RDBCI | Revista Digital de Biblioteconomia e Ciência da Informação
Digital Journal of Library and Information Science

ISSN 1678-765X doi 10.20396/rdbci.v19i00.8665529

ARTIGO

Gestão da segurança da informação e comunicações
análise ergonômica para avaliação de comportamentos inseguros

Rogério Batista dos Santos [1] https://orcid.org/0000-0001-8545-4236
Tiago Barros Pontes e Silva [2] https://orcid.org/0000-0003-2149-5973

[1] Empresa Brasileira de Pesquisa Agropecuária, Brasília, DF, Brasil / e-mail: rogerio.bst@gmail.com
[2] Universidade de Brasília, Brasília, DF, Brasil / e-mail: tiagobps@gmail.com

RESUMO
Introdução: Este relato consiste em um estudo de caso sobre o comportamento inseguro dos funcionários de uma Instituição da Administração Pública Federal sob a ótica da Ergonomia. Objetivo: Assim, a partir da compreensão dos conceitos da Segurança da Informação e da Abordagem Ergonômica, busca-se identificar os principais fatores que levam o sujeito a assumir comportamentos que colocam em risco a Segurança da Informação da instituição ao desempenhar suas atividades cotidianas do trabalho. Método: Os dados foram coletados por meio de observações do trabalho em condições reais, levando em consideração a sua variabilidade, a situação de trabalho e os instrumentos utilizados para a realização das atividades cotidianas. Também foram realizadas entrevistas no contexto de trabalho para auxiliar os pesquisadores na compreensão dos comportamentos dos funcionários. Resultados: Foram identificados casos em que a dificuldade em seguir as recomendações de segurança da instituição está relacionada a um conflito existente na própria organização do trabalho. Conclusão: O presente trabalho aponta para uma questão que demanda maior aprofundamento na literatura: o conflito existente na própria prescrição de trabalho. Esse pode ser um dos fatores responsáveis pela dificuldade das pessoas em se comportarem de maneira segura nas instituições púbicas brasileiras.

PALAVRAS-CHAVE
Comportamento do usuário. Ergonomia. Segurança da informação.

Information and communications security management
ergonomic assessment to evaluate unsafe behaviors

ABSTRACT
Introduction: This report consists of a case study on the unsafe behavior of employees of a Federal Public Administration Institution from the Ergonomics perspective. Objective: Thus, from the understanding of the concepts of Information Security and the Ergonomic Approach, we seek to identify the main factors that lead the subject to assume behaviors that put the institution's Information Security at risk when performing their daily work activities. Methods: The data were collected through observations of the work in real conditions, considering its variability, the work situation and the instruments used to carry out daily activities. Interviews were also carried out in the work context to assist the researchers in understanding the employees' behaviors. Results: There were identified cases in which the difficulty in following the institution's safety recommendations is related to a conflict existing in the work organization itself. Conclusion: The present study points to an issue that requires further study in the literature: the conflict in the work prescription itself. This may be one of the factors responsible for the difficulty of people in behaving safely in Brazilian public institutions

KEYWORDS
User behavior. Ergonomics. Information security.

JITA: BJ. Communication

1 INTRODUÇÃO

Nos dias atuais, os avanços tecnológicos têm alterado significativamente a maneira como produzimos, organizamos e disponibilizamos informação. O aumento da capacidade de comunicação, a interação entre sistemas, a evolução das redes convergentes e o surgimento das redes móveis vêm proporcionando comunicação contínua e em diversos locais, possibilitando várias maneiras de acesso à informação. Inicialmente, esses ambientes foram projetados para fins de pesquisa, visando permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo e, por isso, a segurança não estava em foco na sua concepção inicial. Atualmente, com o crescimento da demanda comercial e a utilização estratégica das comunicações por estes meios, a Segurança da Informação (SI) tornou-se um fator prioritário para as corporações que necessitam manter seguras as suas informações, como o lançamento de um novo produto no mercado, ou o número do cartão de crédito de seus clientes.

Para as empresas privadas e as organizações públicas, o uso efetivo da informação e das comunicações com auxílio de Tecnologia da Informação (TI) permite o aumento e a eficiência de suas operações. Dados sobre cliente, produto, serviço e sobre o negócio, circulam pelos diversos setores do ambiente corporativo, auxiliando funcionários da área operacional e gestores na execução das atividades diárias. A influência dos Sistemas de Informação no desempenho das organizações pode ser vista em todas as áreas operacionais e gerenciais das empresas. Tais sistemas visam coletar, recuperar, processar, armazenar e distribuir informações, de forma automática ou não, envolvendo no seu processo pessoas, máquinas e métodos organizados. As organizações têm se tornado cada vez mais dependente da disponibilidade desses sistemas para a manutenção do seu fluxo de trabalho. Com o objetivo de garantir que a informação esteja acessível quando solicitada, protegida de acesso indevido e íntegra, a Segurança da Informação implementa uma série de controles de segurança como: políticas, procedimentos, práticas, estruturas organizacionais, hardware e software.

Os benefícios de implantar, gerenciar e controlar a SI nas organizações vão além das características de privacidade inicialmente pretendida e agregam propriedades que auxiliam as organizações a alcançarem seus objetivos (FRÓIO, 2008). Para Balloni (2007), a Segurança dos Sistemas de Informação deve contemplar não só os aspectos técnicos, como também os sociais, relacionados ao ambiente organizacional e às pessoas. Fontes, Balloni e Laudon (2015, p. 2) afirmam ainda que “devemos considerar a cultura da organização e seu momento de participação no mercado”. Por isso, além de considerar todos os fatores físicos, como ambientes e equipamentos, devem ser também consideradas as pessoas.

É necessário estar atento em manter a integridade física, psíquica e social do ser humano no contexto do trabalho, evitando que as adversidades dos tempos atuais fragilizem este que é o fator determinante da Segurança. Neste cenário, podemos observar que a competitividade, produtividade e busca por proteção das informações, entre outros fatores, têm feito com que as organizações adotem diversas ferramentas tecnológicas e metodologias de gestão para atingirem seus objetivos. No entanto, estas composições pré-estabelecidas nem sempre fornecem soluções completas e suficientes para serem diretamente aplicadas, por não contemplarem os aspectos da ação contextualizada das pessoas como sendo significativos para o resultado do trabalho.

Desta forma, guiados pelo olhar da Ergonomia, busca-se explorar as atividades realizadas pelas pessoas dentro de uma organização, com o intuito de compreender o motivo pelo qual as prescrições (políticas, normas e regras) não têm sido cumpridas conforme o esperado. Apoiada em métodos e técnicas de análise própria, a ação ergonômica busca respostas aos problemas resultantes da inadequação dos artefatos, da organização do trabalho e dos

ambientes ao modo de funcionamento humano (ABRAHÃO et al., 2009). Com ela, é investigado o trabalho real do sujeito, respeitando a sua variabilidade, assim como da situação de trabalho e dos instrumentos.

No cotidiano de trabalho de instituições ligadas ao Governo Brasileiro, são comuns os incidentes relacionados a Segurança da Informação. A Instituição da Administração Pública Federal (IAPF) na qual a pesquisa foi realizada, não identificada por questões de proteção da informação, é um exemplo na qual essas adversidades têm impactado diretamente no seu o fluxo normal de trabalho. São exemplos comuns de comportamentos inseguros que podem ser observados na instituição o compartilhamento de senha, o compartilhamento de informações com permissões além das necessárias, o uso de equipamentos tecnológicos de cunho particular dentro da instituição, entre outros. Assim, surge a necessidade de se compreender os fatores que levam as pessoas a adotarem esse comportamento.

Portanto, o objetivo do presente trabalho é identificar os principais fatores relacionados aos comportamentos inseguros adotados na Instituição Pública Federal. Para tanto, pretende-se: descrever as diretrizes e recomendações de Segurança da Informação vigentes na instituição no momento em que a pesquisa foi realizada; descrever os principais incidentes de Segurança da Informação ocorridos na IAPF no período; identificar os comportamentos dos funcionários relacionados aos incidentes considerados inseguros; e relatar as dificuldades das pessoas em cumprir as diretrizes de segurança.

Destaca-se que o ano exato de coleta dos dados também será omitido no relato para fins de proteção institucional. Entretanto, observa-se a evolução da regulamentação vigente sobre o tema, como, por exemplo, a Instituição da Política Nacional de Segurança da Informação (PNSI), formalizada pelo decreto nº 9.637 de dezembro de 2018 (BRASIL, 2018). No mesmo sentido, é importante considerar que a coleta dos dados ocorreu antes da pandemia de COVID-19 que se iniciou em 2020, de modo que todas as implicações do uso de tecnologias para o trabalho remoto, e suas decorrências em termos de segurança da informação, não foram contempladas no presente estudo.

2 SEGURANÇA DA INFORMAÇÃO

No passado, a questão da Segurança da Informação era muito mais simples, os dados eram armazenados em papéis que ficavam guardados em gavetas e arquivos. A segurança consistia apenas em restringir o acesso físico àquele local. Com a chegada dos computadores de grande porte, a estrutura de segurança ficou mais sofisticada, dotada de controles de acesso lógicos, segurança física do ambiente de computação e conscientização das poucas pessoas envolvidas. Com o advento dos computadores pessoais, dos dispositivos móveis e das redes convergentes, os aspectos da segurança tornaram-se complexos. Os dados e as informações são acessados continuamente e em diversos locais, as possibilidades de utilização são mais amplas que em sistemas fechados, assim como os riscos à privacidade e a integridade da informação.

O uso cada vez mais amplo das Tecnologias da Informação (TI) para as várias atividades pessoais, como lazer e trabalho, é uma característica central da sociedade da informação. Apesar de uma parcela dos dados e informações disponíveis nos Sistemas de Informação ser destinada ao acesso público, outras operações requerem algum nível de segurança, como as transações com número de cartões de crédito, dados de contas bancárias, além de acesso a informações privadas. Nesse sentido, a Segurança Cibernética é definida por

> ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade

> dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (BRASIL, 2019).

Em uma perspectiva mais ampla, para o psicólogo americano Abraham Maslow (1954), segurança é uma estabilidade básica desejada por todos. É uma necessidade do ser humano que surge na medida em que as necessidades fisiológicas estejam razoavelmente satisfeitas, como; comer, dormir e respirar. “Apenas os seres humanos e suas organizações são capazes de desenvolver ou alcançar a segurança”. (FERNANDES, 2009, p. 9).

Antes de se discutir a segurança no contexto informacional, é necessário definir o conceito de informação. Informação é o resultado do tratamento de dados existentes acerca de alguém ou de alguma coisa, um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor do fato em si (STAIR, 1998). Ela consiste em “dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato” (BRASIL, 2019). Quando íntegra e disponível, ela tem valor altamente significativo e pode representar grande poder para quem a possui, pois permite aos seus detentores tomarem iniciativas ou mesmo antecipar-se na ação, produzir conhecimento e aplicá-lo às suas necessidades, e às novas demandas originadas no enriquecimento da vida, seja ela pessoal ou organizacional.

Informação é atribuição de significado a um conjunto de dados. O dado pode ser entendido como uma sequência de símbolos é um ente sintático. Ele é apenas um índice, um registro, uma manifestação objetiva, passível de análise, exigindo interpretação da pessoa para sua manipulação. Os dados podem ser representados por sons, imagens, textos, números e estruturas, e quando estes são organizados ou configurados de uma maneira significativa, se tornam uma informação (SIMON, 1999).

Para as empresas, a capacidade de captar e absorver informação correta e de forma ágil determina suas possibilidades de inovar produtos, aumentar a lucratividade e atender bem ao seu cliente, sendo competitiva em um mercado altamente instável e ágil como o dos tempos atuais. De acordo com Chiavegatto (2002), a falta de informação apropriada e de conhecimento como subsídio ao processo decisório causa lentidão, ineficiência e elevação de custo quando na implementação de ações. Diante disso, as organizações sentem a necessidade de fazer uso das informações, de maneira proativa e dinâmica, com a finalidade de garantir a sobrevivência em um ambiente cada vez mais complexo e competitivo.

A cada dia torna-se mais claro o papel econômico da informação como insumo para o desenvolvimento de produtos, captação de recursos, conhecimento de mercado e sobrevivência de muitas empresas do setor privado. No que diz respeito ao setor público, o uso da informação e do conhecimento não está voltado para a competitividade em mercados, mas sim para a prestação de serviços em prol da sociedade de determinada localidade. Nas organizações públicas, a Segurança da Informação (SI) é utilizada para incrementar a possibilidade de prestar bons serviços aos cidadãos. Sendo pública ou privada, o propósito de uma organização no tocante à SI é sempre o mesmo: proteger os recursos mais importantes da organização, sejam eles tangíveis ou não, como os recursos físicos, financeiros, sua posição legal, conhecimento institucional etc.

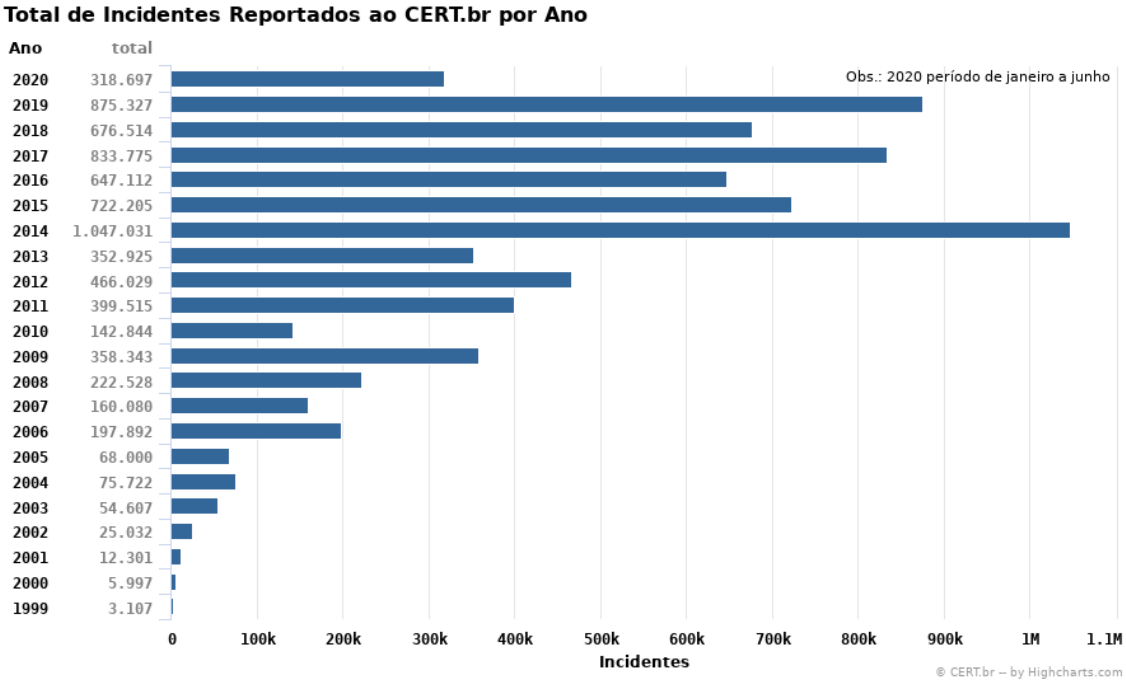
Neste sentido, a Segurança da Informação pode ser compreendida por “ações que objetivam viabilizar e assegurar a disponibilidade, integridade, a confidencialidade e a autenticidade das informações” (BRASIL, 2019). Informações adulteradas, não disponíveis quando necessárias, sob o domínio de pessoas de má fé ou de concorrentes, podem expor a organização e seus profissionais a prejuízos consideráveis.

Todos os dias os Sistemas de Informação e redes de computadores das organizações são colocados à prova por diversos tipos de ameaças. Para Dias (2000), a informação é o principal patrimônio da empresa e está sob constante risco.

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à SIC, incluindo fraudes eletrônicas, roubo de informação, espionagem, sabotagem, vandalismo, fogo, inundação e outros acidentes. (NETTO, FREIRE e ALEMMAND, 2008, p. 6).

Diante desse fato, ela deve ser protegida adequadamente, assim como os ambientes e os equipamentos utilizados para o seu processamento, que também estão sob constante ameaça. Problemas causados por vírus, *hackers* e indisponibilidade dos sistemas estão se tornando cada vez mais comuns, mais ambiciosos e mais sofisticados (ABNT, 2005). Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), o número total de notificação de incidentes reportados vem crescendo de forma considerável nos últimos anos, chegando a 875.327 casos em 2019 (Figura 1).

Figura 1. Estatística dos Incidentes Reportados ao CERT.br



Fonte: http://www.cert.br/stats/incidentes

No contexto atual, as organizações são dependentes dos Sistemas de Informação, que crescem em quantidade e em complexidade e que controlam os mais variados tipos de operação, além do próprio fluxo de informação nas organizações. Os SI adquiriram grande importância para a sobrevivência da maioria das organizações modernas, não apenas na imagem da organização perante seus clientes e parceiros, como também no andamento dos próprios processos organizacionais. “É possível inviabilizar a continuidade de uma organização se não for dada à devida atenção à segurança de suas informações” (BRASIL, 2008, p 26).

Nesse sentido, a Segurança da Informação (SI) é um processo de gerenciamento que visa a proteção de equipamento computacional e não-computacional, instalações, dados e informação contra o mau uso por parte de terceiros não autorizados. Essa definição engloba também equipamentos como computadores, faxes e fotocopiadoras, e todos os tipos de mídia, até mesmo documento em papel (BALLONI, 2007). Os benefícios de implantar, gerenciar e controlar as informações e comunicações nas organizações vai além da simples restrição ao acesso da informação. Ela também visa:

a) Aumentar a produtividade dos usuários por meio de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática, viabilizando até o

uso de aplicações de missão crítica;
b) Demonstrar responsabilidade em prol da proteção do cliente e da própria informação;
c) Reduzir custo devido à melhora do controle operacional e do gerenciamento de perdas;
d) Manter a imagem da organização aprimorada elevando a confiabilidade em seus serviços;
e) Conduzir a empresa a alcançarem os seus objetivos, pois seus sistemas de informação serão mais confiáveis.

Portanto, permite que a organização se adeque às legislações e códigos de ética vigentes, mantendo sua imagem íntegra e transparente para investidores, auditores e sociedade. Para Balloni (2007), a SI visa garantir a disponibilidade, integridade, confidencialidade da informação. Outros autores também discutem sobre as propriedades que devem ser observadas para se obter uma informação segura. De acordo com a norma ABNT (2006), a Segurança da Informação é caracterizada pela preservação da disponibilidade, integridade e confidencialidade da informação, além de outras propriedades como Autenticidade, Confiabilidade, Não-Repúdio e Responsabilidade sobre a informação. Para Dias (2000); Albuquerque e Ribeiro (2002) e Sêmola (2003), para uma informação ser considera segura, o sistema que o administra ainda deve respeitar, Autenticidade, Não-repúdio, Legalidade e Auditoria.

A **Disponibilidade** pode ser compreendida como a garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário e requerido (ALBUQUERQUE; RIBEIRO, 2002). As informações armazenadas nos Sistemas de Informações devem estar acessíveis a quem de direito, quando solicitadas. Quando as informações ficam impedidas por algum motivo de serem acessadas quando solicitadas, fica caracterizada a ausência da disponibilidade. A **Integridade** é a garantia de que as informações e métodos de processamento somente sejam alterados por meio de ações planejadas e autorizadas (NETTO, FREIRE e ALLEMAND, 2008). As informações trocadas entre indivíduos devem ter a garantia de que não foram modificadas. Quando um elemento, sem autorização, intercepta, modifica e reenvia a mensagem ao destinatário, fica caracterizada a quebra da integridade. A **Confidencialidade** é a garantia de que a informação é acessível somente a pessoas autorizadas. As informações trocadas entre indivíduos e empresas nem sempre deverão ser conhecidas por todos, e muitas informações geradas pelas pessoas se destinam a um grupo específico de indivíduos, muitas vezes a uma única pessoa. Quando um elemento, sem autorização, tiver acesso a uma determinada informação, e, ao mesmo tempo, manipular ou armazená-la, fica caracterizada a quebra da confidencialidade. A **Autenticidade** está relacionada à devida autorização de uma determinada pessoa física ou de sistema, órgão ou entidade que produz, expede, modifica ou destrói informações da organização. É a identificação e certeza da origem da informação. **Não-repúdio** consiste em impedir que uma entidade participe de uma dada operação e posteriormente negue esta participação (FRÓIO, 2008, p 12).

Também são características importantes do processo de gestão da Segurança da Informação (SI) a **Legalidade**, como a garantia de que as medidas legais cabíveis são aplicadas quando necessárias, e **Auditoria**, que possibilita a apuração e avaliação de responsabilidade contra erros e atos cometidos por usuários autorizados nos sistemas de informação. Para identificar autores e ações, são utilizadas trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando.

Atualmente, a Segurança da Informação é conhecida até mesmo por presidentes de empresas, em virtude da importância da informação na condução dos negócios (BALLONI, 2007). Segundo o autor, para a realização de um negócio viável, a segurança deve garantir que o uso da informação nas várias iniciativas empresariais aconteça de forma regulada.

Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças. Esse novo contexto requer das organizações, equipes e métodos de segurança permanentes e em constante evolução, levando em consideração o controle a acesso físico, lógico e principalmente a conscientizarão das pessoas envolvidas no processo. Contudo, este universo está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações.

A **ameaça** pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, por meio de uma vulnerabilidade gerando um determinado impacto. **Vulnerabilidade** é uma falha no projeto, implementação, configuração de um software ou sistema operacional que, quando explorada por uma ameaça, resulta na violação da segurança. Quando existem ameaças e vulnerabilidades em um determinado ambiente, consequentemente temos o risco de segurança. O **risco** é um evento possível e potencialmente danoso a um organismo. Isto é, um evento hipotético que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante (FERNANDES, 2009). Quaisquer eventos adversos, confirmados ou sob suspeita, que possam ameaçar a Segurança da Informação (SI) são denominados **incidentes** de segurança. Já o **evento** de segurança é a ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação (ABNT, 2005).

Além das fragilidades internas aos Sistemas de Informação, existe a possibilidade de que um agente externo tente obter ou modificar informações de maneira não autorizada, como um ataque. O **ataque** pode ser definido como um assalto ao sistema de segurança que deriva de uma ameaça inteligente, isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um método ou técnica) para invadir serviços de segurança e violar as políticas do sistema (SHIREY, 2000). O ataque é ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente.

A fim de evitar os problemas relacionados à Segurança da Informação, são utilizados pela instituição os **controles**, que são todos os meios e dispositivos para promover, direcionar, restringir, governar e verificar as várias atividades que têm como propósito principal a observação de que os objetivos da empresa são alcançados. De acordo com a ABNT (2006), uma série de controles devem ser utilizados a fim de conduzir os negócios das empresas de forma eficiente, garantindo a salvaguarda das informações, mantendo a sua disponibilidade, integridade, confidencialidade e autenticidade.

Diante destes desafios surge a necessidade de um processo de Gestão da Segurança da Informação (GSI), que visa sistematizar e organizar a aplicação das práticas de Segurança da Informação (SI) para que os negócios das organizações estejam seguros e seus objetivos sejam alcançados com sucesso (FRÓIO, 2008).

Gestão da Segurança da Informação é um conjunto de práticas e métodos de gestão que visam promover e manter os ativos da organização em níveis aceitáveis e necessários de segurança para que os objetivos do negócio sejam atingidos conforme planejado (FRÓIO 2008, p. 14).

A GSI adota uma abordagem sistemática para minimizar o risco do acesso não-autorizado ou perda de informação e garantir o gerenciamento eficaz das medidas de proteção acionadas. Eles fornecem uma estrutura para que as organizações gerenciarem sua conformidade com requerimentos legais, entre outros, além de melhorarem o desempenho do gerenciamento de informação com segurança.

Para compor um modelo de gestão mais completo e robusto, a Gestão da Segurança da Informação baseia-se na interação entre processos, procedimentos, controles, melhores práticas e tecnologias para nortear os modelos atualmente utilizados. A Política de Segurança da Informação (POSI) é um conjunto de regras, padrões e procedimentos claramente definidos e os controles apropriados para reduzir os riscos a níveis aceitáveis. Nela se encontram as orientações necessárias para a condução segura dos negócios da organização de forma a garantir a continuidade institucional. “A adoção de políticas e GSI deve ser uma decisão estratégica da organização, observando que essa decisão é influenciada pelas necessidades, objetivos, requisitos de segurança, tamanho e estrutura da organização” (NETTO, FREIRE e ALLEMAND, 2008, p. 4).

A POSI é encarada pelas organizações e especialistas como um dos mais importantes componentes de uma solução corporativa de segurança. Ela contribui para a melhoria do comportamento das pessoas que trabalham nas empresas e manipulam a informação. A Política de Segurança da Informação tem como objetivo direcionar e suportar a proteção dos ativos de informação quanto a revelação intencional ou não-intencional, modificação, destruição ou negação, por meio da implementação de planos que permitam o retorno imediato do negócio, procedimentos e rotinas (PELTIER, 2004). Para a ABNT (2005), o objetivo da Política de Segurança da Informação é prover orientação e apoio da direção para a Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Alertando para o fato de que o documento de política deve ser aprovado pela direção, publicado e comunicados a todos os empregados.

Pesquisas em Segurança da Informação revelam que nos ambientes de trabalho, os problemas internos, que envolvem as pessoas, têm se mostrado mais representativos do que os externos (LOPES, 2009). É perceptível nas organizações que, mesmo após altos investimentos em treinamento e conscientização dos funcionários, muitos ainda tendem a se comportarem de maneira irregular, cometendo erros e descuidos que comprometem a Segurança da Informação. Na busca de possíveis soluções para o processo de avaliação do comportamento humano é adotada a ótica da Ergonomia, focada na compreensão das interações entre os seres humanos e outros elementos ou sistemas. A Ergonomia tem a análise da situação real de trabalho como sua principal ferramenta, norteando a ação ergonômica e delimitando os instrumentos e procedimentos mais adequados para a análise (ABRAHÃO e PINHO, 1999).

O grande desafio da análise ergonômica neste trabalho consiste em identificar os reais problemas existentes no ambiente de trabalho da organização no tocante a Segurança da Informação, que aumentam os riscos, proporcionando a exposição das vulnerabilidades do sistema, resultando em perdas e danos para a instituição. Acredita-se que, a partir da perspectiva Ergonômica, com foco no fator humano, é possível pensar em políticas e regras adaptadas às habilidades e limitações das pessoas. Com isso, espera-se maior eficiência na implementação e alcance dos objetivos na criação de ambientes seguros.

3 A ABORDAGEM ERGONÔMICA

Esta pesquisa se caracteriza como aplicada, pois procura melhorar o entendimento de problemas dentro uma instituição específica, no caso as bibliotecas da Universidade Federal de Minas Gerais (UFMG); criar soluções para os problemas; e desenvolver conclusões de relevância prática para resolução desses problemas.

Neste tópico é descrita a abordagem da Ergonomia para a investigação do comportamento das pessoas em seus postos de trabalho. Para a Ergonomia, o trabalho é definido por uma prescrição (tarefa) que é diferente do trabalho real (atividade). Devido a essas diferenças, as pessoas elaboram estratégias para poderem manter o fluxo de trabalho e realizarem os objetivos da tarefa. A Ergonomia tem como objetivo transformar o trabalho (ou mesmo as ferramentas de trabalho) de forma a adaptá-lo às características e variabilidade das pessoas e do processo produtivo. Assim, "a ação ergonômica busca resposta aos problemas resultantes da inadequação dos artefatos, da organização do trabalho e dos ambientes ao modo de funcionamento humano" (ABRAHÃO et al., 2009, p. 11).

De acordo com a Associação Internacional de Ergonomia (IEA), define-se Ergonomia como uma disciplina científica relacionada ao entendimento das interações entre os seres humanos e outros elementos ou sistema, e à aplicação de teorias, princípios, dados e métodos a projetos a fim de otimizar o bem-estar humano e o desempenho global do sistema (IEA, 2000). Nesta perspectiva, a Ergonomia foi se desenvolvendo adotando como referência a noção de variabilidade, a distinção entre tarefa e atividade, e a regulação das ações ao reconhecimento da competência dos trabalhadores (ABRAHÃO et al., 2009).

A **tarefa** pode ser entendida como o conjunto de prescrições daquilo que o trabalhador deve fazer segundo determinadas normas e padrões e por meio de equipamentos e ferramentas específicas, segundo padrões específicos de qualidade e quantidade. Ela não é o trabalho em si, e sim as normas, preceitos e regras que determina e autoriza o trabalhar. Pode-se dizer que, para o trabalhador, a tarefa é o que ele tem que fazer, com os meios que lhe são oferecidos. Já a **atividade** é aquilo que o trabalhador faz (real), suas ações, decisões e estratégias que visam atingir os objetivos definidos pela sua tarefa. Ela significa o que efetivamente é feito pelo trabalhador, a forma como ele consegue desenvolver as suas tarefas. Assim, podemos dizer que a atividade é o modo como as pessoas, em uma situação de trabalho real, relaciona-se com os objetivos propostos, a organização do trabalho, os outros trabalhadores e os meios fornecidos para realizá-los. A atividade é o eixo norteador para ações ergonômicas, é a maneira pela qual o sujeito articula suas competências para cumprir as exigências da tarefa, o objetivo estabelecido e as condições de trabalho efetivas que lhes são dadas (FERREIRA, 2000). A atividade é dinâmica e incerta, dada à variabilidade das pessoas e das situações de trabalho.

A **variabilidade** na organização do trabalho decore da diferença entre a prescrição e a realidade, e pode ser compreendida considerando as características do trabalhador, ressaltando a noção de variabilidade inter e intraindividual, e a organização do trabalho, onde destaca-se a variabilidade dos equipamentos e dos procedimentos (ABRAHÃO, 2000). O organismo humano possui limitações que influenciam a forma pela qual compreendemos e agimos sobre o mundo. Experiências anteriores modificam as estratégias adotadas e as ações futuras (ABRAHÃO et al., 2009). Assim, podemos dizer que existe variabilidade na forma de agir de cada indivíduo, uma variabilidade Intraindividual. Essa variabilidade é influenciada pelas alterações fisiológicas do ser humano, como envelhecimento, adoecimentos, ritmo circadiano, assim, como pelos conhecimentos formais e informais das pessoas. Logo, considera-se que o mesmo indivíduo não se comporta sempre da mesma maneira o tempo todo. Geralmente, em situações de trabalho as pessoas não estão sozinhas, e o ambiente é compartilhado com outros

indivíduos. Cada um possui suas características, experiências e fazeres diferentes. Assim, podemos dizer que existe uma variabilidade Interindividual. Além da variabilidade intra e interindividual, na perspectiva da organização do trabalho, existem as variabilidades previstas, como as mudanças das estações do ano, e as variabilidades imprevisíveis como a falha de um equipamento.

O **trabalho** pode ser considerado como uma ação coletiva, realizada por diferentes atores, por meio de ações finalísticas relacionadas aos objetivos organizacionais. Essas ações são realizadas sobre as regras e delineamento próprios da instituição, integrando a cultura da organização e as prescrições relativas às tarefas dos trabalhadores. Portanto, para o ergonomista é muito importante compreender a tarefa dentro do seu contexto organizacional. Para isso, é necessário primeiro entender a organização do trabalho em cada instituição, seu contexto social, econômico, geográfico e histórico. Somente assim, é possível situar a tarefa no contexto de produção que ela está inserida. Assim, cada empresa esta organizada pela divisão de tarefas, a divisão de pessoas, estruturas hierárquicas, tempos de trabalho e pausa, ritmos e as cadências.

Ainda, "A Ergonomia também pode considerar os aspectos cognitivos e de conduta na relação entre o homem e o trabalho mediada pela utilização de artefatos, conhecida como Ergonomia Cognitiva (EC)" (ABRAHÃO et al., 2009, p 239). O seu papel é compatibilizar as soluções tecnológicas com as características e necessidades dos usuários. A EC não tem como meta tentar entender a natureza da cognição humana, mas descrever como a cognição humana afeta o trabalhar e por ele é afetada. Um dos objetivos da análise dos processos cognitivos é compreender como os indivíduos regulam a situação de trabalho, ao solucionar os problemas decorrentes da discrepância entre o que é prescrito (tarefa) e a realidade encontrada.

A forma como o trabalhador gerencia seu processo de trabalho pode ser mais bem compreendida a partir do conceito de **Competências para Ação**. Ele pode ser entendido como a articulação de conhecimentos, representações, tipos de raciocínio e estratégias cognitivas que o sujeito constrói e modifica no decorrer da atividade (MONTMOLLIN, 1990 apud ABRAHÃO et al., 2009). Para a Ergonomia Cognitiva, as competências não estão relacionadas à noção de excelência do desempenho, elas são constituídas pelos conhecimentos e pelas estratégias que o indivíduo elabora para ação. As competências são inerentes a todos os indivíduos.

A análise e intervenção adotada na expressão da cognição humana levam em consideração as capacidades e os limites de natureza fisiológica e cognitiva do ser humano. No entanto, muitas vezes se consegue explicar a origem dos erros e dos incidentes atribuídos às falhas humanas. Para a EC interessa compreender o porquê desta "falha humana" por meio da análise dos processos de aquisição, processamento e recuperação de informações, que constituem um importante objeto de estudo (SILVINO, ABRAHÃO e SARMET, 2005).

As Competências para Ação compreendem a Representação para Ação e as Estratégias Operatórias. De acordo com ABRAHÃO e colegas (2009), a **Representação para Ação** é uma estrutura cognitiva, que pode ser um modelo mental, um mapa mental, uma imagem ou mesmo um esquema, cuja função é permitir que a pessoa possa compreender a situação na qual se encontra e recuperar seus conhecimentos para agir. Os conhecimentos utilizados no dia a dia para realizar as tarefas no trabalho também são representações. Para enviar um fax, utilizar uma fotocopiadora ou mesmo efetuar uma chamada telefônica é necessário evocar nossos conhecimentos, ou parte deles, que sejam mais relevantes de acordo com a situação. Para cada situação diferente evocam-se conhecimentos diferentes para agir. É por meio das representações que os indivíduos elaboram as estratégias mais relevantes e os procedimentos mais adequados para se realizar uma tarefa.

O conceito de **Estratégias Operatórias** pode ser entendido como um conjunto ordenado de passos que envolvem o raciocínio e a resolução de problemas, possibilitando a

ação (MONTMOLLIN, 1995 apud ABRAHÃO et al., 2009, p 328). As estratégias operatórias são definidas por Silvino e Abrahão (2003) como sendo um processo de regulação que pressupõe mecanismos cognitivos como a categorização, a resolução de problemas e o processo decisório. A Estratégia Operatória envolve atenção e resolução de problemas que resultam em um conjunto de ações denominadas Modo Operatório. O Modo Operatório é um conjunto de ações e operações que as pessoas adotam em função das exigências da tarefa e da sua competência no processo de trabalho.

Na EC, procura-se compreender quais são as estratégias elaboradas que favorecem o direcionamento da atenção, assim como a forma como é distribuída a atenção das pessoas. Também é importante identificar a partir de quais elementos da situação se estabelece uma hierarquia sobre o que é mais relevante ao desenvolvimento da atividade. Ao se identificar na situação real as informações e as estratégias utilizadas no processo de trabalho, pode-se definir os parâmetros de transformação ou critérios de flexibilização a serem incorporados no processo de forma a facilitar a seleção das informações pertinentes. Para responder as demandas de maneira diversificada, o ergonomista necessita de um conjunto de procedimentos e técnicas com características especiais para essa amplitude, conhecida como Análise Ergonômica do Trabalho (AET).

> A AET é estruturada em várias etapas que se encadeiam com o objetivo de produzir conhecimento e transformar o trabalho. Podemos dizer que ela constitui um método bastante aberto, uma vez que as ferramentas usuais da coleta dos dados podem variar e que a sua escolha é feita em função da natureza dos problemas colocados no momento da demanda (ABRAHÃO et al., 2009, p. 348).

Para atingir seus objetivos, a AET compreende a inter-relação homem trabalho com base na atividade, ou seja, da situação real em um nível micro de análise que enfatiza as ações e operações do sujeito, bem como suas estratégias para articular as suas características pessoais (idade, competências, dimensões físicas, entre outros) às variabilidades do trabalho (metas de produção, equipamentos, fatores ambientais, outros) (SILVINO, 2004). Segundo Abrahão e colegas (2009, p. 349), “compreender o trabalho é sempre um desafio, pois ele é fruto de um emaranhado de variáveis que precisam ser apreendidas em um determinado contexto”. Este é o fio condutor que guiou vários pesquisadores e profissionais na área ergonômica a um incessante trabalho de pesquisa que resultou em um método, aberto a complementação, útil e validado. Nesse sentido, considera-se pertinente o uso dessa abordagem na tentativa de identificar os comportamentos inseguros realizados na IAPF, assim como dos possíveis fatores a eles associados.

4 A TECNOLOGIA DA INFORMAÇÃO NA IAPF ESTUDADA

O presente relato consiste em um estudo de caso realizado em uma instituição pública não identificada por questões de segurança, denominada de Instituição da Administração Pública Federal (IAPF). Para melhor compreensão dos resultados, são apresentados, a seguir, a estrutura organizacional da IAPF e o papel do seu Departamento de Tecnologia da Informação no contexto organizacional. A Instituição da Administração Pública Federal (IAPF), é uma empresa pública de direito privado, está presente em quase todo o território nacional com suas unidades e em alguns países da Europa, África e Estados Unidos. Sua Sede é constituída por Unidades Administrativas que possuem a função de planejar, coordenar, controlar e avaliar as atividades relacionadas aos objetivos sociais consignados na missão e estratégias da Empresa. As Unidades Administrativas, também chamadas Unidades Centrais (UC’s) são, ao lado da Diretoria Executiva, órgãos integrantes da administração superior da Empresa, às quais

compete planejar, supervisionar, coordenar e controlar as atividades relacionadas a atividade fim da instituição.

A TI na IAPF possui o papel de oferecer suporte ao desenvolvimento organizacional e a manutenção do seu processo de trabalho. Sua missão é viabilizar soluções em Tecnologia da Informação de forma a contribuir para o desenvolvimento institucional, a sustentabilidade e a competitividade da instituição. O DTI atua no desenvolvimento e gerenciamento de soluções corporativas de TI para a IAPF, relativas às vertentes organizacionais e gerenciais. Existe ainda o Comitê Gestor de Tecnologia da Informação, que é um colegiado deliberativo que atua no âmbito corporativo junto à Diretoria-Executiva, constituído pelo Diretor-Presidente, por chefes dos principais processos estratégicos da Empresa e por chefes de Unidades Descentralizadas.

O Departamento de Tecnologia da Informação é uma Unidade Central técnico-administrativa, responsável pelos processos de fornecimento e gerenciamento de soluções de Tecnologia da Informação para a IAPF de modo a torná-la mais competitiva. Suas funções básicas são: assessorar a Diretoria Executiva no planejamento e gestão da Tecnologia da Informação e identificar as necessidades e gerenciar os recursos de TI fornecendo soluções inovadoras. Estrategicamente, o Departamento tem a função de alinhar a TI com os processos de negócio da Empresa e definir políticas de acesso e administrar os ambientes de banco de dados e rede de comunicação de modo a garantir a Segurança das Informações que por ali transitem ou estejam armazenadas. O DTI tem sua estrutura formada por uma chefia-geral, as coordenadorias de Sistemas de Informação; Infraestrutura e Atendimento ao Usuário (AU) e duas funções de Supervisão.

Em janeiro de 2010, o AU passou por um processo de reestruturação. O antigo sistema de HelpDesk é agora uma Central de Serviços, baseada nas melhores práticas do ITIL, que é um conjunto de boas práticas aplicadas na infraestrutura, operação e manutenção de serviços de Tecnologia da Informação. Isso torna a coordenadoria em um ponto único de contato entre os usuários e o gerenciamento de serviços de TI da instituição. A partir desta transformação, o AU agregou novas atividades como a de atender diretamente os pedidos e reclamações simples, recepcionar, registrar, priorizar e acompanhar os chamados de serviços de TI e manter os clientes sempre informados sobre o estado e andamento das suas requisições. Os pedidos são feitos a central por telefone, por um formulário na intranet ou por meio de memorandos. Os chamados que não competem a AU são escalonados (encaminhados) as outras coordenações de acordo com as atribuições de cada um.

A Central de Serviços utiliza dois tipos de atendimento aos funcionários da sede da IAPF. A primeira, por meio de acesso remoto, no qual o atendente acessa pela rede local o microcomputador do funcionário que está fisicamente distante. A segunda ocorre presencialmente, cabendo ao atendente se deslocar ao encontro do o funcionário. Já as demandas das Unidades Descentralizadas são atendidas através de ligações telefônicas. A Central de Serviços é a principal interface operacional entre a TI da sede da IAPF e seus funcionários, isso permite aos seus atendentes o contato direto com todas as demandas. Este contato direto proporciona ao atendente mapear comportamentos, levantar dados gerenciais e eventualmente identificar oportunidades de negócios.

Assim, este setor é estratégico para o estudo, pois é nele onde ficam registrados todas as demandas relacionadas à Tecnologia da Informação, fonte de dados essencial para alcance dos objetivos do presente trabalho. Considera-se pertinente a descrição da rotina do DTI, registrada a partir da experiência prévia de um dos pesquisadores como funcionário do departamento. De acordo com os dados extraídos do sistema de registro de ordens de serviços do DTI, a Central de Serviços atende uma média mensal de 2.000 ligações. Destas, 500 tornam-se efetivamente solicitação de serviço para a TI. Já as demandas que surgem por meio de memorandos e do formulário disponível na intranet não ultrapassam 30 mensais. Utilizando os

registros de ordem de serviços prestados pelo DTI nos últimos 15 meses, foram levantados vários problemas relacionados aos comportamentos adotados pelos funcionários da IAPF que colocam em risco diariamente a Segurança de suas Informações. São exemplos, o compartilhamento de senhas de acesso à rede local e aos sistemas de informação, o armazenamento de arquivos pessoais (como fotos, vídeos e músicas) nos servidores de rede. Também, a exposição das informações de acesso restrito por meio do compartilhamento indiscriminados e a utilização de mídias do tipo *flash memory* e ópticas que podem ser facilmente roubadas, perdidas ou danificadas para armazenar arquivos corporativos, e esta situação se agrava quando estes dispositivos são de propriedade particular.

Além disso, equipamentos pessoais como *notebooks*, *netbooks* e *palm tops* são utilizados para acessar a rede local da organização, as estações de trabalhos não são bloqueadas durante a ausência do funcionário do posto de trabalho, e todo tipo de documento impresso tem permanecido sobre a mesa. Ainda, vários usuários possuem privilégios administrativos sobre a sua estação de trabalho, e comumente são encontrados instalados pelos próprios funcionários, programas sem a devida licença ou proibidos pelo DTI. Do mesmo modo, os funcionários alteram a configuração padrão do sistema operacional das estações de trabalho e chegam ao ponto de remover programas básicos como o antivírus. Ademais, são observados dentro da organização funcionários de departamentos administrativos desenvolvendo aplicações e pequenos sistemas de informação sem autorização. Em relação aos sistemas de comunicação da organização, a utilização dos ramais telefônicos e do VoIP não recebem qualquer controle. Apenas o correio eletrônico possui normas para a sua regulação.

Esses comportamentos inseguros colocam em risco as Informações e Comunicações da IAPF, pois permitem que as vulnerabilidades possam ser exploradas por ameaças internas e externas, causando possíveis incidentes de segurança. Apesar da IAPF não registrar os incidentes de Segurança da Informação oficialmente, é possível observar alguns em registrados de outros sistemas de informação do DTI. Assim, perante os problemas apresentados, verifica-se que podem acontecer diversas ocorrências geradas pelos comportamentos irregulares relacionados à Segurança da Informação na Sede da IAPF. Nesse sentido, considera-se pertinente uma descrição mais detalhada das diretrizes de segurança da instituição, assim como dos comportamentos inseguros de seus funcionários.

5 METODOLOGIA

O trabalho é parte da cultura organizacional da empresa e é realizado no intuito de cumprir os objetivos institucionais. Ele é organizado por meio de regras e delimitadores prescritos pela instituição. Isso inclui as políticas, regras e normas de Segurança da Informação. No entanto, durante o processo de trabalho cotidiano existem situações que fogem as prescrições, assim as pessoas, visando à realização dos objetivos da tarefa, precisam elaborar estratégias para manterem o fluxo de trabalho, o que muitas vezes, não está de acordo com as diretrizes de Segurança da Informação da instituição. Com o intuito de identificar os principais fatores que geram comportamentos inseguros, propõe-se neste estudo uma metodologia de análise das situações reais do trabalho. Essa metodologia tem como fundamento a Análise Ergonômica do Trabalho (AET).

5.1 Análise Ergonômica do Trabalho (AET)

A abordagem metodológica proposta pela ergonomia tem uma lógica de investigação indutiva, na qual o ergonomista vai até o campo para produzir conhecimento. Assim, a AET propõe que a investigação aconteça onde o problema está ocorrendo de forma real. Desta forma, ela permite uma possibilidade concreta de transformação do trabalho em conjunto com a produção do conhecimento. O método AET é constituído de um conjunto de etapas e ações que mantém uma coerência interna. As diferentes técnicas são utilizadas de acordo com o problema e a configuração da demanda. É comum o uso de observações sistemáticas cursivas, participativas, não-participativas e pensar em voz alta. Também são utilizadas entrevistas abertas, semiestruturadas, fechadas, coletivas ou individuais. Podem ser usados questionários abertos, fechados ou *surveys*. Outras técnicas utilizadas são a análise documental (documentos disponibilizados pela empresa), a mensuração direta com instrumentos apropriados das variáveis determinantes das condições físicas do ambiente de trabalho e a confrontação (devolver os dados/resultados coletados aos trabalhadores).

Essas técnicas são selecionadas de acordo com a natureza do trabalho, as características de seu ambiente e os objetivos do pesquisador em diversas etapas de investigação. As etapas da Análise Ergonômica do Trabalho são compostas pelas seguintes fases:

a) Análise da demanda;
b) Coleta de informações sobre a empresa;
c) Levantamento das características da população;
d) Escolha da situação para análise;
e) Análise do processo técnico e da tarefa;
f) Observações globais e abertas da atividade;
g) Elaboração de um pré-diagnóstico – hipótese explicativa nível 2;
h) Observações sistemáticas – Análise dos dados;
i) Validação;
j) Diagnóstico;
k) Recomendações e Transformações.

O presente estudo consiste em uma intervenção ergonômica baseada na AET, que foi conduzido até a etapa de elaboração de um pré-diagnóstico da situação de trabalho. Apesar da das observações sistemáticas permitirem uma melhor mensuração da realidade de trabalho, entende-se o presente estudo como exploratório, que visa identificar as principais variáveis associadas ao comportamento inseguro no ambiente de trabalho. Assim, o diagnóstico foi elaborado a partir da combinação de observações globais e entrevistas semiestruturadas realizadas no ambiente de trabalho. Ainda, para a compreensão do comportamento das pessoas, a presença do ergonomista na situação real de trabalho durante a sua realização é um fator determinante. Essa presença constitui uma das diferenças fundamentais entre ergonomia e as outras abordagens de estudo do trabalho (ABRAHÃO et al., 2009).

5.2 O Delineamento Adotado no Estudo

Esse trabalho não se propõe a fazer uma análise precisa de cada um dos problemas de segurança identificados, mas obter um diagnóstico geral dos vários problemas relacionados aos comportamentos inseguros dos funcionários. Como primeiro passo para a pesquisa, foram levantadas as regras, normas, políticas e recomendações de Segurança da Informação (SI) relacionadas à instituição como requisito para compreender as tarefas. Logo após, buscou-se

entender a estrutura organizacional da IAPF. Sequencialmente foram levantados os problemas de Segurança da Informação relacionados ao comportamento inseguro, registrados na rotina diária do Departamento de Tecnologia da Informação (DTI). Finalmente, buscou-se compreender do ponto de vista das pessoas sobre os motivos do não cumprimento das diretrizes de SI, quais as razões reais que conduzem os funcionários a adotarem um comportamento considerado inseguro, visando a sua compreensão mais ampla. As técnicas utilizadas no estudo foram a Análise Documental de registros e sistemas de informação disponíveis na instituição, entrevistas semiestruturadas com trabalhadores e Observações Globais Participativas dos funcionários da Sede da IAPF.

A Análise Documental ocorreu com o objetivo de compreender a estrutura organizacional e a posição da IAPF no cenário nacional e internacional. Essas informações foram adquiridas na página da instituição na internet. Posteriormente elas foram complementadas com a consulta ao seu Plano Diretor da IAPF. Em seguida foram levantados, por meio do Plano Diretor de Tecnologia da Informação (PDTI), o papel do Departamento de Tecnologia da Informação no contexto organizacional, bem como sua missão, visão, valores e estrutura organizacional. Igualmente por meio do PDTI, foram coletadas informações sobre as coordenações que compõem o DTI e principalmente sobre a Central de Serviços deste departamento. Como complemento foi investigado o regimento interno do Departamento de Tecnologia da Informação.

Para compreender o volume de demandas relacionadas à Tecnologia da Informação na sede da IAPF, foi levantado no sistema que gerencia a telefonia na IAPF o número de ligações telefônicas recebidas mensalmente pela Central de Serviços. Da mesma forma, por meio dos relatórios expedidos pelo software de registro dos serviços, foram levantadas as quantidades de serviços prestados mensalmente. Por meio de entrevista semiestruturada com a coordenadora da área de desenvolvimento de sistemas de informação do DTI, foi obtido o número de sistemas desenvolvidos sem permissão por departamentos administrativos. Da mesma forma, um funcionário da biblioteca da IAPF foi entrevistado a respeito da estrutura organizacional. Ainda com o auxílio das ferramentas de registro de ordens de serviço, a ferramenta de escrita colaborativa e a de inventário de hardware software, foram coletados os incidentes relacionados aos comportamentos dos funcionários nos 15 meses anteriores ao período de observação (o ano não pode ser identificado por questões de segurança).

As diretrizes de Segurança da Informação da IAPF foram levantadas por meio da norma interna N.º 20, onde está publicada a política do uso de e-mail, instrução de serviço do DTI, referente o uso de equipamentos móveis na rede local, e a Cartilha de Segurança da Informação que está publicada na intranet. Outras diretrizes de SI foram consultadas no site do Tribunal de Contas da União, como a Cartilha de Boas Práticas em Segurança da Informação, os acórdãos e decisões do tribunal. Da mesma forma, houve a consulta a página na internet do Departamento de Segurança da Informação (DSI) do Gabinete de Segurança da Institucional da Presidência da República.

Por meio da Análise da Atividade de trabalho real foram coletados os comportamentos considerados inseguros durante a realização do trabalho de alguns funcionários. As observações globais participativas do comportamento das pessoas na Central de Serviços foram registradas no período de três semanas, paralelas às verbalizações relacionadas aos incidentes causados pelo comportamento inseguro. As Observações Globais e as Observações Globais Participativas aconteceram do seguinte procedimento: primeiramente foi escolhido um funcionário por dia para a realização do primeiro contato, no qual o pesquisador apresentou sua lotação e seu trabalho desenvolvido na IAPF. Em seguida foram apresentados os objetivos do presente estudo de caso, dito que ele seria observado executando seu trabalho pelo período de 1 hora, e que poderia haver intervenções por parte do pesquisador para entender o trabalho e

tirar dúvidas sobre as suas ações. Então, foi realizado o convite para sua participação na pesquisa. Neste momento, também lhe foi garantido o sigilo sobre a sua identidade e os dados coletados. Nos casos em que houve a autorização, formalizada com um termo de consentimento, as observações começaram imediatamente e o pesquisador se posicionava sentado ao lado da mesa do funcionário para iniciar a observação. Nos casos de resposta negativa, o pesquisador agradeceu e procurou outro funcionário. Durante as observações da atividade de trabalho na sede da IAPF, cada comportamento que não estava adequado às diretrizes de Segurança da Informação da instituição foi registrado. Durante algumas ações foram feitas intervenções por parte do pesquisador a partir de três perguntas pré-formuladas. O objetivo foi compreender os reais motivos que conduziam os funcionários a adotarem um comportamento inseguro. Ao final das observações, foi permitido ao funcionário ler o registro.

Entende-se que outras etapas da AET poderiam ser realizadas com o objetivo de inferir e medir os fatores relacionados ao comportamento inseguro, como o processo de Observação Sistemática. No entanto, devido ao objetivo de cunho exploratório do presente estudo de caso, apenas a identificação desses fatores foi realizada pela combinação das observações globais e entrevistas semiestruturadas.

5.3 Características dos Participantes

Participaram da pesquisa dez pessoas ao todo. Durante a etapa de análise documental, duas pessoas auxiliaram o processo de levantamento e identificação dos registros. Um possui nível médio completo e exerce a função de assistente administrativo, o outro possui nível superior completo e exerce a função de analista de sistemas. As oito pessoas restantes participaram da pesquisa sendo observadas em seu local de trabalho. Destas, quatro são do sexo feminino. A primeira possui nível médio, ocupa o cargo de secretária. A Segunda possui nível superior incompleto e ocupa o cargo de assistente administrativo. A terceira e a quarta possuem nível superior com formação nas áreas humanas.

Os cargos ocupados por elas são da área de Comunicação e recurso humanos. Dos quatro participantes do sexo masculino, o primeiro possui nível superior com formação na área de tecnologia e ocupa o cargo de assistente. O segundo também possui nível superior com formação na área de ciências exatas e ocupa o cargo de analista. O terceiro possui mestrado em análise de sistemas e ocupa o cargo na área de tecnologia da instituição. O quarto e último possui doutorado em ciências exatas.

6 RESULTADOS E DISCUSSÃO

Esta seção tem como objetivo apresentar os resultados obtidos na pesquisa e, simultaneamente, proceder a sua discussão. A organização adotada se inicia com a apresentação dos incidentes registrados no período. Em seguida, são enfatizados os incidentes de Segurança da Informação observados diretamente, relacionados à adoção de comportamento inseguro pelos funcionários. Posteriormente, são discutidas as suas dificuldades em adotar um comportamento seguro no dia a dia de trabalho.

6.1 Os Incidentes de Segurança

Quanto aos principais incidentes associados aos comportamentos inseguros, foi verificado que na sede IAPF não os registra oficialmente. Portanto, para identificá-los foi utilizada a ferramenta de registro de ordens de serviço da Central de Serviços, o programa de

inventários de hardware e software computacional, relatórios do servidor de antivírus e entrevistas semiestruturadas com funcionários do DTI.

O principal incidente de segurança da informação relacionado aos comportamentos dos funcionários foi o compartilhamento de senha de um funcionário com várias outras pessoas, que resultou no seu uso por um estagiário para efetuar ligações externas, incluindo interurbanos e serviços de "disk amizade", bem como, acessar sites de conteúdo pornográfico. Outros cinco funcionários suspeitaram que suas senhas pudessem estar sendo usadas por terceiros e solicitaram auxílio para troca. Semelhantemente, foram registradas oito ocorrências de usuários que excederam o limite de armazenamento do disco local de seu microcomputador, comprometendo o armazenamento de informações institucionais. Da mesma forma, dez casos de discos locais das estações de trabalho que deixaram de funcionar impossibilitando o acesso à informação e/ou a sua perda total.

Conforme dados extraídos do sistema de inventário de hardware e software, durante o ano de coleta na IAPF, 97 suítes de escritório sem a devida licença foram encontrados instalados nas estações de trabalho e posteriormente removidos. De acordo com o relatório do gerenciador de antivírus, esta aplicação necessitou ser reinstalada em cinco equipamentos após terem sido removidas por usuários que possuem privilégios administrativos sobre seu microcomputador. Todas estas foram infectadas por pragas virtuais por estarem sem o programa. Destes, em três casos o sistema operacional teve que ser reinstalado. Ainda, dois outros equipamentos com direitos administrativos concedidos aos seus usuários tiveram seu sistema operacional reinstalado devido a alterações na sua configuração padrão. Ainda assim, 31 usuários permanecem com privilégios administrativos sobre sua estação de trabalho.

Segundo a coordenadora da área de desenvolvimento de sistemas do DTI, no mesmo ano foi feito um levantamento para o PDTI da IAPF, e foram contabilizadas 15 aplicações que estão em produção desenvolvidas por funcionários não autorizados de outros departamentos. Com isso, houve 24 chamados para o DTI visando solucionar problemas destas aplicações, como erro de programação, falta de suporte a um número alto de conexões e estouro de memória. Ademais, foram removidos sete compartilhamentos de diretórios nas máquinas de usuário que estavam permitindo o acesso a dados sensíveis. quatro *flash drives* apresentaram problemas impossibilitando o acesso aos arquivos armazenados, sendo que, dois destes foram causados por vírus no dispositivo.

Para efeito de comparação, somente no primeiro trimestre do ano seguinte, já houve sete solicitações de recuperação de dados corporativos em *flash drives* e *HDs* externos, um disco da estação de trabalho excedeu seu limite de armazenamento, mais oito solicitações para remoção de vírus em microcomputadores, três reinstalações do sistema operacional, nos quais os usuários com privilégios administrativos, alteraram as configurações padrão do sistema. Além disso, três discos locais apresentaram problema que impossibilitou o acesso aos dados, três usuários executaram *backup* em mídias óticas e já ocorreu a reinstalação do antivírus em duas máquinas.

Assim, com estes indicadores de problemas levantados durante os atendimentos aos usuários de TI da IAPF pelos atendentes da área de suporte, verifica-se que existe um número significativo de ocorrências geradas por comportamentos irregulares relacionados à Segurança da Informação. Estes incidentes podem comprometer a Reputação e a Confiabilidade da empresa em relação à população. Também podem causar a descontinuidade do negócio, na qual a sociedade é quem seria a maior prejudicada com a perda ou atraso nas suas ações ou os prejuízos causados aos cofres públicos.

6.2 Os Comportamentos Inseguros Observados

De acordo com os objetivos do trabalho, além dos principais comportamentos inseguros registrados nos sistemas do DTI, são descritos os coletados por meio da observação direta da atividade de trabalho. Também são apresentados o número de ocorrências e as consequências que estes comportamentos podem trazer para a instituição. Os resultados são apresentados no Quadro 1, e detalhados a seguir.

Quadro 1. Comportamentos inseguros observados e problemas de segurança relacionados

Comportamento inseguro observados	Qtd.	Problemas de segurança
Compartilhamento de senha	7	Acesso não autorizado (confidencialidade)
Não bloqueio da tela ao se ausentar	6	Roubo e acesso não autorizado (disponibilidade e confidencialidade)
		Alteração do conteúdo dos documentos (integridade)
Política de mesa limpa	6	Roubo e acesso não autorizado (disponibilidade e confidencialidade)
		Alteração do conteúdo dos documentos (integridade)
Uso de garrafas e copos com água sobre a mesa	5	Indisponibilidade dos documentos
		Indisponibilidade da estação de trabalho
Armazenamento de dados corporativos em mídias do tipo *flash memory*	3	Perda ou roubo da mídia (disponibilidade e confidencialidade)
		Falha da mídia (disponibilidade)
Backup em mídias do tipo ópticas	3	Perda ou roubo da mídia (disponibilidade e confidencialidade)
		Falha na mídia (disponibilidade)
Utilização de *notebook* pessoal na rede local	3	Não há controle de patch de atualização, programa antivírus (disponibilidade)
		Pode permitir o acesso não autorizado a informação (Confidencialidade)
Armazenamento dos arquivos em diretórios públicos nas estações de trabalho	2	Acesso indevido (confidencialidade)
		Alteração indevida de documentos (integridade)
		Exclusão indevida (disponibilidade)
Armazenamento de dados corporativos na estação de trabalho	2	Exclusão e corrupção dos dados (disponibilidade e integridade)
Desenvolvimento de sistemas de informação por funcionários não autorizados	2	Sistema não suporta o número de conexões necessárias (disponibilidade)
Utilização de *e-mail* pessoal para assuntos institucionais.	2	Interceptação da mensagem (confidencialidade)
		Não há garantia de privacidade do conteúdo das mensagens. (confidencialidade)
Armazenamento de dados pessoais no driver de rede	1	Falta de recuso para os dados institucionais e contaminação por vírus (disponibilidade)
Compartilhamento com permissões além das necessárias	1	Acesso indevido (confidencialidade)

Instalação de programas não autorizados	1	Multa
		Pirataria
		Cavalo de Tróia
Remoção do antivírus	1	Contaminação por vírus (disponibilidade)
		Acesso não autorizado da informação (confidencialidade)
		Indisponibilidade do sistema e recursos de rede (disponibilidade)
Rotina de *backup*	1	Falha na restauração dos dados (disponibilidade e integridade)
Troca de senha periódica	1	Acesso não autorizado (confidencialidade)

Fonte: pesquisa de campo

Foram apresentados os principais comportamentos inseguros registrado no Departamento de Tecnologia da Informação ao longo das observações. No entanto, ainda fica a dúvida acerca dos motivos pelos quais são adotados, quais foram as dificuldades e os obstáculos que os funcionários encontram para cumprir as recomendações relacionadas à Segurança da Informação. Assim, são apresentadas as principais dificuldades relatadas pelos funcionários observados em cumprir as diretrizes de Segurança da Informação vigentes na instituição.

6.3 As Dificuldades Relacionadas ao Comportamento Seguro

Na presente seção são discutidas as dificuldades relatadas pelos funcionários em cumprir as diretrizes da Segurança da Informação vigentes na instituição, organizadas por categorias de problemas identificados.

6.3.1 Do Compartilhamento de Senhas

No que diz respeito ao compartilhamento de senhas, dos sete casos observados, cinco funcionários alegam a necessidade de receber a ajuda de outras pessoas. O motivo é que existe uma grande quantidade de trabalho em seu setor e pouco tempo para a sua realização. Segundo os funcionários, geralmente a ajuda que recebem são dos estagiários e, devido à forma diferenciada de contrato de trabalho, eles não possuem acesso aos sistemas de informação.

Nesse caso, é percebido um conflito existente entre as normas de produção e as diretrizes de segurança da instituição. O funcionário possui muitas tarefas e necessita de ajuda para realizá-las e a instituição não oferece suporte à sua realização. Consequentemente, os funcionários elaboram estratégias para conseguir realizar o seu trabalho, que nesse caso, consiste no compartilhamento da senha, que permite o acesso completo aos sistemas a pessoas não autorizadas. Para os funcionários, o trabalho possui caráter primário, assim se for deixado de ser realizado as consequências serão imediatas. Por isso, talvez exista uma priorização dos objetivos do trabalho em relação às recomendações de segurança. Como as diretrizes possuem caráter preventivo, tendem a ficar em segundo plano no dia a dia de trabalho em situações de conflito ou de pressão temporal.

Dos cinco casos relatados, um em especial tem maior gravidade. O funcionário declara que não altera a sua senha periodicamente. Com isso, os estagiários, mesmo depois de terem sidos desligados da empresa, continuam com a possibilidade de acessarem serviços e informações de fora da instituição, pois vários deles estão disponíveis na internet. Ele alega que não efetua a troca porque isso lhe trará transtorno, sendo que terá que divulgá-la novamente a

todos que precisam utilizá-la. Desta forma, o funcionário criou uma organização do trabalho em seu setor, redistribuiu as tarefas entre os estagiários, criando objetivos de trabalhos diferentes das atribuições formais. Para que esta organização funcione, ele não pode alterar a senha.

No sexto caso, o funcionário observado executa exclusivamente uma determinada atividade. Assim, para evitar uma possível interrupção do fluxo de trabalho diante de um imprevisto, como por exemplo, uma licença médica, a estratégia elaborada é o compartilhamento da senha com um de seus superiores. Com isso, ele prevê que outras pessoas poderão executar as suas atividades em um caso de emergência. Nesse caso, pode ser evidente um problema na organização do trabalho, que possui prescrições conflitantes. O trabalho precisa ter fluxo contínuo e, no entanto, apenas uma pessoa é designada para a sua execução. Não foram consideradas situações previsíveis como férias e licenças médicas na proposta da tarefa. Além disso, as recomendações de Segurança da Informação da instituição sugerem que a senha seja mantida confidencial. Neste caso, se esta recomendação for cumprida, o fluxo de trabalho deve ser interrompido. Esse contexto de conflito entre as prescrições obriga o funcionário a escolher entre realizar o trabalho ou cumprir a diretriz de segurança. Novamente foi verificada uma escolha baseada no caráter primário de realização do trabalho, pois as consequências serão imediatas caso ele não seja executado.

No sétimo e último caso de compartilhamentos de senha, o funcionário declara ter conhecimento dos riscos existentes quando o compartilhamento ocorre, No entanto, alega que, ao chegar na instituição há poucos meses, esta prática já era comum. Em virtude disso, sentiu-se obrigado a incorporar tal prática nas suas atividades diárias e, declara ainda, não saber o que fazer para mudar esta situação.

Percebe-se que as práticas de elaboração de estratégias operatórias que descumprem as normas de segurança devido aos conflitos das prescrições têm ocorrido inúmeras vezes na instituição e, como resultado, possivelmente já se tenha gerado uma cultura organizacional de não cumprimento das recomendações de SI da IAPF.

6.3.2 Do Desenvolvimento de Sistemas Sem Autorização e Armazenamento de Dados

Também foram observados casos mais graves, como os dois funcionários de um departamento administrativo que estavam desenvolvendo aplicações e utilizando-as na instituição sem autorização do Departamento de Tecnologia da Informação. Segundo eles, o departamento onde trabalham solicitou ao DTI o desenvolvimento de um sistema para automatizar vários processos. O DTI alegou que existiam várias demandas em sua fila e que o pedido somente poderia ser atendido em um prazo de dois anos. Diante da necessidade da aplicação e o longo prazo estipulado pelo DTI, o chefe deste departamento resolveu reunir dois de seus funcionários e desenvolver o sistema por conta própria. Neste caso, evidencia-se que um problema de organização de trabalho pode estar desencadeando vários outros problemas de SI. Como para o Departamento de Tecnologia da Informação existem várias demandas e a quantidade de pessoal não é suficiente, os demandantes criam estratégias para solucionar suas necessidades imediatas. Com isso, surgem sistemas desenvolvidos sem autorização do DTI, que geralmente são mal planejados e fora do padrão da instituição. Essas soluções geralmente sequer suportam as demandas de acesso e armazenamento de um ambiente corporativo.

O desenvolvimento de programas por parte dos funcionários de departamentos administrativos também gera outros problemas de Segurança da Informação, como por exemplo, a rotina de *backup*. Além dela ser manual e não ser testada periodicamente, a fita com o backup fica armazenada na sala dos desenvolvedores. Um dos funcionários foi questionado

sobre os riscos de armazenar a fita nestas condições. Ele respondeu que tinha conhecimento dos perigos e que pretendia retirar a fita daquela sala e guardá-la em outro andar do prédio.

A partir desses relatos, entende-se que o problema da organização do trabalho desencadeou vários outros problemas. Nesse sentido, a falta de pessoas em determinado setor levou o DTI a não cumprir suas tarefas e obrigar os outros departamentos a criar estratégias próprias para resolver o problema, afetando diversos aspectos da Segurança da Informação institucional.

Além disso, na rede local da sede da IAPF, cada departamento possui um espaço reservado nos servidores de rede para armazenar e compartilhar arquivos, eles são mais conhecidos como *drivers* de rede. Estes locais recebem uma rotina diária de *backup*, o que garante a disponibilidade dos arquivos lá armazenados. Outros dois funcionários foram observados gravando os dados corporativos no disco local de suas estações de trabalho, em vez de usarem o disco de rede. Questionados sobre esta prática, um dos funcionários relatou que, em casos de indisponibilidade na rede, os dados irão continuar acessíveis por estarem armazenados em seu microcomputador. O segundo afirmou que parte dos arquivos gerados por ele é gravado no *driver* de rede, mas que não mantém todos os arquivos neste local porque ter recebido notificações de havia excedido o limite de armazenamento há alguns anos.

No caso do primeiro funcionário, entende-se que o comportamento inseguro é ocasionado pela falta de confiabilidade na rede local da instituição. Para ele uma parada repentina da rede irá impedi-lo de realizar seu trabalho. Para que isso não aconteça, ele elabora a estratégia de armazenar os arquivos em seu microcomputador, com isso ele declara que tem a sensação de estar seguro.

O segundo caso está relacionado com a falta de condições de trabalho. O funcionário não possui espaço suficiente no driver de rede para armazenar todos os arquivos necessários. Esta falta leva o funcionário a elaborar a estratégia de classificar os arquivos e armazená-los até o limite do disco. Também é perceptível outro problema, a falta de informação. A sede da IAPF aumentou sua capacidade de armazenamento nos últimos anos e, atualmente, não existe mais o problema de falta de espaço em disco. No entanto, o funcionário continua com a informação antiga, mantendo a estratégia para evitar problemas de espaço.

Em dois casos, os funcionários foram vistos armazenando dados corporativos na estação de trabalho em locais de acesso público. Questionado sobre o comportamento, um alegou desconhecimento acerca da possibilidade de outras pessoas poderem acessar aos dados armazenados em seu microcomputador. Para ele, os dados estavam seguros. Já o segundo declarou que grava os dados fora do perfil com o objetivo de facilitar a busca, pois desenvolveu uma estrutura de diretórios própria que agiliza seu trabalho.

No primeiro caso, o comportamento inseguro adotado pelo funcionário pode ter causas como a falta de conhecimento técnico ou desconhecimento das diretrizes de segurança. Para armazenar os dados na estação de trabalho faltava-lhe o conhecimento técnico. Então para agir, ele evocou outros conhecimentos que lhe foram significativos em situações semelhantes, visando tentar resolver o problema, o que levou a utilizar um local não recomendável para o armazenamento. Os conhecimentos evocados por este funcionário, não contemplaram as recomendações de Segurança da Informação, e isso pode ter sido ocasionado por falta de conhecimento ou falta de treinamento. Se ele não conhece as diretrizes de segurança, não as levará em consideração em suas ações. Caso tenha sido treinado, isso pode não ter sido fixado e, por não fazer parte da rotina, acabou não sendo lembrado.

No segundo caso, percebemos que a interface do microcomputador não está adaptada às representações do funcionário, ou seja, a estrutura de diretórios dificulta a localização da informação. Por isso, ele elabora a estratégia de criar um modelo de estrutura alternativo de acordo com suas experiências, o que facilita o gerenciamento das informações. No entanto, a

estrutura de arquivos do sistema é inflexível fazendo com que as recomendações sejam descumpridas para criar uma estrutura mais adequada a representação do seu modelo mental.

Quanto ao armazenamento de arquivos pessoais nos discos de rede, um funcionário foi observado mantendo músicas, fotos e vídeos pessoais nesse local, ocupando o espaço que é destinado aos arquivos institucionais. Ele afirmou que conhece a rotina de *backup* que é realizada diariamente nos discos de rede e que, como não gostaria de perder nenhum dos seus arquivos, decidiu armazená-los neste local. Neste caso, para o funcionário havia o risco de os arquivos serem perdidos, e seu objetivo era mantê-los seguros, disponíveis, íntegros. Utilizando-se da informação de que os arquivos armazenados nos discos de rede têm rotina de *backup* diária, ele lança mão desta regra de produção da instituição e armazena os arquivos pessoais na rede. Com isso, ele mantém seus arquivos bem mais seguros que em qualquer outro meio de armazenamento disponível em seu posto de trabalho. Assim, o funcionário elabora uma estratégia de resolução de problema sem levar em consideração que seu comportamento prejudica a segurança das informações institucionais, pois os espaços reservados para arquivos institucionais estão ocupados por arquivos pessoais.

6.3.3 Da Política de Mesa Limpa e do Compartilhamento de Arquivos

Nos casos em que quatro pessoas mantiveram documentos sobre a mesa durante a sua ausência da sala e não bloquearam a tela do microcomputador. Quando indagados sobre os riscos dos arquivos e documentos serem roubados, alterados e apagados, dois responderam que confiam nas pessoas que trabalham a sua volta, e que nunca tiveram problemas relacionados a estes casos. Apesar disso, declararam ter consciência dos perigos em relação às pessoas desconhecidas que visitam a sua sala. Um funcionário afirmou que se esqueceu apenas durante o tempo que estava sendo observado, mas que geralmente mantém a mesa limpa, armários e gavetas trancados e tela bloqueada. O último afirmou que guarda os documentos e bloqueia a tela da estação de trabalho somente nas saídas que considera mais longa, como por exemplo, na hora do almoço e o final do expediente, pois para ele este é o período de maior risco.

Nesses casos, percebe-se que os funcionários utilizam à estratégia que lhes proporciona menos esforço. Para eles, guardar os documentos todas as vezes que irão se retirar do posto de trabalho e devolvê-los à mesa quando voltar, aumenta a carga de trabalho. Pelos relatos dos funcionários, os incidentes com estes documentos são baixos, e existe confiança entre as pessoas que estão em sua volta. Também não há registros oficiais na instituição acerca desses casos, por esse motivo, a estratégia escolhida é a carga mais leve de trabalho. Com isso, eles canalizam seus esforços para outras atividades.

Sobre o compartilhamento de arquivos sensíveis, um funcionário mantinha em sua estação de trabalho um diretório com arquivos confidenciais (auditoria interna) que estavam com permissão de acesso além das necessárias. Isso possibilitava o acesso de todos os usuários da rede local ao conteúdo deste diretório. Questionado sobre as permissões de acesso, o funcionário informou que necessitava compartilhar alguns arquivos com alguns funcionários, e que ao fazê-lo, escolheu apenas as opções padrão do sistema. O usuário verbalizou que não imaginou que tal ação estava permitindo o acesso de qualquer usuário da rede ao conteúdo do diretório.

Este fato nos leva a perceber que o funcionário elaborou uma estratégia inadequada em termos de segurança para resolver o problema. Ele possuía arquivos em sua estação de trabalho e necessitava compartilhá-los com algumas pessoas de seu setor. Ao analisar as possibilidades para resolver o problema, ele verificou que o compartilhamento pela rede local é o mais viável. Assim, o funcionário executa a ação de compartilhar e utiliza as opções padrão do sistema, com isso, permitiu o acesso de todos da rede local ao conteúdo. O funcionário

considerou que o problema estava resolvido, e não imaginava que também estava gerando um problema de segurança da informação. A interface do sistema pode ter influenciado quando não informou de forma clara que tal ação disponibilizaria os arquivos a todos os funcionários e consistia em uma operação com riscos de segurança.

6.3.4 Do Uso de Equipamento Pessoal na Rede Local e Uso de E-mail Particular

Também foram encontrados três *notebooks* pessoais acessando a rede local. De acordo com um dos funcionários, o motivo está relacionado ao fato de que ele desenvolve aplicações para o seu departamento e, como a instituição não possui uma licença disponível de um determinado *software*, ele utiliza seu equipamento que possui uma cópia da licença. O comportamento inseguro deste funcionário é gerado por uma falha nas condições de trabalho oferecidas pela organização. Ele possui a tarefa de desenvolver um programa para computador, mas para isso necessita de uma ferramenta não disponível oficialmente pela instituição. Assim, ele elabora a estratégia de levar para a instituição o seu equipamento pessoal e, realiza os seus objetivos de trabalho. A falta de condição de trabalho leva o funcionário a adotar o comportamento inseguro. Cabe ressaltar que, para a realização desse trabalho, a instituição propõe o uso de outra ferramenta, com potencial de produtividade menor, que aumenta a carga de trabalho do funcionário.

O segundo usuário argumentou que sempre usou seu *notebook* na rede, e que isso facilita seu trabalho, fornecendo mobilidade e agilidade na execução de suas atividades. Neste caso, o funcionário recebeu da instituição um microcomputador, mas prefere usar o *notebook*, e argumenta que a falta de mobilidade gera um impacto grande no seu fluxo de trabalho, pois as informações e sistemas contidos ali são essenciais para cumprimentos dos objetivos de seu trabalho.

Já o terceiro funcionário explicou que, de acordo com suas atribuições, ele deve realizar atividades tanto no edifício sede da IAPF quanto em um campo de coleta de dados. Assim, é necessário utilizar um dispositivo móvel para o trabalho. No entanto, conforme sua declaração, o seu departamento não dispõe de um equipamento semelhante. Por isso, ele utiliza o seu equipamento pessoal. Neste terceiro caso, a falta de instrumentos de trabalho ocasiona o comportamento inseguro, pois a natureza da tarefa exige mobilidade para que os dados e os sistemas fiquem disponíveis nos dois postos de trabalho.

Em outros dois casos, foi observado o uso de *e-mail* particular para assuntos institucionais. De acordo com um dos funcionários, existem problemas constantes de disponibilidade do e-mail corporativo e do limite do tamanho do anexo. Para isso, ele utiliza cinco diferentes contas de e-mails particulares paralelamente ao da instituição para enviar as mensagens eletrônicas. O segundo funcionário afirma que faz uso do *e-mail* particular durante a indisponibilidade do serviço ou quando tem problema no recebimento de mensagens no *e-mail* corporativo.

Percebe-se que nos dois casos a falta de confiabilidade no sistema de *e-mail* da Sede da IAPF leva os funcionários a adotarem o comportamento inseguro. Eles utilizam o *e-mail* particular para os assuntos corporativos. No primeiro caso também existe o problema de condições inadequadas de trabalho, pois o funcionário tem a necessidade de enviar arquivos anexados à mensagem maiores do que os limites permitidos pelo sistema. Com isso, ele utiliza o *e-mail* particular como forma de atingir os objetivos de sua tarefa.

6.3.5 Do Uso de Dispositivos do Tipo Flash Memory e Backup de Arquivos

Dos três funcionários observados que armazenam dados institucionais em dispositivos do tipo *flash memory* e *HD* (*Hard Disk*), dois responderam que mantém cópias de dados que julgam importantes nestes dispositivos. Indagados sobre se conheciam o disco de rede e a rotina de *backup* diária, eles responderam que conhecem, mas que ao utilizar estes dispositivos sentem-se mais seguros. Outro funcionário respondeu que manipula uma quantidade de dados muito grande e quando usa a rede as transferências de arquivos são demoradas. Usando este dispositivo ele agiliza a suas atividades.

Nos dois primeiros casos é perceptível a falta de confiabilidade no sistema de *backup* e da rede local da Sede da IAPF, com isso eles elaboram a estratégias de armazenarem dados institucionais nestes dispositivos e ficam com a sensação de estarem seguros contra qualquer imprevisto. Já no terceiro caso, a falta de tempo o conduz a elaborar a estratégia que irá agilizar o seu trabalho. Nos três casos apresentados, a falta de confiabilidade e a pressão temporal fazem com que os funcionários adotem comportamentos inseguros.

Além disso, foram observados três usuários gerando *backup* em mídias óticas. Um alegou que a quantidade de dados que ele manipulava era muito grande para ser colocado em um *driver* de rede, e que isso levaria muito tempo. Um segundo funcionário argumentou que estava preocupado com a possibilidade de os dados serem perdidos caso houvesse algum problema com o disco local de sua estação de trabalho. Então, usou a estratégia de armazenar a cópia de segurança em uma mídia ótica já que o seu computador possui um gravador de CD. Perguntado se conhecia o *driver* de rede, o usuário respondeu que não. Após ser esclarecido sobre a existência e o funcionamento do *driver*, ele disse que iria começar a utilizar este recuso. O terceiro alegou que teria seu microcomputador trocado e estava apreensivo com a possibilidade de perder alguns dados durante a mudança.

No primeiro caso, entende-se novamente que a organização do trabalho exerce sobre o funcionário pressão temporal. Com isso, ele adota a estratégia de armazenar os dados em um disco de memória *flash* sem se preocupar com a insegurança que este comportamento traz a informação. Já o segundo, desconfia dos sistemas de informação da instituição e decide gravar as informações em um dispositivo de *flash memory*. O terceiro declara que a falta de conhecimento dos recursos institucionais provoca o comportamento inseguro.

6.3.6 Do Uso de Programas Sem a Devida Licença

No caso do usuário que utiliza um programa sem a devida licença, ele relatou que possui privilégios administrativos sobre o computador, e que instalou uma cópia não licenciada do produto, pois alegou possuir mais habilidades no uso deste produto do que com o oferecido pela instituição. Neste caso, a estratégia do funcionário é a que lhe traz menor carga de trabalho e mais flexibilidade. Como o seu objetivo primário é a realização da tarefa, ele descumpre a política de segurança, que é preventiva e não causa consequências imediatas.

Por último, um funcionário, que também possui privilégios administrativos sobre um *notebook* da instituição, havia removido o programa de antivírus do equipamento. Questionado sobre este comportamento, ele declarou que o antivírus estava deixando o funcionamento do sistema muito lento, e isso estava o impedindo de trabalhar. Percebe-se neste caso que o funcionário tinha como objetivo primário novamente a realização do trabalho. Como para ele o antivírus estava atrapalhando suas atividades, elaborou a estratégia de removê-lo e realizar o trabalho. Como o antivírus era apenas preventivo ele escolheu correr o risco de sofrer um ataque de vírus e realizar o trabalho.

6.3.7 Diagnóstico Inicial

Realizada a análise sobre o trabalho efetivo dos funcionários da IAPF, verifica-se a existência de comportamentos inseguros que têm colocado em risco a Segurança da Informação da Instituição. Além disso, é evidente que grande parte dos casos de comportamentos considerados inseguros que foram observados advém da falta de planejamento da organização do trabalho, a falta de uma Política de Segurança da Informação institucionalizada, a falta de conhecimento das diretrizes de Segurança da Informação vigentes, do conflito entre as prescrições e as regras de segurança, pressão temporal e condições práticas para realização do trabalho. Esses problemas conduzem os funcionários a elaborarem estratégias que mantenham o fluxo de trabalho em detrimento das normas de segurança.

Percebe-se que todas as estratégias, mesmo colocando em risco a segurança da informação da instituição, estão focadas na execução das atividades do trabalho. O trabalho é priorizado, pois se deixado de ser realizado, terá consequências imediatas. Já as diretrizes de segurança são de caráter preventivo, suas consequências nem sempre são imediatas e, por isso, deixam de serem levadas em consideração na elaboração das estratégias de trabalho. Estas estratégias aparentam um resultado positivo a curto prazo, mas a longo prazo geram prejuízos para a instituição, como o redirecionamento da carga de trabalho de outros funcionários para resolver os problemas de segurança criados, incidentes de segurança e efeitos no bem-estar dos funcionários.

Em muitos casos, as pessoas responsáveis por elaborar as diretrizes de Segurança da Informação na instituição são diferentes das que organizam o trabalho, e isso gera dissonância entre o objetivo do trabalho das pessoas e as prescrições de segurança. Entende-se que o objetivo fim da organização não é a segurança em si, mas a produção e gestão do conhecimento. Nesse sentido, as diretrizes precisam vir como um meio de apoio aos objetivos institucionais, e não de maneira contrária. Para isso, entende-se que é necessário que os responsáveis em elaborar as diretrizes de segurança da informação entendam melhor o que realmente é realizado pelos funcionários de cada setor para a realização do seu trabalho a fim de gerar normas, regras e procedimentos mais adequadas à instituição de maneira contínua.

7 CONSIDERAÇÕES FINAIS

O presente estudo identificou os principais fatores relacionados ao comportamento inseguro na Sede da IAPF. Foram identificados fatores já previstos na literatura de Segurança da Informação, como a falta de uma Política de Segurança da Informação, o desconhecimento das recomendações de Segurança da Informação vigentes. Ainda, foi verificado um possível conflito existente entre o suporte para a realização do trabalho e as prescrições das diretrizes de Segurança da Informação. Não foram identificados outros fatores que podem também influenciar o comportamento inseguro, como os alvos de atacantes que exploram a necessidade de benefícios pessoais dos funcionários, por exemplo. Para tanto, foi utilizada uma abordagem de investigação originada na Análise Ergonômica do Trabalho, focada na comparação das prescrições do trabalho e de sua execução prática.

O estudo limitou-se em mostrar apenas um panorama geral dos principais fatores relacionados ao comportamento inseguro. São considerados limites da pesquisa o pouco tempo disponível para a sua realização, que conciliou as horas de trabalho do pesquisador à coleta de dados, as dificuldades para encontrar pessoas na instituição dispostas ou disponíveis para contribuir com a pesquisa e situações de falta de espaço físico para acomodação do pesquisador durante as observações. Outro fator que limitou o aprofundamento do estudo foi a dificuldade

para obter dados precisos nos sistemas informatizados da instituição, como os incidentes e acidentes de Segurança da Informação, visto que não são registrados oficialmente. Também não foi identificada a falta do documento oficial Políticas de Segurança da Informação. Além disso, por se tratar de um trabalho que envolve informações sensíveis, algumas informações tiveram que ser omitidas para não comprometer a Segurança da Instituição. Outro sim, o Departamento de Tecnologia da Informação está em um processo de reestruturação. Este momento de transição dificultou o relato fiel de sua estrutura e fluxos, pois atualmente existem muitos processos indefinidos.

No entanto, acredita-se que, apesar de ser um primeiro estudo, o presente trabalho aponta para uma questão que demanda maior aprofundamento na literatura: o conflito existente na própria prescrição de trabalho. Esse pode ser um dos fatores responsáveis pela dificuldade das pessoas em se comportarem de maneira segura nas instituições públicas brasileiras. Com isso, evita-se que a responsabilidade por tal comportamento recaia somente sobre os indivíduos, eliminando apenas os sintomas e não o foco real do problema. Nesse sentido, percebe-se que novos estudos, com o uso da abordagem ergonômica, possibilitarão uma nova forma de compreender o papel da concepção das políticas, normas, padrões e procedimentos de Segurança da Informação, o que permitirá compreender como se comportam as pessoas na situação real de trabalho.

Diante da realidade em que as organizações têm se tornado cada vez mais dependentes da disponibilidade, sigilo e integridade das informações, a fim de aumentar a eficiência de suas operações, a busca por mecanismos de proteção, como ferramentas tecnológicas e metodologias, tornou-se fundamental. Outros estudos acerca do comportamento inseguro podem produzir mais evidências de maneira que, futuramente, possa surgir uma nova abordagem para a elaboração de diretrizes de Segurança da Informação que contemple as reais necessidades das pessoas na situação de trabalho, promovendo a criação de uma cultura de segurança.

CRediT

RECONHECIMENTOS: Não é aplicável.
FINANCIAMENTO: Não é aplicável.
CONFLITOS DE INTERESSE: Os autores certificam que não têm interesse comercial ou associativo que represente um conflito de interesses em relação ao manuscrito.
APROVAÇÃO ÉTICA: Não é aplicável.
DISPONIBILIDADE DE DADOS E MATERIAL: Não é aplicável.
CONTRIBUIÇÕES DOS AUTORES: Conceituação, Curadoria de Dados, Análise Formal, Investigação, Metodologia, Administração de Projetos, Recursos, Visualização, Escrita – rascunho original: SANTOS, R.B.; SILVA, T.B. P. e; Escrita – revisão & edição: SILVA, T.B. P. e

REFERÊNCIAS

ABRAHÃO, Júlia Issy. **Reestruturação produtiva e variabilidade do trabalho:** uma abordagem da ergonomia. Psicologia: Teoria e Pesquisa, Brasília, Vol. 16 n. 1, p. 49-54, jan/abr. 2000.

ABRAHÃO, Júlia Issy; PINHO, Diana Lúcia Moura. **Teoria e prática ergonômica**: seus limites e possibilidades. Em: M. G. T. da Paz & A. Tamayo (orgs.), Escola, saúde e trabalho: estudos psicológicos. Brasília, Universidade de Brasília. p. 229-239. 1999.

ABRAHÃO, Júlia Issy *et al*. **Introdução à ergonomia**: da prática à teoria. Brasília: Edgard Blucher, 2009.

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software:** como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Rio de Janeiro: Campus, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Versão 2. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001** Tecnologia da informação - Técnicas de segurança - Requisitos. Rio de Janeiro, 2006.

ASSOCIAÇÃO INTERNACIONAL DE ERGONOMIA - IEA **O que é ergonomia.** Disponível em: https://iea.cc/what-is-ergonomics/. Acessado em: 29 junho 2020.

BALLONI, Antônio José. **Por que gestão em sistemas e tecnologias de informação?** Segurança, inovação e sociedade. São Paulo: Komedi, 2007.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Dispõe sobre a governança da segurança da informação e institui a Política Nacional de Segurança da Informação (PNSI). Brasília, 2018.

BRASIL. Presidência da República/Gabinete de Segurança Institucional. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, 2019.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação. **Boas práticas em segurança da informação.** Brasília, DF, 2008. 70 p.

CERT.BR: **Estatísticas dos incidentes reportados ao Cert.br**. Disponível em: http://www.cert.br/stats/incidentes. Acesso em: 10 de fev. 2010.

CHIAVEGATTO, Myrza Vasques. **A gestão da informação e o processo decisório na administração municipal de Belo Horizonte**, Informática Pública, Belo Horizonte: v. 2, n. 2, p. 53-57, dez 2002.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

FERNANDES, Jorge Henrique Cabral. **Introdução à gestão de riscos de segurança da informação.** Texto desenvolvido para suporte às atividades de ensino do programa de pesquisas e Formação de Especialistas para Elaboração da Metodologia Brasileira de Gestão da Segurança da Informação e Comunicações, do módulo Gestão de Riscos de Segurança I. Departamento de Ciência da Computação. Universidade de Brasília. 81 p. 2009.

FERREIRA, Mário César. **Atividade, categoria central na conceituação de trabalho em ergonomia.** Revista Aletheia, Canoas, RS, n. 11, p. 71-82, 2000.

FONTES, Edison Luiz Gonçalves; BALLONI, Antonio José; LAUDON, Kenneth. **A segurança de sistemas da informação**: aspectos sociotécnicos. 2015.

FRÓIO, Leandro Ramalho. **Um modelo faseado de gestão da segurança da informação.** 2008. 134 f. Dissertação (Mestrado em Engenharia Elétrica) Departamento de engenharia elétrica, Universidade de Brasília, Brasília, 2008.

LOPES, Ângela Cristina Figueiredo. **Segurança da informação versus prontuário eletrônico:** hospital geral de Fortaleza – CE. 2009, 49 f. Monografia (especialização em aplicações complementares às ciências militares), Escola Superior do Exército. Rio de Janeiro, 2009.

MASLOW, Abraham Harold. **Motivation and personality**. New York: Harper.1954.

NETTO, Gilberto FREIRE, Pedro; ALLEMAND, Marcos. **Gestão operacional de segurança da informação.** Texto desenvolvido para suporte às atividades de ensino do programa de pesquisas e Formação de Especialistas para Elaboração da Metodologia Brasileira de Gestão da Segurança da Informação e Comunicações, do módulo Gestão Operacional de Segurança da Informação. Departamento de Ciência da Computação. Universidade de Brasília. 50 p. 2008.

PELTIER, Thomas. **Information security policies and procedures:** a practitioner's reference. 2. Ed. Auerbach Publications, Flórida, 2004.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SILVINO, Alexandre Magno Dias; ABRAHAO, Júlia Issy; SARMET, Mauricio Miranda. **Ergonomia, cognição e trabalho informatizado.** Psicologia: Teoria e Pesquisa, Brasília, v. 21, n. 2, p.163-171, 2005.

SILVINO, Alexandre Magno Dias; ABRHAO, Júlia Issy. Navegabilidade e inclusão digital: navegabilidade e competência. **Revista de Administração de Empresas**, São Paulo, RAE-Eletrônica. v. 2, jul/dez. 2003.

SILVINO, Alexandre Magno Dias. **Ergonomia cognitiva e exclusão digital:** a competência como elemento de (re)concepção de interfaces gráficas. 2004, 193 f. Tese (Doutorado em Psicologia), Universidade de Brasília, Brasília, 2004.

SIMON, Imre. **A revolução digital e a sociedade do conhecimento**: o que é informação? como ela age? 1999 Disponível em: http://www.ime.usp.br/~is/ddt/mac333/aulas/tema-11-24mai99.html. Acesso em: 18 jan. 2010.

SHIREY, Robert. **RFC 2828: internet security glossary**. the internet society, 2000. Disponível em: http://www.ietf.org/rfc/rfc2828.txt?number=2828. Acessado em: 15 fev. 2010.

STAIR, Ralph. **Princípios de sistemas de informação**: uma abordagem gerencial. Rio de Janeiro: LTC, 1998.

Artigo submetido ao sistema de similaridade

Submetido em: 03/05/2021 – Aprovado em: 16/09/2021 – Publicado em: 30/09/2021