Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Curso de Especialização em Gestão da Segurança da Informação e Comunicações

PAULO SÉRGIO BEZERRA DANTAS

ANÁLISE DE VULNERABILIDADES À ENGENHARIA SOCIAL NO PROCESSO DE ATENDIMENTO AO PÚBLICO DA ORGANIZAÇÃO OXP

Brasília

2014

Paulo Sérgio Bezerra Dantas

ANÁLISE DE VULNERABILIDADES À ENGENHARIA SOCIAL NO PROCESSO DE ATENDIMENTO AO PÚBLICO DA ORGANIZAÇÃO OXP

Brasília
2014

Paulo Sérgio Bezerra Dantas

ANÁLISE DE VULNERABILIDADES À ENGENHARIA SOCIAL NO PROCESSO DE ATENDIMENTO AO PÚBLICO DA ORGANIZAÇÃO OXP

Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a obtenção do título de Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações.

Orientadora: Profa. ME Helena Célia de Souza Sacerdote

SEEDF

Brasília

Setembro de 2014

Desenvolvido em atendimento ao Termo de Cooperação nº 06.1/2012-67-GSI/PR.

D192a

Dantas, Paulo Sérgio Bezerra

Análise de Vulnerabilidades à Engenharia Social no Processo de Atendimento ao Público da Organização OXP / Paulo Sérgio Bezerra Dantas. – Brasília: O autor, 2014. 117 p.

Monografia (Especialização) - Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília. 2014.

Inclui Bibliografia.

1. Engenharia Social. 2. Segurança da Informação. 3. Ativos de Informação. 3. Vulnerabilidades. 4. Organizações Públicas. I. Título.

CDU 004.056
CDD 004.02

ATA DE APROVAÇÃO

*Monografia de Pós-Graduação *Lato Sensu (Especialização),* defendida sob o título "Análise de Vulnerabilidades à Engenharia Social no Processo de Atendimento ao Público da Organização OXP, do aluno Paulo Sérgio Bezerra Dantas, em 19 de setembro de 2014, nas Dependências do Departamento de Ciência da Computação – CIC/UnB, em Brasília-DF, e aprovada pela banca examinadora constituída por:

Profa Me. Helena Célia de Souza Sacerdote
Orientadora - Secretaria de Estado de Educação - DF

Me. Rafael Henrique Santos Soares
Membro – Banco Central do Brasil

Esp. Raul Carvalho de Souza
Membro - Procuradoria Geral do Distrito Federal

Prof. Dr. Jorge Henrique Cabral Fernandes
Coordenador do Curso de Especialização em Gestão da
Segurança da Informação e Comunicações – CEGSIC 2012/2014.

***Desenvolvida em atendimento ao Termo de Cooperação N. 06.1/2012 GSI/PR, celebrado entre o Gabinete de Segurança Institucional da Presidência da Republica e a Fundação Universidade de Brasília, com recursos do Gabinete de Segurança Institucional da Presidência da República.**

Dedicatória

Dedico este trabalho a todos aqueles que fazem da perseverança um instrumento para materializar o triunfo diante dos desafios, por mais hercúleos que sejam.

Agradecimentos

À minha organização, pela anuência dada para que eu participasse deste curso de especialização e pelo apoio dado durante a realização dos encontros presenciais.

A meus colegas de trabalho, pela cooperação durante os períodos de realização dos exercícios de estudos de caso, como também pelas dúvidas dirimidas na fase de elaboração do TC.

À minha família, pelo suporte afetivo e pessoal empenhado durante o período de desenvolvimento da pesquisa.

À direção e aos funcionários da organização OXP, pela decisiva contribuição ao desenvolvimento do presente trabalho.

Ao *staff* do CEGSIC, pelas incontáveis horas de trabalho dedicadas ao suporte ao curso, bem como à transmissão de conhecimentos aos discentes. O agradecimento é extensivo aos tutores e colegas integrantes da turma Azul-Claro.

À banca examinadora, por ter emprestado seu precioso tempo para a análise deste trabalho.

À minha orientadora, Helena Célia de Souza Sacerdote, por ter acreditado no projeto e por sua valiosa participação no direcionamento da pesquisa, mesmo em momentos de dificuldades.

Meus sinceros agradecimentos a todos vocês!

Lista de Figuras

Figura 1 - Questão 1: Conhecimento acerca dos princípios de segurança da informação usados como referência na APF.....59
Figura 2 – Questão 2: Conhecimento acerca do papel da segurança da informação na organização.....60
Figura 3 – Questão 3: Conhecimento acerca do documento da política de segurança da informação da organização 61
Figura 4 – Questão 4: Conhecimento acerca das normas de segurança da informação relacionadas às atividades no trabalho.....62
Figura 5 – Questão 5: Conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às atividades no trabalho 63
Figura 6 – Questão 6: Conhecimento acerca de ativos de informação organizacionais 64
Figura 7 – Questão 7: Conhecimento acerca de tipos de informações que devem ser protegidas na organização 65
Figura 8 – Questão 8: Conhecimento acerca da realização de atividades de sensibilização em segurança da informação na organização 66
Figura 9 – Questão 1: Conhecimento acerca do que a engenharia social representa para a organização.....69
Figura 10 – Questão 2: Conhecimento acerca de técnicas e métodos empregados em ações de engenharia social.....70
Figura 11 – Questão 3: Conhecimento acerca de ferramentas que apoiam ações de engenharia social 71
Figura 12 – Questão 4: Conhecimento acerca do tipo de alvo de uma ação de engenharia social 72
Figura 13 – Questão 5: Conhecimento acerca de tipos de abordagens que podem ser utilizadas em uma ação de engenharia social.....73

Figura 14 – Questão 6: Conhecimento acerca de como ocorre uma ação de *phishing* 74
Figura 15 – Questão 7: Conhecimento acerca de casos de engenharia social.....75
Figura 16 – Questão 8: Conhecimento acerca de procedimentos de segurança da informação que podem obstar ações de engenharia social 76
Figura 17 – Questão 1: Exposição de documentos em mesas de trabalho 79
Figura 18 – Questão 2: Exposição de documentos abertos em computadores corporativos.....80
Figura 19 – Questão 3: Uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores.....81
Figura 20 – Questão 4: Compartilhamento de senhas de computadores corporativos com colegas de trabalho 82
Figura 21 – Questão 7: Conexão de dispositivos de armazenamento USB pessoais em computadores da organização 83
Figura 22 – Questão 9: Transporte de documentos físicos ou digitais da organização para trabalhos em ambientes externos 84
Figura 23 – Questão 10: Publicação em redes sociais de informações relacionadas ao trabalho 85
Figura 24 – Questão 5: Comportamento seguro de navegação na internet, baseado em normas e procedimentos documentados.....88
Figura 25 – Questão 6: Uso seguro do correio eletrônico baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações 89
Figura 26 – Verificação 1: Exposição de documentos institucionais em papel em mesas de trabalho.....91
Figura 27 – Verificação 2: Exposição de mídias de armazenamento digital em mesas de trabalho 92
Figura 28 – Verificação 3: Alcance visual das telas de computadores corporativos em relação ao público atendido 93
Figura 29 – Verificação 4: Exposição de documentos em telas de computadores corporativos no ambiente de trabalho 94
Figura 30 - Resultado dos indicadores de segurança associados ao conhecimento acerca da segurança da informação no contexto organizacional.....99

Figura 31 - Resultados dos indicadores de segurança associados ao conhecimento acerca da engenharia social.....100
Figura 32 - Resultados dos indicadores de segurança associados ao manuseio de ativos de informação 101
Figura 33 - Resultados dos indicadores de segurança associados à exposição de ativos de informação em salas de atendimento 103

Lista de Quadros

Quadro 1 - Correspondência de Parâmetros: conhecimento acerca da segurança da informação no contexto organizacional/conhecimento acerca da engenharia social 54
Quadro 2 - Correspondência de Parâmetros: procedimentos relacionados ao manuseio de ativos de informação organizacionais 55
Quadro 3 - Correspondência de Parâmetros: procedimentos relacionados ao manuseio de ativos de informação (questões 5 e 6) 56
Quadro 4 - Exposição de ativos de informação em ambientes de trabalho 56
Quadro 5 - Consolidação dos Resultados 98

Sumário

Ata de Defesa da Monografia....3
Agradecimentos....5
Lista de Figuras....6
Lista de Quadros....9
Sumário....10
Resumo....13
Abstract....14
1 Delimitação do Problema....15
1.1 Introdução....15
1.2 Formulação da situação problema (Questões de pesquisa)....16
1.3 Objetivos e escopo....17
1.3.1 Objetivo Geral....17
1.3.2 Objetivos Específicos....17
1.3.3 Escopo e Contexto....18
1.4 Justificativa....20
1.5 Hipóteses (possíveis respostas)....21
1.6 Estrutura Geral do Trabalho....21
2 Fundamentação Conceitual ou Revisão de Literatura....23
2.1 Aspectos da Segurança da Informação em Organizações Públicas....23
2.2 Aspectos da Segurança da Informação em Recursos Humanos....27

2.3 Procedimentos de Segurança da Informação relacionados ao manuseio de ativos de informação organizacionais 31
2.4 Engenharia Social 37
3 Metodologia 50
3.1 Classificação da pesquisa 50
3.2 Coleta De Dados 51
3.3 Instrumentos de coleta de dados 51
3.4 Tabulação e Apresentação dos Dados 53
4 Resultados, Análise e Discussão 58
4.1 Conhecimento acerca da segurança da informação no contexto organizacional 58
4.2 Análise dos resultados relativos ao conhecimento acerca da segurança da informação no contexto organizacional 67
4.3 Conhecimento acerca da engenharia social 68
4.4 Análise dos resultados relativos ao conhecimento acerca da engenharia social 77
4.5 Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação 78
4.6 Análise dos resultados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação 86
4.7 Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação (navegação e troca de informações) 87
4.8 Análise dos resultados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação (navegação e troca de informações) 90
4.9 Exposição de ativos de informação em ambientes de trabalho 91
4.10 Análise dos resultados relativos à exposição de ativos de informação em ambientes de trabalho 95
5 Conclusão da Análise e Consolidação dos Resultados Obtidos 96

5.1 Consolidação dos Resultados 97
5.2 Resultados dos indicadores de segurança associados ao conhecimento acerca da segurança da informação no contexto organizacional 99
5.3 Resultados dos indicadores de segurança associados ao conhecimento acerca da engenharia social 100
5.4 Resultados dos indicadores de segurança associados ao manuseio de ativos de informação 101
5.5 Resultados dos indicadores de segurança associados à exposição de ativos de informação em salas de atendimento 103
5.6 Conclusão acerca da Hipótese e Questão de Pesquisa 104
6 Conclusões e Trabalhos Futuros 106
6.1 Conclusões 106
6.2 Limitações da Pesquisa 108
6.3 Trabalhos Futuros 108
Referências e Fontes Consultadas 110
Apêndice A – Entrevistas estruturadas 113
Apêndice B – Observação Direta não participante 115
Apêndice C – Guia resumido para aplicação da metodologia 116

Resumo

A adequada proteção de seus ativos de informação é condição essencial para o eficiente desempenho da missão institucional de organizações brasileiras integrantes da Administração Pública Federal. Ameaças à segurança da informação podem explorar vulnerabilidades humanas com vistas à obtenção de acesso não autorizado a ativos de informação organizacionais, o que pode acarretar em danos ao negócio da organização. Nesse contexto, ataques de engenharia social provocados por agentes externos ou internos podem resultar na perda de confidencialidade de ativos de informação sensíveis resguardados por instituições públicas nacionais, entre outros danos. O presente estudo, baseado no método de estudo de caso proposto por Yin (2010), teve como objetivo analisar vulnerabilidades à engenharia social no processo de atendimento ao público de uma organização partícipe da Administração Pública Federal. Foram investigados aspectos relevantes para a segurança da informação, como também o emprego de técnicas e ferramentas utilizadas em ações de engenharia social, com base em Mitnick (2002), Mann (2008) e Hadnagy (2011). Esse entendimento aplicado à metodologia de pesquisa conduziu à descoberta de vulnerabilidades humanas e organizacionais que podem ser exploradas por ações de engenharia social na organização pesquisada.

Palavras-chave: Engenharia Social. Segurança da Informação. Ativos de Informação. Vulnerabilidades. Organizações Públicas.

Abstract

Proper protection of information assets is essential to brazilian organizations members of the Federal Public Administration, so they can efficiently achieve their institutional mission. Threats to information security can exploit human vulnerabilities in order to obtain unauthorized access to organizational information assets, which can result in damage to the organization's business. In this context, social engineering attacks, promoted by external or internal agents, can result in loss of confidentiality of sensitive information safeguarded by national public institutions, among other damages. The present study, based on case-research method proposed by Yin (2010), aimed to analyze vulnerabilities to social engineering in the process of public attendance of a participant organization of the Federal Public Administration. Relevant aspects for information security were investigated, as well the employment of tools and techniques used in social engineering actions, according to Mitnick (2002), Mann (2008) and Hadnagy (2011). This understanding applied to research methodology led to the discovery of human and organizational vulnerabilities that can be exploited by social engineering actions in the researched organization.

Keywords: Social Engineering. Information Security. Information Assets. Vulnerabilities. Public Organizations.

1 Delimitação do Problema

Este capítulo tem como objetivo introduzir a pesquisa e apresentar a delimitação do problema de pesquisa investigado nesta monografia. O capítulo é composto por seis seções: Introdução, Formulação da Situação Problema, Objetivos e Escopo, Justificativa, Hipóteses e Estrutura Geral do Trabalho.

1.1 Introdução

A informação é um ativo essencial para os negócios de uma organização, por conseguinte necessita ser adequadamente protegida. Isto é de alta relevância no ambiente dos negócios, cada vez mais globalizado. Como resultado do aumento da interconectividade gerada pela globalização, a informação está mais propensa à exposição para um crescente número de pessoas aumentando, assim, a variedade de ameaças e vulnerabilidades aos ativos (NBR ISO/IEC 27002, 2005).

O aumento da interconectividade entre as organizações viabiliza o fluxo de informações oportunas, o que tende a dinamizar processos de trabalho e a provocar reflexos em processos decisórios de corporações. Tais processos podem estar lastreados em informações estratégicas para o negócio, as quais necessitam de medidas adequadas de proteção.

> As instituições governamentais possuem um estoque imenso de dados operacionais, gerenciais e estratégicos, que formam um ativo valioso para a gestão pública exercer seu papel com mais eficiência. Esses ativos são bens públicos que, sob custódia do Estado, tem gerado a necessidade de esforços bem orquestrados para promover a segurança necessária e suficiente, especialmente no que concerne à disponibilidade, à integridade, à confidencialidade e à autenticidade dessas informações (RODRIGUES e FERNANDES, 2013, p. 11).

A adequada proteção dos próprios ativos de informação é condição essencial

para o eficiente desempenho da missão institucional das organizações integrantes da Administração Pública Federal (APF). Conforme expõe Borges (2011, p. 17),

> como prestadoras de serviço público ao cidadão, das organizações públicas se exige a prestação eficiente dos serviços, assegurando que estejam sempre disponíveis aos seus usuários (cidadãos brasileiros) e com a garantia da confidencialidade e integridade das informações fornecidas.

Ameaças à segurança da informação podem explorar vulnerabilidades humanas com vistas à obtenção de acesso não autorizado a ativos de informação organizacionais, o que pode acarretar em danos ao negócio da organização. Nesse contexto, ataques de engenharia social provocados por agentes externos ou internos podem resultar na perda de confidencialidade de ativos de informação sensíveis resguardados por instituições públicas nacionais, entre outros prejuízos.

A observação de rotinas de trabalho em organizações pode revelar vulnerabilidades decorrentes de procedimentos inseguros comuns relacionados ao manuseio de ativos de informação corporativos, a exemplo de mesas e telas de computadores repletas de documentos, uso de senhas fracas, compartilhamento de senhas, acesso a conteúdos pessoais por meio de *sites*, uso particular de *e-mail* corporativo, uso de dispositivos *Universal Serial Bus* (USB) pessoais ou de terceiros em computadores corporativos, conexão de computadores ou *smartphone*s, de uso pessoal, em computadores corporativos, entre outros. Tais situações evidenciam a necessidade de se implementar controles de Segurança da Informação direcionados ao elemento humano, a fim de que seja minimizada a exposição de ativos de informação organizacionais a ameaças, notadamente humanas.

1.2 Formulação da situação problema (Questões de pesquisa)

A proteção inadequada de informações sensíveis pertencentes a organizações públicas, num cenário em que se ampliam oportunidades de comunicação por meio do acelerado desenvolvimento de tecnologias de informação e comunicações, em sua maioria apoiadas pela internet, constitui-se atrativo para que criminosos virtuais empreendam ações a fim de obter acesso não autorizado a tais ativos. De outra forma, a ausência de medidas de proteção física também pode

viabilizar acesso físico não autorizado de ameaças humanas a áreas que resguardam informações sensíveis dessas organizações.

Na perspectiva deste estudo, a engenharia social representa ameaça potencial para organizações públicas, uma vez que ações dessa natureza podem ter como objetivo finalístico violar a segurança de ativos de informação possuídos por essas organizações.

Ataques de engenharia social, embora direcionados a explorar vulnerabilidades humanas, podem tirar proveito de falhas organizacionais, a exemplo de vulnerabilidades em políticas ou procedimentos de segurança da informação da organização alvo.

Tais situações expõem a necessidade de se investigar como ocorrem vulnerabilidades a ações de engenharia social no ambiente institucional público. À vista disso, levanta-se a seguinte questão de pesquisa: como se manifestam vulnerabilidades humanas e organizacionais que podem ser exploradas por ações de engenharia social no processo de atendimento ao público da organização OXP?

1.3 Objetivos e escopo

1.3.1 Objetivo Geral

Caracterizar vulnerabilidades à engenharia social no processo de atendimento ao público da organização OXP.

1.3.2 Objetivos Específicos

Para o alcance do Objetivo Geral, serão realizadas as seguintes etapas:

1. Abordar aspectos relevantes para a segurança da informação em organizações públicas;
2. Abordar aspectos relevantes para a segurança da informação em recursos humanos;

3. Abordar aspectos relevantes acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação organizacionais;
4. Desenvolver conceito de engenharia social baseado em reflexão no tocante a definições de pesquisadores da área;
5. Identificar e discutir o emprego de técnicas e ferramentas que podem ser utilizadas em ações de engenharia social;
6. Analisar aspectos relacionados ao conhecimento de estagiários e servidores acerca da segurança da informação no contexto organizacional;
7. Analisar aspectos relacionados ao conhecimento de estagiários e servidores acerca da engenharia social;
8. Analisar aspectos de segurança da informação relacionados ao manuseio de ativos de informação organizacionais por parte de estagiários e servidores;
9. Analisar exposição de ativos de informação organizacionais em ambientes de trabalho de estagiários e servidores;
10. Identificar vulnerabilidades humanas e organizacionais que podem ser exploradas por ações de engenharia social no processo de atendimento ao público da organização OXP.

1.3.3 Escopo e Contexto

O contexto organizacional da pesquisa é a organização OXP, cujas identificação e natureza da atividade fim se decidiu preservar, por razões de segurança da informação. A escolha se justifica pelos fatos de esta organização pertencer à APF, exercer relevante papel social e resguardar informações sensíveis, associadas principalmente a sua atividade finalística.

A organização OXP, cuja sede se localiza em Brasília/DF, está presente em diversos estados brasileiros. As atividades da sede e de suas unidades regionais abrangem tanto a área fim como a administrativa, subdivididas em setores e processos de trabalho. Na estrutura corporativa, os setores de Tecnologia da Informação (TI) e Recursos Humanos (RH) estão correlacionados ao desenvolvimento deste trabalho.

No que tange à estrutura de TI, a unidade regional da organização dispõe de rede de computadores, a qual provê acessos à internet e à intranet. Há setor dedicado a TI, o qual além de participar da administração da rede local e fornecer serviços internos de suporte, também é responsável pela segurança da informação, ainda que a unidade regional não disponha de política de segurança da informação.

O setor de RH é responsável pela administração de pessoal na unidade regional. Não há alinhamento deste setor com a área de TI, no que concerne ao desenvolvimento de ações institucionais consistentes de segurança da informação.

A unidade de análise deste estudo de caso é o processo de atendimento ao público da organização OXP, no qual serão investigadas vulnerabilidades à engenharia social associadas ao nível de conhecimento de servidores e estagiários acerca do papel da segurança da informação na organização; ao nível de conhecimento de servidores e estagiários acerca da engenharia social; à realização de procedimentos inseguros de servidores e estagiários relacionados ao manuseio de ativos de informação; e à exposição insegura de ativos de informação nas salas onde é realizado o processo de atendimento ao público.

Carece elucidar que o processo de atendimento ao público analisado nesta pesquisa não consiste em atendimento convencional de balcão, por intermédio do qual usuários normalmente buscam informações básicas. Em vez disso, caracteriza-se por processo interno dedicado a atender demandas específicas de usuários, relacionadas à própria atividade fim da organização.

A escolha de pesquisar essa unidade se justifica porque tanto os servidores como os estagiários que atuam no referido processo têm acesso a informações e a documentos sensíveis, produzidos e custodiados pela instituição. Além disso, o atendimento é realizado, em regra, nas próprias salas desses profissionais, onde são manuseados documentos em suporte de papel e também digital.

A exposição desnecessária de ativos de informação corporativos no ambiente de trabalho, somada à prática de procedimentos inseguros de servidores e estagiários em relação ao manuseio desses ativos, e ao desconhecimento ou baixo conhecimento acerca do papel da segurança da informação na organização em que trabalham, bem como acerca do que caracteriza a engenharia social, podem ampliar

a suscetibilidade desses profissionais a investidas de um engenheiro social que tenha o objetivo de acessar informações sensíveis da organização.

1.4 Justificativa

Este estudo, cujo objetivo consiste em analisar vulnerabilidades à engenharia social em uma organização pública, assume relevância para a esfera pública, uma vez que seus resultados poderão gerar reflexões a respeito do papel das pessoas na proteção de ativos de informação produzidos ou custodiados por essas organizações.

Esta pesquisa poderá contribuir com o conhecimento científico acerca do campo estudado, tendo em vista que possibilitará a identificação de métodos de ataque de engenharia social que podem ser relacionados a determinadas vulnerabilidades de segurança da informação, no ambiente de uma organização pública. Dadas as especificidades desse tipo de organização, tal confronto pode propiciar um novo vislumbre, com a identificação e análise de vulnerabilidades ainda não detectadas em trabalhos científicos conhecidos.

O resultado da investigação pode subsidiar a adoção de medidas que visem à preservação da segurança de ativos informacionais custodiados por órgãos públicos e, assim, contribuir para o aprimoramento de políticas de segurança da informação nesse ambiente.

Dentre as vantagens e benefícios que podem ser obtidos com o desenvolvimento deste estudo, releva-se a oportunidade de despertar a atenção de instituições públicas nacionais a respeito da ameaça que a engenharia social pode representar para a segurança de seus ativos de informação, haja vista a possibilidade de se replicar o referido protocolo de pesquisa em diversas organizações dessa natureza.

Ademais, a pesquisa em questão poderá subsidiar a elaboração de políticas segurança da informação e o desenvolvimento de metodologias para diagnosticar vulnerabilidades à engenharia social em organizações públicas, e ainda instigar pesquisas no campo da segurança da informação.

1.5 Hipóteses (possíveis respostas)

Se as pessoas que atuam no processo de atendimento ao público da organização OXP não estiverem engajadas com a segurança da informação, então elas estão vulneráveis a ações de engenharia social. Essas vulnerabilidades humanas e organizacionais se manifestam no limitado conhecimento acerca da segurança da informação no contexto organizacional, no restrito entendimento acerca da engenharia social e, ainda, na adoção de procedimentos inseguros, no que concerne ao manuseio de ativos de informação organizacionais.

1.6 Estrutura Geral do Trabalho

Este trabalho está organizado em sete capítulos, conforme detalhado a seguir:

No capítulo 1 - Delimitação do Problema, a proposta de pesquisa é contextualizada à luz da problemática da engenharia social no âmbito de organizações públicas. Compõem o capítulo as seções de Introdução, Formulação da Situação Problema, Objetivos e Escopo, Justificativa, Hipóteses e Estrutura Geral do Trabalho.

No capítulo 2 - Fundamentação Conceitual ou Revisão de Literatura, é apresentada a fundamentação teórica da pesquisa, na qual são alinhavados os assuntos que balizam este estudo de caso, os quais são decompostos em quatro segmentos: Aspectos da Segurança da Informação em Organizações Públicas, Aspectos da Segurança da Informação em Recursos Humanos, Procedimentos de Segurança da Informação Relacionados ao Manuseio de Ativos de Informação Organizacionais, e por fim, Engenharia Social.

No capítulo 3 - Metodologia, realiza-se explanação acerca da natureza e do planejamento da pesquisa, e ainda é descrito o processo de coleta de dados. O capítulo abrange as seções Classificação da Pesquisa, Coleta de Dados, Instrumentos de Coleta de Dados e, por fim, Tabulação e Apresentação dos Dados.

No capítulo 4 - Resultados, Análise e Discussão, são discutidos e analisados os resultados da coleta de dados. Esta etapa se desdobra nos segmentos Conhecimento Acerca da Segurança da Informação no Contexto organizacional, Conhecimento Acerca da Engenharia Social, Procedimentos de Segurança da Informação Relacionados ao Manuseio de Ativos de Informação, e Exposição de Ativos de Informação em Salas de Atendimento. Ao final de cada segmento, é apresentada a respectiva análise dos resultados.

No capítulo 5 - Conclusão da Análise e Consolidação dos Resultados Obtidos, é apresentada a Consolidação dos Resultados analisados, além da Conclusão Acerca da Hipótese e Questão de Pesquisa.

No capítulo 6 - Conclusões e Trabalhos Futuros, são apresentadas as Conclusões a respeito do trabalho, em sua integralidade. Neste capítulo, realiza-se explanação relacionada às Limitações da Pesquisa, bem como são apontadas sugestões para aprimorar o referido estudo de caso em Trabalhos Futuros.

2 Fundamentação Conceitual ou Revisão de Literatura

Este capítulo apresenta o referencial teórico que embasa a pesquisa em questão. Abordam-se aspectos referentes à segurança da informação em organizações públicas, segurança da informação em recursos humanos, procedimentos de segurança da informação relacionados ao manuseio de ativos de informação organizacionais, além de conceitos de engenharia social, bem como técnicas e recursos empregados nesse tipo de investida maliciosa.

2.1 Aspectos da Segurança da Informação em Organizações Públicas

A Norma NBR ISO/IEC 27002 (2005) define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Conforme dispõe o documento,

> a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (NBR ISO/IEC 27002, 2005).

No âmbito da APF, em vez do conceito de segurança da informação disposto

na Norma NBR ISO/IEC 27002 (2005), utiliza-se, como referência, o conceito de Segurança da Informação e Comunicações (SIC), constante na Norma Complementar 10/IN01/DSIC/GSIPR (2012, p. 3), segundo o qual a SIC "compreende ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação".

A Norma Complementar 10/IN01/DSIC/GSIPR (2012, p. 2-3) define os atributos elencados no conceito de SIC. Conforme expõe a norma, Disponibilidade "é a propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade"; Integridade "é a propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental"; Confidencialidade "é a propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado"; e Autenticidade "é a propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade".

Embora a perda de qualquer um dos atributos de SIC possa provocar danos à atividade fim de uma organização pública, a violação da confidencialidade dos ativos de informação é o cenário de maior criticidade para o escopo deste trabalho, uma vez que nessa perspectiva o objetivo precípuo de um engenheiro social é obter acesso não autorizado a informações que tenham valor para a organização.

> Os ativos de informação correspondem àquelas informações e todos os recursos associados que têm alto valor para o negócio público ou privado. Consideram-se como ativos de informação os processos organizacionais e processuais (procedimentos, roteiros, atividades), itens físicos (instalações, equipamentos, cabeamento) e lógicos (programas, sistemas, estruturas de dados), que devem ser auditados continuamente (RODRIGUES e FERNANDES, 2013, p. 12).

Ativos de informação sensíveis correspondem às informações que tenham valor crítico para a atividade fim de uma organização (ainda que a própria organização não tenha noção desse valor), como também aos funcionários que tenham acesso a tais conhecimentos. A divulgação não autorizada dessas informações pode frustrar a execução de planos estratégicos organizacionais, obstaculizar ações relacionadas à atividade fim e provocar danos à imagem institucional, entre outros prejuízos.

> As ameaças que pairam sobre todos os ativos organizacionais, físicos ou lógicos, tangíveis ou intangíveis, podem ter como fonte ou origem os seres humanos e o ambiente, sendo que seres humanos podem agir deliberadamente ou acidentalmente. Dessa forma, quanto à origem, as ameaças podem ser classificadas em (ABNT, 2008): humanas deliberadas (D); humanas acidentais (A); e ambientais (E - *Environmental*) (VIDAL e FERNANDES, 2013, p. 8).

A Norma Complementar 04/IN01/DSIC/GSIPR (2009, p. 2) define Ameaça como um "conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização". No entanto, tal conceito não contemplou ameaças humanas internas à organização, que podem ser caracterizadas por funcionários descontentes, mal treinados, demissionários, ou ainda indivíduos com o propósito de se infiltrar na organização para prejudicar o negócio em ações como roubo, vazamento de informações ou sabotagem de atividades ou processos de trabalho.

A Norma ABNT NBR ISO/IEC 27002 (2005, p. 3) define Vulnerabilidade como "fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças".

Vulnerabilidades podem ser exploradas por ameaças a partir de procedimentos inseguros de funcionários em relação ao manuseio ativos de informação organizacionais. "O comportamento inseguro pode ocorrer, originado pelo conflito existente entre as metas de trabalho e o próprio suporte organizacional" (SARMET, 2013, p. 12).

Organizações públicas são detentoras de muitas informações que podem despertar o interesse de um engenheiro social, a exemplo de processos administrativos, dados cadastrais de funcionários, procedimentos investigativos, dados financeiros, contratos, parcerias, projetos de investimentos, planejamento estratégico da organização, armazenamento de equipamentos sensíveis, bem como informações relacionadas a sistemas de segurança corporativos, entre outras.

Num patamar de maior criticidade estão informações públicas consideradas imprescindíveis à segurança da sociedade ou do Estado, as quais são passíveis de classificação. A Lei de Acesso à Informação estabelece os graus de sigilo Reservado, Secreto e Ultrassecreto para informações cuja divulgação não autorizada possa provocar risco à segurança da sociedade ou do Estado (BRASIL, 2011).

No que concerne à Gestão da Segurança da Informação e da Comunicação nos órgãos e entidades do Poder Executivo Federal, desenvolve-se a Gestão da Segurança da Informação e Comunicações, que considera, entre outros aspectos que:

> as informações tratadas no âmbito da APF, direta e indireta são ativos de valor para a eficiente prestação dos serviços públicos; o cidadão brasileiro é o beneficiário dos serviços prestados pelos órgãos e entidades da APF, direta e indireta; é dever do Estado a proteção das informações pessoais do cidadão; é necessário incrementar a segurança das redes e bancos de dados governamentais; é necessário orientar a condução de políticas de Segurança da Informação e Comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta (FERNANDES e RODRIGUES, 2013, p. 11-12).

Em 2012, o Plenário do Tribunal de Contas da União (TCU) publicou o Acórdão 2.585/2012 - TC 007.887/2012-4, o qual consiste em Relatório de Levantamento a respeito da situação da governança de TI no âmbito da APF. Em relação à segurança da informação nas organizações, o documento informa que 24% dispõem de inventário de seus ativos de informação, 17% classificam informações, 10% realizam análise de riscos, 16% implementaram processo de gestão de incidentes em segurança da informação, 51% designaram equipe para gerenciar a segurança da informação e 45% possuem política de segurança da informação (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

O relatório do TCU buscou avaliar a gestão da segurança da informação, tendo como critérios principais a Instrução Normativa 01/DSIC/GSIPR e controles previstos nas normas da Associação Brasileira de Normas Técnicas (ABNT) que tratam de práticas para a gestão da segurança da informação, ABNT NBR ISO/IEC 27002 (gestão da segurança da informação) e NBR ISO/IEC 27005 (gestão de riscos da segurança da informação) (TRIBUNAL DE CONTAS DA UNIÃO, 2012). De acordo com o documento, "uma gestão inadequada da segurança da informação pode causar prejuízos significativos à instituição, e ainda, no caso de entes públicos, afetar ou interromper serviços necessários à sociedade e aos cidadãos" (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 16).

Em 2008, o TCU tinha recomendado por meio do Acórdão nº 1.603 ao GSIPR que orientasse os órgãos/entidades da APF a respeito da importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que visassem estabelecer e/ou aperfeiçoar a gestão da

continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

À vista disso, o Departamento de Segurança da Informação e Comunicações (DSIC) do GSIPR emitiu ainda em 2008 a Instrução Normativa 01, que disciplina a gestão de SIC na APF. Ademais, desde aquele ano foi publicado um conjunto de normas complementares à referida instrução normativa, constituindo abrangente arcabouço normativo voltado a promoção da SIC em toda a APF (TRIBUNAL DE CONTAS DA UNIÃO, 2012). As normas contemplam aspectos como implementação de políticas de SIC, gestão de incidentes, gerenciamento de riscos e uso de recursos criptográficos, entre outros. No entanto, percebe-se que os números apresentados em 2012 pelo TCU revelam um descompasso entre esse universo normativo e a realidade da segurança da informação na APF.

Com efeito, o levantamento do TCU mostra que muitas organizações públicas carecem de políticas de segurança da informação para proteger seus ativos de informação e apoiar o próprio negócio. Além disso, muitas sequer documentam procedimentos básicos de segurança da informação, a exemplo das normatizações do uso de senhas e do manuseio de dispositivos USB no ambiente de trabalho. O resultado disso é um cenário propício ao surgimento de vulnerabilidades de segurança da informação em processos de trabalho corporativos, e a consequente exposição de ativos de informação a ameaças.

2.2 Aspectos da Segurança da Informação em Recursos Humanos

O fator humano constitui aspecto crítico na segurança da informação, tendo em vista seu papel central em relação a processos e tecnologias. Segundo Mann (2008), a segurança humana é a conexão que falta entre segurança de TI e segurança física. Enquanto a segurança de TI está voltada para *firewalls*, detecção de intrusão e antivírus, entre outros aspectos, a segurança física se volta para

proteção de portas e janelas, monitoramento de áreas por meio de sistemas de Circuito Fechado de TV (CFTV) e detecção de intrusão, entre outras medidas.

Para proteger seus ativos de informação, a maioria das organizações se concentra quase que completamente em segurança técnica. Atacantes detém essa informação e muitas vezes tomam o caminho mais fácil a fim de obter informações confidenciais de uma organização: as pessoas (MANN, 2008).

Nessa perspectiva,

> departamentos de recursos humanos têm o especial encargo de proteger funcionários daqueles que tentam descobrir informações pessoais por meio do seu local de trabalho. Profissionais da área de RH também têm a responsabilidade de proteger sua companhia das ações de ex-funcionários descontentes (MITNICK, 2002, p. 322).

Na estrutura da norma NBR ISO/IEC 27002 (2005), a seção Segurança em Recursos Humanos estabelece controles de segurança da informação voltados para RH, distribuídos em três categorias: Antes da Contratação, Durante a Contratação e no Encerramento ou Mudança da Contratação.

Tais controles não preveem recomendações específicas contra ameaças externas direcionadas a pessoas, diferentemente de controles de segurança física dispostos na mesma norma, que dispõem de medidas de proteção contra ameaças externas e do meio ambiente. Em que pese a limitada abrangência da referida seção, percebe-se que houve preocupação por parte dos elaboradores da norma com o elemento humano no contexto da segurança da informação.

A categoria Antes da Contratação apresenta controles relativos à definição de papéis e responsabilidades, ao processo seletivo e aos termos e condições de contratação. O objetivo da categoria consiste em assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, para que sejam reduzidos os riscos de roubo, fraude ou mau uso de recursos de informação (NBR ISO/IEC 27002, 2005).

Os controles da categoria Antes da Contratação estabelecem que: as responsabilidades pela segurança da informação devem ser atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação; todos os candidatos ao emprego, fornecedores e terceiros devem ser adequadamente analisados, especialmente em cargos com

acesso a informações sensíveis; e, por fim, todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, devem assinar acordos relativos a seus papéis e responsabilidades pela segurança da informação (NBR ISO/IEC 27002, 2005).

A adequada implementação destes controles constitui aspecto crítico para uma política de segurança da informação, haja vista que tais medidas podem contribuir para minimizar riscos de contratação de funcionários capazes de ameaçar a segurança de ativos de informação sensíveis da organização. Caso não seja possível detectar a "ameaça" no decorrer do processo seletivo, a definição de papéis e responsabilidades, bem como a assinatura de termos e condições de contratação, constituiriam instrumentos para promover responsabilização em caso de violações da política de segurança da informação vigente na organização.

A categoria Durante a Contratação apresenta controles relacionados às responsabilidades da direção, à conscientização, educação e treinamento em segurança da informação e ao estabelecimento de processo disciplinar. O objetivo da categoria é assegurar que os funcionários, fornecedores e terceiros estejam conscientes das ameaças e preocupações relativas à segurança da informação, bem como de suas responsabilidades e obrigações, e estejam preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir riscos de erro humano (NBR ISO/IEC 27002, 2005).

De acordo com os controles da categoria Durante a Contratação, as responsabilidades pela direção devem ser definidas para garantir que a segurança da informação seja aplicada em todo trabalho individual dentro da organização; um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação deve ser fornecido para todos os funcionários, fornecedores e terceiros, para que sejam minimizados possíveis riscos de segurança da informação; e, um processo disciplinar formal deve ser estabelecido para tratar das violações de segurança da informação (NBR ISO/IEC 27002, 2005).

A implementação dos controles supracitados assume relevância não somente pela ênfase dada às responsabilidades da direção, como condutora de práticas de

segurança da informação, e ao estabelecimento de processo disciplinar, como um mecanismo de dissuasão a violações de segurança da informação. Sobretudo, atividades voltadas à educação e treinamento em procedimentos de segurança da informação constituem aspectos indispensáveis para que seja disseminada entre as pessoas da organização a devida conscientização acerca de ameaças à segurança dos ativos de informação organizacionais. Tais ações, se adequadamente implementadas, além do apoio que poderiam fornecer à manutenção da política de segurança da informação, fomentariam uma cultura de segurança da informação na organização.

A categoria Encerramento ou Mudança da Contratação apresenta controles relacionados ao encerramento de atividades, devolução de ativos e retirada de direitos de acesso. O objetivo da categoria é assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada (NBR ISO/IEC 27002, 2005).

Os controles constantes na categoria Encerramento ou Mudança da Contratação estabelecem que sejam definidas responsabilidades para assegurar que a saída de funcionários, fornecedores e terceiros da organização ocorra de modo controlado e que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso estejam concluídas ao final do processo; e que as mudanças de responsabilidades e de trabalhos dentro de uma organização sejam gerenciadas quando do encerramento da respectiva responsabilidade ou trabalho (NBR ISO/IEC 27002, 2005).

A eficaz implementação destes controles pode reduzir riscos de vazamento ou acesso indevido a informações organizacionais, uma vez que a comunicação do encerramento de atividades inclui requisitos de segurança, responsabilidades legais existentes e responsabilidades contidas em acordos de confidencialidade. No processo de desligamento de funcionários, a ciência dada pela organização acerca das responsabilidades relativas ao sigilo de informações corporativas, as quais esses funcionários tenham tido acesso no desempenho da função, pode dissuadir ações de vazamento de informações institucionais. Ademais, a adequada devolução de ativos de informação, a retirada de acesso lógico e o estabelecimento de restrições de acesso físico às instalações da organização, no ato do desligamento

de funcionários, minimiza a possibilidade de exposição desses ativos a ameaças humanas externas à organização.

A implementação dos controles elencados na seção Segurança em Recursos Humanos não deve ser feita de forma estanque, tendo em vista que deve estar em conformidade com a política de segurança da informação da organização. Segundo Ferreira e Araújo (2008, p. 36), a política de segurança da informação é um documento que "define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação".

Um aspecto que merece destaque é a ausência na seção Segurança em RH de controles especificamente voltados à prevenção, detecção e/ou neutralização de ataques de engenharia social. A ameaça sequer é citada no documento, considerado referência para a gestão corporativa da segurança da informação. Embora alguns controles contemplados no referido código possam ser adaptados para minimizar vulnerabilidades à engenharia social, a presente lacuna dificulta o adequado tratamento da ameaça em organizações que balizem suas políticas de segurança da informação pela Norma NBR ISO/IEC 27002 (2005).

2.3 Procedimentos de Segurança da Informação relacionados ao manuseio de ativos de informação organizacionais

Procedimentos inseguros de funcionários podem expor ativos de informação sensíveis a ações de *crackers*[1], vazamento não intencional e ataques de engenharia social, entre outras ameaças ao negócio da organização. À vista disso, a política de segurança da informação deve abranger responsabilidades dos usuários em relação ao manuseio de ativos de informação organizacionais.

A Norma NBR ISO/IEC 27002 (2005) abrange na seção Controle de Acessos a categoria Responsabilidades dos Usuários, a qual estabelece controles para uso de senhas, equipamento de usuário sem monitoração e política de mesa e tela

[1] *Crackers* são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Disponível em: <http://www.tecmundo.com.br>.

limpa. O objetivo da categoria é prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.

Conforme dispõem os controles dessa categoria, a cooperação de usuários autorizados é essencial para uma efetiva segurança; os usuários devem estar conscientes de suas responsabilidades para manter efetivo controle de acesso, particularmente em relação ao uso de senhas e de segurança dos equipamentos de usuários; e ainda deve ser implementada política de mesa e tela limpa para reduzir o risco de acessos não autorizados ou danos a documentos/papéis, mídias e recursos de processamento da informação (NBR ISO/IEC 27002, 2005).

Em relação ao uso de senhas, a Norma NBR ISO/IEC 27002 (2005) preconiza que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas. Para tal, os usuários devem manter a confidencialidade das senhas; alterar a senha, se houver indícios de comprometimento do sistema ou da própria senha; utilizar senhas com caracteres alfanuméricos e especiais; modificar senhas regularmente, de forma a evitar a reutilização de senhas antigas; modificar senhas temporárias no primeiro acesso ao sistema; evitar a inclusão de senhas em processos automatizados para acessar os sistemas; não compartilhar senhas de usuários individuais; e não utilizar a mesma senha para uso profissional e pessoal.

Vulnerabilidades decorrentes da ausência de boas práticas de segurança da informação em relação ao uso de senhas podem ser exploradas em ataques de engenharia social. Dados organizacionais obtidos em páginas hospedadas na internet, ou até mesmo coletados na *deepweb*[2], somados a informações a respeito da pessoa-alvo obtidas por meio de contato interpessoal ou a partir de mídias sociais podem viabilizar a tarefa de "adivinhar senhas" por parte do atacante. Conforme expõe Hadnagy (2011, p. 42), há *softwares* capazes de vasculhar *websites* de organizações e criar listas com sugestões de senhas a partir das palavras coletadas. Esses dados podem ser combinados com sequências alfabéticas, numéricas ou alfanuméricas simples, ou até mesmo com datas.

[2] *Deepweb* se refere ao conteúdo da internet que não pode ser indexado pelos sites de busca, e dessa forma, não está disponível diretamente para quem navega na internet. Disponível em: <http://www.tecmundo.com.br>.

Softwares que utilizam a técnica de força bruta para quebrar senhas, também podem facilitar a empreitada de um engenheiro social em coletar dados com vistas à preparação de um ataque.

No que concerne às políticas de mesa e tela limpa, recomenda-se que seja adotada política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação. Essas políticas devem levar em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente, além de aspectos culturais da organização. De acordo com as diretrizes para sua implementação, deve-se evitar a exposição desnecessária de ativos de informação sensíveis tanto à mesa como na tela do computador (NBR ISO/IEC 27002, 2005).

A ausência de política de mesa limpa e tela limpa propicia o surgimento de vulnerabilidades que podem colocar em risco ativos de informação à exploração por parte de ameaças humanas. O acesso não autorizado às informações ocorreria *in loco*, em ambientes de trabalho com documentos sensíveis expostos em mesas de funcionários. Além disso, telas de computadores com documentos abertos, em muitos casos posicionadas ao alcance visual do atacante, e ainda estações de trabalho desprovidas de mecanismo de travamento de tela, facilitariam a tarefa de um engenheiro social, cujo propósito estaria direcionado à obtenção de acesso direto ao ativo desejado, como também à coleta e dados para apoiar um futuro ataque.

Na seção Gestão de Ativos, a categoria Responsabilidade pelos Ativos tem como objetivo alcançar e manter a proteção adequada dos ativos da organização. Nessa categoria, o controle Uso Aceitável dos Ativos preconiza que sejam identificadas, documentadas e implementadas regras que permitam o uso de informações e de ativos associados aos recursos de processamento da informação. Para a implementação do controle, recomenda-se que todos os funcionários, fornecedores e terceiros sigam as regras para uso permitido de informações e de ativos associados aos recursos de processamento da informação, incluindo regras para uso de *softwares* baseados na internet e do correio eletrônico, além de diretrizes para o uso de dispositivos móveis, especialmente fora das instalações da organização (NBR ISO/IEC 27002, 2005).

O adequado uso corporativo de navegadores e outros *softwares* baseados na internet, como também do correio eletrônico, depende do estabelecimento e formalização de políticas, procedimentos e controles para proteger a troca de informações em todos os tipos de recursos de comunicação (NBR ISO/IEC 27002, 2005).

Procedimentos inadequados de funcionários em relação à navegação em *websites* e ao uso de correio eletrônico tendem a resultar no surgimento de diversas vulnerabilidades, as quais podem expor ativos de informação corporativos a uma gama de ameaças, tecnológicas ou humanas. Pode-se afirmar que uma conexão direta entre vulnerabilidades decorrentes desses procedimentos e a engenharia social se materializa por meio de um ataque de *phishing*. De acordo com a Cartilha de Segurança para a Internet - Versão 4.0, *phishing* ou *phishing-scam* "é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social" (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012, p. 9). Cabe observar que esse conceito apresenta limitações, uma vez que o objetivo de um ataque de *phishing* pode ir além do acesso a dados pessoais ou financeiros do usuário alvo. O golpe pode ser aplicado com vistas a obter acesso não autorizado a ativos de informação organizacionais.

Conforme explica Pinheiro (2010, p. 312), a fraude por *phishing* ocorre da seguinte forma:

> (1) um código malicioso é enviado por *e-mail* para as vítimas; (2) as quais, não analisando a veracidade do conteúdo nem o remetente da mensagem, acessam a informação, executam o arquivo e, consequentemente; (3) o computador do usuário é infectado; (4) comprometendo suas informações confidenciais, tais como senhas, dados pessoais, etc.; (5) essas informações são transmitidas para o fraudador.

Após um ataque de *phishing* bem-sucedido, o golpista pode fazer uso das informações obtidas ilegalmente de forma a provocar danos à atividade fim da organização atingida, como também à sua própria imagem institucional.

Num cenário em que proliferam páginas maliciosas hospedadas na internet e são disseminados diariamente *spams*[3] contendo *malwares*[4] em milhares de caixas

[3] *Spam* é um termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Disponível em: <http://www.antispam.br>.

de correio eletrônico em todo o mundo, a ausência de normatização do uso seguro de navegadores de internet e do correio eletrônico no ambiente de uma organização pública amplia de forma significativa a possibilidade de que um engenheiro social obtenha acesso indevido a ativos de informação organizacionais por meio de um ataque de *phishing*.

Acerca do uso corporativo de dispositivos de armazenamento USB, a seção Gerenciamento das Operações e Comunicações elenca a categoria Manuseio de Mídias, cujo principal objetivo consiste em prevenir contra divulgação não autorizada, modificação, remoção ou destruição de ativos, e interrupções das atividades do negócio. Na categoria, o controle Gerenciamento de Mídias Removíveis recomenda que existam procedimentos implementados para o gerenciamento de mídias removíveis. Nesse quesito, devem ser consideradas medidas voltadas à destruição de dispositivos de armazenamento USB quando não houver necessidade da manutenção do conteúdo nessa mídia, em caso de retirada da organização; autorização para remoção dos dispositivos da organização, bem como a manutenção de registro das remoções; armazenamento dos dispositivos em ambiente protegido; registro dos dispositivos, para evitar perda de dados; redundância de informações que devam ser armazenadas por muito tempo nos dispositivos; e habilitação desses dispositivos condicionada às necessidades do negócio (NBR ISO/IEC 27002, 2005).

A ausência de procedimentos padronizados e documentados voltados ao manuseio corporativo de dispositivos de armazenamento USB viabiliza o surgimento de vulnerabilidades de segurança que poderão facilitar a investida de um engenheiro social contra a organização alvo. Um dos principais artifícios empregados é a tentativa de convencer a pessoa-alvo a conectar um *pen-drive*[5] infectado em seu computador corporativo. Isso pode ocorrer tanto de forma direta, com o pedido à vítima para que execute determinado arquivo no dispositivo, como de maneira indireta, em que o atacante pode posicionar intencionalmente o *pen-drive* contendo arquivo malicioso em lugares como corredores ou banheiros, de forma a aparentar

---

[4] O termo *Malware* está associado a diferentes tipos de códigos maliciosos, a diversas formas de infecção, bem como a ações danosas e atividades maliciosas executadas por eles. Disponível em: <http://www.cert.br>.

[5] *Pen-drive* é um dispositivo portátil de armazenamento com memória *flash*, acessível por meio da porta USB. Disponível em: <http://www.tecmundo.com.br>.

que alguém o tenha perdido, na esperança de que seja apanhado por um funcionário curioso o bastante para verificar o conteúdo do equipamento em sua estação de trabalho.

Na categoria Troca de Informações, também disposta na seção Gerenciamento das Operações e Comunicações, o controle Mídias em Trânsito apresenta recomendações acerca da proteção de informações contidas em mídias contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização (NBR ISO/IEC 27002, 2005).

A inexistência de controles voltados ao transporte de mídias tende a expor ativos de informação organizacionais a diversas vulnerabilidades. Temos como exemplo o transporte externo de documentos institucionais armazenados em *pen-drives*, sem que haja normatização. A situação se agrava quando funcionários transportam tais dispositivos com o objetivo de executar tarefas de trabalho em computadores alheios à instituição e sem autorização da política de segurança da informação para realizar tal procedimento. Isso provoca riscos tanto de perda de documentos corporativos quanto de roubo de informações sensíveis que possam estar armazenadas no dispositivo. Na primeira situação, caso o equipamento seja perdido durante o transporte, pode fortuitamente ser encontrado por um engenheiro social. No outro cenário, o roubo das informações pode constituir o objetivo de um ataque de engenharia social planejado contra o portador do *pen-drive*.

Outro quesito a ser considerado diz respeito ao uso particular de mídias sociais por parte dos funcionários de uma organização, o qual deve estar presente no escopo da política de segurança da informação. A ausência de sensibilização no que concerne aos cuidados para se evitar a divulgação não autorizada de informações da organização no ambiente de mídias sociais pode favorecer comportamentos descuidados, os quais podem resultar na divulgação de informações que, se aparentemente inofensivas de forma isolada, quando agrupadas com outros dados coletados facilitariam sobremaneira a tarefa de um engenheiro social para reunir informações com vistas a empreender um ataque de engenharia social contra uma pessoa chave da instituição.

Em que pese a implementação de políticas, normas ou procedimentos formalizados de segurança da informação em toda a organização, se não houver

processo estruturado de sensibilização em segurança da informação de maneira recorrente para todos os seus integrantes, os esforços para assegurar a adequada proteção dos ativos de informação organizacionais, em especial ativos sensíveis, provavelmente serão inócuos. Tal processo de sensibilização deve ter como foco o manuseio dos ativos de informação em alinhamento com as diretrizes estabelecidas pela política de segurança da informação vigente na organização, que por sua vez deve estar balizada nas melhores práticas de segurança da informação.

2.4 Engenharia Social

Entre diversas ameaças à segurança de ativos de informação corporativos, a engenharia social assume papel crítico, justamente por constituir ameaça direcionada a vulnerabilidades humanas, tendo em vista que em ataques de engenharia social são exploradas fragilidades na pessoa-alvo por meio do emprego de recursos ardilosos ou fraudulentos.

No âmbito de organizações públicas, ataques de engenharia social objetivariam o acesso não autorizado a ativos de informação organizacionais. As investidas podem ser executadas pessoalmente ou de forma remota, com o uso de sistemas de informação, embora o alvo das ações seja sempre o elemento humano. Esses ataques podem provocar danos à atividade fim e obstar, ainda que temporariamente, o cumprimento da missão institucional de organizações integrantes da APF.

Mitnick (2002) define engenharia social como a arte de levar pessoas a executar coisas que ordinariamente não fariam para um desconhecido. Esse conceito apresenta dois pontos que merecem reflexão. O primeiro é a ausência de esclarecimento acerca dos meios empregados na "arte de levar pessoas a executarem coisas". Sugere-se o preenchimento da lacuna com termos como persuasão ou influência, o que poderia melhorar essa descrição. O segundo ponto é a sugestão, inerente ao conceito, de que ataques de engenharia social são perpetrados por estranhos. Isso não constitui uma máxima, visto que um ataque planejado de engenharia social pode exigir conhecimento prévio ou até mesmo o

estabelecimento de uma relação de confiança entre atacante e vítima, o que naturalmente pode demandar um período razoável de tempo para ser firmada.

Conforme explica Mann (2008, p. 11), engenharia social é o ato de "manipular pessoas, pela enganação, para que forneçam informações, ou executem uma ação". Nesta definição, a expressão "manipular pessoas" atribui peso desproporcional à relação entre o engenheiro social e seu alvo, pois sugere que o atacante exerce total controle sobre o comportamento da vítima. Isso não necessariamente ocorre em uma investida de engenharia social, tendo em vista que uma razoável influência sobre o alvo pode ser suficiente para a consecução dos objetivos do executor da ação. Sugere-se a substituição da expressão por "influenciar pessoas", o que traria equilíbrio ao conceito apresentado.

Segundo Hadnagy (2011, p. 9), "engenharia social é a arte ou, melhor ainda, a ciência, de habilidosamente manobrar seres humanos a realizar ações em algum aspecto de suas vidas". A amplitude desta assertiva sugere que a engenharia social pode ser utilizada por qualquer pessoa no dia-a-dia, a exemplo de crianças que tentam convencer os pais a atender suas demandas. O autor argumenta que pode ser utilizada na maneira em que professores interagem com seus alunos, na forma em que médicos, advogados ou psicólogos obtêm informações de seus pacientes e clientes, entre outras situações. Não obstante, aprofunda a abordagem, ao asseverar que

> uma verdadeira definição de engenharia social é o ato de manipular uma pessoa a realizar uma ação que pode ou não estar no melhor interesse do alvo. Isso pode incluir obter informações, obter acesso, ou fazer o alvo realizar determinada ação (HADNAGY, 2011, p. 9).

Entre os autores supracitados, entende-se nesse trabalho que Hadnagy (2011) define engenharia social com maior completude e precisão que os demais. Sua abordagem permite a exploração do assunto tanto sob o prisma da segurança da informação quanto sob o enfoque da psicologia, haja vista os aspectos psicológicos que permeiam o conceito. Todavia esse autor, semelhantemente a Mann (2008), emprega o termo "manipular" em sua definição.

Tendo como base os conceitos e reflexões supracitados, apresenta-se a definição de engenharia social como uma ação ou um conjunto de ações voltadas a explorar vulnerabilidades humanas com o emprego de recursos ardilosos ou

fraudulentos, os quais podem ser apoiados por técnicas de influência ou persuasão, para que a pessoa-alvo forneça informações ambicionadas ou execute tarefa planejada em benefício do atacante. Entre muitas situações, ataques de engenharia social podem ter como objetivo roubar objetos, desviar dinheiro, destruir reputações ou obter acesso a informações não autorizadas.

Numa descrição alinhada com o escopo deste estudo, o engenheiro social pode ser considerado como o indivíduo capaz de executar ações de engenharia social contra integrantes de uma organização pública, com vistas a obter acesso a ativos de informação corporativos, para os quais não tenha a devida autorização.

As chances de êxito de um engenheiro social tendem a aumentar com um ataque meticulosamente planejado, apoiado por um eficiente trabalho de coleta de dados a respeito do alvo. A fase de coleta de informação compreende estágio preparatório para um ataque de engenharia social. Há uma gama de fontes de informação por meio das quais o atacante pode obter acesso a dados que, após reunidos e organizados, podem exercer papel decisivo para o êxito de uma investida. Assim, quanto maior for a qualidade da informação, maior será a possibilidade de alcançar o objetivo (HADNAGY, 2011).

Entre importantes fontes de coleta de informação se destacam observação do alvo, abordagem de pessoas ligadas ou possuidoras de informações a respeito do alvo, o lixo e fontes de informação abertas.

Embora não seja usada o bastante como uma ferramenta de engenharia social, a simples observação do alvo pode revelar informações relevantes a respeito da vítima (HADNAGY, 2011). A observação da rotina da pretensa vítima, bem como de pessoas com as quais ela se relaciona, combinada ou não com outras fontes de coleta de dados, pode viabilizar a construção de um perfil com elevada probabilidade de exatidão a respeito do alvo. A análise desse perfil pode revelar pontos vulneráveis, e assim permitir a exploração de vulnerabilidades humanas. Isso tende a ampliar as chances de êxito de um ataque de engenharia social.

Abordagens de pessoas ligadas ou possuidoras de informações a respeito do alvo podem fornecer dados relevantes como insumo para construção de um perfil a respeito da vítima, como também para mapear o ambiente em que se planeja a ação

de engenharia social. Essas pessoas podem ser familiares, colegas de trabalho ou indivíduos que não tenham relações interpessoais com o alvo, mas que detenham alguma informação (de interesse do atacante) a respeito dele ou do ambiente no qual será realizado a investida. Ao abordar pessoas ligadas ou possuidoras de informações a respeito do alvo, um engenheiro social habilidoso poderia se valer de um arsenal de técnicas e recursos, conforme a necessidade, para obter as informações desejadas. Nesse caso, pode-se dizer que essas pessoas são vítimas secundárias de um ataque de engenharia social. Peixoto (2006) classifica como Vítima Ativa (VA) funcionários de uma empresa alvos de um ataque de engenharia social, e como Vítima Superficial (VS) pessoas que podem ser parentes e/ou amigos da vítima, além de ex-funcionários da empresa, prestadores de serviços terceirizados ou concorrentes.

No campo de estudo da engenharia social, a busca de informações no lixo é conhecida como a técnica de mergulho no lixo (*dumpster diving*), cujo termo descreve a ação de remexer o lixo em busca de informações valiosas (MITNICK, 2002).

O mergulho no lixo pode viabilizar a coleta de dados relevantes acerca da pessoa a ser atacada, acerca do ambiente planejado para a execução do ataque e ainda a respeito dos ativos de informação cobiçados pelo engenheiro social. Caso a organização alvo não tenha política implementada para o descarte seguro de informações no lixo, o engenheiro social pode se deparar com uma relevante e regular fonte de dados para apoiar sua empreitada.

Hadnagy (2011, p. 39), esclarece que

> tão difícil quanto imaginar se divertir em pular através do lixo, é imaginar que isso pode produzir um dos mais lucrativos rendimentos para a coleta de informação. As pessoas muitas vezes jogam fora faturas, avisos, cartas, CDs, computadores, dispositivos USB, e uma infinidade de outros dispositivos e memórias que realmente podem fornecer surpreendentes quantidades de informação.

Conforme enfatiza Mitnick (2002, p. 158),

> seu lixo pode ser o tesouro de seu inimigo. Nós não damos muita atenção aos materiais que descartamos em nossas vidas pessoais, então porque devemos acreditar que as pessoas tenham uma atitude diferente no local de trabalho? Tudo se resume a educar os trabalhadores a respeito do perigo (pessoas inescrupulosas cavando informações valiosas) e a vulnerabilidade (informações sensíveis não sendo trituradas ou devidamente apagadas).

A pesquisa de informações a respeito do alvo em fontes abertas pode fornecer os dados que o engenheiro social precisa para concluir a elaboração de um ataque, com a vantagem de evitar sua exposição ao perigo de ser apanhado procurando materiais, documentos ou vasculhando o lixo nas dependências da organização. Livros, jornais, revistas e documentos ostensivos, além de meios de comunicação por intermédio dos quais o público tem acesso a informações ostensivas, a exemplo de rádio, televisão e internet, constituem fontes de informações abertas. A internet se destaca entre esses meios, tendo em vista sua abrangência mundial, sua capacidade quase inesgotável de oferecer informações aos usuários e a versatilidade de congregar em sua plataforma diversas mídias de comunicação.

Para a tarefa de um engenheiro social, a internet amplia as possibilidades de se encontrar informações pessoais e institucionais desejadas, haja vista a disponibilidade de recursos que viabilizam a realização de buscas específicas, o refino de preferências de pesquisa e a organização dos resultados obtidos. O uso desses recursos otimiza o tempo de coleta e análise de dados disponíveis em páginas pessoais, páginas corporativas, portais, *sites* colaborativos, *blogs* e mídias sociais, entre outras plataformas. A partir dessas fontes, o engenheiro social pode ter acesso a uma quantidade elevada de dados, os quais após reunidos, organizados, categorizados e analisados podem viabilizar a construção de um de perfil detalhado acerca do alvo, que disponibilize ao atacante informações pessoais (local de residência, familiares, amigos, *e-mail* pessoal, estado de saúde, situação econômica, passatempos, religião, escolaridade, visão política, idiomas que fala, esportes que pratica, restaurantes e clubes que frequenta, viagens pessoais, entre outras) e profissionais (organização em que trabalha, local de trabalho, setor em que está lotado, horário do expediente, *e-mail* corporativo, cargo, função, salário, colegas de trabalho, clientes que atende, organizações com as quais se relaciona, projetos em que está envolvido, tipos de informações que tem acesso, viagens a trabalho, período de férias, entre outros) a respeito da vítima.

Muitas vezes funcionários de uma empresa farão parte dos mesmos fóruns, listas de passatempo ou mídias sociais. A descoberta de um funcionário em mídias sociais como *LinkedIn* ou *Facebook* tende a aumentar as chances de se encontrar seus colegas de trabalho nesse ambiente. Tentar reunir todos os dados que possa

encontrar pode ajudar um engenheiro social a perfilar a empresa, como também seus empregados. Muitos funcionários divulgam em mídias sociais informações relacionadas ao seu trabalho. Isso pode ajudar um engenheiro social a perfilar quantas pessoas trabalham em determinado departamento de uma organização e como tal departamento está estruturado (HADNAGY, 2011).

A pesquisa em fontes abertas também pode ser realizada com o auxílio de motores de busca (*search engines*). Tais ferramentas consistem em *softwares* baseados na internet que oferecem serviços de busca por informações contidas em páginas hospedadas na rede mundial de computadores, a partir de solicitações na forma de palavras-chave fornecidas pelo usuário.

É importante observar que na fase de coleta de informação o engenheiro social pode se deparar com dados isolados, aparentemente sem valor para o propósito do ataque. Entretanto, a reunião de dados obtidos a partir de diversas fontes de coleta, e sua posterior organização e análise, pode revelar informações de significativo valor para apoiar sua investida contra o alvo.

A compreensão de que a fase de coleta de informação pode viabilizar a montagem de um perfil com o máximo de exatidão a respeito da vítima, bem como acerca da organização em que ela trabalha, infere que o objetivo estratégico desta etapa consiste em subsidiar a tomada de decisão do engenheiro social em um ataque planejado de engenharia social, uma vez que a partir da análise do perfil do alvo o atacante poderá selecionar as técnicas e recursos adequados para empreender sua ação.

A abordagem ao alvo configura o ataque de engenharia social propriamente dito, tendo em vista que nessa ocasião o engenheiro social terá a oportunidade de aplicar *in loco* suas habilidades e técnicas contra a vítima escolhida.

Segundo Hadnagy (2011), engenharia social não é apenas uma ação, mas um conjunto de habilidades reunidas em um *framework*, as quais quando agrupadas compõem a ação, a habilidade e a ciência denominada de engenharia social. O autor explana que em uma investida de engenharia social podem ser empregadas técnicas de elicitação, pretexto, Programação Neuro-Linguística (PNL), influência e persuasão, e ainda uma diversidade de ferramentas para apoiar o ataque.

A elicitação compreende estímulo direcionado a instigar uma particular classe de comportamentos. Materiais de treinamento da NSA[6] a definem como “sutil extração de informação durante uma conversação aparentemente normal e inocente”. "Ser capaz de utilizar de forma eficaz a elicitação significa que você pode moldar questões que instigam pessoas e as estimulam a tomar a direção de um comportamento que você quer" (HADNAGY, 2011, p. 55-56).

Uma breve reflexão acerca dos conceitos apresentados pressupõe que a elicitação está intrinsecamente ligada à engenharia social, uma vez que nessa técnica há naturalmente o emprego de influência e persuasão, de maneira ardil, para que no decorrer de uma conversação o alvo seja direcionado a um comportamento pré-estabelecido, o qual pode consistir na revelação de informações sigilosas da organização em que trabalha.

A elicitação tanto pode ser empregada na fase de coleta de informação como na abordagem, ou seja, no ataque propriamente dito. Sua eficiente aplicação na investida contra o alvo pode solidificar o pretexto utilizado pelo engenheiro social (HADNAGY, 2011).

No âmbito da engenharia social, pretexto pode ser definido como o ato de criar um cenário fictício para persuadir o alvo a fornecer informações ou realizar alguma ação. A técnica é muito mais complexa do que a simples criação de uma mentira, pois em alguns casos o atacante pode incorporar uma nova identidade e utilizá-la para manipular a recepção de informações (HADNAGY, 2011).

Entre muitas possibilidades, o pretexto pode ser utilizado pelo atacante para convencer a vítima de que ele é profundo conhecedor de assuntos que de fato não domina; que ocupa determinado cargo ou função, quando na realidade não possui vínculo empregatício com a organização; ou que possui grau de parentesco ou relações de amizade com integrantes-chave da organização, sem ao menos conhecer tais pessoas.

O pretexto também pode ser perfeitamente empregado para burlar controles de acesso físico, uma vez que o impostor, munido de uniforme ou crachá, pode

[6] *A Nacional Security Agency* é uma agência de segurança pertencente ao Departamento de Defesa dos Estados Unidos, a qual presta serviços de Inteligência de Sinais (SIGINT) ao governo daquele país.

tentar penetrar nas instalações físicas de uma organização disfarçado de funcionário terceirizado ou prestador de serviços em diversas funções, a exemplo dos papéis de técnico em manutenção de equipamentos, encarregado de suporte à TI, auxiliar de serviços gerais, encarregado pelo recolhimento e descarte de materiais, entre outros. No entanto, a eficácia da técnica nessas situações depende de conhecimento prévio acerca da organização, em especial a respeito do seu sistema de segurança física. Isso justifica a importância da fase de coleta de informação para o uso do pretexto na engenharia social. Hadnagy (2011, p. 79) salienta que “a qualidade do pretexto está diretamente ligada à qualidade da informação coletada”. Quanto mais relevantes forem as informações obtidas, mais fácil será desenvolver o pretexto, e consequentemente obter êxito.

A utilização da técnica de pretexto não se limita a situações de ataques presenciais, uma vez que pode ser aplicado de forma remota, por meio de correspondências, telefonemas ou solicitações via internet. Cartas fraudulentas podem induzir pessoas a revelar informações a um engenheiro social, a exemplo da solicitação de dados cadastrais, contábeis ou financeiros para um suposto órgão público. O uso do telefone constitui um método rápido para solidificar um pretexto, além de permitir que o engenheiro social falsifique quase tudo (HADNAGY, 2011). De fato, a ausência de contato visual com a vítima em uma ligação telefônica facilita o trabalho do atacante, haja vista que a ação nessa circunstância dispensa o uso de disfarces, cartões ou crachás, por exemplo.

No ambiente da internet, o pretexto é amplamente utilizado em golpes de *phishing*, cujas chances de sucesso tendem a aumentar com o envio de mensagens que apresentam razoável composição visual e redação correta, e que contenham dados capazes de induzir a vítima a acreditar que a mensagem é fidedigna. Normalmente são atingidos por golpes de *phishing* usuários alheios à segurança no uso de navegadores e do correio eletrônico.

O engenheiro social pode se valer de técnicas de PNL para apoiar sua investida contra o alvo. De acordo com a Sociedade Brasileira de Programação Neuro-linguística (2014), “a PNL oferece um modelo de ajuda a entender melhor como o ser humano pensa, age e se comunica, para que cada um seja capaz de identificar e aproveitar suas capacidades para alcançar os resultados que deseja”.

Técnicas de PNL podem ser exploradas na engenharia social para inserir comandos de voz, interpretar e espelhar gestos, manter a atenção do interlocutor e analisar os canais representacionais, também conhecidos como modos de pensamento.

Consoante abordagem de Hadnagy (2011), embora tenhamos cinco sentidos, os modos de pensamento estão associados a somente três deles: visão (pensamento visual), audição (pensamento auditivo) e tato (pensamento sinestésico). A descoberta do sentido dominante do alvo pode ser realizada por meio da leitura de seus gestos ou do lançamento de perguntas aparentemente despretensiosas. O entendimento do modo de pensamento da vítima a torna vulnerável à exploração de aspectos psicológicos. Munido com essa informação, o atacante pode utilizar gestos ou palavras a fim de estabelecer *rapport* com o alvo.

Conforme elucida ROBBINS apud TUCCI (2008),

> *Rapport* é a capacidade de entrar no mundo de alguém, fazê-lo sentir que você o entende e que vocês têm um forte laço em comum. É a capacidade de ir totalmente do seu mapa do mundo para o mapa do mundo dele. É a essência da comunicação bem-sucedida.

O estabelecimento de *rapport* contribui para abrir caminho para um ataque bem-sucedido de engenharia social. De acordo com Mann (2008), se queremos estabelecer confiança com alguém na intenção de enganá-lo para que forneça informações ou execute uma ação, desenvolver rápido *rapport* pode ser a chave para o alcance desses objetivos. Por sua vez, Mitnick (2002, p. 109-110) evidencia a importância do conhecimento acerca da organização para o estabelecimento de *rapport* com seus empregados: "uma vez que o engenheiro social sabe como as coisas funcionam dentro da empresa-alvo, torna-se fácil usar esse conhecimento para desenvolver *rapport* com funcionários legítimos".

Influência e Persuasão constituem a essência da engenharia social, haja vista que para alcançar o objetivo de convencer a vítima a fornecer informações ou executar determinada tarefa, o engenheiro social necessitará se valer das habilidades de influir e persuadir, as quais poderão estar associadas a outras técnicas e recursos. No entanto, o adequado uso dessas habilidades dependerá da capacidade de comunicação do atacante.

De acordo com Hadnagy (2011, p. 181), “Influência e a arte da persuasão constituem o processo de fazer alguém mais executar, reagir, pensar ou acreditar da

maneira que se quer que o faça". O autor apresenta cinco fundamentos da influência e persuasão, os quais considera essenciais para que o engenheiro social obtenha qualquer tipo de influência bem-sucedida sobre a vítima: estabelecer claros objetivos, construir *rapport*, observar o que está em volta, ser flexível e estar em contato consigo mesmo.

> Um engenheiro social usa a psicologia da influência para conduzir o alvo a cumprir com seu pedido. Engenheiros sociais experientes são hábeis em desenvolver artimanhas que simulam emoções como medo, excitação ou culpa. Isso é feito com o uso de gatilhos psicológicos - mecanismos automáticos que levam pessoas a atender solicitações sem uma análise aprofundada de todas as informações disponíveis (MITNICK, 2002, p. 105).

Não se pode esquecer que a aplicação eficaz da influência e persuasão em uma investida de engenharia social, em regra, dependerá do apoio de um eficiente trabalho de coleta de informação. O prévio conhecimento acerca do perfil do alvo, bem como a respeito de assuntos que possam despertar seu interesse, facilita o trabalho do atacante, que pode direcionar suas habilidades de influenciar e persuadir para situações específicas. Esse lastro proporcionado pela coleta de dados, acrescido à combinação das técnicas anteriormente descritas, tende a ampliar sobremaneira as chances de êxito do golpista em uma investida, uma vez que o conhecimento acerca de vulnerabilidades do alvo, associado às habilidades que um engenheiro social experiente normalmente deve possuir em extrair informações de forma sutil, criar um cenário convincente, modelar efetiva comunicação e direcionar o comportamento da vítima, compõem um conjunto de situações capaz de abreviar o alcance dos objetivos do atacante.

Um ataque de engenharia social pode ser potencializado com o uso de ferramentas específicas, capazes de apoiar tanto a fase de coleta de informação como a ação de abordagem do alvo. Hadnagy (2011) cita as diferenças entre ferramentas físicas, ferramentas de telefonia e ferramentas baseadas em *software*. Segundo o autor, ferramentas físicas envolvem chaves-mestras, gazuas[7], câmeras móveis, dispositivos de gravação portáteis e rastreadores de GPS[8], entre outras; ferramentas de telefonia envolvem essencialmente dispositivos falsificadores de

[7] Gazua é uma chave falsa ou ferro curvo, ou de gancho, com que se podem abrir fechaduras (Dicionário Michaelis).

[8] *Global Positioning System* (Sistema de Posicionamento Global) é um elaborado sistema de satélites e outros dispositivos cuja função básica consiste em prestar informações precisas sobre o posicionamento individual no globo terrestre. Disponível em: <http://www.tecmundo.com.br>.

identificação de chamadas; ferramentas baseadas em *software* envolvem aplicativos capazes de coletar, catalogar e correlacionar dados, programas voltados à sugestão de senhas e um kit de aplicativos, conhecido como kit de ferramentas do engenheiro social. O kit contém *softwares* que viabilizam o desenvolvimento de um ataque de *phishing*, os quais permitem anexar códigos maliciosos em diversos formatos de arquivos, como também possibilitam a clonagem de *sites* para que sejam acessados pelas vítimas. Ademais, o pacote de aplicativos oferece recursos que permitem inserir códigos maliciosos em mídias como CDs, DVDs ou *pen-drives*, para alcançar alvos previamente escolhidos.

Embora o rol de ferramentas elencado possa impressionar por sua diversidade, é necessário que se estabeleça distinção entre ferramentas que apoiam a coleta de informação e as que auxiliam diretamente a ação do pretexto, uma vez que esta segregação viabiliza o entendimento acerca do papel destes recursos em apoio a um ataque de engenharia social. Aplicativos e ferramentas *online* empregados na coleta e organização de dados, programas com funções para sugerir senhas, rastreadores de GPS, câmeras móveis e dispositivos de gravação de áudio portáteis compreendem ferramentas que apoiam a coleta de informação. Por sua vez, dispositivos de telefonia utilizados para falsificar identificação de chamadas ou alterar reconhecimento de voz, dispositivos de mídia contendo arquivos maliciosos, *softwares* empregados no desenvolvimento de ataques de *phishing*, disfarces, uniformes, bem como crachás e cartões de apresentação falsificados, compreendem ferramentas que apoiam a ação do pretexto.

A adequada aplicação de técnicas e ferramentas que podem ser utilizadas na engenharia social, associadas a um planejamento de ataque meticulosamente elaborado contra indivíduos vulneráveis, amplia as possibilidades de êxito na empreitada, principalmente se a organização em que trabalham apresentar vulnerabilidades no que concerne à segurança de seus ativos de informação. Os estudiosos Hadnagy (2011), Mann (2008) e Mitnick (2002) abordam diversos casos de engenharia social para estudo, nos quais se verifica o emprego de técnicas de elicitação, pretexto e persuasão, como também o uso de ferramentas em apoio a ataques.

A dificuldade de se detectar investidas de engenharia social contra funcionários é um desafio para gestores de segurança da informação de organizações públicas e privadas. Hadnagy (2011) revela que a elicitação funciona bem porque apresenta baixo risco, não ameaça o alvo e é frequentemente complexa de se detectar. A respeito da influência, o autor assevera que "a verdadeira influência é elegante e suave e na maioria das vezes indetectável para aqueles que estão sendo influenciados" (HADNAGY, 2011, p. 181). Entre as técnicas mencionadas, o pretexto é provavelmente a que apresenta menor grau de complexidade para detecção, tendo em vista que controles de acesso eficientes podem barrar a tentativa de um engenheiro social em obter acesso às dependências da organização munido de uniforme ou crachá falsificados. Uma história fictícia também pode ser descoberta por um funcionário suficientemente atento para verificar a autenticidade dos dados fornecidos pelo atacante.

Ainda que a implementação de política de segurança da informação balizada pelas melhores práticas possa ampliar a segurança dos ativos de informação no ambiente corporativo, tal iniciativa não é suficiente para assegurar que a organização fique imune aos riscos de ataques de engenharia social contra seus integrantes. Em que pese o estabelecimento de procedimentos padronizados de controles de acesso físico e lógicos e controles relacionados ao manuseio de ativos de informação corporativos, como aspectos de uma política de segurança da informação capazes de diminuir oportunidades que podem ser exploradas por um engenheiro social, essas medidas não são suficientes para eliminar as vulnerabilidades, pelo fato de que as pessoas estão sujeitas, independentemente do cargo ou função que exerçam, a um elevado número de variáveis subjetivas que podem originar vulnerabilidades de segurança, ou seja, funcionários descontentes, desmotivados, autoconfiantes ou até mesmo ignorantes, entre outras situações, podem ser influenciados ou persuadidos a tomar decisões que comprometam a segurança de ativos de informação organizacionais.

As reflexões ora apresentadas quanto ao potencial nocivo da engenharia social para a segurança da informação no ambiente corporativo conduzem a uma questão central nessa problemática: como evitar que pessoas da organização sejam alvos de ataques de engenharia social direcionados a obter acesso indevido a ativos de informação organizacionais?

Embora inexista fórmula capaz de proteger permanentemente as pessoas de uma organização contra iniciativas maliciosas de um engenheiro social, vulnerabilidades à engenharia social podem ser minimizadas com a implementação de uma política de segurança da informação alinhada ao negócio da organização, que tenha como referência as melhores práticas e dê ênfase a atividades de sensibilização recorrentes direcionadas a todos os seus membros, bem como a seus colaboradores, incluindo funcionários terceirizados, estagiários e também prestadores de serviços. Tais atividades devem ter como foco o papel das pessoas no contexto da segurança da informação e destacar aspectos da política de segurança da informação que possam dificultar a atuação furtiva de um engenheiro social, a exemplo da adequada implementação de controles de acesso físico e lógicos e controles relacionados ao manuseio de ativos de informação corporativos. Além disso, devem promover o entendimento acerca da ameaça que a engenharia social representa para a organização, e ainda expor de forma detalhada como vulnerabilidades humanas podem ser exploradas em ataques de engenharia social. Esse conjunto de iniciativas de sensibilização, em apoio à política de segurança da informação, constitui instrumento relevante para conscientizar as pessoas da organização acerca dos riscos da engenharia social. A conscientização, em última instância, constitui a base para a prevenção contra ataques de engenharia social.

Mann (2008) evidencia que elevar a conscientização acerca da ameaça de um ataque de engenharia social pode ampliar as possibilidades de que o ataque seja detectado e impedido. Hadnagy (2011) salienta que educação é a melhor defesa contra a maioria dos ataques de engenharia social, pois além de contribuir para aprimorar as próprias habilidades, também ajuda a manter as pessoas alertas contra a ameaça. Mitnick (2002, p. 72-73) entende que “todos são tão vulneráveis a ataques de engenharia social que a única defesa efetiva de uma organização é educar e treinar suas pessoas, dando-lhes a prática que precisam para identificar um engenheiro social”.

3 Metodologia

Este capítulo apresenta a metodologia utilizada neste trabalho e descreve o planejamento da pesquisa e o processo de coleta de dados. O capítulo abrange as seções Classificação da Pesquisa, Coleta de Dados, Instrumentos de Coleta de Dados, e por fim Tabulação e Apresentação dos Dados.

3.1 Classificação da pesquisa

Esta pesquisa está delimitada a investigar vulnerabilidades humanas à ataques de engenharia social e relacioná-las a ações de engenharia social. Isso aponta para uma abordagem descritiva, “na qual se procura observar e relacionar fenômenos sem manipulá-los e sem controlar suas ocorrências” (FERNANDES e BORGES, 2013, p. 11).

A busca por interpretar e atribuir valor a resultados alcançados a partir do confronto entre dados subjetivos, a serem obtidos na etapa de coleta de dados, evidencia o caráter qualitativo desta pesquisa. Conforme esclarece Fernandes (2009 apud BORGES, 2011, p. 98),

> a abordagem qualitativa usada – sobretudo – nas ciências sociais, é empregada em situações para a qual os fenômenos observados não são precisamente mensuráveis, nem tampouco é simples estabelecer uma relação numérica entre causas e consequências.

Esta pesquisa se classifica como aplicada, uma vez que “objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos” (MORESI, 2003, p. 8).

A estratégia utilizada neste trabalho é a de estudo de casos do tipo único com abordagem descritiva e qualitativa.

De acordo com Yin (2010, p. 39), um estudo de caso “é uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente evidentes”. Nessa esteira, Yin (2010) explica que os estudos de caso são o método preferido quando as questões "como" ou "por que" são propostas; o investigador tem pouco controle sobre os eventos; e o enfoque está relacionado a um fenômeno contemporâneo no contexto da vida real. Todas essas características estão presentes no contexto desta pesquisa, tendo em vista sua pretensão em investigar como se manifestam vulnerabilidades humanas e organizacionais a ataques de engenharia social em uma organização.

A escolha de uma organização específica como objeto deste estudo indica que o estudo de caso em questão será do tipo único. “O estudo de caso único considera que será estudado um único contexto durante a pesquisa, que seria, por exemplo, uma organização, projeto, pesquisa ou atividade” (FERNANDES, 2009 apud BORGES, 2011, p. 97).

3.2 Coleta De Dados

A etapa da coleta de dados permite a constituição de evidências confrontando com a base teórica deste trabalho.

O desenvolvimento deste trabalho está apoiado pelo emprego de múltiplas técnicas de coleta de dados. Yin (2010, p. 142-143) elucida que "um importante ponto forte da coleta de dados de um estudo de caso é a oportunidade de usar diferentes fontes de evidências”, pois “isso permite ao investigador abordar uma variação maior de aspectos históricos e comportamentais".

3.3 Instrumentos de coleta de dados

Neste trabalho, foram empregados como instrumentos de coleta de dados as técnicas de levantamento bibliográfico, entrevista estruturada e observação direta

não participante.

O levantamento bibliográfico abordou aspectos relacionados à segurança da informação em organizações públicas, segurança da informação em recursos humanos no ambiente organizacional e procedimentos de segurança da informação voltados ao manuseio de ativos de informação organizacionais. Também abordou de forma detalhada a engenharia social, com o delineamento de técnicas, recursos e ferramentas empregados para apoiar ataques. Esse levantamento teve como objetivos apresentar um panorama geral acerca da segurança da informação no contexto de organizações públicas, fornecer uma abordagem relacionada a controles de segurança da informação em recursos humanos e associados ao manuseio de ativos de informação, em conformidade com a Norma NBR ISO/IEC 27002:2005, e ainda caracterizar a engenharia social como um campo de estudo relevante para a segurança da informação.

Entrevistas estruturadas foram aplicadas a servidores e estagiários que atuam no processo de atendimento ao público da organização OXP, em um total de oito estagiários e seis servidores. Estes números correspondem a 89% dos estagiários e 86% dos servidores que efetivamente atuam no referido processo. Ressalva-se que se buscou abarcar a totalidade de pessoas envolvidas no processo pesquisado, tendo em vista a intenção de se obter resultados mais precisos nesta fase.

Os questionários foram disponibilizados num período de cinco dias úteis. Foram avaliados de forma segmentada conhecimentos dos entrevistados acerca da segurança da informação no contexto organizacional e da engenharia social. Objetivou-se investigar se evidências obtidas a partir dos dados coletados podem ser relacionadas a vulnerabilidades a ações de engenharia social (ver Apêndice A).

Também foram avaliados por meio de entrevista estruturada a periodicidade de realização de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação por parte dos mesmos servidores e estagiários. Objetivou-se investigar a existência de vulnerabilidades decorrentes de procedimentos inseguros em relação ao uso institucional desses ativos e associá-las a ataques de engenharia social.

A observação direta não participante foi realizada em sessões de 30 minutos,

num período de três dias úteis, nas salas de três estagiários e três servidores. Embora a observação dos ambientes de trabalho de todos os estagiários e servidores envolvidos na pesquisa pudesse ampliar as possibilidades de se obter resultados mais acurados, limitações de tempo para o desenvolvimento desta etapa acarretaram na escolha de apenas seis ambientes de observação.

A aplicação da técnica teve como foco a exposição de ativos de informação organizacionais nas salas onde é realizado o processo de atendimento ao público da organização OXP. Objetivou-se investigar vulnerabilidades à engenharia social decorrentes da exposição insegura de ativos de informação organizacionais na unidade de análise.

Os dados levantados constituíram anotações, manuscritas ou digitadas, as quais foram registradas na forma de arquivos eletrônicos de textos ou imagens em um banco de dados, para posterior categorização e análise.

Yin (2010, p. 143) explana que “qualquer achado ou conclusão do estudo de caso é, provavelmente, mais convincente e acurado se for baseado em diversas fontes de informação, seguindo um modo corroborativo". Desse modo, construiu-se um embasamento para explicar, de maneira convincente, como se manifestam vulnerabilidades humanas e organizacionais que podem ser exploradas por ações de engenharia social no processo de atendimento ao público da organização OXP.

3.4 Tabulação e Apresentação dos Dados

Os dados coletados nesta etapa foram tabulados conforme os procedimentos detalhados a seguir:

Nas entrevistas estruturadas, aplicadas tanto aos servidores quanto aos estagiários envolvidos no processo de atendimento ao público da organização OXP, foram avaliados níveis de conhecimento desses profissionais acerca da segurança da informação no contexto organizacional e acerca da engenharia social. Os parâmetros empregados em cada quesito para avaliar esses níveis de conhecimento foram: "inexistente", "restrito", "mediano" e "amplo", conforme se observa no Quadro 1.

Nessa dinâmica, conhecimentos acerca da segurança da informação no contexto organizacional, como também acerca da engenharia social, foram mensurados de forma segmentada, considerando-se os totais de respostas atribuídos aos parâmetros em cada quesito aplicado. Na tabulação dos resultados, o maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo, que por sua vez foi associado ao indicador de segurança correspondente. Os parâmetros: "inexistente", "restrito," "mediano" e "amplo" corresponderam de forma respectiva aos indicadores de segurança: "muito vulnerável", "vulnerável", "medianamente seguro" e "seguro". Para situações em que houve igualdade de totais acumulados na definição do parâmetro mais significativo, considerou-se o indicador de segurança com maior grau de vulnerabilidade ou menor grau de segurança, entre os indicadores associados aos parâmetros empatados.

PARÂMETRO	INDICADOR DE SEGURANÇA
Inexistente	Muito vulnerável
Restrito	Vulnerável
Mediano	Medianamente seguro
Amplo	Seguro

Quadro 1 - Correspondência de Parâmetros: conhecimento acerca da segurança da informação no contexto organizacional/conhecimento acerca da engenharia social

Também foi aplicada a esses servidores e estagiários, entrevista estruturada com vistas a avaliar a periodicidade da realização procedimentos de segurança da informação relacionados ao manuseio de ativos de informação no mesmo ambiente organizacional.

Os parâmetros empregados em cada quesito para avaliar essa periodicidade foram: "nunca", "ocasionalmente", "frequentemente" e "sempre" (Quadro 2). A incidência de tais procedimentos foi mensurada levando em conta os totais de respostas atribuídos aos parâmetros em cada quesito aplicado. Na tabulação dos resultados, o maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo, que por sua vez foi associado ao indicador de segurança correspondente.

Os parâmetros: "nunca", "ocasionalmente", "frequentemente" e "sempre" corresponderam de forma respectiva aos indicadores de segurança: "seguro", "medianamente seguro", "vulnerável" e "muito vulnerável" (Quadro 2). Para situações em que houve igualdade de totais acumulados na definição do parâmetro mais significativo, considerou-se o indicador de segurança com maior grau de vulnerabilidade ou menor grau de segurança, entre os indicadores associados aos parâmetros empatados.

PARÂMETRO	INDICADOR DE SEGURANÇA
Nunca	Seguro
Ocasionalmente	Medianamente seguro
Frequentemente	Vulnerável
Sempre	Muito vulnerável

Quadro 2 - Correspondência de Parâmetros: procedimentos relacionados ao manuseio de ativos de informação organizacionais

Em razão de erros na formulação das questões 5 e 6 da entrevista a respeito de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação organizacionais, houve a necessidade de se modificar, apenas para essas duas questões, a ordem de sequência dos parâmetros. Assim, decidiu-se realizar a tabulação dos resultados desses quesitos em separado, na discussão dos resultados (Item 4.7). Nesta situação específica, embora os resultados tenham sido tabulados conforme as regras anteriormente descritas, os parâmetros: "sempre", "frequentemente", "ocasionalmente" e "nunca" corresponderam de forma respectiva aos indicadores de segurança: "seguro", "medianamente seguro", "vulnerável" e "muito vulnerável" (Quadro 3).

No quadro de Consolidação dos Resultados (Quadro 5), as referidas questões estão posicionadas ao final do conjunto de quesitos a respeito de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação.

PARÂMETRO	INDICADOR DE SEGURANÇA
Nunca	Muito vulnerável
Ocasionalmente	Vulnerável
Frequentemente	Medianamente seguro
Sempre	Seguro

Quadro 3 - Correspondência de Parâmetros: procedimentos relacionados ao manuseio de ativos de informação (questões 5 e 6)

Na observação direta não participante foi avaliada a exposição de ativos de informação corporativos em ambientes de trabalho de estagiários e servidores. Os parâmetros empregados em cada quesito para avaliar essa exposição foram: "não observado", "vulnerabilidade detectada" e "vulnerabilidade não detectada" (Quadro 4). A exposição dos ativos foi mensurada levando em conta a quantidade de verificações atribuídas aos parâmetros em cada quesito aplicado.

Na tabulação dos resultados, o maior valor resultante da soma dos totais obtidos nas verificações em cada parâmetro definiu o parâmetro mais significativo, que por sua vez foi associado ao indicador de segurança correspondente. Os parâmetros: "não observado", "vulnerabilidade detectada" e "vulnerabilidade não detectada" corresponderam de forma respectiva aos indicadores de segurança: "não observado", "vulnerável" e "seguro". Para situações em que houve igualdade nos totais acumulados para a definição do parâmetro mais significativo, considerou-se o indicador de segurança com maior grau de vulnerabilidade ou menor grau de segurança, entre os indicadores associados aos parâmetros empatados.

PARÂMETRO	INDICADOR DE SEGURANÇA
Não observado	Não observado
Vulnerabilidade detectada	Vulnerável
Vulnerabilidade não detectada	Seguro

Quadro 4 - Exposição de ativos de informação em ambientes de trabalho

A tabulação dos dados oriundos da observação direta tomou por base apenas três indicadores de segurança, ao passo que na tabulação das informações decorrentes das entrevistas estruturadas foram empregados quatro indicadores. Por

conseguinte, somente os indicadores "vulnerável" e "seguro" são comuns entre segmentos associados a essas duas técnicas de coleta de dados.

4 Resultados, Análise e Discussão

Esse capítulo consolida e interpreta as informações levantadas com base nos dados coletados no ambiente da organização OXP, relacionados ao processo de atendimento ao público prestado pela organização.

4.1 Conhecimento acerca da segurança da informação no contexto organizacional

Buscou-se por meio de entrevista estruturada (ver Apêndice A) coletar dados que permitissem mensurar de forma segmentada conhecimentos de estagiários e servidores, que atuam no processo de atendimento ao público da organização OXP, acerca da segurança da informação no contexto organizacional. Foram entrevistados oito estagiários e seis servidores. Ressalta-se que essa diferença numérica prejudica a comparação isonômica entre as respostas correspondentes às duas categorias.

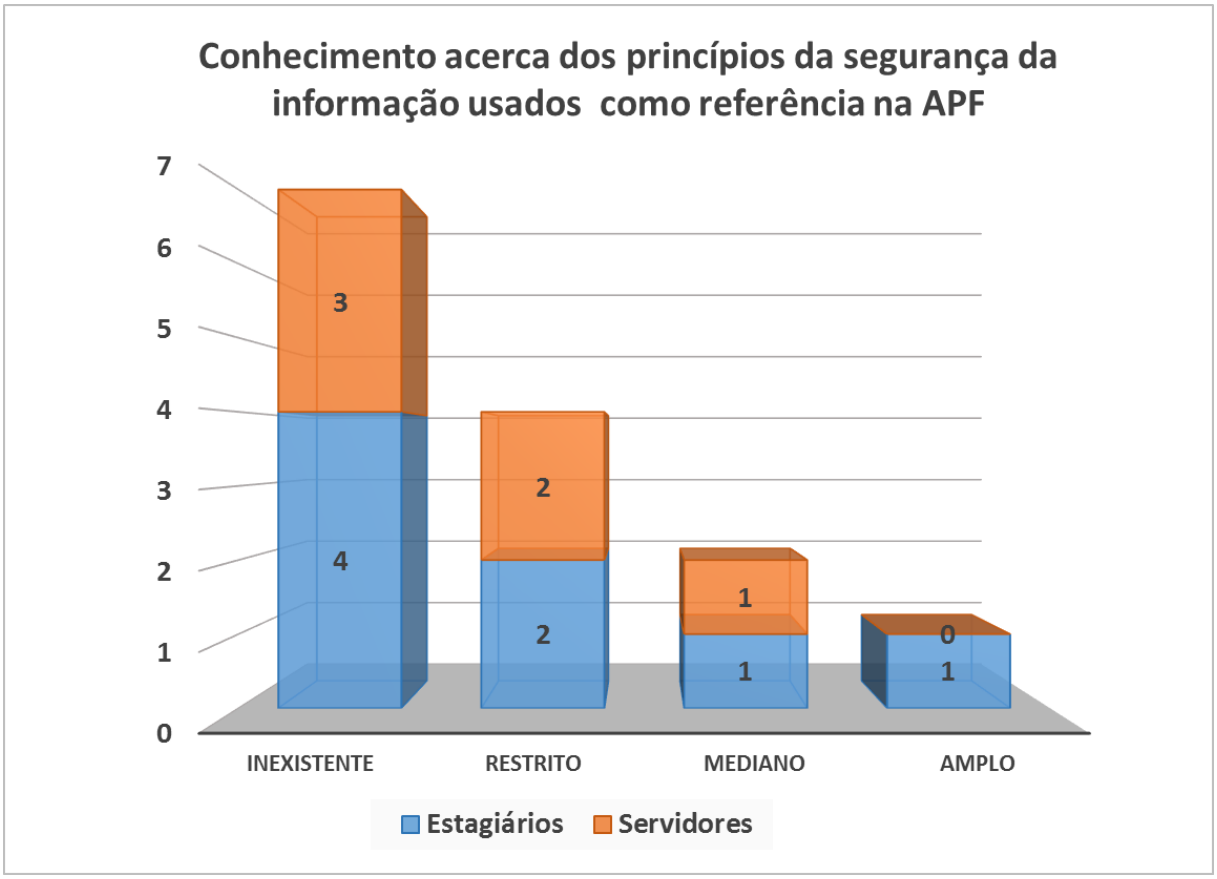

Figura 1 - Questão 1: Conhecimento acerca dos princípios de segurança da informação usados como referência na APF

Os resultados do questionamento revelam que quatro estagiários e três servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca dos princípios da segurança da informação usados como referência na APF. Nos parâmetros restantes, quatro entrevistados apontaram a opção “restrito”, dois assinalaram “mediano” e um indicou como resposta o parâmetro “amplo”. O gráfico revela proeminência dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”. Nota-se ainda equilíbrio entre os totais de respostas de estagiários e servidores nos parâmetros “inexistente”, “restrito” e “mediano”. A exceção foi o parâmetro “amplo”, respondido por um estagiário e não indicado por nenhum servidor.

Conforme critérios estabelecidos para tabulação dos dados coletados, o maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito

conhecimento acerca dos princípios da segurança da informação usados como referência na APF (Disponibilidade, Integridade, Confidencialidade e Autenticidade).

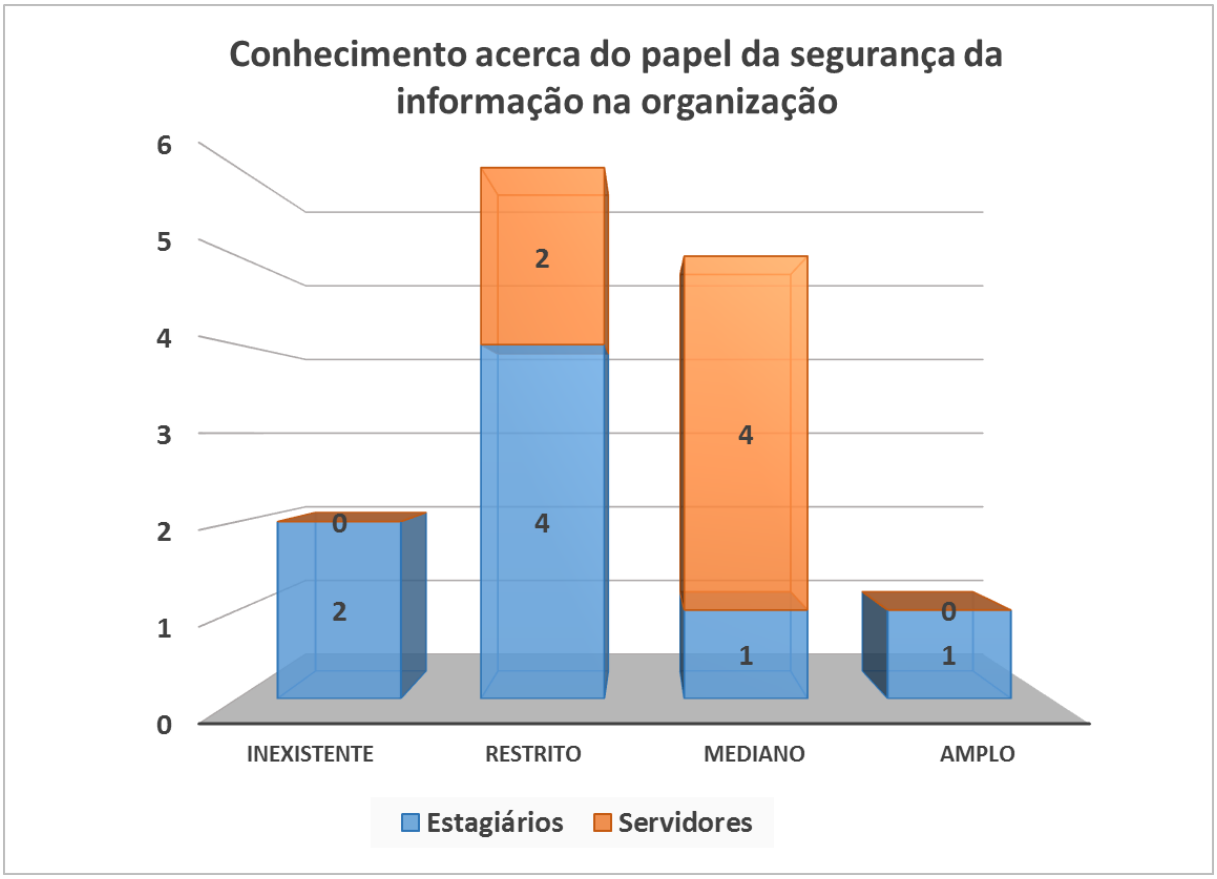

Figura 2 – Questão 2: Conhecimento acerca do papel da segurança da informação na organização

Os resultados revelam que quatro estagiários e dois servidores, o equivalente a 43% dos entrevistados, apontaram o parâmetro “restrito” no quesito conhecimento acerca do papel da segurança da informação na organização. O parâmetro “mediano” foi assinalado por quatro servidores e um estagiário. Por sua vez, os parâmetros “inexistente” e “amplo” foram indicados por dois e um estagiários, respectivamente. Não houve indicações aos parâmetros "inexistente" e “amplo” nas respostas dos servidores. No gráfico, relevam-se os totais acumulados de respostas nos parâmetros “restrito” e “mediano”. Nesses parâmetros, verificam-se diferenças relevantes entre os totais de respostas de estagiários e servidores, uma vez que, enquanto as respostas de quatro estagiários predominaram no parâmetro “restrito”, o mesmo total teve prevalência nas respostas dos servidores ao parâmetro “mediano”. No gráfico fica patente a maior distribuição das respostas de estagiários,

enquanto as respostas dos servidores se concentraram apenas nos parâmetros “restrito” e “mediano”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “restrito”, associando assim o indicador de segurança “vulnerável” ao quesito conhecimento acerca do papel da segurança da informação na organização.

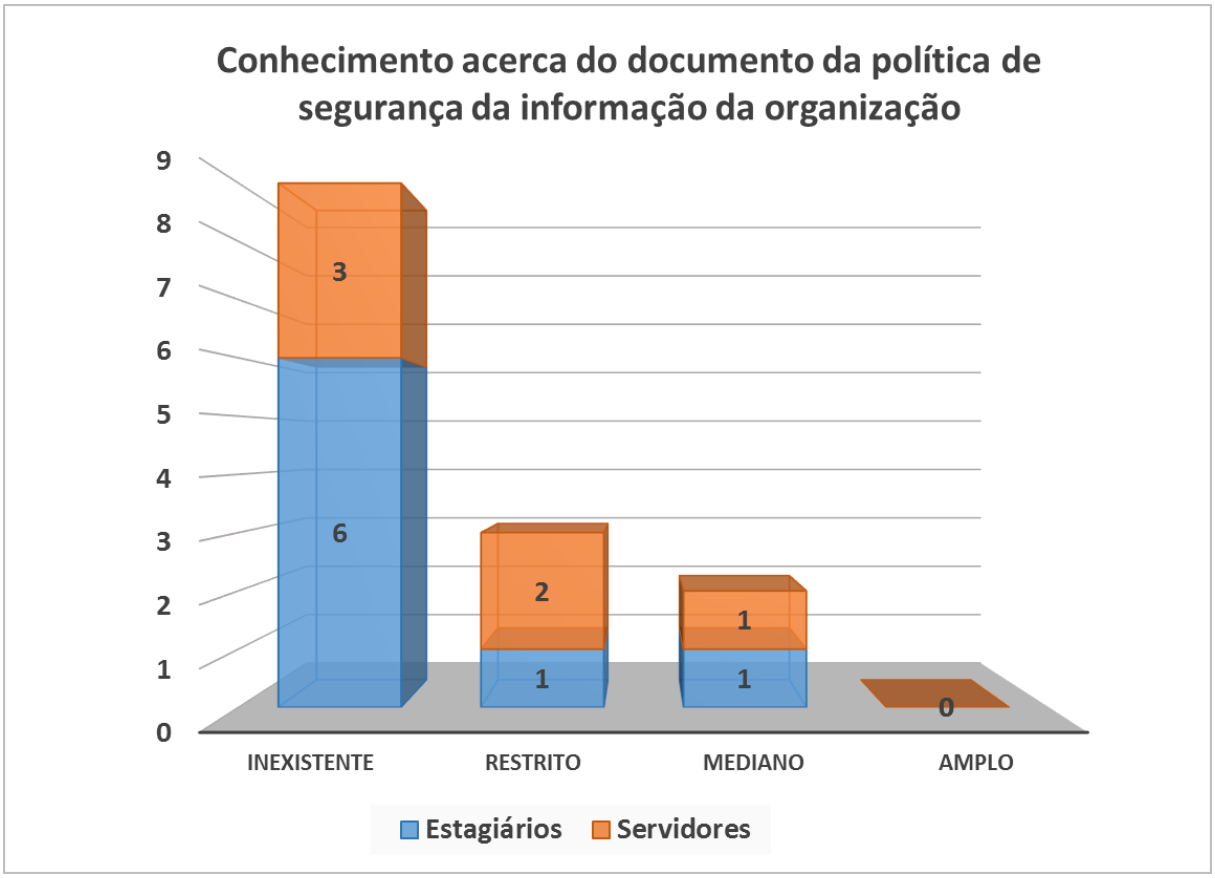

Figura 3 – Questão 3: Conhecimento acerca do documento da política de segurança da informação da organização

Os resultados mostram que seis estagiários e três servidores, o equivalente a 64% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca do documento da política de segurança da informação da organização. Nos parâmetros restantes, três entrevistados apontaram a opção “restrito” e dois assinalaram o parâmetro “mediano”. Não houve respostas ao parâmetro “amplo”. Percebe-se que o total acumulado de respostas ao parâmetro "inexistente" é significativamente maior do que os totais de respostas aos demais

parâmetros. Essa divergência também se mostrou visível na comparação entre as respostas dos estagiários. Outro aspecto relevante foi verificado no escalonamento dos totais de respostas dos servidores.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca do documento da política de segurança da informação da organização.

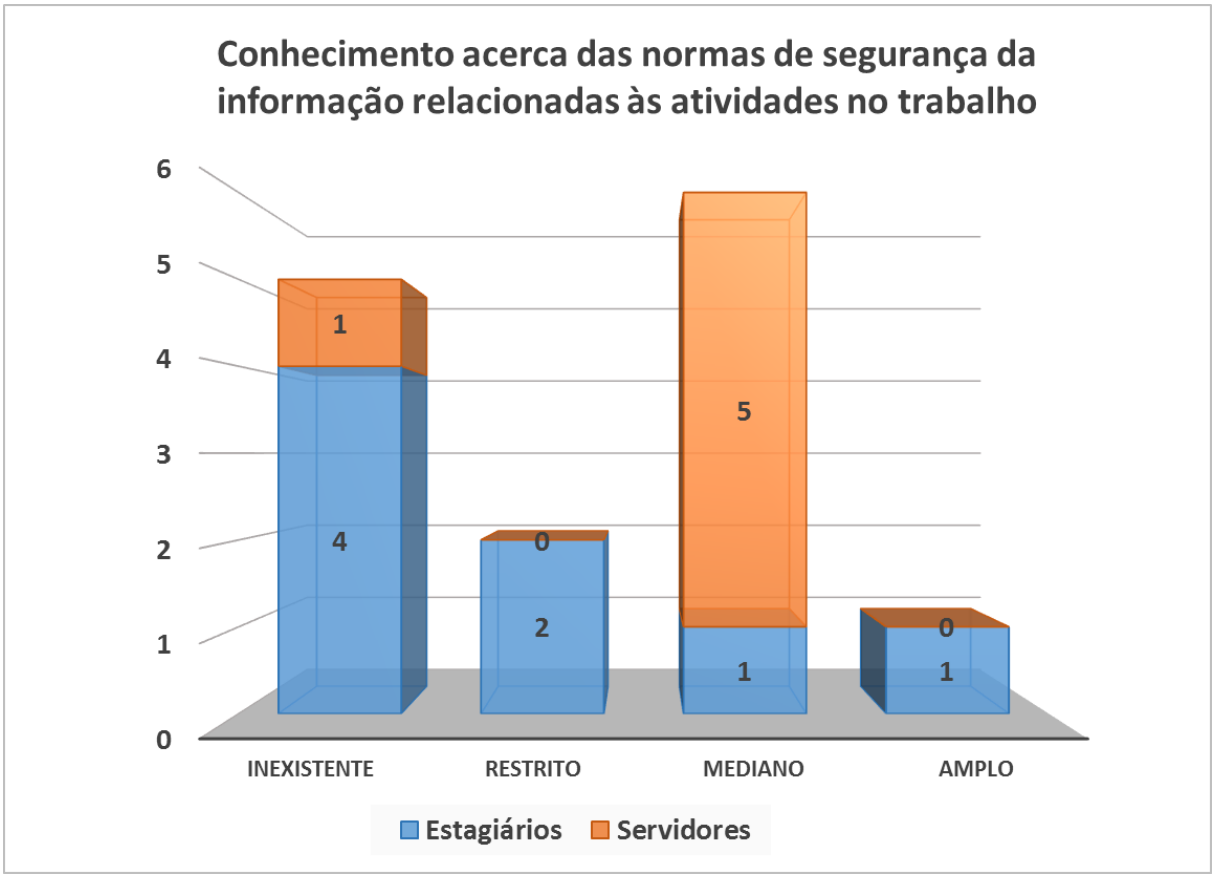

Figura 4 – Questão 4: Conhecimento acerca das normas de segurança da informação relacionadas às atividades no trabalho

Os resultados revelam que cinco servidores e um estagiário, o equivalente a 43% dos entrevistados, assinalaram o parâmetro “mediano”, no quesito conhecimento acerca das normas de segurança da informação relacionadas às atividades no trabalho. O parâmetro “inexistente” foi assinalado por quatro estagiários e um servidor. Por conseguinte, os parâmetros “restrito” e “amplo” foram

assinalados respectivamente por dois e um estagiários, como também não foram indicados nas respostas dos servidores. O gráfico revela predomínio dos totais acumulados de respostas nos parâmetros “inexistente” e “mediano”. Em relação a esses parâmetros, verificam-se diferenças significativas entre os totais de respostas de estagiários e servidores, haja vista que as respostas de quatro estagiários predominaram no parâmetro “inexistente”, enquanto as respostas de cinco servidores prevaleceram no parâmetro “mediano”. Nota-se maior distribuição das respostas de estagiários, enquanto as respostas dos servidores se concentraram apenas nos parâmetros “mediano” e “inexistente”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “mediano”, associando assim o indicador de segurança “medianamente seguro” ao quesito conhecimento acerca das normas de segurança da informação relacionadas às atividades no trabalho.

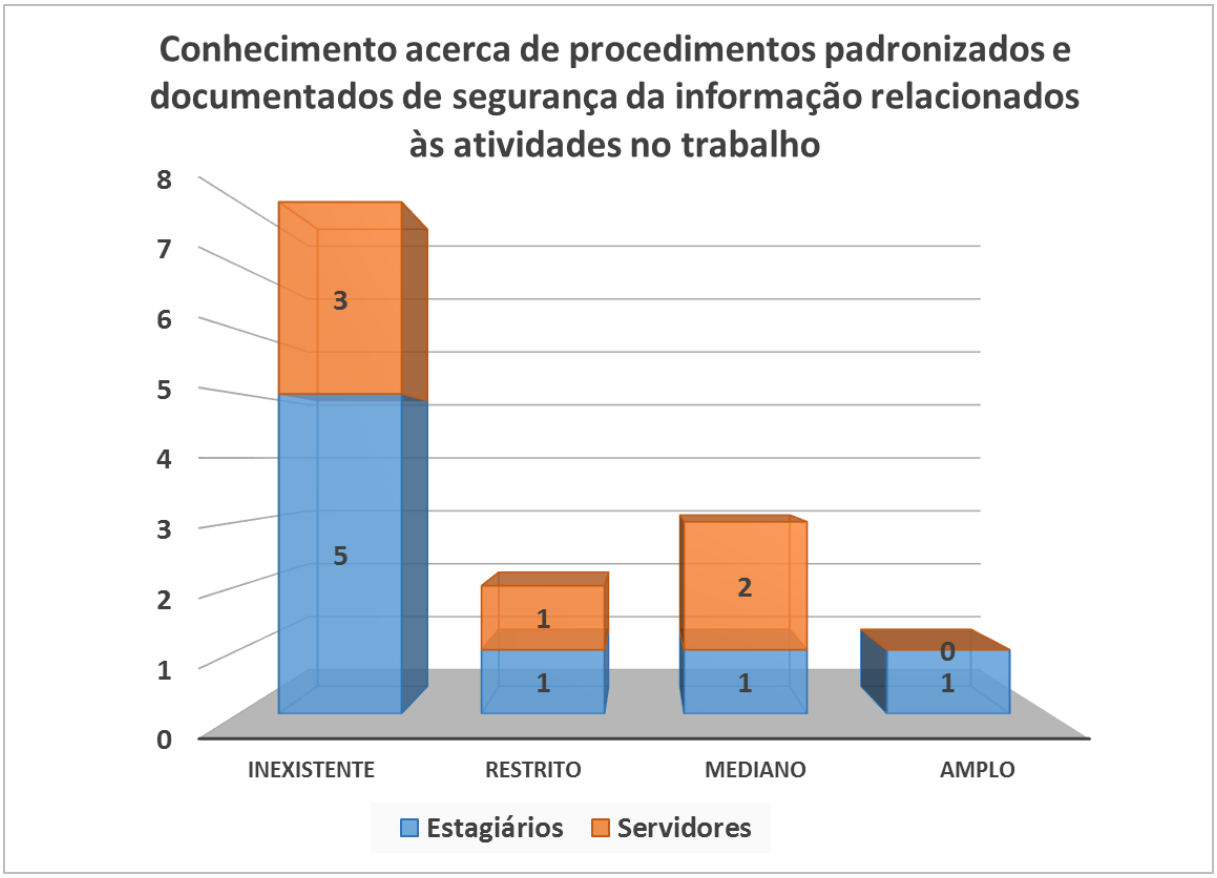

Figura 5 – Questão 5: Conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às atividades no trabalho

Os resultados mostram que cinco estagiários e três servidores, o equivalente a 57% dos entrevistados, assinalaram o parâmetro “inexistente”, no quesito conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às atividades no trabalho. Nos parâmetros restantes, dois entrevistados apontaram a opção “restrito”, três assinalaram “mediano” e somente um escolheu a opção “amplo”, não indicada nas respostas dos servidores. O gráfico revela proeminência do total acumulado de respostas no parâmetro “inexistente” e igualdade nos totais das respostas dos estagiários nos demais parâmetros. As respostas dos servidores foram significativamente direcionadas aos parâmetros “inexistente” e “mediano”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às atividades no trabalho.

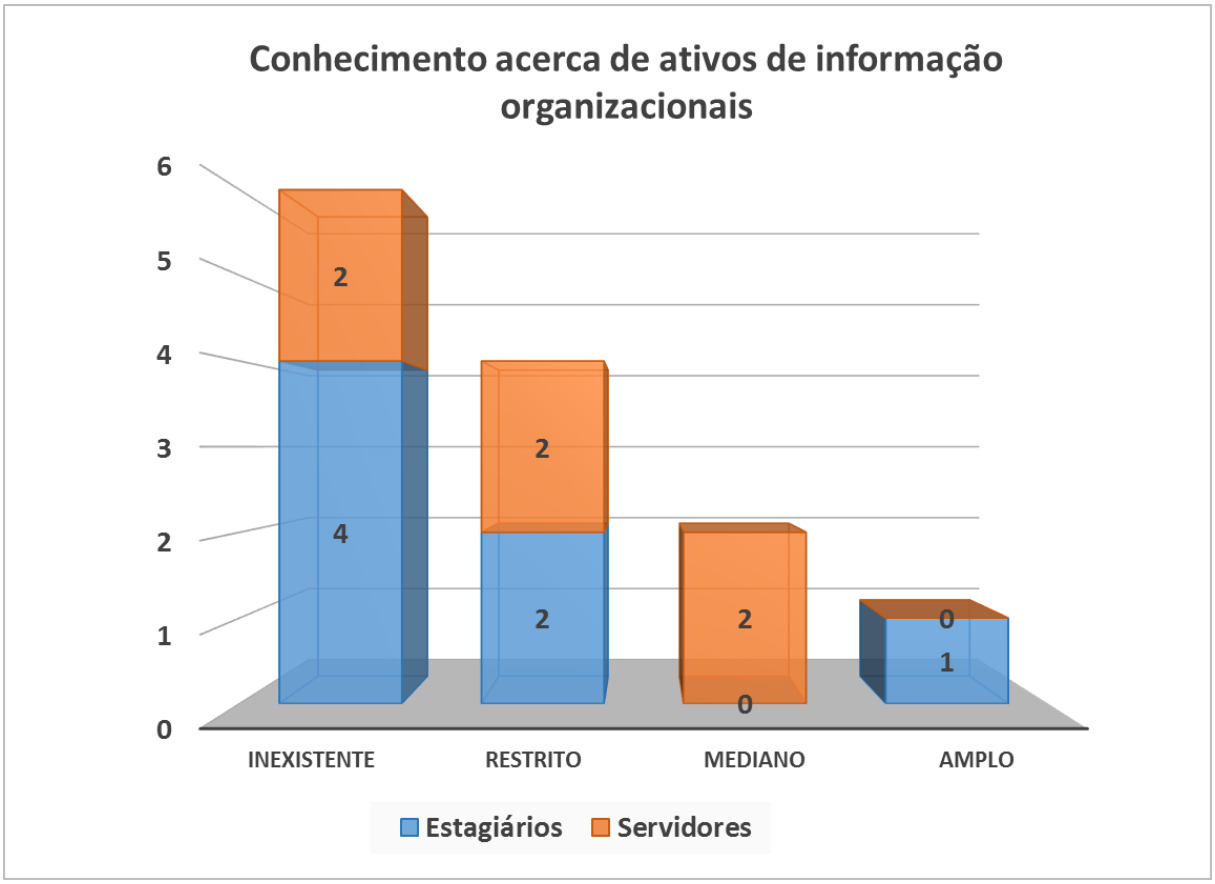

Figura 6 – Questão 6: Conhecimento acerca de ativos de informação organizacionais

Os resultados do questionamento revelam que quatro estagiários e dois servidores, o equivalente a 43% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de ativos de informação organizacionais. Nos parâmetros restantes, quatro entrevistados apontaram o parâmetro “restrito”, dois assinalaram a opção “mediano” e um indicou o parâmetro “amplo”. Percebe-se prevalência dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”, além da ausência de indicação do parâmetro “mediano” nas respostas dos estagiários. Nas respostas dos servidores, observa-se que o mesmo total foi replicado entre os parâmetros “inexistente”, “restrito” e “mediano”, e ainda que não houve indicação ao parâmetro “amplo”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de ativos de informação organizacionais.

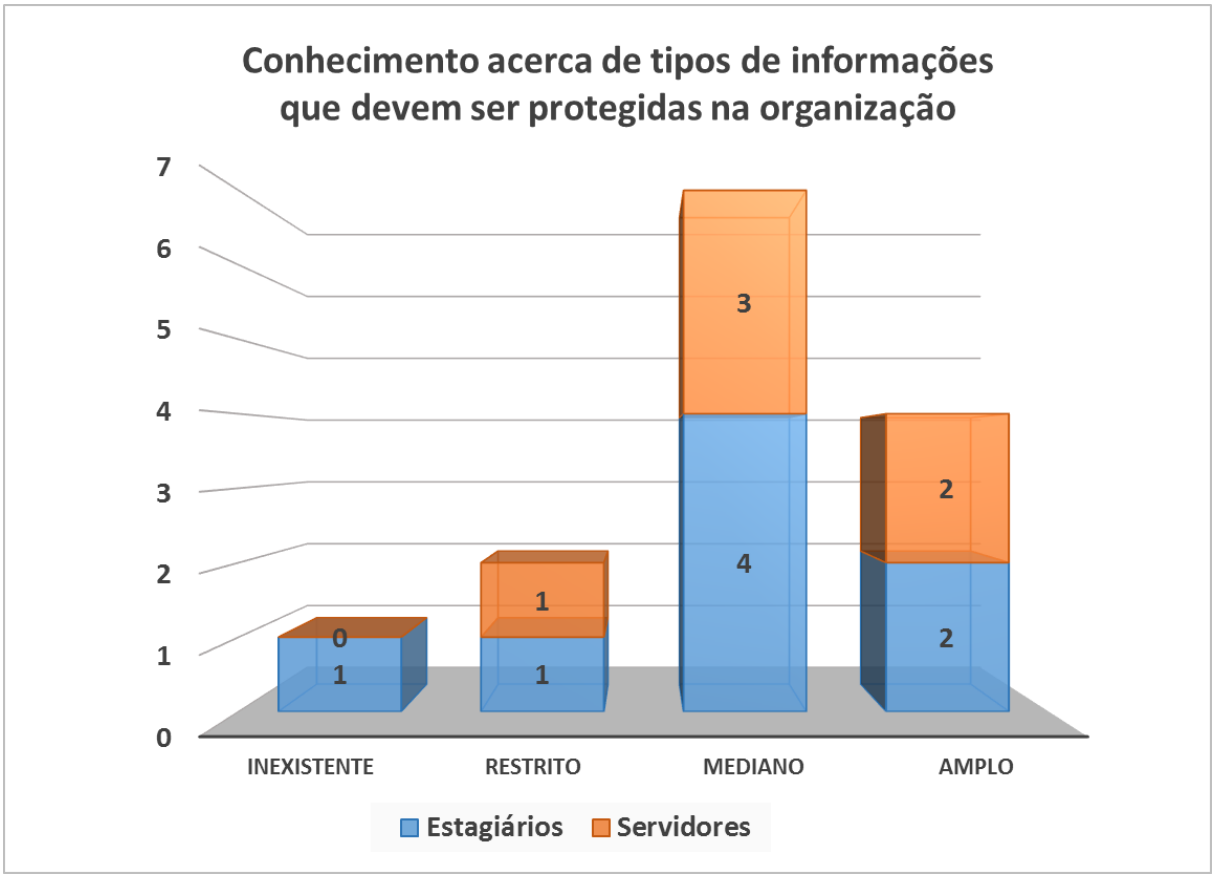

Figura 7 – Questão 7: Conhecimento acerca de tipos de informações que devem ser protegidas na organização

Os resultados revelam que quatro estagiários e três servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “mediano” no quesito conhecimento acerca de tipos de informações que devem ser protegidas na organização. O parâmetro “amplo” foi assinalado igualmente por dois estagiários e dois servidores. Os parâmetros “inexistente” e “restrito” foram escolhidos respectivamente por um e dois entrevistados. No primeiro, não houve indicação de resposta dos servidores. Verifica-se ainda no gráfico, proeminência dos totais acumulados de respostas nos parâmetros “mediano” e “amplo”, com aparente equilíbrio entre os totais de respostas de estagiários e servidores.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “mediano”, associando assim o indicador de segurança “medianamente seguro” ao quesito conhecimento acerca de ativos de informação organizacionais.

Figura 8 – Questão 8: Conhecimento acerca da realização de atividades de sensibilização em segurança da informação na organização

Os resultados mostram que seis estagiários e dois servidores, o equivalente a 57% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca da realização de atividades de sensibilização em segurança da informação na organização. Nos parâmetros restantes, quatro entrevistados assinalaram o parâmetro “restrito”, ao passo que um indicou a opção “mediano”, mesmo total obtido no parâmetro “amplo”. Não houve indicação dos estagiários ao parâmetro “mediano”, enquanto que o parâmetro “amplo” não foi apontado pelos servidores. Percebe-se que o total acumulado de respostas ao parâmetro “inexistente" é maior do que os totais de respostas aos demais parâmetros. As respostas dos estagiários se concentraram quase que totalmente neste parâmetro, enquanto as respostas dos servidores ficaram distribuídas entre os parâmetros “inexistente”, “restrito” e “mediano”, com destaque para o parâmetro “restrito”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca da realização de atividades de sensibilização em segurança da informação na organização.

4.2 Análise dos resultados relativos ao conhecimento acerca da segurança da informação no contexto organizacional

Entre os fenômenos que impactaram nos resultados do conjunto das questões aplicadas a respeito do conhecimento dos estagiários e servidores acerca da segurança da informação no contexto organizacional, verificou-se a definição do parâmetro “inexistente” como o mais significativo em cinco dos oito quesitos apresentados:

- Conhecimento acerca dos princípios da segurança da informação usados como referência na APF;
- Conhecimento acerca do documento da política de segurança da informação da organização;

- Conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às atividades no trabalho;
- Conhecimento acerca de ativos de informação organizacionais;
- Conhecimento acerca da realização de atividades de sensibilização em segurança da informação na organização.

A correspondência do parâmetro “inexistente” aos quesitos supracitados constituiu significativo conjunto de evidências de que em regra há baixo nível de conhecimento entre os estagiários e servidores entrevistados, no que diz respeito à segurança da informação no contexto da organização OXP.

No comparativo geral entre os grupos, verificou-se que os estagiários apresentaram níveis de conhecimento mais baixos do que os servidores, no que diz respeito ao rol de quesitos aplicados.

Entre as possíveis causas do baixo nível de conhecimento percebido se destacam a ausência de atividades de sensibilização e treinamento que tenham como foco o papel das pessoas no contexto da segurança da informação, além da inexistência de política de segurança da informação na organização investigada.

4.3 Conhecimento acerca da engenharia social

Buscou-se por meio dessa entrevista estruturada (ver Apêndice A) coletar dados suficientes para mensurar de forma segmentada conhecimentos de estagiários e servidores, que atuam no processo de atendimento ao público da organização OXP, acerca da engenharia social. Foram entrevistados oito estagiários e seis servidores.

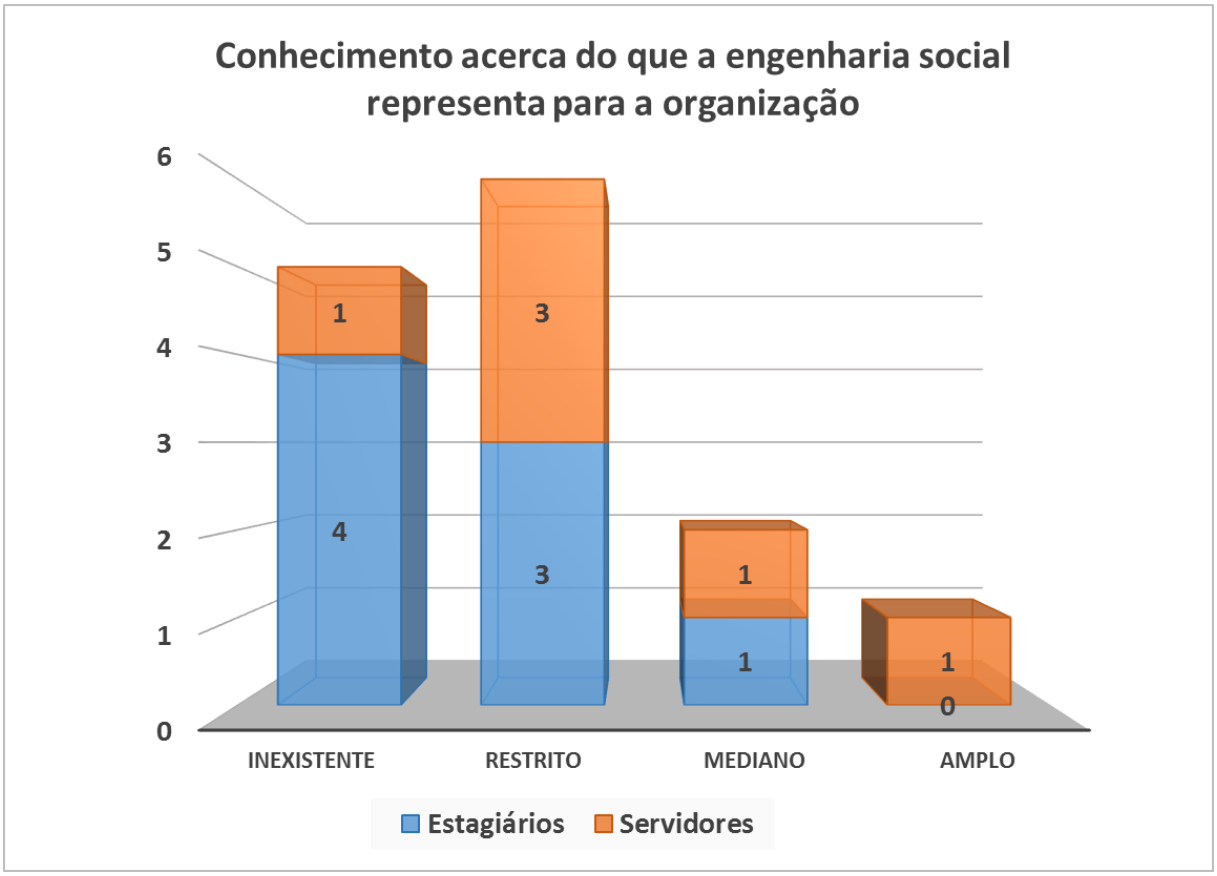

Figura 9 – Questão 1: Conhecimento acerca do que a engenharia social representa para a organização

Os resultados revelam que três estagiários e três servidores, o equivalente a 43% dos entrevistados, assinalaram o parâmetro “restrito” no quesito conhecimento acerca do que a engenharia social representa para a organização. O parâmetro “inexistente” foi assinalado por quatro estagiários e um servidor. Os parâmetros “mediano” e “amplo” foram assinalados respectivamente por dois e um entrevistados. Neste último, não houve indicação de resposta dos estagiários. Verifica-se, no gráfico, proeminência dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”. No primeiro, destaca-se o expressivo total de respostas dos estagiários, ao passo que no segundo há paridade entre os totais.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “restrito”, associando assim o indicador de segurança “vulnerável” ao quesito conhecimento acerca do que a engenharia social representa para a organização.

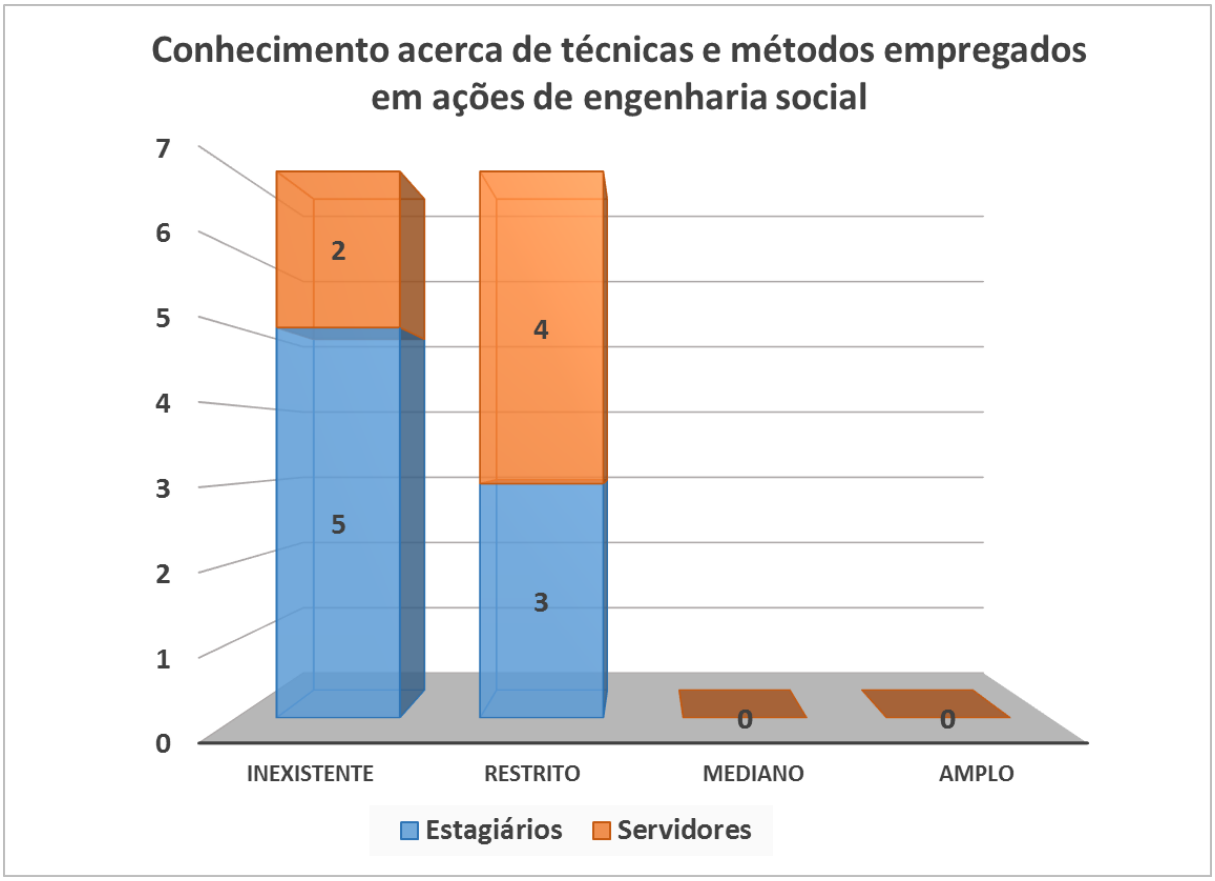

Figura 10 – Questão 2: Conhecimento acerca de técnicas e métodos empregados em ações de engenharia social

Os resultados do questionamento revelam que cinco estagiários e dois servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de técnicas e métodos empregados em ações de engenharia social. O parâmetro “restrito” foi assinalado por três estagiários e quatro servidores, cujo resultado também correspondeu a 50%. Fica patente no gráfico a proeminência dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”. A despeito do equilíbrio absoluto verificado entre os totais acumulados dos referidos parâmetros, verificam-se divergências relevantes nas respostas de estagiários e servidores, haja vista a prevalência das respostas dos estagiários ao parâmetro “inexistente” e o predomínio das respostas dos servidores ao parâmetro “restrito”. Percebe-se ainda que não houve indicações aos parâmetros “mediano” e “amplo”.

A equidade entre os maiores valores resultantes da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu os parâmetros “inexistente” e “restrito” como os mais significativos. À vista disso, conforme critério

de tabulação (Item 3.4), associou-se o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de técnicas e métodos empregados em ações de engenharia social.

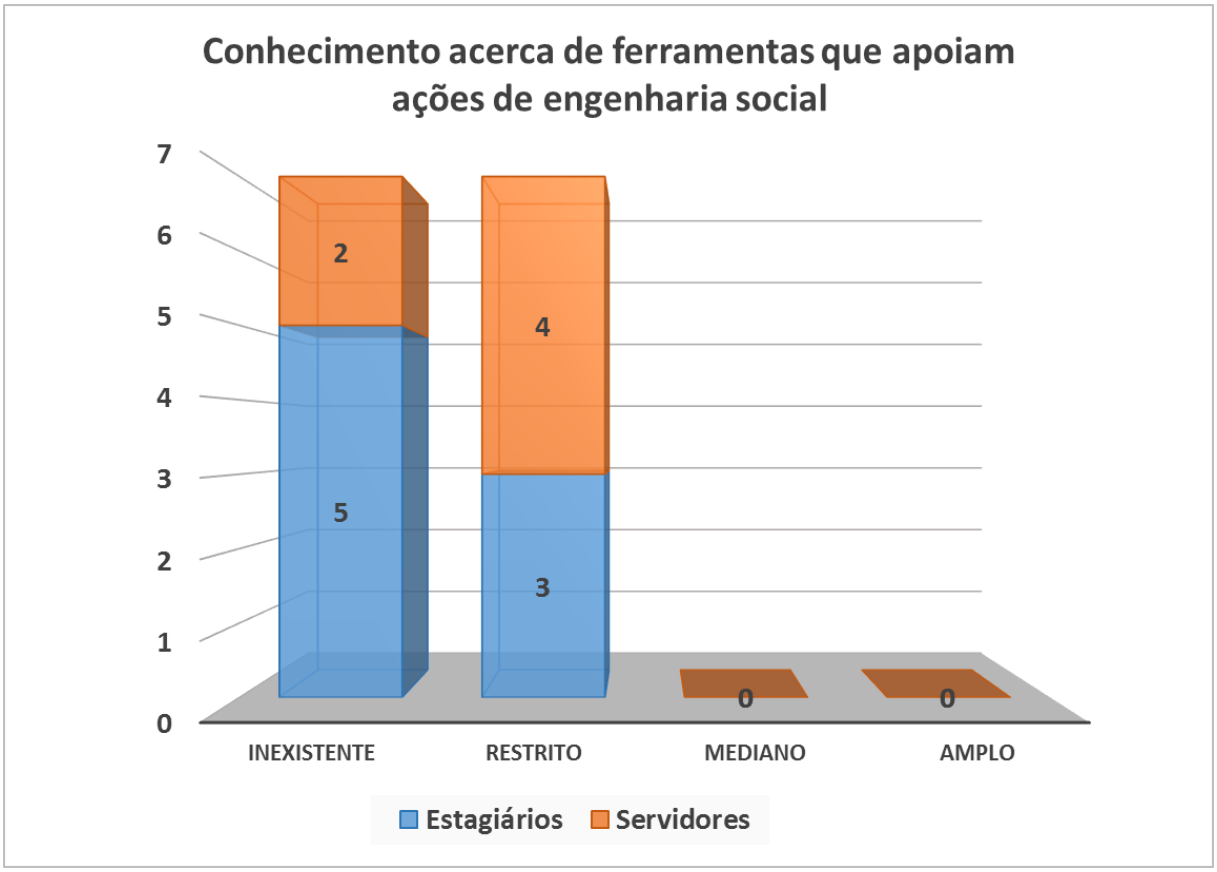

Figura 11 – Questão 3: Conhecimento acerca de ferramentas que apoiam ações de engenharia social

De forma idêntica ao quesito anterior, os resultados revelam que cinco estagiários e dois servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de ferramentas que apoiam ações de engenharia social. O parâmetro “restrito” foi assinalado por três estagiários e quatro servidores, cujo resultado também correspondeu a 50%. No gráfico, destacam-se os totais acumulados de respostas nos parâmetros “inexistente” e “restrito”. Em que pese o equilíbrio verificado entre os referidos parâmetros, verificam-se divergências significativas nas respostas de estagiários e servidores, tendo em vista a prevalência das respostas dos estagiários ao parâmetro “inexistente” e o predomínio das respostas dos servidores ao parâmetro “restrito”. Percebe-se ainda que não houve indicações aos parâmetros “mediano” e “amplo”.

A paridade entre os maiores valores resultantes da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu os parâmetros “inexistente” e “restrito” como os mais significativos. À vista disso, conforme critério de tabulação (Item 3.4), associou-se o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de ferramentas que apoiam ações de engenharia social.

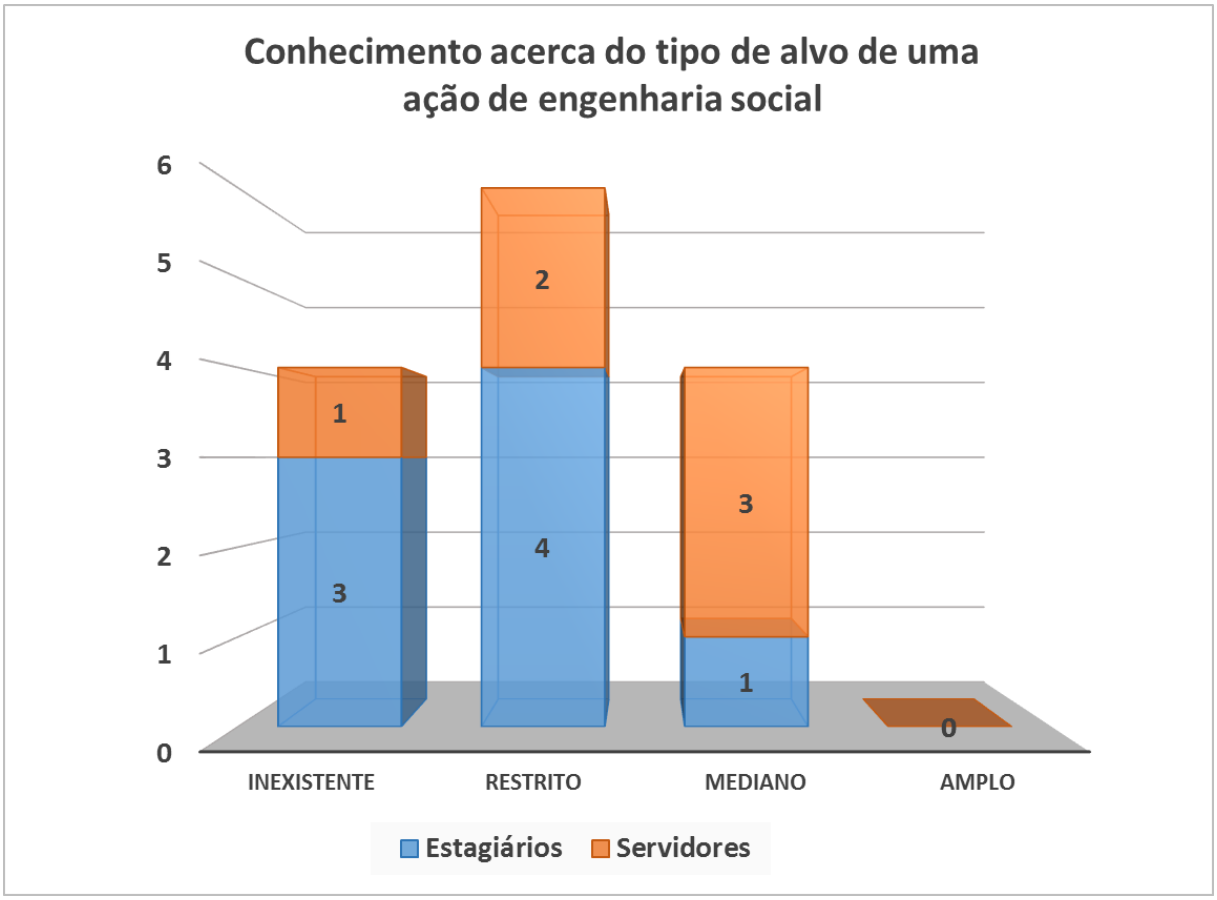

Figura 12 – Questão 4: Conhecimento acerca do tipo de alvo de uma ação de engenharia social

Os resultados do questionamento revelam que quatro estagiários e dois servidores, o equivalente a 43% dos entrevistados, assinalaram o parâmetro “restrito” no quesito conhecimento acerca do tipo de alvo de uma ação de engenharia social. Não houve indicação ao parâmetro “amplo”. Nota-se o predomínio do total acumulado de respostas no parâmetro “restrito”, como também o equilíbrio entre os totais acumulados nos parâmetros “inexistente” e “mediano”. Enquanto os totais de respostas dos estagiários foram significativamente maiores

nos parâmetros “inexistente” e “restrito”, predominaram as respostas dos servidores no parâmetro “mediano”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “restrito”, associando assim o indicador de segurança “vulnerável” ao quesito conhecimento acerca do tipo de alvo de uma ação de engenharia social.

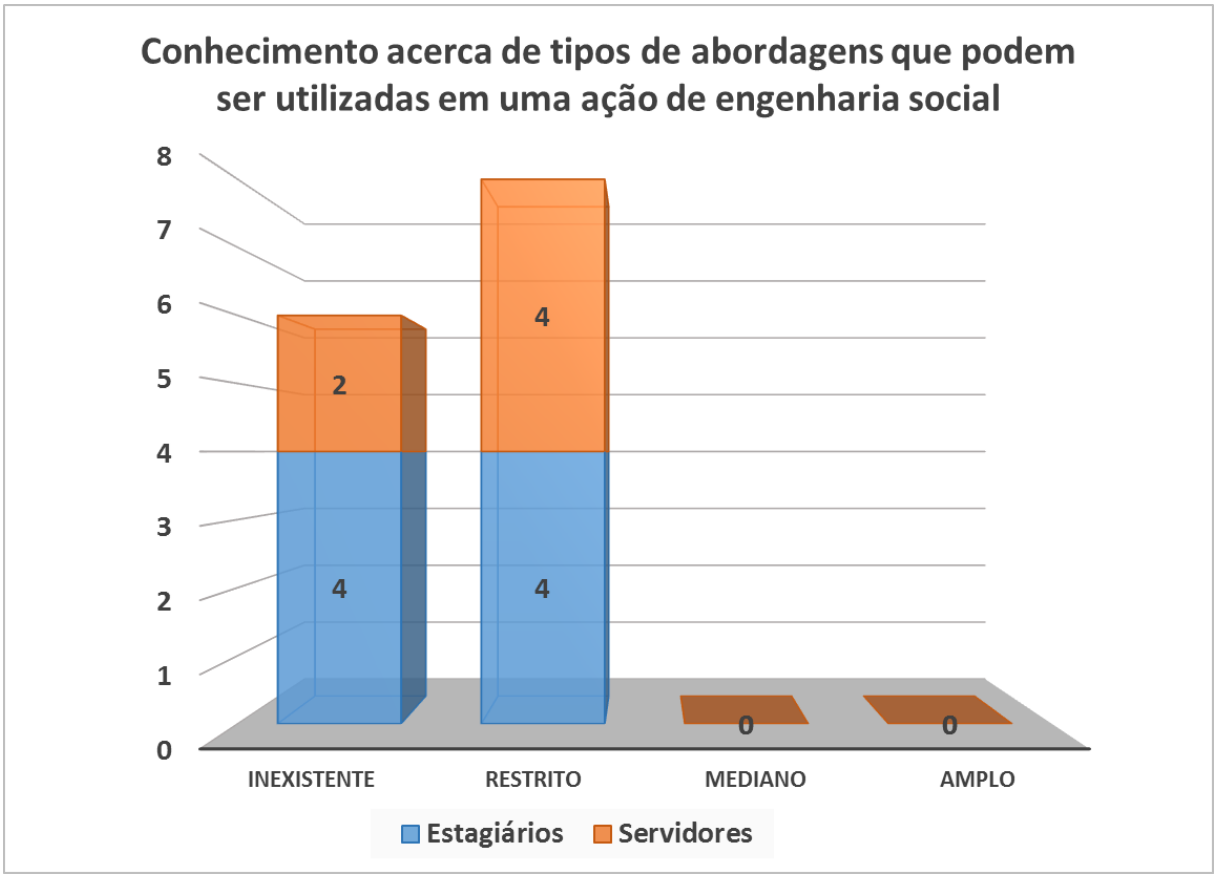

Figura 13 – Questão 5: Conhecimento acerca de tipos de abordagens que podem ser utilizadas em uma ação de engenharia social

Os resultados revelam que quatro estagiários e quatro servidores, o equivalente a 57% dos entrevistados, assinalaram o parâmetro “restrito” no quesito conhecimento acerca de tipos de abordagens que podem ser utilizadas em uma ação de engenharia social. O parâmetro “inexistente” foi assinalado por quatro estagiários e dois servidores. Os parâmetros “mediano” e “amplo” não foram assinalados. Observa-se, no gráfico, proeminência dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”. Ressalta-se o expressivo total de

respostas dos servidores no parâmetro “restrito” e o equilíbrio das respostas dos estagiários, no que concerne aos parâmetros “inexistente” e “restrito”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “restrito”, associando assim o indicador de segurança “vulnerável” ao quesito conhecimento acerca de tipos de abordagens que podem ser utilizadas em uma ação de engenharia social.

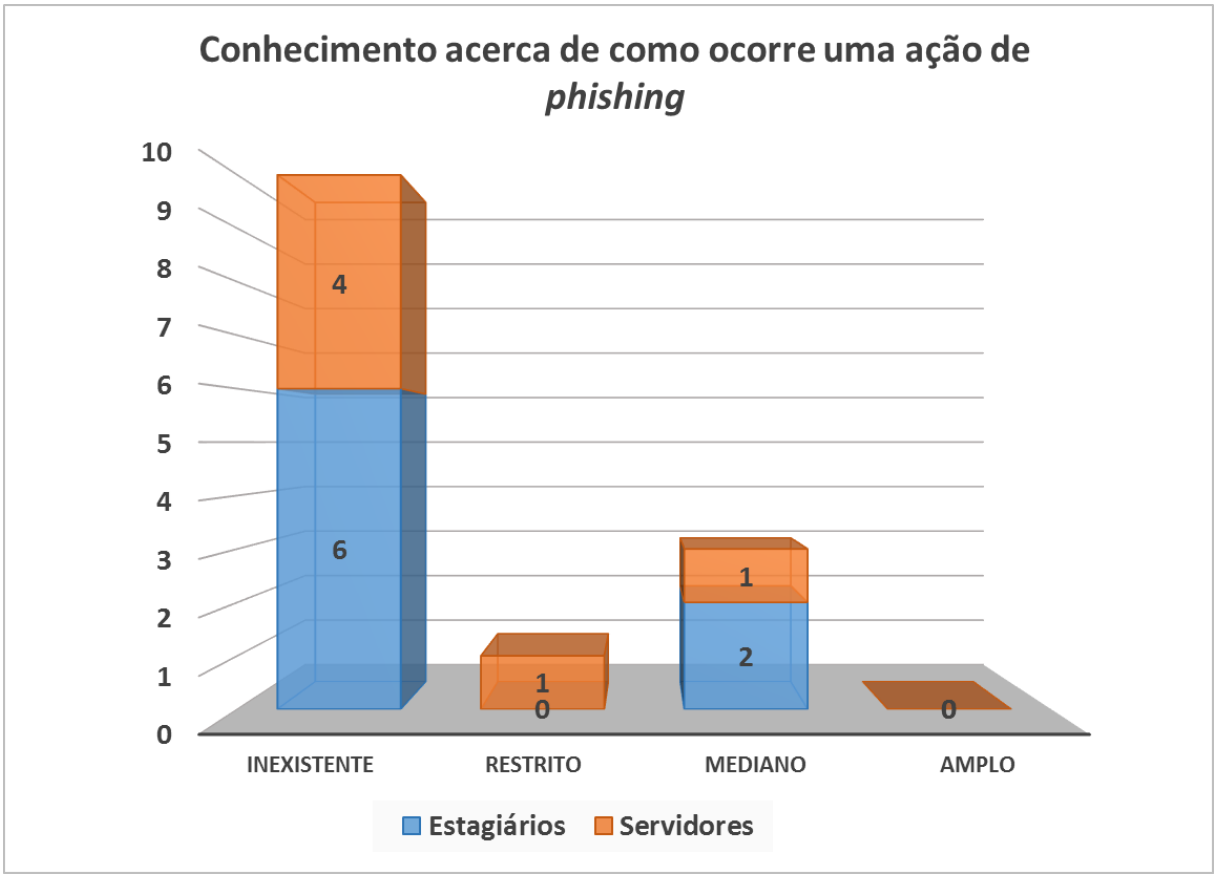

Figura 14 – Questão 6: Conhecimento acerca de como ocorre uma ação de *phishing*

Os resultados mostram que seis estagiários e quatro servidores, o equivalente a 71% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de como ocorre uma ação de *phishing*. Nos parâmetros restantes, a opção “restrito” foi apontada por um entrevistado, ao passo que a opção “mediano” foi assinalada por três. Não houve indicações de respostas ao parâmetro “amplo”. Na ilustração, verifica-se que o total acumulado de respostas ao parâmetro “inexistente” é significativamente maior do que os totais de respostas aos demais

parâmetros. As respostas, tanto dos estagiários como dos servidores, foram expressivamente direcionadas a esse parâmetro.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de como ocorre uma ação de *phishing*.

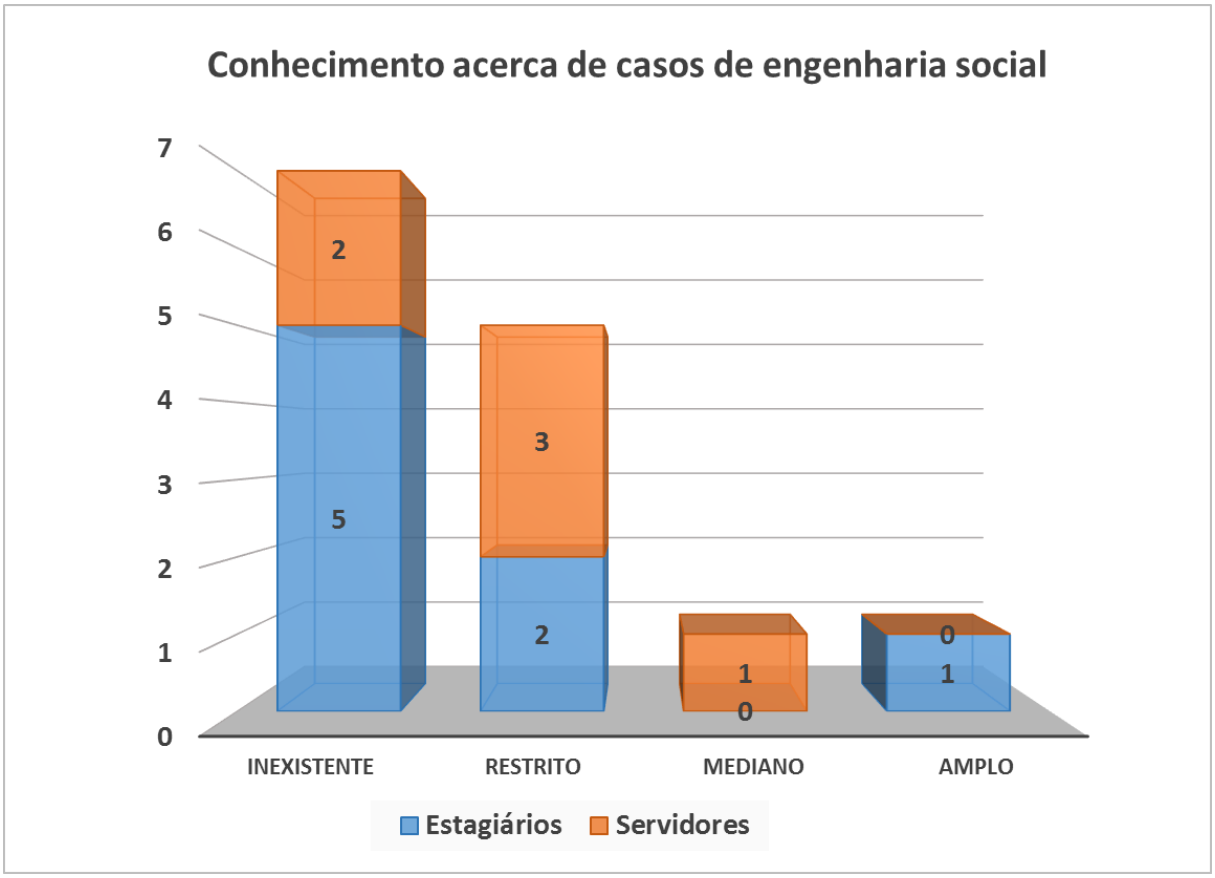

Figura 15 – Questão 7: Conhecimento acerca de casos de engenharia social

Os resultados do questionamento revelam que cinco estagiários e dois servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de casos de engenharia social. Nos parâmetros restantes, cinco entrevistados apontaram o parâmetro “restrito”, um assinalou a opção “mediano”, e também um indicou o parâmetro "amplo". Percebe-se a relevância dos totais acumulados de respostas nos parâmetros “inexistente” e “restrito”, diferentemente dos baixos totais atribuídos aos parâmetros “mediano” e “amplo”. Evidenciam-se também contrastes nas respostas de estagiários e

servidores, tanto na comparação entre os parâmetros “inexistente” e “restrito” como entre “mediano” e “amplo”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de casos de engenharia social.

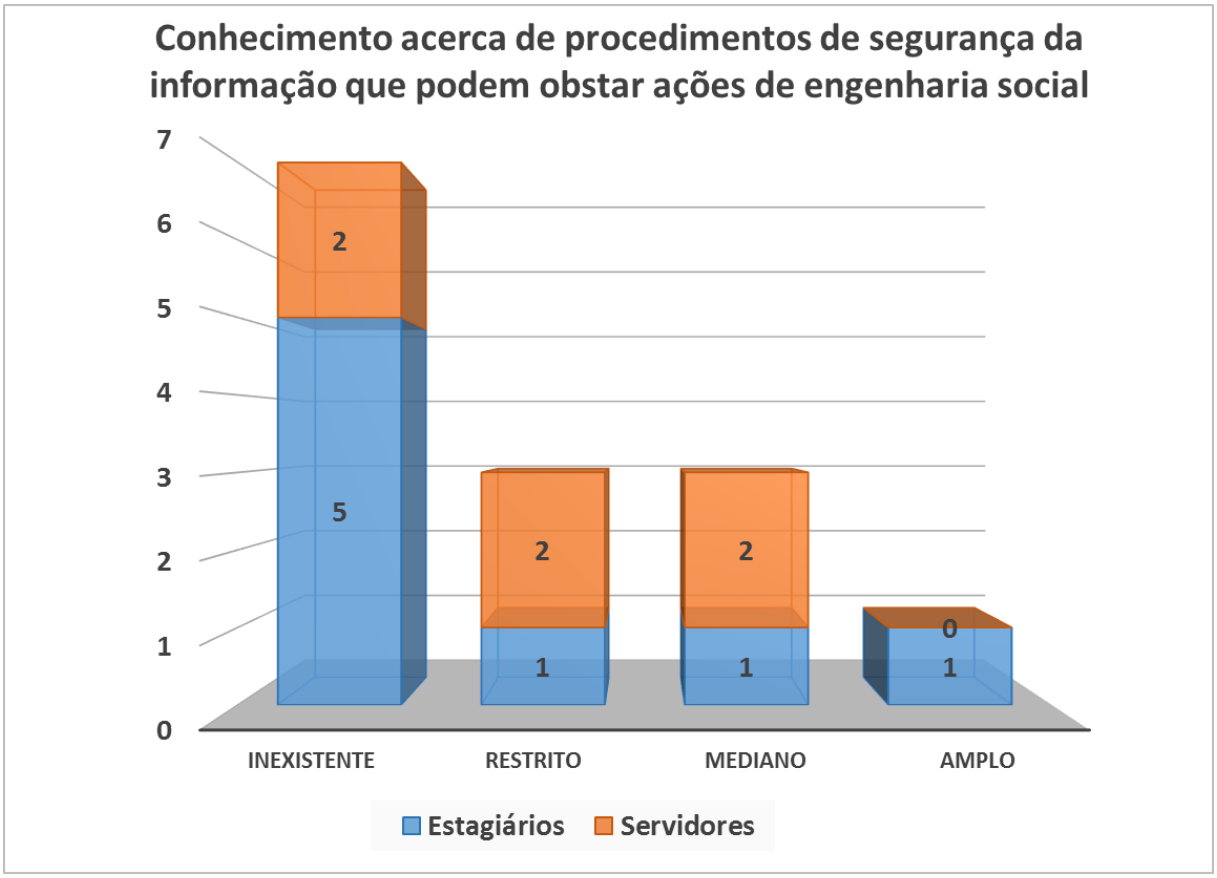

Figura 16 – Questão 8: Conhecimento acerca de procedimentos de segurança da informação que podem obstar ações de engenharia social

Os resultados do questionamento revelam que cinco estagiários e dois servidores, o equivalente a 50% dos entrevistados, assinalaram o parâmetro “inexistente” no quesito conhecimento acerca de procedimentos de segurança da informação que podem obstar ações de engenharia social. Nos parâmetros restantes, dois servidores e um estagiário indicaram tanto a opção “restrito” como a “mediano”, ao passo que somente um estagiário indicou o parâmetro “amplo”. Percebe-se prevalência dos totais acumulados de respostas no parâmetro

“inexistente”, além da distribuição igualitária das respostas dos servidores nos parâmetros “inexistente”, “restrito” e “mediano”, e dos estagiários nos parâmetros “restrito”, “mediano” e “amplo”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “inexistente”, associando assim o indicador de segurança “muito vulnerável” ao quesito conhecimento acerca de procedimentos de segurança da informação que podem obstar ações de engenharia social.

4.4 Análise dos resultados relativos ao conhecimento acerca da engenharia social

Entre os fenômenos que impactaram nos resultados do conjunto das questões aplicadas a respeito do conhecimento dos estagiários e servidores acerca da engenharia social, verificou-se a definição do parâmetro “inexistente” como o mais significativo em cinco dos oito quesitos apresentados:

- Conhecimento acerca de técnicas e métodos empregados em ações de engenharia social;
- Conhecimento acerca de ferramentas que apoiam ações de engenharia social;
- Conhecimento acerca de como ocorre uma ação de *phishing*;
- Conhecimento acerca de casos de engenharia social;
- Conhecimento acerca de procedimentos de segurança da informação que podem obstar ações de engenharia social.

A correspondência do parâmetro “inexistente” aos quesitos supracitados constituiu significativo conjunto de evidências de que em regra há baixo nível de conhecimento entre os estagiários e servidores entrevistados acerca da engenharia social.

No comparativo geral entre os grupos, verificou-se que os estagiários apresentaram níveis de conhecimento mais baixos do que os servidores, no que diz respeito ao rol de quesitos aplicados.

Entre as possíveis causas dos baixos níveis de conhecimento percebidos se destacam a ausência de atividades de sensibilização que promovam entendimento acerca da ameaça que a engenharia social representa para a organização, e que exponham de forma detalhada como vulnerabilidades humanas podem ser exploradas em ataques de engenharia social.

4.5 Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação

Buscou-se por meio dessa entrevista estruturada (ver Apêndice A) coletar dados que permitissem mensurar de forma segmentada a periodicidade de realização de procedimentos de segurança da informação, relacionados ao manuseio de ativos de informação, por parte de estagiários e servidores que atuam no processo de atendimento ao público da organização OXP. Foram entrevistados oito estagiários e seis servidores.

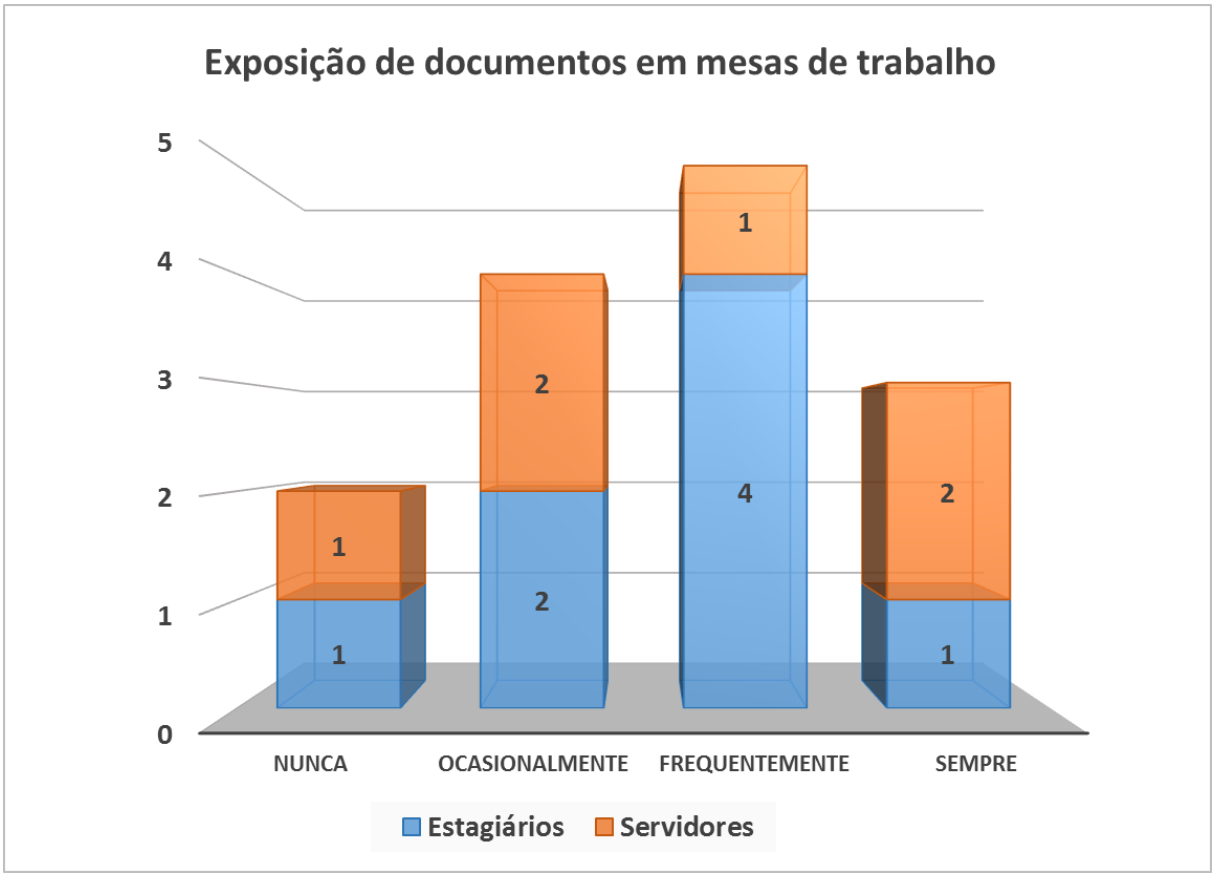

Figura 17 – Questão 1: Exposição de documentos em mesas de trabalho

Os resultados revelam que quatro estagiários e um servidor, o equivalente a 36% dos entrevistados, apontaram o parâmetro “frequentemente” em relação ao quesito exposição de documentos em mesas de trabalho. O parâmetro “ocasionalmente” foi assinalado por dois estagiários e pelo mesmo número de servidores. Por sua vez, os parâmetros opostos “nunca” e “sempre” foram escolhidos por dois e três entrevistados, respectivamente. No gráfico, destacam-se os totais acumulados de respostas nos parâmetros “frequentemente” e “ocasionalmente”. Observa-se também equilíbrio dos totais acumulados nos parâmetros “nunca” e “ocasionalmente”, bem como antagonismo nas respostas de estagiários e servidores aos parâmetros “frequentemente” e “sempre”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “frequentemente”, associando assim o indicador de segurança “vulnerável” ao quesito exposição de documentos em mesas de trabalho.

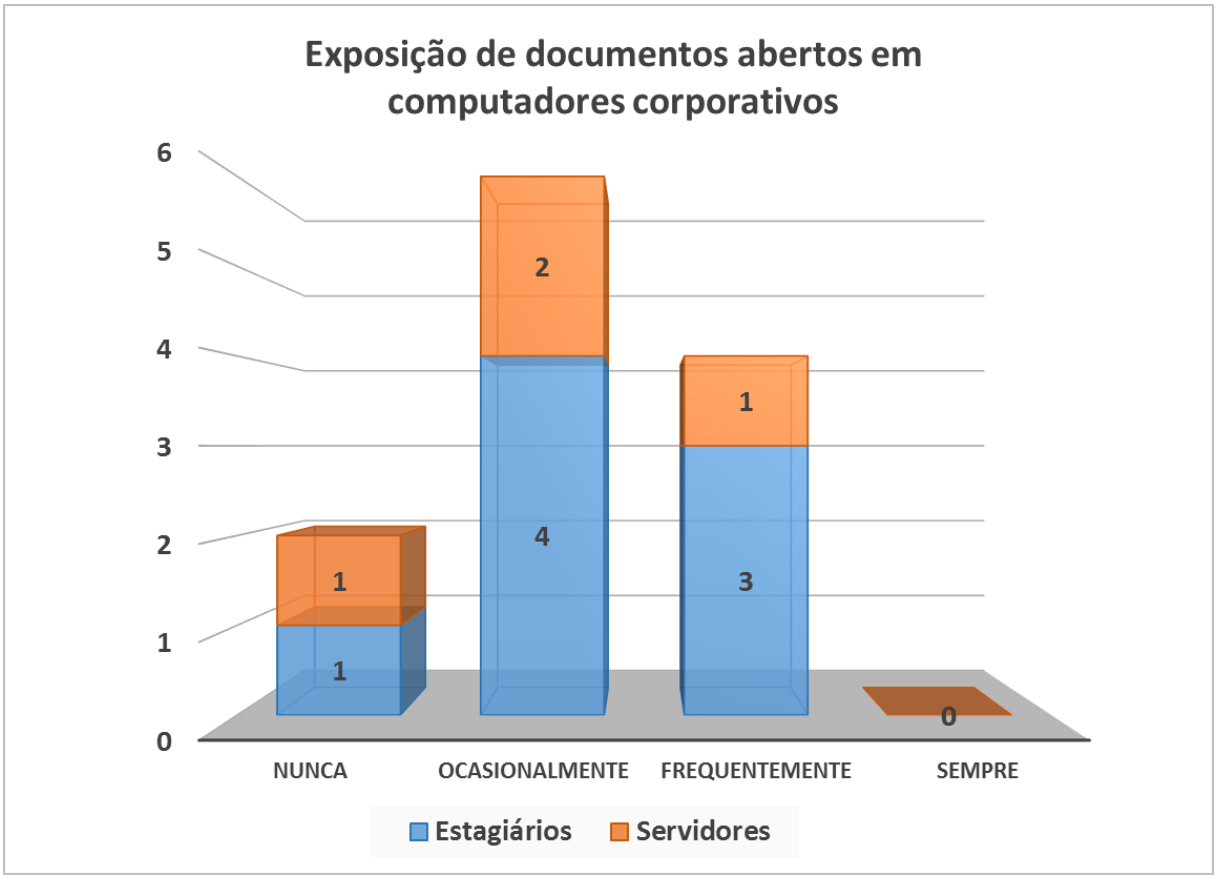

Figura 18 – Questão 2: Exposição de documentos abertos em computadores corporativos

Os resultados mostram que quatro estagiários e dois servidores, o equivalente a 43% dos entrevistados, apontaram o parâmetro “ocasionalmente” em relação ao quesito exposição de documentos abertos em computadores corporativos. O parâmetro “frequentemente” foi assinalado por três estagiários e um servidor. O parâmetro “nunca” foi assinalado por dois entrevistados, ao passo que não houve indicações ao parâmetro “sempre”. Observa-se, no gráfico, proeminência dos totais acumulados de respostas nos parâmetros “ocasionalmente" e "frequentemente”. Nesses parâmetros, houve predomínio dos totais de respostas dos estagiários. Cabe registrar que o baixo total geral de respostas dos servidores se deveu à ausência das respostas de dois servidores no presente quesito.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “ocasionalmente”, associando assim o indicador de segurança “medianamente seguro” ao quesito exposição de documentos abertos em computadores corporativos.

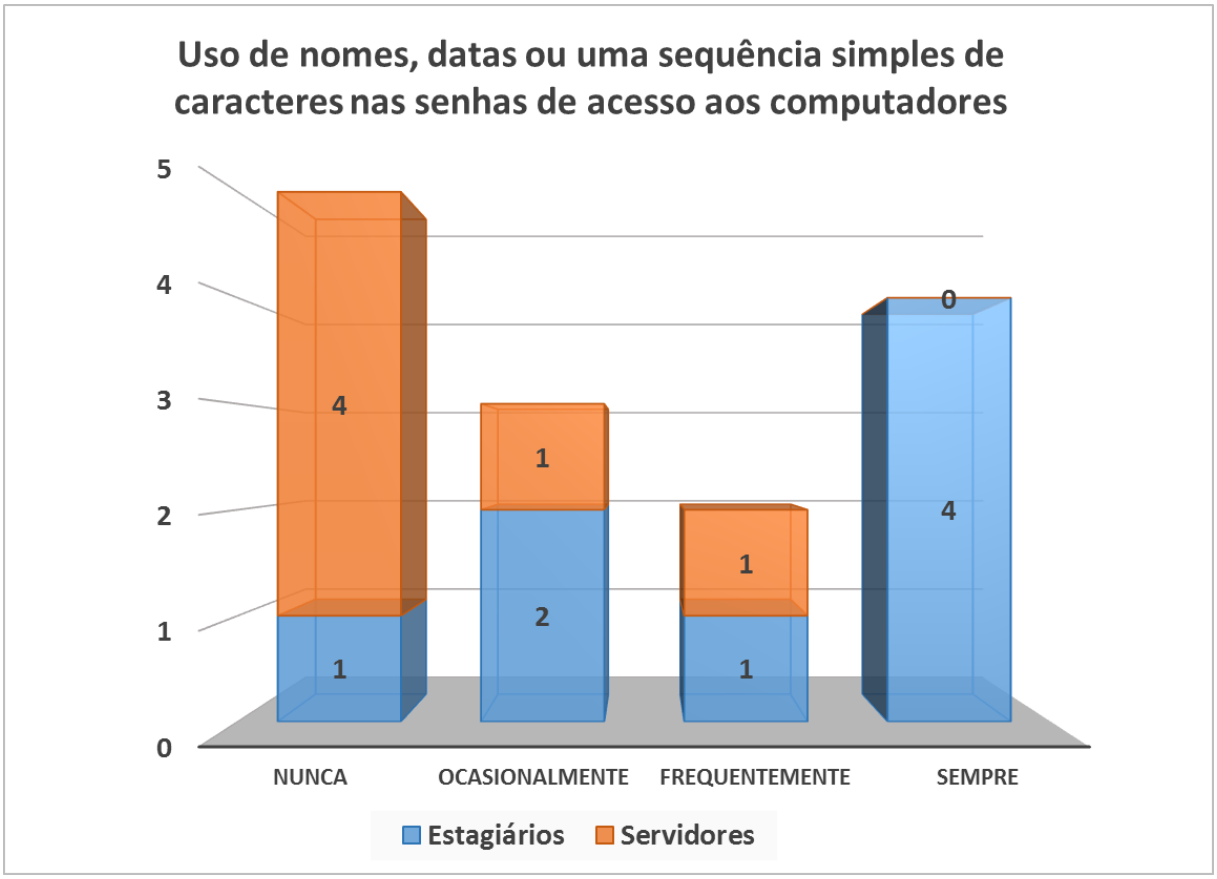

Figura 19 – Questão 3: Uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores

Os resultados obtidos revelam que quatro servidores e um estagiário, o equivalente a 36% dos entrevistados, apontaram o parâmetro “nunca” em relação ao quesito uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores corporativos. O parâmetro “sempre” foi assinalado somente por quatro estagiários. Por seu turno, os parâmetros “ocasionalmente” e “frequentemente” foram escolhidos por três e dois entrevistados, respectivamente. O gráfico destaca os expressivos totais acumulados de respostas nos parâmetros opostos “nunca” e “sempre”. A comparação entre esses parâmetros torna saliente o contraste entre os totais de respostas, que tiveram predomínio dos servidores no parâmetro “nunca”, e dos estagiários no parâmetro “sempre”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “nunca”, associando assim o indicador de segurança “seguro” ao quesito uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores corporativos.

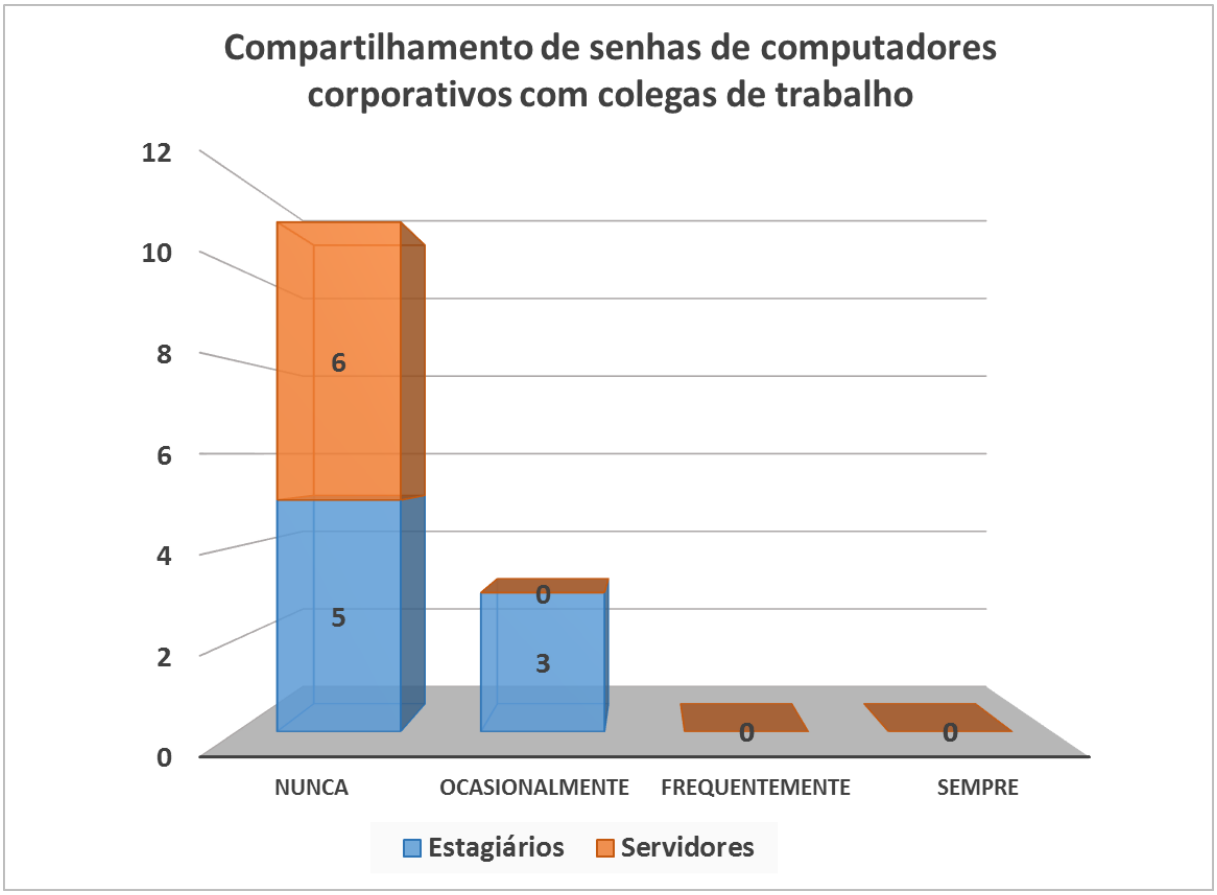

Figura 20 – Questão 4: Compartilhamento de senhas de computadores corporativos com colegas de trabalho

Os resultados obtidos revelam que cinco estagiários e seis servidores, o equivalente a 79% dos entrevistados, apontaram o parâmetro “nunca” em relação ao quesito compartilhamento de senhas de computadores corporativos com colegas de trabalho. O parâmetro “ocasionalmente” foi assinalado somente por três estagiários. Não houve indicações aos parâmetros “frequentemente” e “sempre”. Nota-se que o total acumulado de respostas ao parâmetro “nunca” é significativamente maior do que os totais de respostas aos demais parâmetros. Percebe-se também situação de equilíbrio entre as repostas de estagiários e servidores no parâmetro “nunca” e a ausência de respostas dos servidores nos demais parâmetros.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “nunca”, associando assim o indicador de segurança “seguro” ao quesito compartilhamento de senhas de computadores corporativos com colegas de trabalho.

As questões 5 e 6 foram alocadas para o Item 4.7 - Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação (navegação e troca de informações).

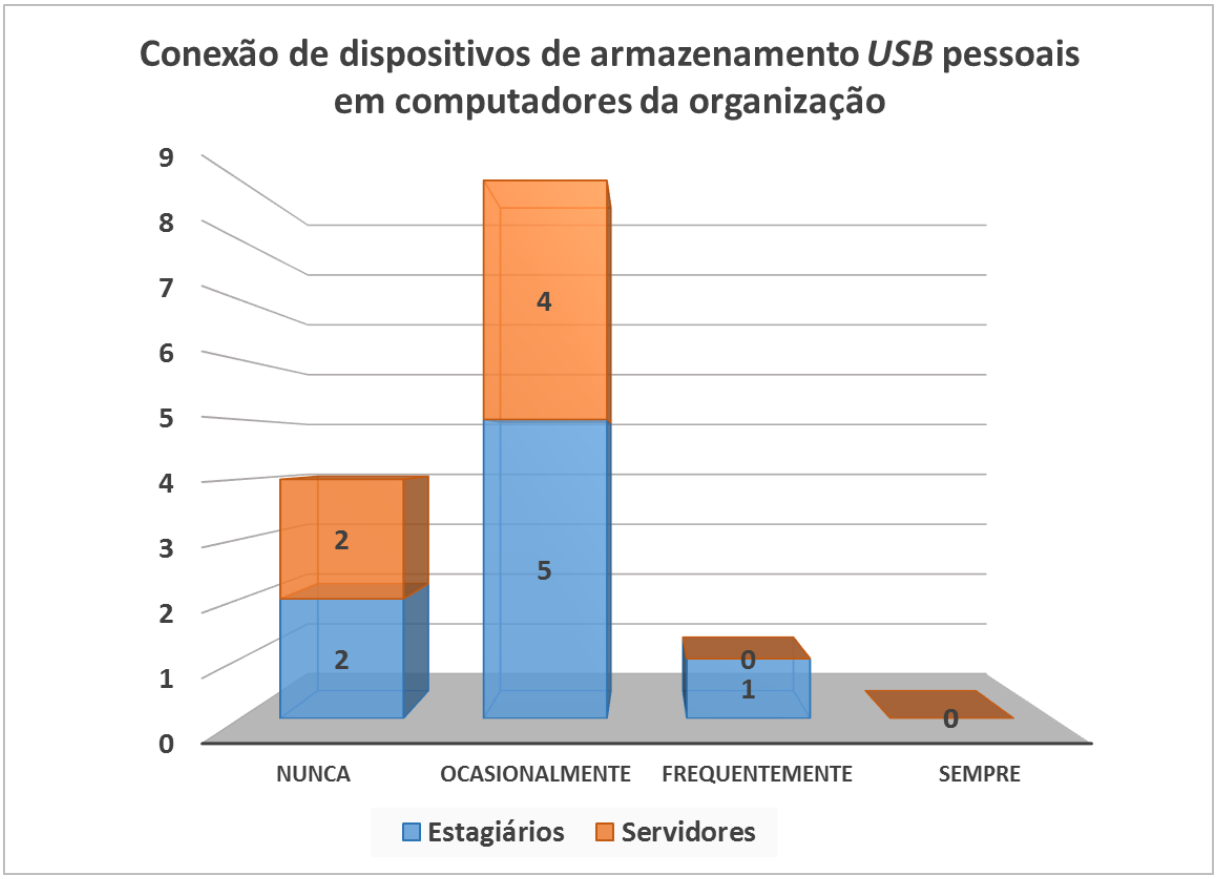

Figura 21 – Questão 7: Conexão de dispositivos de armazenamento USB pessoais em computadores da organização

Os resultados evidenciam que cinco estagiários e quatro servidores, o equivalente a 64% dos entrevistados, apontaram o parâmetro “ocasionalmente” em relação ao quesito conexão de dispositivos de armazenamento USB pessoais em computadores da organização. O parâmetro “nunca” foi assinalado por dois estagiários e o mesmo número de servidores. O parâmetro “frequentemente” foi assinalado por um estagiário, ao passo que não foi indicado por nenhum servidor. Não houve respostas ao parâmetro “sempre”. Observa-se, no gráfico, proeminência do total acumulado de respostas no parâmetro “ocasionalmente”, como também equilíbrio entre as respostas de estagiários e servidores neste parâmetro. O parâmetro “nunca” também apresentou cenário de equilíbrio.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “ocasionalmente”, associando assim o indicador de segurança “medianamente seguro” ao quesito conexão de dispositivos de armazenamento USB pessoais em computadores da organização.

A questão 8 foi anulada, pelo fato de ter repetido, no questionário aplicado, a pergunta constante na questão 7.

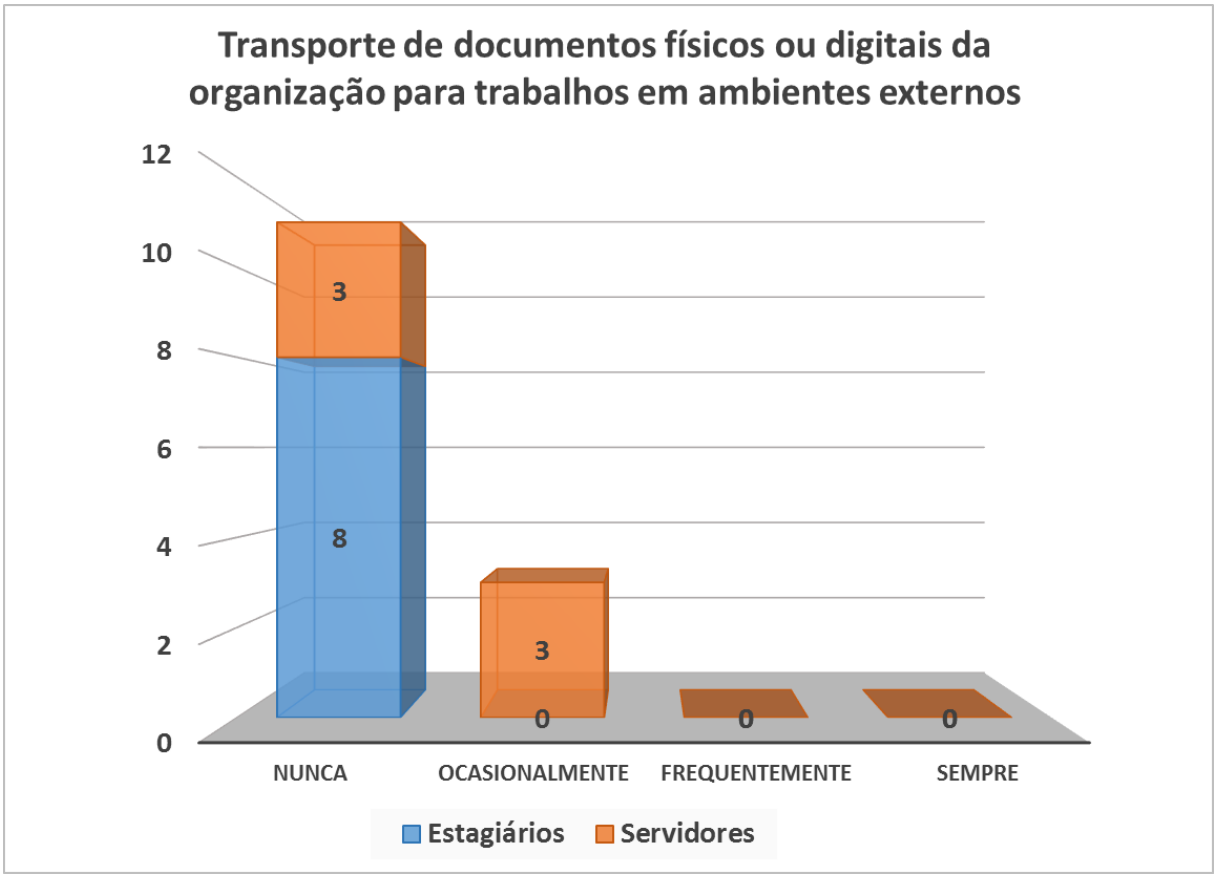

Figura 22 – Questão 9: Transporte de documentos físicos ou digitais da organização para trabalhos em ambientes externos

Os resultados indicam que 8 estagiários e três servidores, o equivalente a 79% dos entrevistados, apontaram o parâmetro “nunca” em relação ao quesito transporte de documentos físicos ou digitais da organização para trabalhos em ambientes externos. O parâmetro “ocasionalmente” foi assinalado por três servidores. Não houve indicações aos parâmetros “frequentemente” e “sempre”. Nota-se que o total acumulado de respostas ao parâmetro “nunca”, no qual

predominaram as respostas dos estagiários, é significativamente maior do que os índices de respostas aos demais parâmetros. Por outro lado, no parâmetro “ocasionalmente” as respostas dos servidores prevaleceram de forma absoluta.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “nunca”, associando assim o indicador de segurança “seguro” ao quesito transporte de documentos físicos ou digitais da organização para trabalhos em ambientes externos.

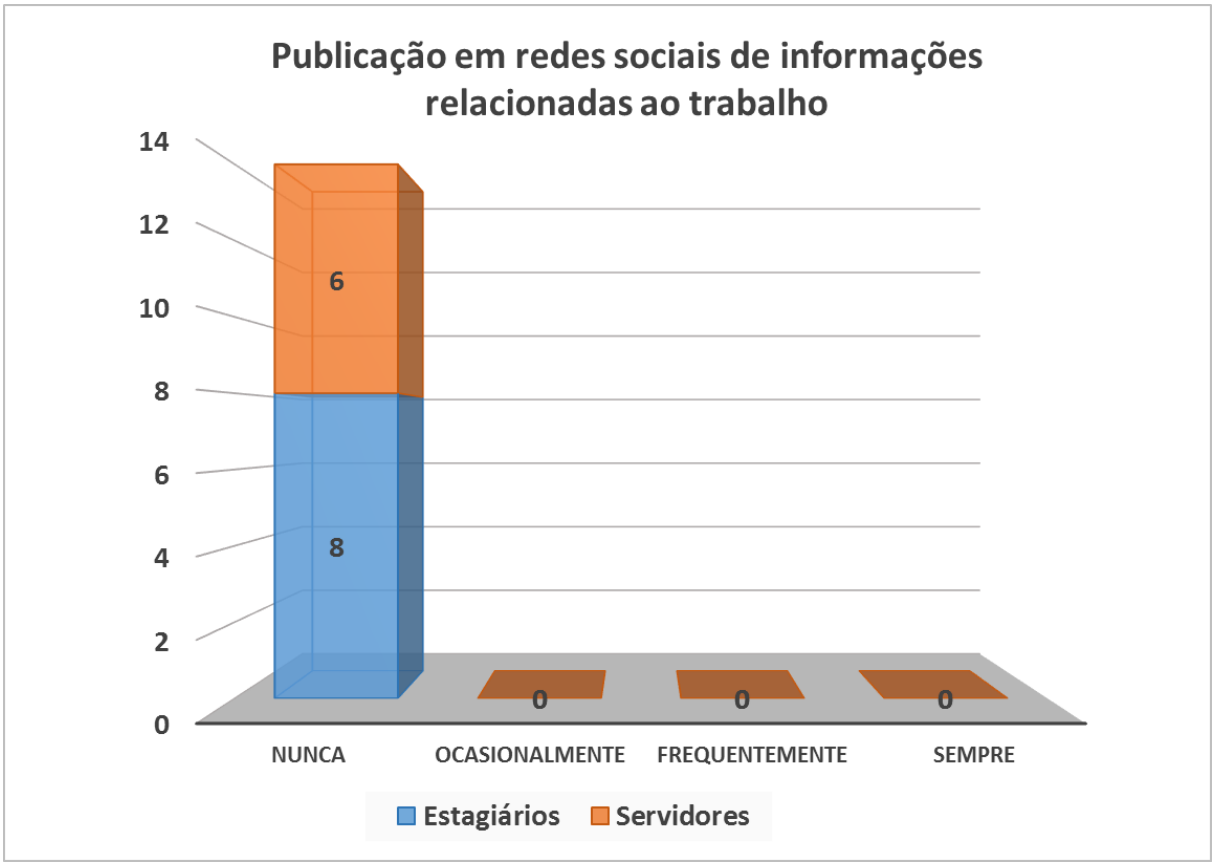

Figura 23 – Questão 10: Publicação em redes sociais de informações relacionadas ao trabalho

Os resultados obtidos mostram que oito estagiários e seis servidores, o equivalente a 100% dos entrevistados, apontaram o parâmetro “nunca” em relação ao quesito publicação, em redes sociais, de informações relacionadas ao trabalho. Não houve indicações dos entrevistados aos parâmetros restantes. Verifica-se no gráfico predomínio absoluto do total acumulado de respostas ao parâmetro “nunca”, no qual prevaleceram as respostas dos estagiários em relação às dos servidores.

Cabe observar que essa diferença no total ocorreu em razão da desigualdade numérica dos grupos envolvidos, uma vez que foram entrevistados oito estagiários e seis servidores.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “nunca”, associando assim o indicador de segurança “seguro” ao quesito publicação, em redes sociais, de informações relacionadas ao trabalho.

4.6 Análise dos resultados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação

Entre os fenômenos que impactaram nos resultados do conjunto das questões aplicadas a respeito da periodicidade de realização de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação por parte de estagiários e servidores que atuam no processo de atendimento ao público da organização OXP, verificou-se a definição do parâmetro “nunca” como o mais significativo em quatro dos sete quesitos apresentados:

- Uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores;
- Compartilhamento de senhas de computadores corporativos com colegas de trabalho;
- Transporte de documentos físicos ou digitais da organização para trabalhos em ambientes externos;
- Publicação em redes sociais de informações relacionadas ao trabalho.

A correspondência do parâmetro “nunca” aos quesitos supracitados constituiu conjunto de evidências de que os estagiários e servidores entrevistados executam de maneira segura esses procedimentos relacionados ao manuseio de ativos de informação corporativos. No entanto, verificaram-se nos quesitos restantes duas correspondências ao parâmetro “ocasionalmente” e uma ao parâmetro “frequentemente”, situações que indicam realização rotineira de procedimentos inseguros voltados ao manuseio de ativos.

No comparativo geral entre os grupos, constatou-se que os estagiários apresentaram maior incidência do que os servidores na execução de procedimentos inseguros, no que diz respeito ao rol de quesitos aplicados.

Entre as possíveis causas da realização dos procedimentos inseguros percebidos se destacam a ausência de procedimentos padronizados e documentados de segurança da informação baseados nas melhores práticas, além da inexistência de política de segurança da informação na organização investigada.

4.7 Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação (navegação e troca de informações)

Conforme explicado no Item 3.4, em razão de erros na formulação das questões 5 e 6, a respeito de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação organizacionais, houve a necessidade de se modificar a ordem de sequência dos parâmetros, para fins de análise dessas questões. Assim, decidiu-se exibir seus resultados em separado.

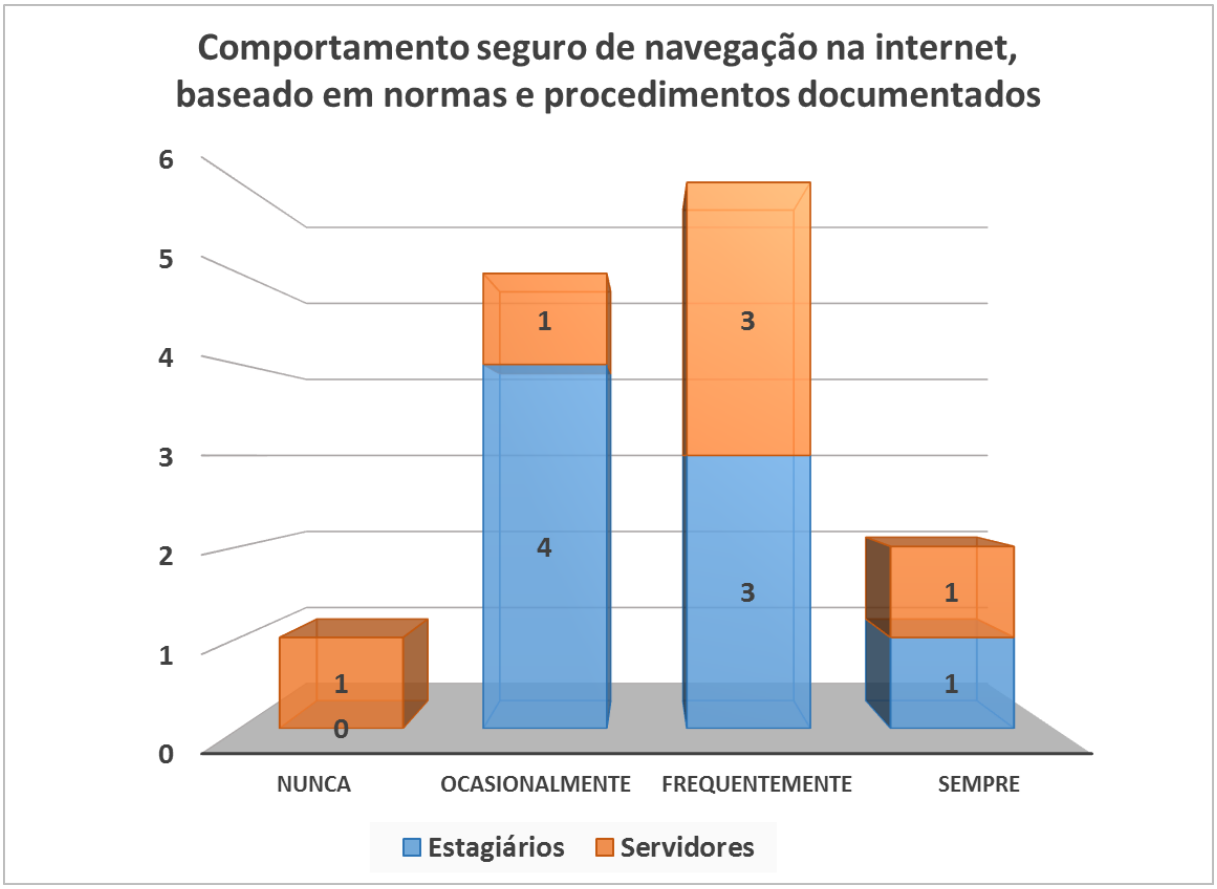

Figura 24 – Questão 5: Comportamento seguro de navegação na internet, baseado em normas e procedimentos documentados

Os resultados revelam que três estagiários e três servidores, o equivalente a 43% dos entrevistados, apontaram o parâmetro “frequentemente” em relação ao quesito comportamento seguro de navegação na internet, baseado em normas e procedimentos documentados contendo regras para navegação segura. O parâmetro “ocasionalmente” foi assinalado por quatro estagiários e por somente um servidor. Por conseguinte, os parâmetros opostos “nunca” e “sempre” foram escolhidos por um e dois entrevistados, respectivamente. Percebe-se, no gráfico, proeminência dos totais acumulados de respostas nos parâmetros “frequentemente” e “ocasionalmente”. Observa-se, ainda, paridade nos totais de respostas aos parâmetros “frequentemente” e “sempre”, como também prevalência do total de respostas dos estagiários no parâmetro “ocasionalmente”.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “frequentemente”, associando assim o indicador de segurança “medianamente

seguro” ao quesito comportamento seguro de navegação na internet, baseado em normas e procedimentos documentados contendo regras para navegação segura. É oportuno frisar que a ordem de sequência dos parâmetros foi modificada para essa questão, conforme critérios estabelecidos para tabulação e apresentação dos dados (Item 3.4).

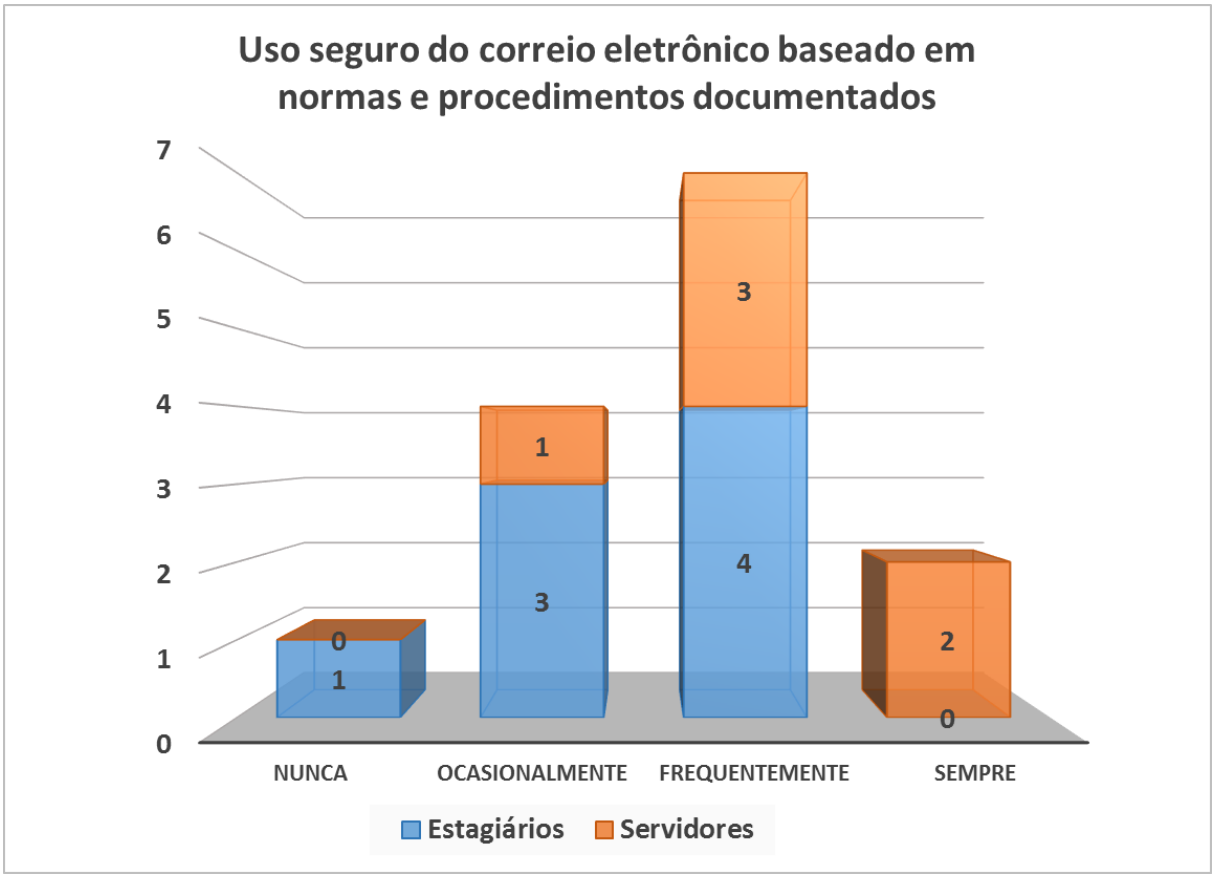

Figura 25 – Questão 6: Uso seguro do correio eletrônico baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações

Os resultados do questionamento mostram que quatro estagiários e três servidores, o equivalente a 50% dos entrevistados, apontaram o parâmetro “frequentemente” em relação ao quesito uso seguro de correio eletrônico nos computadores da organização, baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações. O parâmetro “ocasionalmente” foi assinalado por três estagiários e um servidor. Por sua vez, os parâmetros opostos “nunca” e “sempre” foram escolhidos por um e dois entrevistados, respectivamente. Percebe-se, no gráfico, predomínio dos totais

acumulados de respostas nos parâmetros “frequentemente” e “ocasionalmente”. Verifica-se também a prevalência das respostas dos estagiários nesses parâmetros.

O maior valor resultante da soma dos totais das respostas de estagiários e servidores em cada parâmetro definiu o parâmetro mais significativo como “frequentemente”, associando assim o indicador de segurança “medianamente seguro” ao quesito uso seguro de correio eletrônico nos computadores da organização, baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações. É oportuno frisar que a ordem de sequência dos parâmetros foi modificada para essa questão, conforme critérios estabelecidos para tabulação e apresentação dos dados (Item 3.4).

4.8 Análise dos resultados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação (navegação e troca de informações)

Entre os fenômenos que impactaram nos resultados das duas questões aplicadas, verificou-se a definição do parâmetro “frequentemente” como o mais significativo nesses quesitos. Isso produziu evidências de que os estagiários e servidores entrevistados executam de maneira segura esses procedimentos relacionados ao manuseio de ativos de informação corporativos. Não obstante, observou-se em ambos os quesitos significativa indicação ao parâmetro “ocasionalmente”. Tais situações levantam dúvidas acerca da segurança na realização dos procedimentos abordados no quesito.

No comparativo entre os grupos, constatou-se que os estagiários apresentaram maior incidência do que os servidores na realização de procedimentos inseguros, no que diz respeito aos quesitos aplicados.

Entre as possíveis causas da realização dos procedimentos inseguros percebidos se destacam a ausência de procedimentos padronizados e documentados de segurança da informação baseados nas melhores práticas, além da inexistência de política de segurança da informação na organização investigada.

4.9 Exposição de ativos de informação em ambientes de trabalho

Buscou-se por meio dessa observação direta não participante (ver Apêndice B) coletar dados suficientes que permitissem quantificar vulnerabilidades de segurança da informação decorrentes da exposição insegura de ativos de informação em ambientes de trabalho de servidores e estagiários, nas salas onde se realiza o processo de atendimento ao público na organização OXP. Foram verificados os ambientes de trabalho de três estagiários e três servidores, em quatro sessões de observação. Na primeira sessão, foram observados os ambientes de um servidor e um estagiário, os quais dividiam a mesma sala. Tanto na segunda como na terceira sessão, foram observadas salas com apenas um servidor. Na última sessão, foram observados os ambientes de trabalho de dois estagiários em uma única sala.

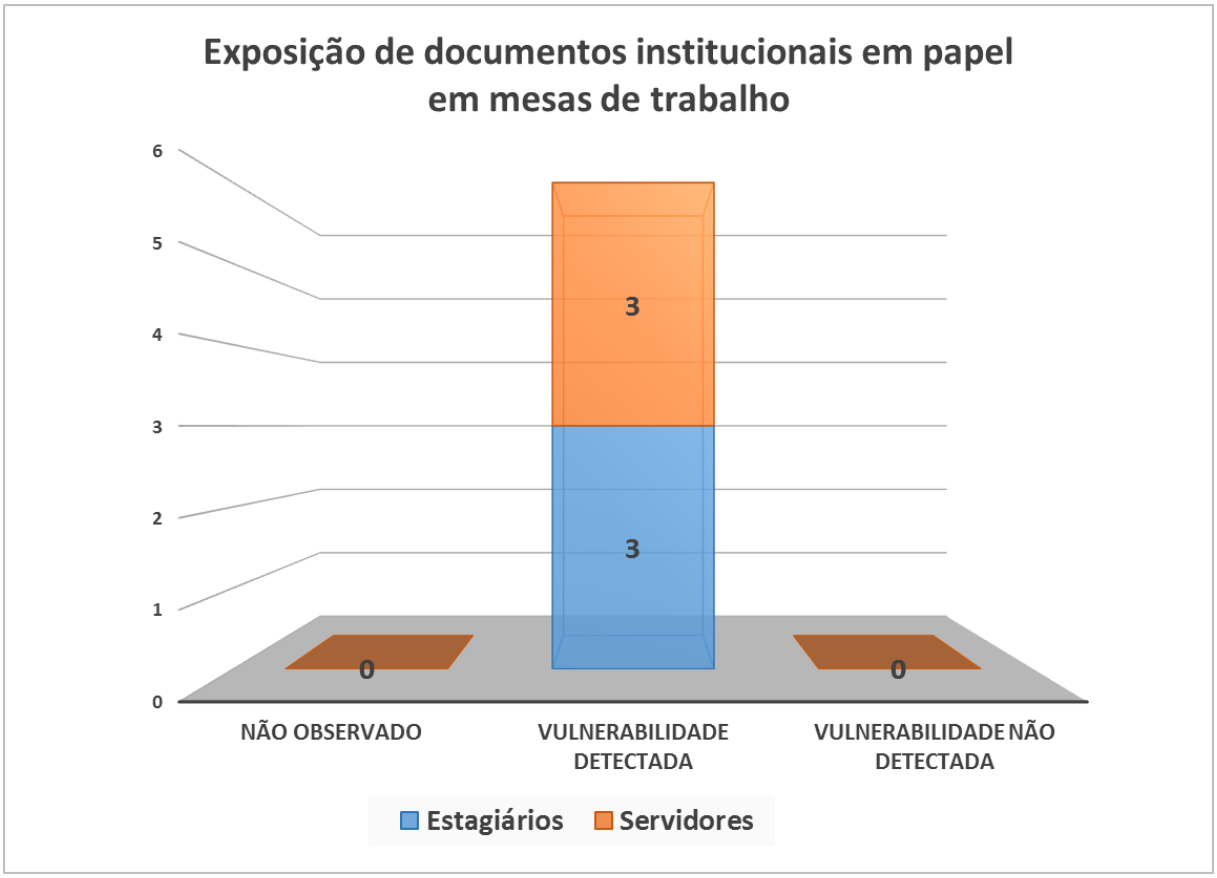

Figura 26 – Verificação 1: Exposição de documentos institucionais em papel em mesas de trabalho

Os resultados obtidos revelam seis situações de vulnerabilidade nos locais de trabalho observados, no que concerne ao quesito exposição de documentos institucionais em papel em mesas de trabalho. Das vulnerabilidades detectadas, três foram verificadas em ambientes de trabalho de estagiários e três em ambientes de servidores. No gráfico apresentado, é evidente o predomínio absoluto do total acumulado de verificações no parâmetro “vulnerabilidade detectada”.

O maior valor resultante da soma dos totais das verificações em cada parâmetro definiu o parâmetro mais significativo como “vulnerabilidade detectada”, associando assim o indicador de segurança “vulnerável” ao quesito exposição de documentos institucionais em papel em mesas de trabalho.

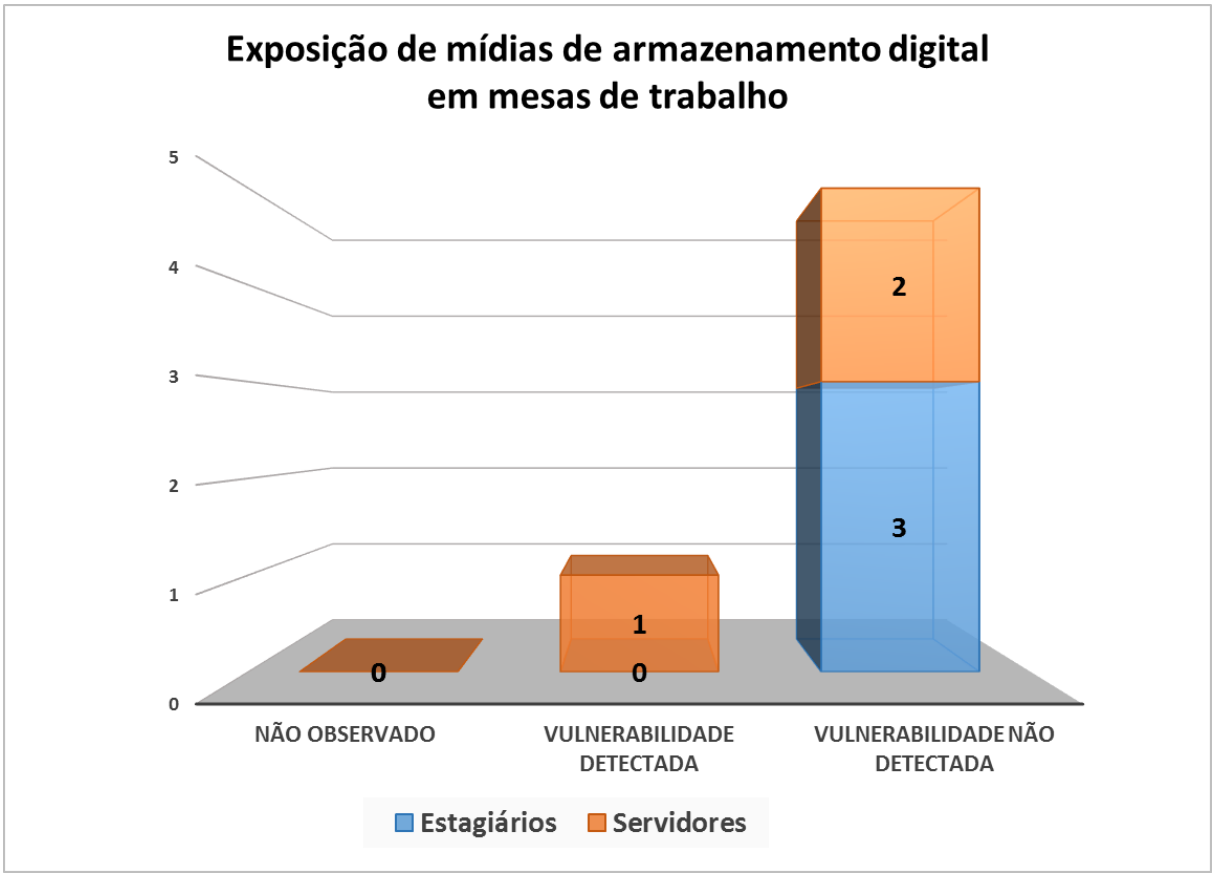

Figura 27 – Verificação 2: Exposição de mídias de armazenamento digital em mesas de trabalho

Os resultados obtidos revelam uma situação de vulnerabilidade nos locais de trabalho observados, no que concerne ao quesito exposição de mídias de armazenamento digital em mesas de trabalho. A vulnerabilidade foi detectada apenas no ambiente de trabalho de um servidor. Não foram detectadas

vulnerabilidades nos ambientes de três estagiários e dois servidores. No gráfico apresentado, é evidente o predomínio absoluto do total acumulado de verificações no parâmetro, “vulnerabilidade não detectada”.

O maior valor resultante da soma dos totais das verificações em cada parâmetro definiu o parâmetro mais significativo como “vulnerabilidade não detectada”, associando assim o indicador de segurança “seguro” ao quesito exposição de mídias de armazenamento digital em mesas de trabalho.

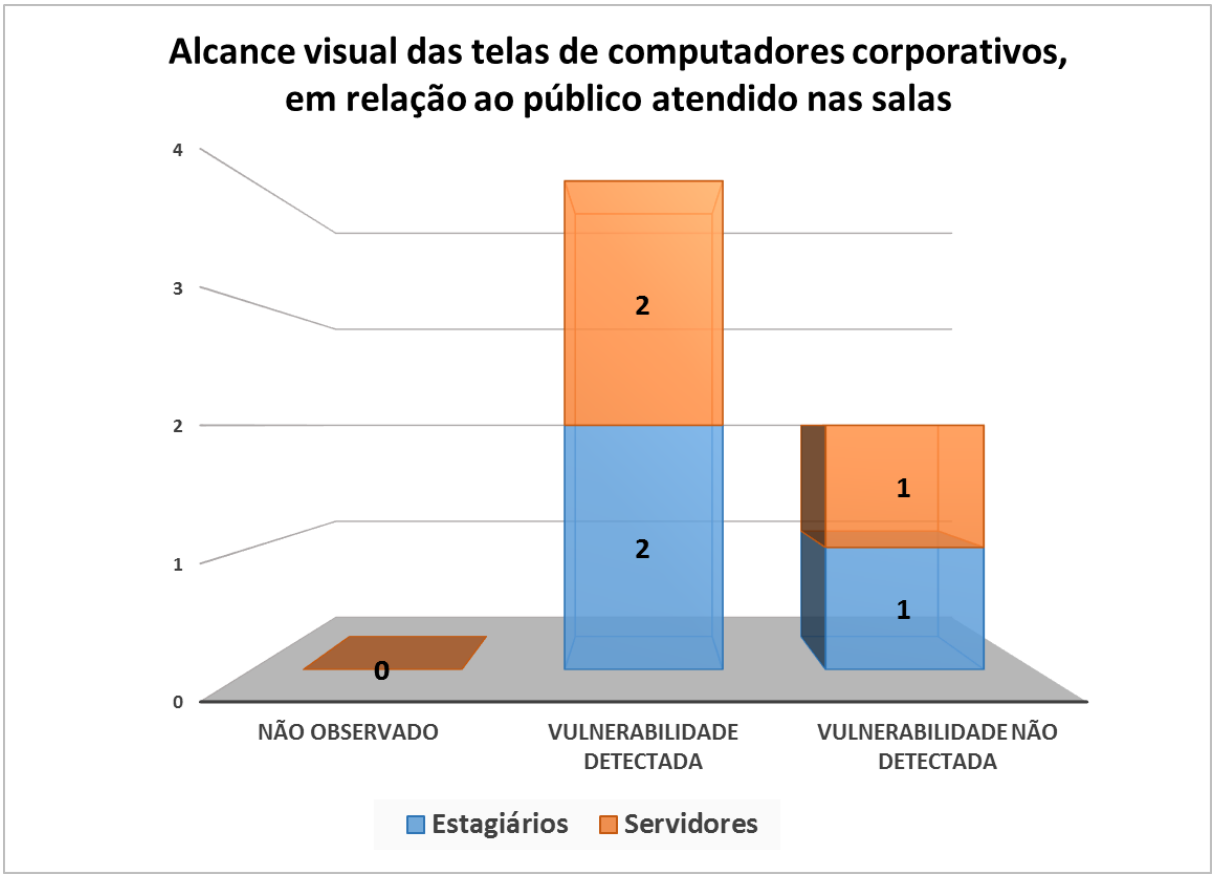

Figura 28 – Verificação 3: Alcance visual das telas de computadores corporativos em relação ao público atendido

Os resultados obtidos revelam quatro situações de vulnerabilidade nos locais de trabalho observados, no que concerne ao quesito alcance visual das telas de computadores corporativos no ambiente de trabalho, em relação ao público atendido. Das vulnerabilidades detectadas, duas foram verificadas em ambientes de trabalho de estagiários e duas em ambientes de servidores. Não foram detectadas vulnerabilidades nos ambientes de um estagiário e um servidor. No gráfico

apresentado, é evidente o predomínio absoluto do total acumulado de verificações no parâmetro “vulnerabilidade detectada”. Percebe-se também equilíbrio nas situações de vulnerabilidade encontradas em relação aos estagiários e servidores.

O maior valor resultante da soma dos totais das verificações em cada parâmetro definiu o parâmetro mais significativo como “vulnerabilidade detectada”, associando assim o indicador de segurança “vulnerável” ao quesito alcance visual das telas de computadores corporativos no ambiente de trabalho, em relação ao público atendido.

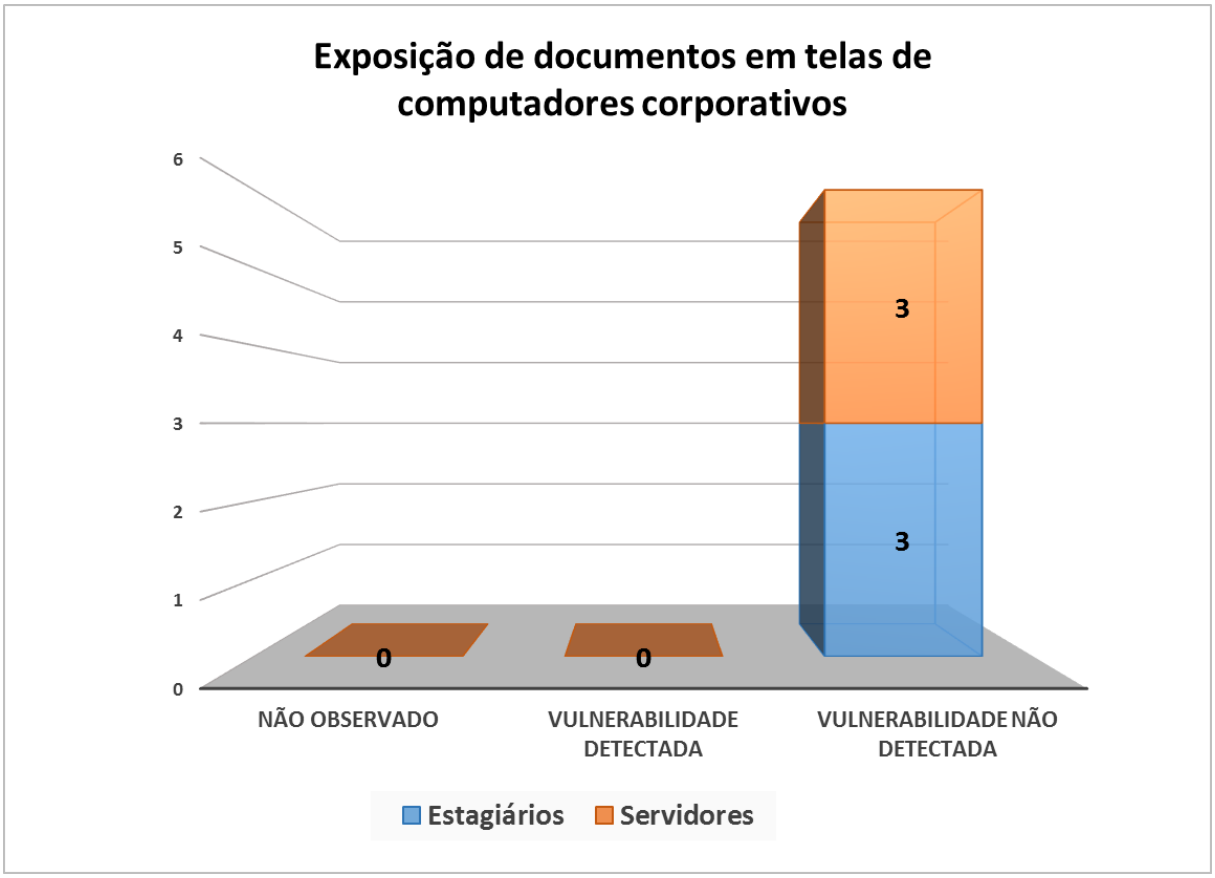

Figura 29 – Verificação 4: Exposição de documentos em telas de computadores corporativos no ambiente de trabalho

Os resultados obtidos não revelam situações de vulnerabilidade nos locais de trabalho observados, no que concerne ao quesito exposição de documentos em telas de computadores corporativos no ambiente de trabalho. Foram verificados três ambientes de trabalho de estagiários e três ambientes de servidores. No gráfico apresentado, é evidente o predomínio absoluto do total acumulado de verificações no parâmetro “vulnerabilidade não detectada”.

O maior valor resultante da soma dos totais das verificações em cada parâmetro definiu o parâmetro mais significativo como “vulnerabilidade não detectada”, associando assim o indicador de segurança “seguro” ao quesito exposição de documentos em telas de computadores corporativos no ambiente de trabalho.

4.10 Análise dos resultados relativos à exposição de ativos de informação em ambientes de trabalho

Entre os fenômenos que impactaram nos resultados do conjunto de observações aplicadas a respeito da exposição de ativos de informação no ambiente de trabalho da organização OXP, verificou-se a definição do parâmetro “vulnerabilidade detectada” como o mais significativo em dois dos quatro quesitos apresentados:

- Exposição de documentos institucionais em papel em mesas de trabalho;
- Alcance visual das telas de computadores corporativos em relação ao público atendido.

A correspondência do parâmetro “vulnerabilidade detectada” aos quesitos supracitados produziu evidências de que nos ambientes de trabalho observados há vulnerabilidades relativas à exposição de ativos de informação organizacionais.

No comparativo geral entre os grupos, verificou-se situação de equidade nas vulnerabilidades descobertas, no que diz respeito ao rol de quesitos aplicados.

Entre as possíveis causas da exposição vulnerável de ativos percebida, destacam-se a ausência de procedimentos padronizados e documentados de segurança da informação baseados nas melhores práticas, além da inexistência de política de segurança da informação na organização investigada.

5 Conclusão da Análise e Consolidação dos Resultados Obtidos

Esta pesquisa teve o propósito de promover o entendimento a respeito da engenharia social, em especial a respeito da ameaça que ações de engenharia social podem representar para organizações integrantes da APF. Para isso, buscou-se investigar vulnerabilidades humanas e organizacionais no processo de atendimento ao público da organização OXP passíveis de exploração em investidas de engenharia social.

Constituíram a base teórica deste trabalho a Norma NBR ISO/IEC 27002 (2005), por intermédio da qual foram abordados aspectos relevantes para a segurança da informação no ambiente organizacional, além das obras de Hadnagy (2011), Mann (2008) e Mitnick (2002), pelas quais foram levantados e discutidos conceitos de engenharia social, técnicas e ferramentas utilizadas em ações de engenharia social e maneiras de prevenir organizações contra essa ameaça.

O referencial teórico pesquisado norteou a etapa de coleta de dados, na qual foram aplicadas as técnicas de entrevista estruturada e observação direta não participante. Nas entrevistas estruturadas, foram obtidos dados relativos aos conhecimentos de estagiários e servidores acerca da segurança da informação no contexto organizacional e acerca da engenharia social, como também foram colhidos dados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação. Na observação direta, foram coletados dados acerca da exposição de ativos de informação corporativos no ambiente de trabalho.

Os dados coletados foram confrontados com o referencial teórico e analisados conforme critérios estabelecidos para sua tabulação. Os resultados dessas análises foram consolidados em parâmetros que correspondem a indicadores de vulnerabilidades, expressos no Quadro 5.

5.1 Consolidação dos Resultados

Conforme explicado no Item 3.4, os indicadores de segurança foram obtidos por meio da definição do maior parâmetro em cada um dos quesitos (questões e verificações) aplicados na etapa de coleta de dados.

A consolidação dos resultados não levou em conta a distinção entre os papéis de estagiários e servidores, uma vez que se entende que, como partícipes do mesmo processo de trabalho, os integrantes dessas categorias têm acesso a informações sensíveis e, portanto, é razoável concluir que devem ser equiparados no dever de proteger tais informações. As pessoas que trabalham em uma organização, mesmo aquelas que não pertençam a seus quadros de carreira, devem estar engajadas com a segurança da informação no contexto organizacional.

O quadro 5 apresenta a consolidação dos resultados analisados, divididos por segmentos, nos quais estão expressos cada quesito aplicado, bem como seus correspondentes parâmetros e indicadores de segurança. Ressaltam-se alterações na ordem dos quesitos pertencentes ao segmento procedimentos de segurança da informação relacionados ao manuseio de ativos de informação, tendo em vista a anulação da questão 8 e o reposicionamento das questões 5 e 6 ao final do bloco de quesitos.

QUESITO	PARÂMETRO	INDICADOR DE SEGURANÇA
Conhecimento acerca da segurança da informação no contexto organizacional		
1 - Conhecimento acerca dos princípios da segurança da informação usados como referência na APF(Disponibilidade, Integridade, Confidencialidade e Autenticidade)	**Inexistente**	**Muito vulnerável**
2 - Conhecimento acerca do papel da segurança da informação na organização	**Restrito**	**Vulnerável**
3 - Conhecimento sobre o documento da política de segurança da informação da organização	**Inexistente**	**Muito vulnerável**
4 - Conhecimento acerca das normas de segurança da informação relacionadas às suas atividades no trabalho	**Mediano**	**Medianamente seguro**
5 - Conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às suas atividades no trabalho	**Inexistente**	**Muito vulnerável**
6 - Conhecimento sobre ativos de informação organizacionais	**Inexistente**	**Muito vulnerável**
7 - Conhecimento sobre os tipos de informações que devem ser protegidas na organização	**Mediano**	**Medianamente seguro**
8 - Conhecimento sobre realização de atividades de sensibilização em segurança da informação na organização	**Inexistente**	**Muito vulnerável**
Conhecimento sobre a engenharia social		
1 - Conhecimento sobre o que a engenharia social representa para a organização	**Restrito**	**Vulnerável**
2 - Conhecimento sobre técnicas e métodos empregados em ações de engenharia social	**Inexistente/Restrito**	**Muito vulnerável**
3 - Conhecimento sobre ferramentas que apoiam ações de engenharia social	**Inexistente/Restrito**	**Muito vulnerável**
4 - Conhecimento sobre o tipo de alvo de uma ação de engenharia social	**Restrito**	**Vulnerável**
5 - Conhecimento sobre tipos de abordagens que podem ser utilizadas em uma ação de engenharia social	**Restrito**	**Vulnerável**
6 - Conhecimento sobre como ocorre uma ação de phishing	**Inexistente**	**Muito vulnerável**
7 - Conhecimento sobre casos de engenharia social	**Inexistente**	**Muito vulnerável**
8 - Conhecimento sobre procedimentos de segurança da informação que podem obstar ações de engenharia social	**Inexistente**	**Muito vulnerável**
Procedimentos de segurança da informação relacionados ao manuseio de ativos de informação		
1 - Exposição de documentos em mesas de trabalho	**Frequentemente**	**Vulnerável**
2 - Exposição de documentos abertos em computadores corporativos	**Ocasionalmente**	**Medianamente seguro**
3 - Uso de nomes, datas ou uma sequência simples de caracteres nas senhas de acesso aos computadores	**Nunca**	**Seguro**
4 - Compartilhamento de senhas de computadores corporativos com colegas de trabalho	**Nunca**	**Seguro**
7 - Conexão de dispositivos de armazenamento USB pessoais em computadores da organização	**Ocasionalmente**	**Medianamente seguro**
9 - Transporte de documentos físicos ou digitais da organização para trabalho em ambientes externos	**Nunca**	**Seguro**
10 - Publicação em redes sociais de informações relacionadas ao trabalho	**Nunca**	**Seguro**
5 - Comportamento seguro de navegação na internet, baseado em normas e procedimentos documentados contendo regras para navegação segura	**Frequentemente**	**Medianamente seguro**
6 - Uso seguro do correio eletrônico nos computadores da organização, baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações	**Frequentemente**	**Medianamente seguro**
Exposição de ativos de informação em ambientes de trabalho		
1 - Exposição de documentos institucionais em papel em mesas de trabalho	**Vulnerabilidade detectada**	**Vulnerável**
2 - Exposição de mídias de armazenamento digital em mesas de trabalho	**Vulnerabilidade não detectada**	**Seguro**
3 - Alcance visual das telas de computadores corporativos no ambiente de trabalho, em relação ao público atendido	**Vulnerabilidade detectada**	**Vulnerável**
4 - Exposição de documentos em telas de computadores corporativos no ambiente de trabalho	**Vulnerabilidade não detectada**	**Seguro**

Quadro 5 - Consolidação dos Resultados

Os indicadores de segurança definidos no Quadro de Consolidação dos Resultados são adiante analisados de forma agrupada em cada um dos segmentos a que pertencem.

5.2 Resultados dos indicadores de segurança associados ao conhecimento acerca da segurança da informação no contexto organizacional

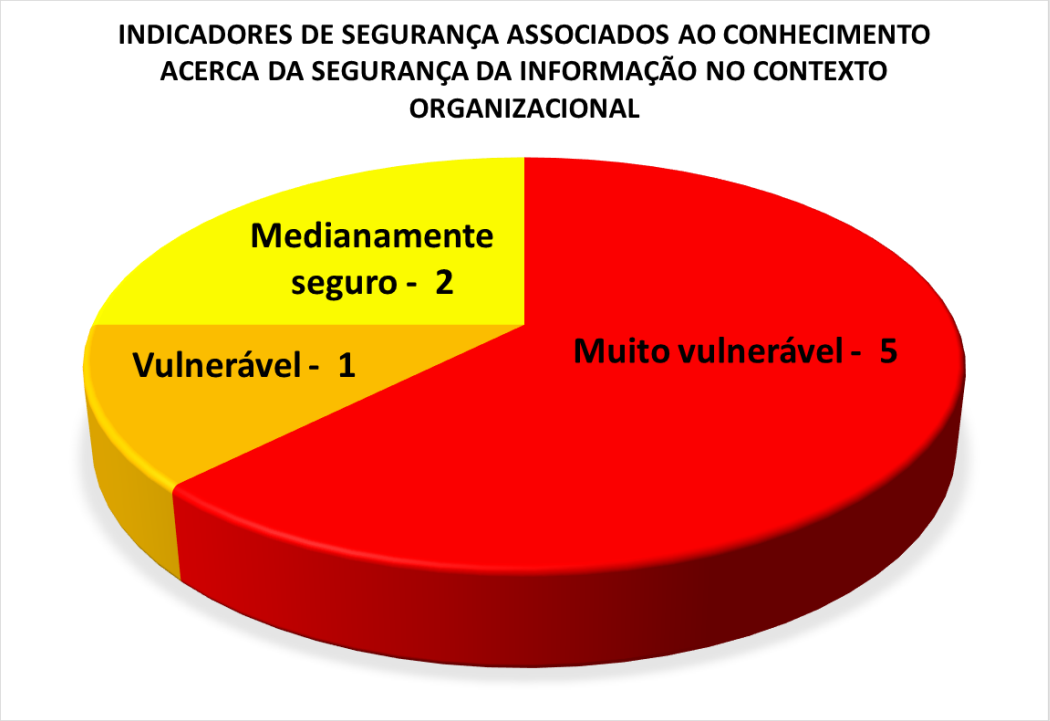

Figura 30 - Resultado dos indicadores de segurança associados ao conhecimento acerca da segurança da informação no contexto organizacional

Os resultados obtidos revelam cenário em que predomina vulnerabilidade elevada, no que diz respeito ao conjunto dos quesitos investigados, relativos ao conhecimento dos estagiários e servidores entrevistados acerca da segurança da informação no contexto da organização OXP. Tal assertiva é corroborada pela significativa presença do indicador de segurança "muito vulnerável" em cinco quesitos aplicados, reforçada ainda pela presença do indicador "vulnerável" em um quesito, o que resulta num quadro com 75% de vulnerabilidade em relação ao conjunto dos quesitos pesquisados. Cabe salientar que os dois quesitos referentes ao indicador "medianamente seguro" podem estar associados a vulnerabilidades, uma vez que a expressão "medianamente" sugere imprecisão no indicador, em que

pese a inclusão do termo "seguro" em sua nomenclatura. Por sua vez, o indicador "seguro" não foi associado a nenhum dos quesitos abordados.

O presente cenário de vulnerabilidade elevada foi definido em razão da predominância do parâmetro mais significativo "inexistente" no segmento analisado, conforme disposto no Quadro de Consolidação dos Resultados (Quadro 5).

5.3 Resultados dos indicadores de segurança associados ao conhecimento acerca da engenharia social

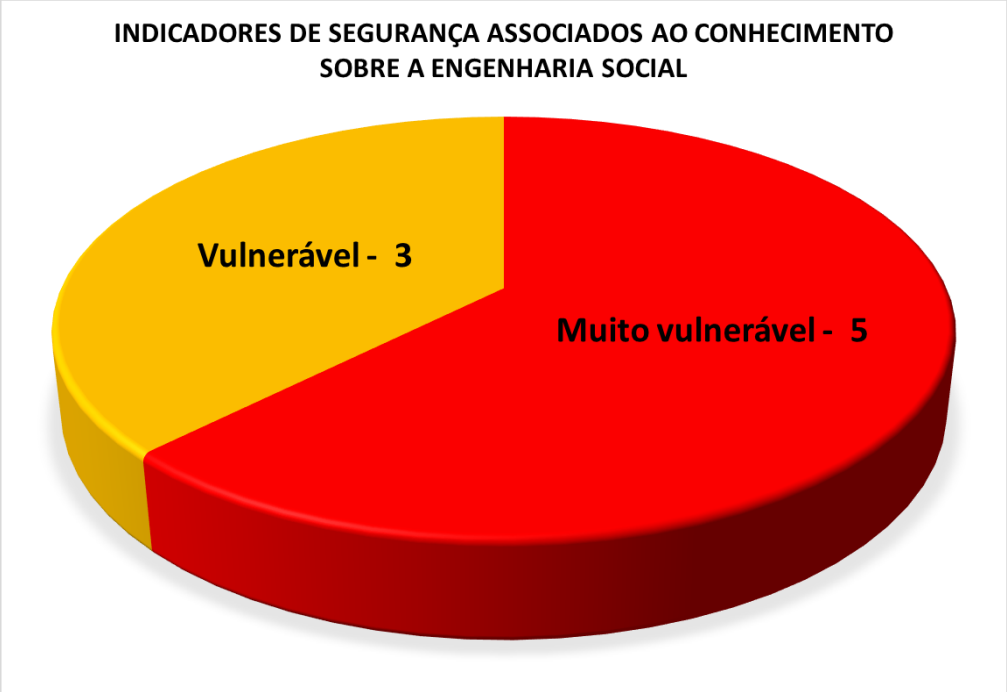

Figura 31 - Resultados dos indicadores de segurança associados ao conhecimento acerca da engenharia social

Os resultados obtidos mostram cenário em que predomina vulnerabilidade elevada em nível crítico, no que concerne ao conjunto dos quesitos investigados, a respeito do conhecimento dos estagiários e servidores entrevistados acerca da engenharia social. Tal alegação é fortalecida pela prevalência do indicador de segurança "muito vulnerável" em cinco quesitos, apoiada pela presença do indicador "vulnerável" em três quesitos, o que resulta num quadro com 100% de vulnerabilidade em relação ao conjunto dos quesitos pesquisados. Destacam-se ainda, no gráfico, as ausências dos indicadores "medianamente seguro" e "seguro".

O presente cenário de vulnerabilidade elevada em nível crítico foi definido em razão da predominância absoluta dos parâmetros mais significativos "inexistente" e "restrito" no segmento analisado, conforme disposto no Quadro de Consolidação dos Resultados (Quadro 5).

5.4 Resultados dos indicadores de segurança associados ao manuseio de ativos de informação

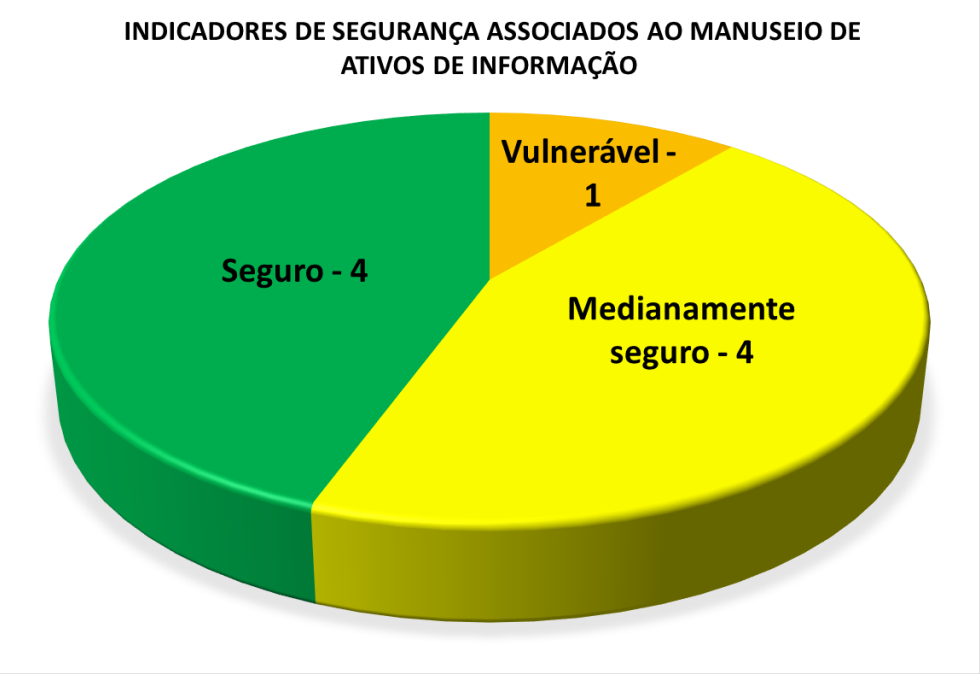

Figura 32 - Resultados dos indicadores de segurança associados ao manuseio de ativos de informação

Os resultados obtidos sugerem um cenário em que predomina segurança, no que tange ao conjunto dos quesitos investigados, acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação, por parte dos estagiários e servidores entrevistados. Os expressivos totais alcançados pelos indicadores de segurança "seguro" e "medianamente seguro", os quais igualmente totalizaram quatro quesitos, resultariam assim num quadro com 88% de segurança.

Não obstante, a imprecisão inerente ao indicador "medianamente seguro" abre perspectivas para um vislumbre com viés de vulnerabilidade, dada a

subjetividade que pode permear sua interpretação. À vista desse raciocínio, o termo "medianamente seguro" poderia perfeitamente ser tratado como "medianamente vulnerável". Nesse caso, teríamos uma situação com ligeira predominância de vulnerabilidade, uma vez que os quatro quesitos associados ao referido indicador teriam o reforço de um quesito associado ao indicador "vulnerável", ocasionando assim um quadro com cinco quesitos associados a vulnerabilidades, apesar da ausência do indicador "muito vulnerável". Por conseguinte, a análise dos números supracitados, à luz das reflexões levantadas, aponta para um cenário de mediana segurança, no tocante ao conjunto dos quesitos investigados.

O presente cenário de mediana segurança foi definido em razão da concorrência entre os parâmetros mais significativos "nunca" e "ocasionalmente"/"frequentemente" no segmento analisado, conforme disposto no Quadro de Consolidação dos Resultados (Quadro 5). Cabe observar que os parâmetros referentes às duas últimas questões divergem da ordem de parâmetros estabelecida para os demais quesitos do segmento, de acordo com explicação no Item 3.4.

5.5 Resultados dos indicadores de segurança associados à exposição de ativos de informação em salas de atendimento

Figura 33 - Resultados dos indicadores de segurança associados à exposição de ativos de informação em salas de atendimento

Os resultados obtidos revelam situação de paridade entre segurança e vulnerabilidade, no que diz respeito ao conjunto dos quesitos investigados acerca da exposição de ativos de informação em salas de atendimento da organização OXP. Observa-se que tanto o indicador de segurança "vulnerável" como o indicador "seguro" estiveram presentes em dois quesitos. Cabe salientar que a definição dos parâmetros associados a esses indicadores foi baseada nos períodos em que os ambientes de trabalho foram observados. Essa limitação temporal restringe a confiabilidade do parâmetro "vulnerabilidade não detectada", bem como de seu correspondente indicador de segurança, "seguro", uma vez que no cotidiano dos ambientes observados pode ocorrer grande incidência de vulnerabilidades em quesitos que receberam o indicador "seguro" na análise em questão.

O presente cenário de paridade entre segurança e vulnerabilidade foi definido em razão do equilíbrio absoluto entre os parâmetros mais significativos "vulnerabilidade detectada" e "vulnerabilidade não detectada" no segmento analisado, conforme disposto no Quadro de Consolidação dos Resultados (Quadro 5).

5.6 Conclusão acerca da Hipótese e Questão de Pesquisa

A análise da consolidação dos resultados, à luz do referencial teórico desenvolvido, direciona à conclusão de que a hipótese aventada nesta pesquisa foi validada, tendo em vista a confirmação de que pessoas que atuam no processo de atendimento ao público da organização OXP não estão engajadas com a segurança da informação, e portanto são vulneráveis a ações engenharia social. Essas vulnerabilidades humanas constituem indicativo de vulnerabilidades organizacionais, e estão expressas nos seguintes achados:

- Situação de vulnerabilidade elevada, no que tange ao conjunto dos quesitos investigados, a respeito do conhecimento dos estagiários e servidores entrevistados acerca da segurança da informação no contexto da organização OXP;
- Situação de vulnerabilidade elevada em nível crítico, no que concerne ao conjunto dos quesitos investigados a respeito do conhecimento dos estagiários e servidores entrevistados acerca da engenharia social;
- Situação de mediana segurança, no que se refere ao conjunto dos quesitos investigados acerca de procedimentos de segurança da informação relacionados ao manuseio de ativos de informação, por parte dos estagiários e servidores entrevistados;
- Situação de paridade entre segurança e vulnerabilidade, no que diz respeito ao conjunto dos quesitos investigados acerca da exposição de ativos de informação em salas de atendimento da organização OXP.

A apreciação do conjunto desses achados viabiliza o entendimento acerca das vulnerabilidades descobertas na organização OXP, do qual advêm as seguintes conclusões:

- Vulnerabilidades humanas à engenharia social se manifestam em conhecimento reduzido ou desconhecimento acerca do papel da segurança da informação no contexto organizacional.

- Vulnerabilidades humanas à engenharia social se manifestam em conhecimento reduzido ou desconhecimento acerca da engenharia social.
- Vulnerabilidades humanas à engenharia social se manifestam na realização de procedimentos inseguros de segurança da informação relacionados ao manuseio de ativos de informação organizacionais.
- Vulnerabilidades humanas à engenharia social se manifestam na exposição insegura de ativos de informação organizacionais.
- As vulnerabilidades mais elevadas à engenharia social correspondem a conhecimentos reduzidos ou desconhecimento acerca do papel da segurança da informação no contexto organizacional e acerca da engenharia social.
- O conjunto de vulnerabilidades humanas deslindado constitui indicativo de vulnerabilidades organizacionais, uma vez que as limitações de conhecimentos de pessoas acerca da segurança da informação no contexto organizacional, bem como acerca da engenharia social, sugerem ineficácia ou ausência de atividades de sensibilização ou treinamento direcionados a esses assuntos. Ademais, a realização de procedimentos inseguros no tocante ao manuseio e à exposição de ativos de informação corporativos também indicam vulnerabilidades organizacionais, as quais podem estar associadas à inexistência de política de segurança da informação na organização, entre outros fatores.

À vista das descobertas supracitadas e das reflexões ora mencionadas, chegou-se à conclusão de que a pergunta de pesquisa formulada neste trabalho foi respondida, porquanto foi possível verificar e analisar como se manifestam vulnerabilidades humanas e organizacionais que podem ser exploradas por ações de engenharia social no processo de atendimento ao público da organização OXP.

6 Conclusões e Trabalhos Futuros

6.1 Conclusões

O desenvolvimento deste trabalho foi permeado por desafios em diversos aspectos. O primeiro se deu ainda na fase de planejamento da pesquisa, quando foi considerada a impossibilidade de se observar, durante a futura etapa de coleta de dados, um ataque real de engenharia social contra pessoas da organização OXP que estariam envolvidas neste trabalho, bem como a inviabilidade de se empreender um ataque simulado de engenharia social contra esses indivíduos, o qual no jargão da segurança da informação seria denominado como teste de penetração (*pentest*). Tal situação, mesmo que tivesse anuência dos dirigentes da organização OXP, poderia ser legalmente questionada.

Assim, os motivos expostos levaram à decisão de se investigar, para os fins desta pesquisa, vulnerabilidades relativas à engenharia social tendo como base níveis de conhecimento dos entrevistados, periodicidade com que essas pessoas realizam procedimentos de segurança da informação e a exposição de ativos de informação em seus ambientes de trabalho.

Outro desafio durante a etapa de planejamento se manifestou na escassa e incipiente literatura disponível acerca da engenharia social, condição que demandou que se realizasse pesquisa refinada, com vistas a elaboração de um referencial teórico que balizasse o trabalho investigativo de maneira satisfatória.

A sequência de desafios prosseguiu com a busca pela definição de uma unidade de análise adequada ao propósito do trabalho, situação que exigiu criatividade para ser contornada, tendo em vista que, ao invés de se considerar

determinado setor ou área física da organização pesquisada, levou-se em conta um processo de trabalho distribuído em diversas salas nas dependências da organização.

Talvez o maior desafio enfrentado no decorrer do TC tenha sido a tarefa de idealizar um processo de coleta de dados concatenado aos objetivos da pesquisa, que viabilizasse a criação de um método capaz de proporcionar uma análise objetiva das informações a serem colhidas, em consonância com o referencial teórico desenvolvido. No entanto, verificou-se que a prematura elaboração e aplicação de um rol de perguntas abertas a respostas subjetivas tornou a referida análise praticamente inexequível. A situação só foi equacionada após a reestruturação dos quesitos constantes nos questionários, com a adaptação das opções de respostas a parâmetros objetivos, capazes de mensurar de forma razoável níveis de conhecimentos dos entrevistados acerca da segurança da informação e da engenharia social, como também a periodicidade com que são realizados procedimentos de segurança da informação e a incidência da exposição de ativos de informação em seus ambientes de trabalho. Esses parâmetros foram correlacionados a indicadores de segurança, cuja principal função, apesar da paradoxal nomenclatura, consistiu em fornecer índices de vulnerabilidade à engenharia social pertinentes aos segmentos investigados.

A superação das mencionadas dificuldades viabilizou o desenvolvimento desta investigação e a consecução dos objetivos estipulados em seu planejamento, voltados em essência ao mapeamento de vulnerabilidades à engenharia social em uma organização pública. Por conseguinte, o presente estudo poderá alertar organizações pertencentes à APF no que diz respeito à criticidade do elemento humano no contexto da segurança da informação, e acerca do potencial nocivo que a engenharia social representa para essas organizações.

Um importante aspecto a ser observado se refere à aderência deste trabalho à realidade de outras organizações, ou seja, a possibilidade de se replicar este protocolo de pesquisa em organizações públicas diversas, as quais poderiam ter a oportunidade de utilizar tal instrumento para subsidiar suas políticas de segurança da informação ou até mesmo para estimular o desenvolvimento de políticas de segurança da informação com foco no elemento humano.

6.2 Limitações da Pesquisa

Em que pese o alcance dos objetivos propostos pelo planejamento da pesquisa em questão, fez-se necessário realizar leitura acurada, bem como levantar reflexões, acerca do trabalho desenvolvido, com o intento de se investigar lacunas que possam trazer contribuições para o aperfeiçoamento deste protocolo de pesquisa, em estudos futuros. À vista disso, foram observadas as seguintes limitações no conteúdo deste estudo de caso:

- Impossibilidade de se planejar a observação de ações reais de engenharia social no ambiente investigado;
- Unidade de análise circunscrita a apenas um processo de trabalho no ambiente corporativo investigado;
- Distorções resultantes da definição do parâmetro mais significativo, em quesitos nos quais se verificou equilíbrio entre índices de parâmetros;
- Imprecisão inerente ao indicador de segurança medianamente seguro, o qual tanto pode ser empregando para indicar relativa segurança como relativa vulnerabilidade.

6.3 Trabalhos Futuros

Afim de que seja mantida a mesma orientação desta pesquisa, bem como sejam preenchidas as lacunas anteriormente observadas, para o emprego deste protocolo de pesquisa em trabalhos futuros de estudo de caso, sugere-se:

- Manter como foco de pesquisa o mapeamento de vulnerabilidades à engenharia social;
- Ampliar o rol de quesitos a serem aplicados na coleta de dados;
- Aumentar a quantidade de pessoas a serem entrevistadas, com a inclusão de funcionários terceirizados e lideranças da organização, especialmente dos setores de TI e RH;
- Realizar análise comparativa do mapeamento de vulnerabilidades à engenharia social entre as categorias de profissionais envolvidas no estudo de caso;

- Definir uma unidade de análise com maior abrangência, no que se refere a processos de trabalho;
- Empregar metodologias específicas de análise qualitativa de dados, com a finalidade de ampliar a precisão dos resultados analisados.

Referências e Fontes Consultadas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação – Técnicas de Segurança - Código de prática para a gestão da segurança da informação**: ABNT NBR ISO/IEC 27002:2005. 2ª. ed. Rio de Janeiro, 2008.

BORGES, Timotheo Barbosa. **Avaliação de Conformidade de Controles de Acesso Lógico de Acordo com as Normas ABNT NBR/ISO/IEC 27002:2005 e NC07/IN01/DSIC/GSI/PR**. Monografia. Campus Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2011.

BRASIL. Casa Civil. Lei n° 12.527 - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: 2011.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar n° 04 - Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC**. Brasília: 2009.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar n° 10 - Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal**. Brasília: 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para a Internet** - Versão 4.0. 2ª. ed. São Paulo: 2008.

FERNANDES, Jorge Henrique; BORGES, Díbio Leandro. **Pesquisa de Estudo de Caso em Gestão da Segurança da Informação** (notas de aula). CEGSIC 2012/2014. Campus Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2013.

FERNANDES, Jorge Henrique; RODRIGUES, Genaína Nunes. **Fundamentos da Gestão da Segurança da Informação** (notas de aula). CEGSIC 2012/2014.

Campus Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2013.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação** - Guia Prático para Elaboração e Implementação. 2ª ed. Rio de Janeiro: Ciência Moderna, 2008.

HADNAGY, Christopher. **Social Engineering**: The Art of Human Hacking. 1th. ed. California: Sage, 2011.

MANN, Ian. **Hacking the Human:** Social Engineering Techniques and Security Countermeasures. 1th. ed. Hampshire: Gower Publishing, 2008.

MITNICK, Robert K. **The Art of Deception:** Controlling the Human Element of Security. 1th. ed. Indianapolis: Wiley Publishing, 2002.

MORESI, Eduardo. **Metodologia da Pesquisa**. Monografia. Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e Tecnologia da Informação: Pró-reitoria de Pós Graduação da Universidade Católica de Brasília. 2003.

PEIXOTO, Mário César Pintaudi. **Engenharia Social e Segurança da Informação**. 1ª ed. Rio de Janeiro: Brasport, 2006.

PINHEIRO, Patrícia Peck. **Direito Digital.** 4ª ed. São Paulo: Saraiva, 2010.

ROBBINS, Anthony apud TUCCI, Alexandre. **Entenda o que é *Rapport***. 2008. Disponível em: <http://www.administradores.com.br/artigos/negocios/entenda-o-que-e-rapport/24502/>. Acesso em: 02 julho 2014.

RODRIGUES, Roberto Wagner da Silva; FERNANDES, Jorge Henrique. **Auditoria de Segurança da Informação** (notas de aula). CEGSIC 2012/2014. Campus Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2013.

SARMET, Mauricio Miranda. **Análise Ergonômica em Segurança da Informação** (notas de aula). CEGSIC 2012/2014. *Campus* Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2013.

SBPNL - SOCIEDADE BRASILEIRA DE PROGRAMAÇÃO NEUROLINGUÍSTICA. **O que é PNL?**. 2014. Disponível em: < http://pnl.com.br/siteSobre/home>. Acesso em: 02 julho 2014.

TRIBUNAL DE CONTAS DA UNIÃO. Acórdão n° 2.585/2012 - TC 007.887/2012-4 - Relatório De Levantamento. **Avaliação Da Governança De Tecnologia Da Informação Na Administração Pública Federal.** Oportunidades De Melhoria. Recomendações. Brasília: 2012.

VIDAL, Flávio de Barros; FERNANDES, Jorge Henrique. **Segurança Física e do Ambiente** (notas de aula). CEGSIC 2012/2014. *Campus* Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da

Universidade de Brasília. 2013.

YIN, Robert K. **Estudo de Caso:** Planejamento e Métodos. 4ª ed. Porto Alegre: Bookman, 2010.

Apêndice A – Entrevistas estruturadas

Conhecimento da Segurança da Informação no contexto organizacional						
Entrevista estruturada		Questão	Inexistente	Restrito	Mediano	Amplo
	1	Tenho conhecimento dos princípios da segurança da informação usados como referência na APF (Disponibilidade, Integridade, Confidencialidade e Autenticidade).				
	2	Conheço o papel da segurança da informação na minha organização.				
	3	Conheço o documento da política de segurança da informação de minha organização.				
	4	Tenho conhecimento acerca das normas de segurança da informação relacionadas às minhas atividades no trabalho				
	5	Tenho conhecimento acerca de procedimentos padronizados e documentados de segurança da informação relacionados às minhas atividades no trabalho.				
	6	Tenho conhecimento sobre ativos de informação organizacionais.				
	7	Conheço os tipos de informações que devem ser protegidas em minha organização.				
	8	Tenho conhecimento sobre a realização de atividades de sensibilização em segurança da informação em minha organização.				
Conhecimento da Engenharia Social						
Entrevista estruturada		Questão	Inexistente	Restrito	Mediano	Amplo
	1	Tenho conhecimento sobre o que a engenharia social representa para minha organização.				
	2	Tenho conhecimento sobre técnicas/métodos empregados em ações de engenharia social.				
	3	Tenho conhecimento sobre ferramentas que apoiam ações de engenharia social.				
	4	Tenho conhecimento sobre o tipo de alvo de uma ação de engenharia social.				
	5	Tenho conhecimento sobre tipos de abordagens que podem ser utilizadas em uma ação de engenharia social.				
	6	Tenho conhecimento sobre como ocorre uma ação de phishing.				
	7	Tenho conhecimento sobre casos de engenharia social.				
	8	Conheço procedimentos de segurança da informação que podem obstar ações de engenharia social.				

Procedimentos de Segurança da Informação relacionados ao manuseio de ativos de informação						
		Questão	Nunca	Ocasionalmente	Frequentemente	Sempre
Entrevista estruturada	1	Há documentos expostos em sua mesa de trabalho?				
	2	Você deixa documentos abertos em seu computador corporativo?				
	3	Você utiliza como senhas nomes, datas ou uma sequência simples de caracteres para acessar seu computador corporativo?				
	4	Você compartilha senhas do seu computador corporativo com colegas de trabalho?				
	5	Seu comportamento de navegação na internet (nos computadores da organização) é seguro, ou seja, é baseado em normas e procedimentos documentados contendo regras para navegação segura?				
	6	Seu uso do correio eletrônico (nos computadores da organização) é seguro, ou seja, é baseado em normas e procedimentos documentados contendo regras para proteger a troca de informações?				
	7	Você conecta dispositivos de armazenamento USB pessoais em computadores de sua organização?				
	8	Você conecta dispositivos de armazenamento USB pessoais em computadores de sua organização?				
	9	Você leva documentos físicos ou digitais de sua organização para trabalhar em ambientes externos?				
	10	Você publica informações relacionadas ao seu trabalho em redes sociais?				

Conceitos de referência

1 - **Segurança da Informação** é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (NBR ISO/IEC 27002, 2005)

2 - A **Política de Segurança da Informação** é um documento que define o conjunto de normas, procedimentos e métodos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação (FERREIRA e ARAÚJO, 2008, p. 36)

3 - Os A**tivos de Informação** correspondem àquelas informações e todos os recursos associados que têm alto valor para o negócio público ou privado (RODRIGUES e FERNANDES, 2013)..

4 - **Engenharia Social** consiste em uma ação ou um conjunto de ações voltadas a explorar vulnerabilidades humanas com o emprego de recursos ardilosos ou fraudulentos, os quais podem ser apoiados por técnicas de influência ou persuasão, para que a pessoa alvo forneça informações ambicionadas ou execute tarefa planejada em benefício do atacante.

5 - **Phishing** é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social" (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

Observação: Esse conceito de **Phishing** apresenta limitações, uma vez que o objetivo desse tipo de ataque pode ir além do acesso a dados pessoais ou financeiros do usuário-alvo. O golpe pode ser aplicado com vistas a obter acesso não autorizado a ativos de informação organizacionais.

Apêndice B – Observação Direta não participante

Exposição insegura de ativos de informação corporativos em salas de atendimento					
Observação direta não participante		Verificação	Não observado	Vulnerabilidade detectada	Vulnerabilidade não detectada
	1	Exposição de documentos institucionais em papel em mesas de trabalho de servidores e estagiários.			
	2	Exposição de mídias de armazenamento digital (CDs, pen-drives) em mesas de trabalho de servidores e estagiários.			
	3	Alcance visual das telas de computadores corporativos, em relação ao público atendido em salas de servidores e estagiários.			
	4	Exposição de documentos em telas de computadores corporativos de servidores e estagiários.			

Apêndice C – Guia resumido para aplicação da metodologia

Ainda que a metodologia desenvolvida nesta pesquisa careça de aperfeiçoamento, ela pode ser aplicada em organizações, tanto públicas como privadas. Para isso foi elaborado de maneira sucinta o guia a seguir:

1. Identificar e selecionar setor ou processo da organização onde será aplicada a metodologia. Recomenda-se priorizar áreas ou processos que abranjam informações sensíveis;
2. Identificar e selecionar as pessoas do setor ou processo da organização que serão abrangidas pela metodologia. Recomenda-se definir percentual significativo de pessoas envolvidas no setor ou processo objeto do estudo;
3. Aplicar a técnica de entrevista estruturada aos grupos participantes da pesquisa, com a implementação de questionários para avaliar conhecimentos a respeito da segurança da informação no contexto organizacional e acerca da engenharia social, bem como avaliar a periodicidade com que são realizados procedimentos de segurança da informação relativos ao manuseio de ativos de informação;
4. Aplicar a técnica de observação direta não participante no ambiente físico integrante do estudo, a fim de que seja verificada a exposição de ativos de informação;
5. Encontrar o parâmetro mais significativo em cada quesito aplicado na coleta de dados, conforme critérios estipulados na Tabulação e Apresentação dos Dados (Item 3.4);
6. Analisar com base no referencial teórico desta pesquisa, ou sua ampliação, os resultados dos quesitos aplicados de forma agrupada por segmento;
7. Associar os parâmetros mais significativos encontrados em cada quesito aos correspondentes indicadores de segurança, conforme disposto na Tabulação e

Apresentação dos Dados (Item 3.4);

8. Consolidar e analisar os resultados dos indicadores de segurança obtidos, tendo como base o referencial teórico desta pesquisa, ou sua ampliação;
9. Discutir os resultados da pesquisa com lideranças da organização.