesquisa do Poder Executivo Federal de destaque internacional, chamada neste trabalho de Fundação F.

A ABNT (2005) define segurança da informação como sendo a "preservação da confidencialidade, da integridade e da disponibilidade da informação". Nesse contexto, confidencialidade pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que tem autorização para acessá-las, integridade é a garantia de que as informações são corretas e completas e disponibilidade é a garantia de que as informações estarão disponíveis para serem acessadas pelas pessoas que tem autorização para vê-las quando forem necessárias. Em outras palavras, segurança da informação é a garantia de que as informações da organização serão protegidas de três maneiras: serão acessadas apenas pelas pessoas que devem ter acesso a elas, estarão corretas e completas e estarão disponíveis sempre que seus usuários precisarem, conforme a norma NBR ISO/IEC 27002:2005, ou "Código de prática para a gestão da segurança da informação" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

A gestão de segurança da informação é definida como o processo de administrar pessoas, políticas e programas com o objetivo de assegurar a continuidade das operações mantendo o alinhamento estratégico com a missão organizacional (CAZEMIER; OVERBEEK; PETERS, 2000, apud HERATH; HERATH; BREMSER, 2010). A continuidade das operações de uma organização é assegurada pela proteção das informações essenciais ao funcionamento da organização e de todos os recursos e ativos envolvidos no seu processamento e armazenamento. Segundo Moura e Gaspary (2008), a proteção da informação é conseguida através da aplicação de segurança física e lógica nas operações das empresas, e o que orienta essas práticas nas organizações são as Políticas de Segurança da Informação, que, conforme Marciano (2006), abrangem recursos computacionais, recursos humanos, infraestrutura e logística.

Para orientar o gerenciamento da segurança da informação, é necessário um documento emitido ou aprovado pela direção da organização apoiando as ações nesse sentido. Segundo a ANBT (2005), a Política de Segurança da Informação é o documento que visa mostrar a orientação e o apoio da direção da organização para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. A ABNT diz ainda que a Política de Segurança da Informação deve expressar formalmente as intenções e diretrizes globais da direção da organização no sentido de promover a preservação da confidencialidade, da integridade e da disponibilidade da informação. Fernandes e Abreu (2008, p.19) definem Política de Segurança da Informação como a "determinação de diretrizes e ações referentes à segurança dos aplicativos, da infraestrutura, dos dados, pessoas e organizações (fornecedores e parceiros)". Em outras palavras, a Política de Segurança da Informação é um documento que deve mostrar os requisitos e orientações dos dirigentes de uma organização para as ações e controles necessários para promover a segurança da informação. A elaboração desse documento está em conformidade com os planos do Governo Federal, segundo Cepik, Canabarro e Possamai (2010), que afirmam que a elaboração de uma Política de Segurança da Informação foi uma das metas previstas na Estratégia Geral de Tecnologia da Informação (EGTI) para o ano de 2009 para todas as instituições do Poder Executivo Federal. Para esse fim, a norma NBR ISO/IEC 27002 é um dos modelos de maior destaque, segundo Lunardi et al. (2007), Moraes e Mariano (2008) e Lunardi, Becker e Maçada (2010).

2.1 A Norma ABNT NBR ISO/IEC 27002:2005

Segundo Fernandes e Abreu (2008), praticamente todas as normas sobre segurança da informação tem origem no Governo Britânico. A British Standard 7799 (BS 7799), criada em 1995 e revisada em 1999 pelo British Standards Institute (BSI), foi adotada em 2000 pela International Organization for Standardization (IOS) com o nome ISO/IEC 17799:2000, que foi revisada em 2005 e teve seu nome alterado para ISO/IEC 27002:2005. A ISO/IEC 17799:2000 foi adotada pela ABNT com o nome NBR ISO/IEC 17799 e, com a revisão e alteração de nome promovida pela ISO, teve também seu nome alterado pela ABNT para NBR ISO/IEC 27002:2005. Essa norma é dedicada aos controles e práticas de segurança da informação, estabelecendo uma diretriz e os princípios gerais para gestão da segurança da informação em uma organização (FERNANDES; ABREU, 2008) e está organizada em 11 seções de controles, que podem ter uma ou mais categorias de controles, além de uma seção sobre análise, avaliação e tratamento de riscos. Cada uma das 39 categorias principais de controle de segurança da informação contém um objetivo de controle e um ou mais controles. No total, a norma contém 133 controles de segurança da informação, cada controle com uma ou mais orientações e boas práticas de segurança da informação.

A NBR ISO/IEC 27002:2005 orienta as organizações a elaborarem uma Política de Segurança da Informação, que, por sua vez, deve orientar na criação de normas mais específicas e procedimentos

para o tratamento seguro das informações e de outros ativos organizacionais que processam ou armazenam informações. Ajuda também na identificação e classificação das informações e dos outros ativos relacionados quanto à sua importância para a instituição, quanto ao risco de perda e de divulgação indevida. A norma sugere uma série de controles para proteção desses ativos e informações, como a análise crítica e manutenção da própria Política de Segurança da Informação, a atribuição de responsabilidades relativas à segurança da informação, a elaboração de contratos e acordos de confidencialidade entre instituições prevendo a preservação da segurança da informação, a execução de inventários de ativos, a contratação de mão de obra e os controles de acesso físico às dependências da organização.

As 11 seções de controles presentes na norma são: Política de segurança da informação; Organizando a segurança da informação; Gestão de ativos; Segurança em recursos humanos; Segurança física e do ambiente; Gerenciamento das operações e comunicações; Controle de acessos; Aquisição, desenvolvimento e manutenção de sistemas de informação; Gestão de incidentes de segurança da informação; Gestão da continuidade do negócio; Conformidade.

Já as 39 categorias de controle previstas na norma são as seguintes: Política de Segurança da Informação; Infra-estrutura de segurança da informação; Partes externas; Responsabilidade pelos ativos; Classificação da informação; Antes da contratação; Durante a contratação; Encerramento ou mudança da contratação; Áreas seguras; Segurança de equipamentos; Procedimentos e responsabilidades operacionais; Gerenciamento de serviços terceirizados; Planejamento e aceitação dos sistemas; Proteção contra códigos maliciosos e códigos móveis; Cópias de segurança; Gerenciamento da segurança em redes; Manuseio de mídias; Troca de informações; Serviços de comércio eletrônico; Monitoramento; Requisitos de negócio para controle de acesso; Gerenciamento de acesso do usuário; Responsabilidades dos usuários; Controle de acesso à rede; Controle de acesso ao sistema operacional; Controle de acesso à aplicação e à informação; Computação móvel e trabalho remoto; Requisitos de segurança de sistemas de informação; Processamento correto nas aplicações; Controles criptográficos; Segurança dos arquivos do sistema; Segurança em processos de desenvolvimento e de suporte; Gestão de vulnerabilidades técnicas; Notificação de fragilidades e eventos de segurança da informação; Gestão de incidentes de segurança da informação e melhorias; Aspectos da gestão da continuidade do negócio, relativos à segurança da informação; Conformidade com requisitos legais; Conformidade com normas e políticas de segurança da informação e conformidade técnica; e Considerações quanto à auditoria de sistemas de informação.

Segundo Moura e Gaspary (2008), para atender aos objetivos de controle de segurança da informação relacionados às essas categorias de controle, mais de uma ferramenta de segurança podem ser necessárias ou utilizadas, o que amplia a complexidade da aplicação prática da segurança da informação. O caminho para alcançar a segurança da informação passa por identificar quais controles são necessários para mitigar os riscos associados aos ativos da organização e uma forma de fazer isso é identificar quais objetivos de controle de segurança da informação são atendidos pelos controles já adotados e quais controles ainda precisam ser adotados, tendo em vista a realidade da organização.

3 Metodologia

A pesquisa foi realizada através de entrevistas estruturadas junto ao coordenador e aos profissionais de TI de um instituto de pesquisa da Fundação F a fim de identificar os objetivos de controle de segurança da informação previstos na norma NBR ISO/IEC 27002:2005 que são atendidos pelos controles de segurança da informação adotados, quais categorias de controle da norma tem mais controles adotados e quais mecanismos e ferramentas de segurança da informação são utilizadas para alcançar esses objetivos de controle. É pressuposto da pesquisa o fato de nenhum objetivo de controle previsto na norma ser plenamente alcançado através da adoção de controles de segurança da informação, o que é motivado pela descentralização e autonomia dos institutos da Fundação F, o que dificulta a adoção desses controles. A pesquisa envolveu três etapas básicas: uma etapa de pesquisa bibliográfica, a partir da qual foi elaborado o instrumento de coleta de dados; uma etapa de coleta de dados, em que os entrevistados responderam às perguntas presencialmente; e uma etapa de análise dos dados coletados, cujos resultados estão na seção de Resultados deste trabalho.

A etapa de pesquisa bibliográfica envolveu uma revisão da literatura sobre segurança da informação e uma leitura da norma NBR ISO/IEC 27002:2005, onde foram identificadas as 11 seções de controles, seus objetivos de controle e os controles associados. A partir dos controles e recomendações previstos na norma, foram elaboradas as perguntas contidas no roteiro utilizado para coletar as informações na etapa de coleta dos dados, resultando em um roteiro abrangendo os 39 objetivos de controle de segurança da informação. A cada pergunta para identificar se um objetivo de controle está sendo atendido, o entrevistado era questionado também quanto à necessidade de o instituto adotar os controles associados ao objetivo e era solicitado que citasse quais controles são efetivamente adotados.

Foram acrescentadas no início do roteiro duas perguntas com a finalidade de identificar se os entrevistados conheciam a norma e saberiam conceituar segurança da informação: "O que você entende por segurança da informação?" e "Você já ouviu falar ou conhece a norma ABNT NBR ISO/IEC 17799 ou ABNT NBR ISO/IEC 27002?". A escolha do instituto se deu pela conveniência de ser onde o pesquisador trabalha, facilitando o acesso aos entrevistados, e a entrevista foi feita apenas com os profissionais da área de TI do instituto pelo fato de as perguntas tratarem de assuntos mais técnicos, inerentes à área de TI.

4 O Caso Estudado

A Fundação F é uma fundação pública federal vinculada ao Poder Executivo que desenvolve diversas atividades de pesquisa e ensino, que tem 16 institutos de pesquisa localizados no Rio de Janeiro e em outros estados do Brasil. Sua estrutura organizacional de gestão descentralizada dá a cada instituto grande autonomia, o que se reflete tanto nas pesquisas desenvolvidas quanto em suas atividades administrativas.

O instituto estudado é um dos cinco que não estão localizados no Rio de Janeiro, onde está a sede administrativa da fundação. Os laboratórios deste instituto desenvolvem diversas atividades de pesquisa, ensino, informação e prestação de serviços para a população que não estão diretamente relacionados à tecnologia da informação. A área responsável pela TI é a Seção de Informática (SEINFO), que conta com quatro servidores efetivos e dois ocupantes de cargo comissionado sem vínculo efetivo, distribuídos de forma que três desenvolvem atividades relacionadas à infraestrutura e três desenvolvem atividades de desenvolvimento de sistemas.

A SEINFO conta ainda uma equipe terceirizada residente composta por sete profissionais. Desses, quatro são para atendimento de primeiro nível, que trabalham aos pares, se revezando a cada seis horas no atendimento de incidentes de baixa complexidade, de maneira que ficam dois profissionais de atendimento de primeiro nível das 7 horas da manhã às 13 horas e outros dois das 13 horas às 19 horas. Os outros três profissionais terceirizados são técnicos para atendimento de segundo nível, que resolvem problemas de média complexidade e de hardware. No total, trabalham 13 pessoas na SEINFO, entre servidores e terceirizados, para aproximadamente 550 usuários de recursos computacionais, entre bolsistas, estudantes de pós-graduação e dos programas de iniciação científica, estagiários, pesquisadores visitantes, servidores e terceirizados que desenvolvem atividades no instituto. Todas as atividades típicas de analistas, normalmente desenvolvidas por profissionais de nível superior, como gerenciamento da rede e de todo o ambiente computacional, análise e desenvolvimento de sistemas, ficam a cargo de servidores públicos do instituto.

5 Resultados

Esta seção apresenta os resultados da análise dos dados da pesquisa. Inicialmente, são apresentadas informações sobre as pessoas que responderam à entrevista. Em seguida, são apresentadas as informações colhidas junto aos entrevistados sobre os controles de segurança da informação do instituto de pesquisa.

Dos 13 entrevistados, quatro são servidores efetivos do instituto, dois são ocupantes de cargos comissionados sem vínculo efetivo e sete são empregados da empresa contratada para prestar serviços de atendimento e suporte ao usuário. Quanto ao gênero, apenas duas mulheres. Quanto ao nível de instrução, sete entrevistados tem apenas nível médio, sendo que três destes estão matriculados em cursos de ensino superior. Cinco entrevistados tem pós-graduação em nível de Especialização e cinco estão cursando Mestrado. Quanto ao tempo de serviço na instituição, um trabalha há 10 anos, um trabalha há cinco anos, quatro trabalham há três anos, seis trabalham há um ano e apenas um entrevistado trabalha há menos de um ano. O Quadro 1 mostra um resumo do perfil de cada entrevistado.

QUADRO 1 – PERFIS DOS ENTREVISTADOS

Função	Vínculo	Tempo de Vínculo	Formação
Coordenador de TI	Servidor	5 anos	Graduação e Especialização em TI
Analista de Suporte	Servidor	10 anos	Graduação em TI
Analista de Suporte	Servidor	3 anos	Graduação e Especialização em TI
Analista de Desenvolvimento	Servidor	4 anos	Graduação e Especialização em TI
Analista de Desenvolvimento	Servidor	4 anos	Graduação e Especialização em TI
Analista de Desenvolvimento	Servidor	3 anos	Graduação e Especialização em TI
Técnico em Informática	Terceirizado	1 ano	Nível médio
Técnico em Informática	Terceirizado	1 ano	Nível médio
Técnico em Eletrônica	Terceirizado	1 ano	Nível médio
Técnico em Atendimento	Terceirizado	1 ano	Nível médio
Técnico em Atendimento	Terceirizado	1 ano	Nível médio
Técnico em Atendimento	Terceirizado	1 ano	Nível médio
Técnico em Atendimento	Terceirizado	1 ano	Nível médio
Técnico em Atendimento	Terceirizado	1 ano	Nível médio

FONTE: Elaboração própria, 2014.

A maioria dos entrevistados descreveu segurança da informação como sendo a proteção dos dados e equipamentos de uma organização. Um dos entrevistados disse entender a segurança da informação como o fornecimento seguro de informações certas para as pessoas certas, e outro disse que envolve diversas formas de proteção e de informações, inclusive daquelas que estão sobre as mesas das pessoas, complementando que é "um erro pensar que segurança da informação está apenas relacionada com tecnologia. Outro relacionou segurança da informação como mecanismos e processos, envolvendo sistema e rotina de backup, controle de acesso, segurança física de equipamentos, ar-condicionado. Já outro entrevistado disser que entende segurança da informação como medias tomadas para proteger as informações da organização. Com isso, percebe-se que os entrevistados, de maneira geral, entendem segurança da informação como processos, procedimentos, requisitos, práticas e infraestrutura para proteger as informações, que mais se aproxima da descrição que a norma traz sobre os meios de se obtê-la. Um entrevistado descreveu segurança da informação como a garantia da disponibilidade, da integridade e da confidencialidade das informações de uma organização e um outro descreveu como a "proteção da informação de maneira que garanta a continuidade do negócio e o retorno sobre os investimentos, e minimizando os riscos associados", respostas que mais se aproximam dos conceitos encontrados na norma.

Os profissionais terceirizados descreveram, de maneira geral, segurança da informação como proteção de dados ou de informações na organização, ou como medidas para proteger as informações da organização. Já as respostas dos servidores do instituto apontam que seus conceitos de segurança da informação se aproximam mais dos conceitos encontrados na NBR ISO/IEC 27002. Entre os analistas de desenvolvimento, apenas um profissional declarou não conhecer a norma, e todos os servidores da área de infraestrutura afirmaram conhecê-la.

Ao serem questionados se conheciam já haviam ouvido falar da norma NBR ISO/IEC 27002 ou de sua denominação anterior, NBR ISO/IEC 17799, seis entrevistados afirmaram conhecer a norma, sendo que cinco conhecem superficialmente e um afirmou conhecer em detalhes. Os outros

sete entrevistados declararam que não a conhecem. Dentre os servidores do instituto, apenas um declarou não conhecer, e dentre os profissionais terceirizados, apenas um afirmou conhecer a norma. Um entrevistado afirmou ter conhecido a norma por necessidade do trabalho e todos os outros que declararam conhecê-la afirmaram que isso ocorreu durante cursos de graduação ou pós-graduação. Os fatos de os profissionais terceirizados não conhecerem a norma e não conseguirem conceituar segurança da informação de maneira mais aprofundada pode significar uma deficiência da organização na seleção de empresas quanto aos critérios de capacitação dos profissionais terceirizados.

As respostas dos profissionais terceirizados foram mais completas quando tratavam de assuntos relacionados ao funcionamento dos recursos tecnológicos do instituto ou de procedimentos técnicos, como utilização de chaves de criptografia, identificação e autenticação do usuário, integridade de mensagens ou procedimentos de análise técnica após mudanças no sistema operacional. Já os servidores públicos do instituto deram respostas mais completas ao tratar de assuntos relacionados a processos e procedimentos de gestão, como análise e especificação de requisitos de segurança, políticas, normas e análise crítica dos direitos de acesso dos usuários. Isso mostra que os profissionais do instituto se preocupam em conhecer aspectos relacionados à segurança da informação, mesmo aqueles que não conhecem a norma ou não souberam conceituar segurança da informação de maneira mais elaborada.

Contrariando o pressuposto de que não havia nenhum objetivo de controle de segurança da informação que fosse atendido pelos controles adotados no instituto pesquisado, as respostas dos entrevistados levaram à conclusão de que o objetivo de controle "Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados", relacionado à categoria de controle Gerenciamento de serviços terceirizados, que está incluída na seção de controle Gerenciamento das Operações e Comunicações, é plenamente alcançado. Os seus três controles (Entrega de serviços terceirizados, Monitoramento e análise crítica de serviços terceirizados e Gerenciamento de mudanças para serviços terceirizados) são utilizados no instituto de pesquisa através de diferentes mecanismos e processos, incluindo os seguintes: é feita análise crítica dos serviços prestados, dos relatórios emitidos e dos registros fornecidos pelas empresas terceirizadas; o instituto controla os dados institucionais acessados pelos empregados da empresa terceirizada através de registros de acesso, quando esse acesso é possível; os contratos de terceirização de serviços incluem controles de segurança, acordos de nível de serviço e definição detalhada dos serviços prestados; as transferências de contratos são feitas com transferência de informações, que são armazenadas em servidores de rede e bancos de dados de bases de conhecimentos; e os serviços são sempre contratados com garantia de funcionamento.

O objetivo de controle "Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte", relacionado à categoria de controle Gerenciamento de segurança em redes, que

também está incluída na seção de controle Gerenciamento das Operações e Comunicações, foi outro objetivo alcançado por meio dos controles adotados no instituto. Essa categoria de controle inclui Controles de redes e Segurança dos serviços de rede. O instituto tem procedimentos de gerenciamento e monitoramento das suas redes, e as responsabilidades sobre o gerenciamento e monitoramento estão formalmente definidas e documentadas. O instituto controla o acesso à sua rede sem fio, restringindo o acesso apenas a equipamentos cadastrados, com seus usuários devidamente identificados. O instituto adota controles que impedem acessos não autorizados a sistemas e serviços da rede local a partir da rede sem fio, como firewalls com listas de controle de acesso restritivas e necessidade de autenticação com conta de usuário e senha. O instituto utiliza um sistema de proxy, com restrições a endereços potencialmente perigosos. O acesso à rede do instituto exige autenticação e os equipamentos precisam estar cadastrados para terem acesso físico à rede. O acesso ao serviço de Webmail é criptografado. O instituto tem uma solução de antivírus corporativa, com gerenciamento centralizado, e utiliza um anti-spam e um serviço que remove códigos maliciosos de mensagens de correio eletrônico.

Do total de 133 controles de segurança da informação previstos na norma, o instituto utiliza apenas 33, conforme as informações apresentadas pelos entrevistados. Os quadros a seguir apresentam os controles adotados pelo instituto, organizados de acordo com as seções de controles e com as categorias de controles presentes na norma.

O Quadro 2 traz os controles e procedimentos da categoria de controle Encerramento ou mudança da contratação, da seção de controle Segurança em recursos humanos. Percebe-se que, dos três controles desta categoria de controle, dois são adotados.

QUADRO 2 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE SEGURANÇA EM RECURSOS HUMANOS.

CATEGORIA DE CONTROLE: ENCERRAMENTO OU MUDANÇA DA CONTRATAÇÃO	
Controles	Procedimentos e Tecnologias Adotados
Encerramento de atividades	As responsabilidades para encerramento ou mudança de um contrato estão definidas na legislação, em instruções normativas do Governo Federal e em procedimentos internos.
	As responsabilidades das empresas contratadas para prestar serviços na instituição estão previstas em contrato e permanecem válidas mesmo após o fim do contrato.
Retirada de direitos de acesso	Há um procedimento formal de retirada de direitos de acesso dos usuários quando perdem o vínculo com a instituição. As contas são bloqueadas no último dia de vigência do vínculo e excluídas após seis meses.

FONTE: Elaboração própria, 2014.

O Quadro 3 mostra os controles e procedimentos das categorias de controle Áreas seguras e Segurança de equipamentos da seção de controle Segurança física e do ambiente, e nele percebe-se que, dos seis controles da norma, quatro são adotados.

QUADRO 3 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE SEGURANÇA FÍSICA E DO AMBIENTE.

CATEGORIA DE CONTROLE: ÁREAS SEGURAS	
Controles	Procedimentos e Tecnologias Adotados
Controles de entrada física	Os acessos às áreas seguras do instituto são controlados por portas trancadas, cujos acessos às chaves são registrados, registrando data e hora de retirada e devolução. Alguns acessos são restritos a pessoas autorizadas.
	O acesso à área onde estão os servidores da rede de computadores é restrito a pessoas autorizadas e o acesso é controlado.
	Prestadores de serviço de suporte tem acesso às áreas onde estão os servidores da rede de computadores apenas acompanhados por pessoal autorizado.
Segurança em escritórios, salas e instalações	Todos os laboratórios, escritórios, salas e instalações tem portas com fechaduras.
Proteção contra ameaças externas e do meio ambiente	A sala onde ficam os servidores e equipamentos de rede tem proteção contra incêndio e portas para evitar acesso indevido.
	Material inflamável, material de papelaria e suprimentos de grande volume são armazenados no almoxarifado do instituto, longe dos servidores de rede.
	Equipamentos para contingência e mídias de backup são armazenados em outro prédio dentro do campus do instituto.
Trabalhando em áreas seguras	Não são divulgadas sem necessidade informações sobre os locais onde estão os servidores e equipamentos de rede do instituto, bem como sobre as atividades desenvolvidas nos locais onde esses equipamentos estão.
	Os locais onde ficam os servidores de rede ficam trancados quando desocupadas.
CATEGORIA DE CONTROLE: SEGURANÇA DE EQUIPAMENTOS	
Controles	Procedimentos e Tecnologias Adotados
Utilidades	Os servidores da rede de computadores tem fontes redundantes e o instituto tem gerador.
	Os servidores da rede de computadores são alimentados por no-breaks.
	A sala onde ficam os servidores de rede tem aparelhos de ar-condicionado redundantes.
	As chaves de desligamento da rede elétrica ficam perto da saída da sala.
	As salas dos servidores de rede contam com iluminação de emergência.
Remoção de propriedade	As retiradas e devoluções de ativos das instalações da instituição precisam ser autorizadas e são registradas.

FONTE: Elaboração própria, 2014.

O Quadro 4 apresenta os controles e procedimentos adotados das categorias de controle Procedimentos e responsabilidades operacionais, Gerenciamento de serviços terceirizados, Planejamento e aceitação dos sistemas, Proteção contra códigos maliciosos e códigos móveis, Gerenciamento da segurança em redes, Manuseio de mídias, Troca de informações, Serviços de comércio eletrônico e Monitoramento, todos da seção de controle Gerenciamento das operações e comunicações, que tem 32 controles, dos quais 15 são adotados.

QUADRO 4 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES.

CATEGORIA DE CONTROLE: PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS	
Controles	Procedimentos e Tecnologias Adotados
Documentação dos procedimentos de operação	Procedimentos para realização de backup e restauração de dados, tratamento de erros conhecidos, reinício de operação de servidores de rede e verificação de trilhas de log estão documentados em uma base de conhecimentos. Endereços e telefones de fornecedores e profissionais de suporte estão documentados. São registrados os autores que realizam alterações nos procedimentos.
Segregação de funções	Sistemas específicos para determinados setores e diretórios de rede para armazenamento de arquivos são segregados por setor ou grupos de trabalho. Os acessos aos diretórios da rede são controlados. Todas as solicitações de acesso a diretórios de outros setores precisam ser autorizadas pelos chefes dos setores. A área de TI tem suas funções internas definidas, com responsáveis formalmente designados.
CATEGORIA DE CONTROLE: GERENCIAMENTO DE SERVIÇOS TERCEIRIZADOS	
Controles	Procedimentos e Tecnologias Adotados
Entrega de serviços terceirizados	Os contratos de serviços incluem cláusulas de nível de serviço e uma definição clara dos serviços contratados. As informações acumuladas por terceiros durante uma execução de contrato são armazenadas em base de conhecimentos e podem ser passadas para outra empresa que a substituir. As contratações são feitas com garantia de funcionamento ou recuperação.
Monitoramento e análise crítica de serviços terceirizados	Os serviços, relatórios e registros fornecidos por empresas terceirizadas são monitorados e analisados criticamente quanto à aderência aos requisitos de contratação e segurança da informação. Os acessos de terceiros a informações sensíveis ou críticas e a recursos de processamento de informações são controlados através de conta individual de acesso à rede e senha.
Gerenciamento de mudanças para serviços terceirizados	As mudanças em serviços terceirizados são controladas quanto à manutenção dos procedimentos existentes e proteção dos softwares.
CATEGORIA DE CONTROLE: PLANEJAMENTO E ACEITAÇÃO DOS SISTEMAS	
Controles	Procedimentos e Tecnologias Adotados
Gestão de capacidade	Sistemas de monitoramento são utilizados para monitorar a utilização de recursos dos servidores de rede e do link de acesso à Internet. As informações colhidas utilizando os sistemas de monitoramento são utilizadas em projeções de crescimento da utilização. Cada novo serviço a ser implantado na rede é verificado quanto aos seus requisitos de capacidade antes de ser adquirido ou entrar em produção.
CATEGORIA DE CONTROLE: PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS E CÓDIGOS MÓVEIS	
Controles	Procedimentos e Tecnologias Adotados
Controles contra códigos móveis	Os sistemas que precisam de autorização dos ordenadores de despesas utilizam criptografia e autenticação digital.
CATEGORIA DE CONTROLE: GERENCIAMENTO DA SEGURANÇA EM REDES	
Controles	Procedimentos e Tecnologias Adotados
Controles de redes	O instituto tem procedimentos para gerenciamento e monitoramento da rede e as responsabilidades referentes a monitoramento e gerenciamento estão formalmente definidas, com os responsáveis formalmente designados. O acesso à rede sem fio é restrito a dispositivos cadastrados e os acessos feitos pelos dispositivos são monitorados. A rede sem fio é segregada da rede local do instituto por um firewall, que não permite acessos aos diretórios localizados nos servidores de rede.
Segurança dos serviços de rede	O instituto tem um firewall, um proxy, um servidor Webmail com chave de criptografia, anti-spam e antivírus. Endereços web potencialmente perigosos são bloqueados pelo proxy.
CATEGORIA DE CONTROLE: MANUSEIO DE MÍDIAS	
Controles	Procedimentos e Tecnologias Adotados
Segurança da documentação dos sistemas	Os acessos à documentação dos sistemas é protegida e controlada, de acordo com as permissões de acesso aos diretórios na rede onde estão armazenadas.

CATEGORIA DE CONTROLE: TROCA DE INFORMAÇÕES	
Controles	Procedimentos e Tecnologias Adotados
Mídias em trânsito	As mídias magnéticas ou óticas que armazenam informações da instituição e que são enviadas para fora das suas instalações são protegidas em caixas lacradas.
Sistemas de informações do negócio	Os sistemas de informação utilizados tem restrições de acesso à funcionalidades que são exclusivas a alguns usuários. Usuários que não tem vínculo com a instituição não acessam os sistemas de informação. Funcionários terceirizados tem acesso apenas durante a vigência dos seus contratos, e são cadastrados individualmente. Usuários que se desligam da instituição tem suas contas de acesso à rede e aos sistemas de informação bloqueadas no fim do último dia de trabalho.
CATEGORIA DE CONTROLE: SERVIÇOS DE COMÉRCIO ELETRÔNICO	
Controles	Procedimentos e Tecnologias Adotados
Comércio eletrônico	As compras eletrônicas passam por um processo de autorização pela direção do instituto. Os sistemas utilizados para efetuar compras são protegidos por criptografia e assinatura digital.
Transações on-line	As transações on-line passam por um processo de autorização pela direção do instituto. Os sistemas utilizados para efetuar transações on-line são protegidos por criptografia e assinatura digital.
CATEGORIA DE CONTROLE: MONITORAMENTO	
Controles	Procedimentos e Tecnologias Adotados
Proteção das informações dos registros (log)	Os registros de log são armazenados em diretórios acessíveis somente para os servidores do instituto que administram a rede de computadores.

FONTE: Elaboração própria, 2014.

O Quadro 5 mostra os controles e procedimentos das categorias de controle Gerenciamento de acesso do usuário, Controle de a

cesso à rede e Controle de acesso ao sistema operacional, da seção de controle de acessos. Neste quadro, dos 25 controles previstos na norma, apenas seis são adotados pelo instituto de pesquisa.

QUADRO 5 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE DE ACESSOS.

CATEGORIA DE CONTROLE: GERENCIAMENTO DE ACESSO DO USUÁRIO	
Controles	Procedimentos e Tecnologias Adotados
Registro de usuário	Os usuários precisam ter um vínculo formal para ter acesso à rede de computadores e outros sistemas. Cada usuário tem sua conta individual de acesso à rede e aos sistemas e serviços disponibilizados. Para ter acesso à rede, o usuário precisa de uma autorização do chefe do setor onde está lotado.
CATEGORIA DE CONTROLE: CONTROLE DE ACESSO À REDE	
Controles	Procedimentos e Tecnologias Adotados
Identificação de equipamento em redes	Todos os dispositivos que acessam a rede e os equipamentos de rede estão devidamente identificados e tombados.
Proteção e configuração de portas de diagnóstico remotas	O acesso às portas de configuração e diagnóstico dos equipamentos de rede exigem conta de acesso e senha exclusivas dos servidores do instituto que trabalham com infraestrutura.
Segregação de redes	O ambiente de rede do instituto está segregado em pelo menos em rede local, uma zona desmilitarizada (DMZ) e uma rede pública. Os perímetros dessa rede estão protegidos por firewall. A rede sem fio do instituto é separada da rede local onde estão os servidores de rede, sistemas de informação, bancos de dados e informações sensíveis ou críticas. O instituto não tem interligação física com redes de parceiros ou fornecedores. São feitos acessos pontuais utilizando tecnologia de redes virtuais privadas (VPN).
Controle de conexão de rede	O acesso à rede sem fio é controlado, embora permitido para computadores pessoais. A rede local é acessível apenas para computadores tombados.
CATEGORIA DE CONTROLE: CONTROLE DE ACESSO AO SISTEMA OPERACIONAL	
Controles	Procedimentos e Tecnologias Adotados
Identificação e autenticação de usuário	Todas as contas de acesso (incluindo as de pessoal de suporte e administradores de rede) são individuais. Os sistemas tem controles para rastrear acessos e atividades desenvolvidas pelos usuários.

FONTE: Elaboração própria, 2014.

O Quadro 6 traz os controles e procedimentos da categoria de controle Segurança dos arquivos do sistema, da seção de controle Aquisição, desenvolvimento e manutenção de sistemas de informação, que tem 16 controles, dos quais seis são adotados pelo instituto de pesquisa.

QUADRO 6 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE AQUISIÇÃO, FONTE: ELABORAÇÃO PRÓPRIA, 2014.

CATEGORIA DE CONTROLE: SEGURANÇA DOS ARQUIVOS DO SISTEMA	
Controles	Procedimentos e Tecnologias Adotados
Proteção dos dados para teste de sistema	Os testes dos sistemas desenvolvidos internamente são feitos utilizando dados falsos.
Controle de acesso ao código-fonte de programa	Os acessos aos códigos-fonte dos sistemas desenvolvidos pelo instituto são restritos aos analistas de desenvolvimento.

FONTE: Elaboração própria, 2014.

Por fim, o Quadro 7 traz os controles e procedimentos adotados pelo instituto de pesquisa relacionados à categoria de controle Conformidade com requisitos legais, da seção de controle Conformidade. Esta seção de controle tem 10 controles, sendo que o instituto de pesquisa estudado adota apenas dois deles.

QUADRO 7 – CONTROLES, PROCEDIMENTOS E TECNOLOGIAS ADOTADOS PARA A SEÇÃO DE CONTROLE CONFORMIDADE.

CATEGORIA DE CONTROLE: CONFORMIDADE COM REQUISITOS LEGAIS	
Controles	Procedimentos e Tecnologias Adotados
Prevenção de mau uso de recursos de processamento da informação	O instituto tem uma norma que estabelece regras de acesso ao serviço de correio eletrônico, prevendo ações disciplinares contra infratores. Os sistemas tem controles para rastrear acessos e atividades desenvolvidas pelos usuários. Os usuários são informados a respeito da norma que estabelece regras de acesso ao serviço de correio eletrônico.
Regulamentação de controles de criptografia	As leis, acordos e regulamentações pertinentes são observados ao adquirir e utilizar recursos de criptografia.

FONTE: Elaboração própria, 2014.

Além daquelas cujos objetivos de controle são alcançados, destacam-se também quatro outras categorias de controle, que estão apresentadas abaixo, juntamente com seus objetivos de controle e com os controles adotados pelo instituto de pesquisa estudado:

- Encerramento ou mudança da contratação, cujo objetivo de controle é assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada, e cujos controles utilizados no instituto são Encerramento de atividades e Retirada de direitos de acesso;
- Áreas seguras, que tem como objetivo de controle prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização, e cujos controles adotados pelo instituto são: Controles de entrada física; Segurança em escritórios, salas e instalações; Proteção contra ameaças externas e do meio ambiente; e Trabalhando em áreas seguras;

- Serviços de comércio eletrônico, cujo objetivo de controle é garantir a segurança de serviços de comércio eletrônico e sua utilização segura, e que tem como controles adotados Comércio eletrônico e Transações on-line;
- Segurança dos arquivos do sistema, que tem como objetivo de controle Garantir a segurança de arquivos de sistema, e cujos controles adotados no instituto pesquisado são Proteção dos dados para teste de sistema e Controle de acesso ao código-fonte de programa.

De cada uma dessas categorias de controle, são adotados pelo menos dois terços dos controles previstos na norma. Segundo os entrevistados que trabalham com infraestrutura e administração da rede de computadores, as contas de acesso à rede das pessoas que perdem o vínculo com o instituto são bloqueadas no último dia de trabalho e excluídas após seis meses de inatividade. Outro entrevistado afirmou que as responsabilidades para realizar o encerramento ou a mudança de um contrato estão definidas e atribuídas formalmente. As áreas seguras do instituto estão protegidas por controles de entrada e saída, evitando a entrada de pessoas não autorizadas, o acesso às áreas de processamento de informações é restrito a pessoas autorizadas. Todas as salas têm portas com chave, protegendo os equipamentos de processamento de informações e são protegidas contra incêndios. Materiais perigosos, de papelaria e outros de grande volume são armazenados nos laboratórios ou no almoxarifado do instituto, distante da sala onde ficam os servidores da rede de computadores. As mídias de backup ficam armazenadas longe do local onde estão os servidores da rede de computadores e as áreas seguras são trancadas e protegidas. Todas as compras e transações on-line realizadas pelo instituto passam por um processo de autorização pela Diretoria e os sistemas de comércio eletrônico que o instituto utiliza para fazer suas compras são protegidos por criptografia e utilizam assinaturas digitais. Os dados utilizados para teste dos sistemas em desenvolvimento u homologação são falsos e o acesso aos códigos-fonte dos sistemas do instituto são protegidos contra acessos indevidos. Esses procedimentos e processos não garantem que os objetivos de controle sejam atingidos, mas são indícios importantes de que controles de segurança da informação estão sendo seguidos.

Das 39 categorias de controle da norma, 17 não tiveram controle adotado, o que demonstra fragilidade em adotar boas práticas de segurança da informação. A categoria de controle Política de segurança da informação, que tem como objetivo de controle prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, não tem nenhum controle adotado no instituto, apesar de ser fundamental para implementar diversos controles relacionados a outros objetivos de controle. A ABNT (2005) diz que a Política de Segurança da Informação é um dos fatores críticos de sucesso para estabelecer a segurança da informação, o que confirma a importância desse documento para a segurança da informação. Apesar disso, dois entrevistados tenham afirmado que a Fundação F tem uma Política de Segurança da Informação aprovada pela sua Presidência e publicada desde fevereiro de 2011. Apesar de a sede da organização ter publicado uma Política, um dos entrevistados identificou que esse documento não é suficiente para

os institutos da Fundação. Na sua opinião, cada unidade descentralizada deveria elaborar sua própria Política de Segurança, em conformidade com a legislação vigente e com a Política da Fundação F, que é válida para toda a organização. Ele justifica dizendo que cada instituto sempre fez e continua fazendo seu planejamento orçamentário e executa de maneira independente, e cada instituto tem características e especificidades que podem não ser atendidas de maneira satisfatória por uma norma geral, exigindo uma complementação na esfera local, elaborada por pessoas que conhecem a realidade do seu instituto.

Um entrevistado da área de infraestrutura afirmou que "As unidades tem equipes de TI independentes, contam com infraestrutura de TI desenvolvidas de maneira independente, com tecnologias diferentes, desempenham atividades diferentes, embora façam coisas semelhantes e todas desenvolvam pesquisa e atividades de ensino. A Fundação demorou demais de organizar e centralizar decisões importantes sobre TI. Somente no final de 2009 a Fundação criou uma estrutura para estabelecer alguns processos de Governança de TI". Até isso acontecer, cada instituto organizou sua área de TI e tomou decisões sobre tecnologia da forma que fosse mais conveniente. "Algumas unidades estão bem estruturadas há algum tempo, com Comitê Gestor de TI e Comitê de Segurança da Informação criados, com Política de Segurança própria", afirmou um dos entrevistados, que completou, afirmando que "Há muita disparidade, mas o certo é cada unidade ter suas políticas, seus comitês e fazer seus planejamentos estratégicos de TI seguindo orientações gerais da sede."

Esse é um indício de que a falta de um direcionamento estratégico centralizado tenha sido um fator determinante para que os institutos desenvolvessem controles de segurança da informação de maneira heterogênea, embora a instituição esteja buscando centralizar a tomada de decisões estratégicas, contexto em que foi publicada a Política de Segurança da Informação geral. O que se faz necessário no momento é cada instituto elaborar sua própria Política, suas normas e seus procedimentos, mais adequados às suas próprias realidades, sem esquecer a orientação dada pela sede da fundação.

6 Considerações Finais

Com este trabalho, pretendia-se identificar as categorias de controles de segurança da informação que tem seus objetivos de controle alcançados na Fundação F, bem como os mecanismos e processos de segurança da informação utilizados para alcançar esses objetivos, tendo como base a norma NBR ISO/IEC 27002:2005. O instrumento de coleta foi um roteiro de entrevista estruturada que foi utilizado em entrevistas com os servidores públicos e profissionais terceirizados da área de TI do instituto de pesquisa.

A maioria dos entrevistados declarou que não conhece a norma NBR ISO/IEC 27002 ou a sua denominação anterior, NBR ISO/IEC 17799. A maioria dos servidores públicos do instituto que trabalham com TI declarou conhecer a norma e a maioria dos profissionais terceirizados declarou não conhecê-la. Isso mostra uma deficiência na seleção dos profissionais terceirizados quanto a capacitação dos profissionais. O fato de poucos controles serem adotados evidencia uma fragilidade da instituição em

adotar boas práticas de segurança da informação, o que, em parte, é fruto de uma falta de direcionamento estratégico da sede da instituição. O fato de haver dois objetivos de controles que são alcançados não garante para o instituto pesquisado que suas informações estejam seguras. Deve-se destacar que os controles relacionados à Política de Segurança da Informação, que tem ligação com diversos outros controles ao longo da norma, não são adotados.

O pressuposto de que não havia nenhum objetivo de controle de segurança da informação atendido pelos controles adotados no instituto pesquisado não foi comprovado. As respostas indicaram que dois objetivos de controle são alcançados com os controles adotados pelo instituto: "Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados", relacionado à categoria de controle Gerenciamento de serviços terceirizados; e "Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte", relacionado à categoria de controle Gerenciamento de segurança em redes. Embora isso tenha acontecido, é primordial que o instituto elabore, aprove e publique sua Política de Segurança da Informação em conformidade com as leis e demais normas do Governo Federal, bem com a Política de Segurança da Informação publicada pela sede da instituição, para alcançar a segurança da informação. Esse documento elaborado e publicado a nível local servirá como orientação da alta direção para a adoção de boas práticas de segurança visando reduzir os riscos associados às informações e aumentar o retorno sobre os investimentos, principalmente sobre aqueles feitos em tecnologia.

Dessa forma, o estudo permitiu uma melhor compreensão sobre a segurança da informação em organizações que realizam pesquisa científica, cujas atividades geram e lidam com informações e conhecimentos que precisam ser protegidos. Contribuiu também para uma melhor compreensão sobre a segurança da informação em organizações públicas, contexto em que também se enquadra o instituto de pesquisa estudado.

Referências

ALEXANDRIA, J. C. S. de. Gestão da Segurança da Informação – Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica. 2009. Tese (Doutorado em Tecnologia Nuclear) – Instituto de Pesquisas Energéticas e Nucleares – Universidade de São Paulo, São Paulo, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BERNASCHI, M.; D'AIUTOLO, E.; RUGHETTI, P. Enforcing Network Security: a Real Case Study in a Research Organization. Computers & Security, v.18, n.6, p.533-543, 1999.

CAMINHA, J.; LEAL, R. T; MARQUES JUNIOR, R. O. P. C.; NASCIMENTO, M. G. do. Implantação da Gestão da Segurança da Informação em um Instituto de Pesquisa Tecnológica. In: Congresso ABIPTI 2006, Campinas. Anais... ABIPTI, 2006.

CEPIK, M.; CANABARRO, D. R; POSSAMAI, A. J. A Institucionalização do SISP e a Era Diginal no Brasil. In: CEPIK, M.; CANABARRO, D. R (Org.). Governança de TI: Transformando a Administração Pública no Brasil. Porto Alegre: WS Editor, 2010.

DONNER, M. L.; OLIVEIRA, L. R. Análise de Satisfação com a Segurança no Uso de Internet Banking em Relação aos Atuais Recursos Disponíveis no Canal Eletrônico. In: XXXII Encontro da ANPAD, EnANPAD 2008, Rio de Janeiro. Anais... ANPAD, 2008. CD-ROM.

FACHINI, G. J. Análise do Nível de Formalização da Política de Segurança da Informação à Luz da NBR ISO/IEC 17799:2005 nas Empresas de Tecnologia da Informação de Blumenau, SC. 2009. Dissertação (Mestrado em Ciências Contábeis) – Universidade Regional de Blumenau, Blumenau, 2009.

FERNANDES, A. A.; ABREU, V. F. Implantando a Governança de TI: Da Estratégia à Gestão dos Processos e Serviços. Rio de Janeiro: Brasport, 2008.

HERATH, T.; HERATH, H.; BREMSER, W. G. Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. Information Systems Management, v. 27, n.1, p.72-81, jan. 2010.

KAYO, E. K.; KIMURA, H.; MARTIN, D. M. L.; NAKAMURA, W. T. Ativos Intangíveis, Ciclo de Vida e Criação de Valor. RAC, v.10, n.3, p.73-90, jul. 2006.

LUNARDI, G. L.; DOLCI, P. C.; BECKER, J. L.; MAÇADA, A. C. G. Governança de TI no Brasil: Uma Análise dos Mecanismos Mais Difundidos Entre as Empresas Nacionais. In: IV Simpósio de Excelência em Gestão e Tecnologia, SEGeT 2007, Resende. Anais... AEDB, 2007.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Governança de TI e suas Implicações para a Gestão da TI: Um Estudo Acerca da Percepção dos Executivos. In: XXXIV Encontro da ANPAD, EnANPAD 2010, Rio de Janeiro. Anais... ANPAD, 2010. CD-ROM.

MANDARINI, M. Segurança Corporativa Estratégica. São Paulo: Usina do Livro, 2004.

MARCIANO, J. L. P. Segurança da Informação – uma abordagem social. 2006. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MELLO, L. B. B.; VASCONCELLOS, L. A.; BRAGANÇA, L. R.; MOTTA, O. M. Contribuição para Gestão de Ativos Intangíveis Organizacionais: Proposição de Um Modelo Baseado no Balenced Scorecard. In: VI Congresso Nacional de Excelência em Gestão, CNEG 2010, Niterói. Anais... CNEG, 2010.

MORAES, E. A. P.; MARIANO, S. R. H. Uma Revisão dos Modelos de Gestão em TI. In: IV Congresso Nacional de Excelência em Gestão, CNEG 2008, Niterói. Anais... CNEG, 2008.

MOREIRA, N. S. Segurança Mínima: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

MOURA, G. C. M.; GASPARY, L. P. Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação. In: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSEG 2008, Gramado. Anais... SBC, 2008.

NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. In: XXXIV Encontro da ANPAD, EnANPAD 2010, Rio de Janeiro. Anais... ANPAD, 2010. CD-ROM.