FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

JULIANO ROSADA

Análise do fator humano na Segurança da Informação em uma prefeitura do Estado de São Paulo

Americana, SP

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

JULIANO ROSADA

Análise do fator humano na Segurança da Informação em uma prefeitura do Estado de São Paulo

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do prof. Me. Benedito Luciano Antunes de França.

Área de concentração: Gestão de Riscos de Segurança da Informação

Americana, SP

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

R697a ROSADA, Juliano

Análise do fator humano na segurança da informação em uma Prefeitura do Estado de São Paulo. / Juliano Rosada. – Americana, 2018.

112f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de França

1 Sistemas de informação – governança 2. Segurança em sistemas de informação I. FRANÇA, Benedito Luciano Antunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.518.3

Juliano Rosada

ANÁLISE DO FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO EM UMA PREFEITURA DO ESTADO DE SÃO PAULO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Engenharia Social.

Americana, 13 de dezembro de 2018.

Banca Examinadora:

Benedito Luciano Antunes de França (Presidente)
Mestre
Fatec Americana

Wladimir da Costa (Membro)
Mestre
Fatec Americana

Clerivaldo José Roccia (Membro)
Mestre
Fatec Americana

DEDICATÓRIA

Dedico este trabalho às almas daqueles que morreram por sua fé em Cristo.

AGRADECIMENTOS

Agradeço aos meus avós que tanto me suportaram por tantos anos de minha vida e que tanta influência tiveram sobre quem sou.

Agradeço minha mãe, sem a qual não haveria Juliano, nem café para minha concentração.

Agradeço minha irmãzinha Giovanna por esperar a hora certa para pedir que a levasse à sua sorveteria favorita.

Agradeço à minha afilhada Aurora e aos meus amigos Marcos e Gisele por não reclamarem (tanto) a falta de minha presença neste meses de trabalho.

Agradeço ao meu caríssimo professor Benê França por toda ajuda e suporte no desenvolvimento deste trabalho, sem ele nada disto seria possível.

Agradeço à Fatec Americana pelo excelente nível de ensino oferecido, pelos excelentes colegas e pelos amigos que fiz. Foram anos de aprendizado que certamente me deram o caminho que eu esperava, e preciso, para meu futuro.

Agradeço a todos os envolvidos na elaboração deste trabalho de graduação, pessoas e instituições.

Agradeço, por fim, à Santa Mãe de Deus e a seu Filho Jesus Cristo, Nosso Senhor, a Sabedoria de Deus, pela inspiração.

RESUMO

Este Trabalho de Graduação aborda, de maneira básica, o contexto atual da Sociedade da Informação na qual vivemos, com seu uso disseminado de sistemas informatizados, para detectar o nível de maturidade do fator humano da prefeitura de um município do interior do estado de São Paulo quanto à segurança da informação, a fim de identificar sua exposição às ameaças a informação a que está sujeita, especificamente para sustentar a necessidade desta prefeitura se adequar às ferramentas de gestão de riscos, e assim propor a adoção de um modelo de gestão de riscos baseado em um sistema de gestão de segurança da informação segundo recomendações das normas da série ISO 27000.

Palavras Chave: Gestão de Riscos de Segurança da Informação; Fator Humano; Governança.

ABSTRACT

This work takes in a basic way the current context of the information society we live, and its widespread use of computerized systems, to detect the maturity level of the human factor of a city hall in the state of São Paulo about its information security in order to identify its exposure to the information threats it is subject to, specifically to justify the need of its city hall administration to fit the tools of risk management, and thus, propose the adoption of a risk management model based in an Information Security Management System according to ISO 27000 series standards recommendations.

Keywords: Information Security Risk management; Human factor; Governance.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
NBR	Norma Brasileira
IBM	*International Business Machines*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
NSA	*National Security Agency*
CIA	*Central Intelligence Agency*
PDCA	*Plan, Do, Check, Act*
SI	Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO

A informação representa parte dos ativos mais importantes para as organizações. Devido ao crescente uso de recursos de informação, houve o aumento da exposição das organizações às ameaças circundantes aos seus principais ativos de informação. Com isto, há uma necessidade maior de proteção.

É importante notar que as informações vão além dos meios informatizados e, em muitos casos, apresentam-se em registros, em forma bruta, como em documentos físicos, ou em processos gerenciais. Mesmo estes registros precisam ser protegidos. Porém, além disto, também deve-se considerar as pessoas que manipulam as informações como parte crucial a serem blindadas contra investidas exteriores.

Se para organizações privadas a informação é particularmente valiosa por seu interesse estratégico, e para a obtenção de lucros, no setor público a informação passa a atender a um interesse relacionado ao bem comum. A informação, aqui, torna-se a matéria-prima para o desenvolvimento de políticas públicas, e transparência para o controle das contas do Estado pelos cidadãos. Em certos aspectos, porém, é necessário e conveniente que a informação não seja desordenada ou livremente disseminada.

Quando em organizações públicas, a quebra de confidencialidade, integridade ou disponibilidade da informação deixa de ser um problema particular de alguns poucos interessados e estende-se a toda sociedade, pois que gerador de ineficiência e gastos de recursos limitados, além da possibilidade de se expor dados particulares de cidadãos e informações confidenciais de ordem pública.

A fim de mitigar as falhas de segurança, as organizações servem-se de inúmeras ferramentas e técnicas. Entre as questões mais problemáticas na SI estão aquelas relacionadas à cultura organizacional e da compreensão pelos usuários dos recursos de TI dos riscos a que estão expostos, e como devem se proteger e se portar. Apesar da gestão da SI se assentar sobre três pilares essenciais – a tecnologia, os processos, e as pessoas –, o pilar mais negligenciado tem sido justamente o mais crítico e que apresenta maiores riscos: o fator humano. Segundo Demarco e Lister (1990, *apud* LAUREANO, 2005), os aspectos humanos representam o elo mais fraco na cadeia da SI. Esta posição é corroborada por Mitnick e Simon (2003, p. 3).

Ainda assim, as organizações despendem enormes fortunas em tecnologias de *firewalls*, antivírus e outros dispositivos de segurança, mas seguem negligenciando este aspecto. Isto torna-se claro quando constatamos que a maioria das falhas de segurança se originam do uso inseguro de recursos de TI por usuários mal treinados para executar suas rotinas, *insiders* – colaboradores insatisfeitos com sua organização –, ou por sedição de pessoas externas à organização, os *outsiders*.

Como tema geral, este trabalho analisará, por um estudo de caso descritivo, levantando-se dados por meio da aplicação de questionários e analisados o cenário do objeto de estudos, segundo a metodologia de pesquisa escolhida, as condições gerais da cultura organizacional voltada à SI dentro de uma prefeitura de um município do interior do Estado de São Paulo. Buscará realizar uma análise preliminar de contexto, levantando ainda seus ativos e possíveis riscos para que possibilite o desdobramento de trabalhos futuros que tenham como fim, propor soluções que mitiguem as eventuais falhas encontradas.

Como tema específico, este trabalho procurará descobrir qual a situação atual do fator humano da SI da prefeitura de um município do interior do Estado de São Paulo; buscará ainda responder quais as preocupações quanto ao valor da informação guardada pelo objeto de estudo, e para onde olhar caso pretenda aplicar um modelo de governança que garanta a melhor orientação aos colaboradores da organização para melhor uso da TI com atenção à SI na administração pública municipal, além de propor, brevemente, quais soluções podem ser adotadas de imediato para minimizar os problemas detectados.

Portanto, o objetivo aqui será buscar identificar, de maneira preliminar, fragilidades e vulnerabilidades no tratamento gerencial da SI no seu pilar relacionado ao fator humano; em seguida, gerar informações e dados a serem tratados, elaborar uma série de recomendações úteis quanto à adoção de políticas e procedimentos de segurança, especificamente quanto ao treinamento e preparo de usuários de recursos de TI para enfrentar riscos de uso indevido dos recursos, ainda que para reagirem adequadamente a tentativas de Engenharia Social, compreender e coibir a ação de *insiders*, gerando orientação adequada e procedimentos quanto ao uso ótimo de processos por usuários finais, com o fim de desenvolver um uso seguro dos recursos de TI da organização. De

forma expandida, o objetivo é gerar um conjunto de recomendações e estabelecer o início de um projeto que possa ser adotado pela prefeitura estudada para que esta possa adotar um plano de orientação, conscientização, capacitação e condicionamento dos usuários para a segurança de sua informação.

Este projeto tentará ser como um primeiro passo a servir de convencimento das lideranças municipais sobre a necessidade de adequar a administração pública quanto às boas práticas de governança nas áreas de TI e SI, levantando a questão das vulnerabilidades do fator humano na gestão de informações da municipalidade.

Este projeto justifica-se por se tratar de um problema comum tanto em empresas privadas como na administração pública a falta de clareza quanto aos riscos envolvidos na manipulação da informação, e por consequência, a falta de organização, estratégias e objetivos relativos à segurança desta. A desorganização e o desperdício de recursos, como nas organizações privadas, levantam questionamentos sobre a vantagem de se arcar com os custos relativos à TI. Por isto, este trabalho proporá um primeiro passo para o caminho da adequação às melhores práticas de SI, buscando convencer as lideranças sobre a importância de se tratar a informação de maneira madura, estabelecendo metas, objetivos, responsabilidades, políticas, limites, procedimentos, e uso consciente dos recursos de TI.

Acerca da metodologia, este trabalho se utilizará do método descritivo, adotando um modelo de estudo de caso em sua investigação, elaborando e aplicando questionários e partindo das recomendações de melhores práticas de gestão de riscos baseadas na norma ABNT NBR ISO/IEC 27005:2011, embora sem aprofundar na norma.

No tocante à natureza da pesquisa, este trabalho adotará uma natureza de pesquisa aplicada. A finalidade desta escolha é gerar conhecimento para que se aplique na prática, dentro da organização, um conjunto de soluções aos problemas que ela pode apresentar.

Referente ao tipo de pesquisa, seguirá uma abordagem de estudo de caso, levantando fenômenos particulares reais do objeto de estudo. Neste trabalho serão abordados dados a partir de documentos, entrevistas e coletas de informações junto aos usuários de recursos de TI do Paço da prefeitura que será objeto de estudo.

O procedimento adotado será o de pesquisa analítica. Este trabalho fará uso de material primário, colhido junto aos administradores e usuários dos serviços de TI da organização, e se aprofundará em sua análise por meio de artigos científicos e livros dentro dos assuntos aqui refletidos.

CAPÍTULO 1 - DEFININDO A SI

Para que se faça claro o que trataremos aqui, precisamos antes de tudo estabelecer alguns conceitos utilizados para a conceituação de SI.

1.1. Glossário

1.1.1. Plano de Negócios

Segundo a cartilha "Como elaborar um plano de negócios" do Sebrae (Serviço Brasileiro de Apoio às Micro e Pequenas Empresas) "um plano de negócios é um documento que descreve por escrito os objetivos de um negócio e quais passos devem ser dados para que esses objetivos sejam alcançados, diminuindo os riscos e as incertezas. Um plano de negócio permite identificar e restringir seus erros no papel, em vez de cometê-los no mercado" (2013, p. 13). Em suma, a finalidade do Plano de Negócios é validar uma ideia, servir de instrumento para contenção de riscos, permitindo ao empreendedor definir seus objetivos estrategicamente e traçar táticas para alcançá-los. Ora, no escopo da SI, o plano de negócio direciona, por meio da gestão de T.I. os investimentos que deverão ser feitos na proteção da informação.

1.1.2. Ativo

Ativos são os bens, recursos e direitos que uma organização dispõe. Ativo é todo bem tangível ou intangível[1] de que dispõe uma organização e pode ser reclamado como um direito. A norma ABNT NBR ISO/IEC 17799 define ainda vários outros tipos, como serviços, ativos físicos, ativos de software, ativos de informação, e recursos humanos. Assim, um ativo físico como um Servidor de Bancos de Dados ou um recurso intelectual, como um código de um sistema são ambos ativos pertencentes ao seu proprietário/autor.

1 . De acordo com Hoss *et al*. (2010, p. 1) "a palavra intangível vem do latim tangere, ou tocar. Os bens intangíveis, portanto, são bens que não podem ser tocados porque não têm corpo".

Também é um ativo o intangível que representa a imagem e a reputação da organização (ABNT, 2005, p. 21).

Um ativo “possui esta denominação oriunda da área financeira, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada” (SÊMOLA, 2006, p. 45).

1.1.3. Ameaças

Ameaça é um evento potencialmente nocivo a um ativo. Sêmola define a ameaça como:

> Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confiabilidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização (2006, p. 47).

Em outras palavras, trata-se de um acontecimento ou atitude indesejável, que represente o rompimento com o desenvolvimento do plano de negócio da organização. Edson Kowask Bezerra, da Escola Superior de Redes, em seu “Gestão de riscos de TI – NBR 27005” detalha a natureza das ameaças. Para ele as ameaças podem ser intencionais, por ação da natureza ou ainda não intencionais. E dá exemplos de ameaças:

- Erros humanos;
- Falhas de hardware;
- Falhas de software;
- Ações da natureza;
- Terrorismo;
- Vandalismo, entre outras (BEZERRA, 2013, p. 3).

PEIXOTO (2006) nos dá ainda a seguinte lista de ameças possíveis, capazes de explorar vulnerabilidades e comprometer um ambiente corporativo:

- Física: infraestrutura precária e/ou mal planejada;
- Naturais: equipamentos com danos decorrentes de fenômenos
- Hardware: equipamento obsoleto, mal utilizado ou desgastado;
- Software: erros de instalação, configuração, falta de atualizações,uso indevido por desconhecimento;
- Mídias: dispositivos de armazenamento que podem ser danificados ou não possuem um local seguro para serem guardados;
- Comunicação: escutas não autorizadas, perdas;
- Humanas: ataques de engenheiros sociais, falta de treinamento e/ou conscientização, ausência de Políticas de Segurança, dentre outros (PEIXOTO, 2006, p. 43-44)

Podemos notar que, à exceção das ameaças naturais, conforme os autores citados, nas ameaças humanas temos duas possibilidades de ocorrência: as acidentais

e as intencionais (BEZERRA, 2013), provenientes de erros humanos, vandalismo e terrorismo, que se traduzem em acidentes por falta de treinamento ou conhecimento, ausência de políticas e ataques de Engenharia Social.

1.1.4. Vulnerabilidades

Vulnerabilidades são as fraquezas presentes nos ativos que os expõe a riscos. Refere-se à fragilidade dos ativos que pode ser explorada por ameaças (BEZERRA, 2013, p. 3), gerando um incidente de segurança. Sêmola define como:

> agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração da vulnerabilidades, provocando perda de confiabilidade, integridade e disponibilidade e, consequentemente, causando impacto nos negócios de uma organização (SÊMOLA, 2006, p. 48).

As vulnerabilidades abarcam inúmeros fatores, cada qual relativo ao seu ativo, especificamente para este trabalho consideremos como relevantes as vulnerabilidades dos aspectos humanos. Aqui temos um amplo campo para tratar, que vão das falhas de operação por incapacidade técnica, até a reação a insídia de pessoas mal intencionadas.

1.1.5. Riscos

Risco é a “probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios” (SÊMOLA, 2006, p. 50).

Segundo a norma ISO/IEC 27005, risco é o “efeito da incerteza nos objetivos” (ABNT, 2011, p. 17). A mesma norma define as medidas de proteção contra riscos para minimizar ou conter a probabilidade de exploração pelas ameaças. A estas medidas de proteção a norma dá o nome de controle (ABNT, 2011, p. 15).

1.1.6. Controles

Segundo a norma NBR ISO/IEC 27005, “controle é uma medida que altera um risco”(ABNT, 2011), adiciona, segundo a nota ISO GUIA 73 que

> os controles da segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, que pode ser de natureza administrativa, técnica, gerencial ou legal que modificam o risco da segurança da informação (ABNT, 2009).

Neste sentido, complementa Sêmola:

> São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidade, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma (2006, p. 49).

Ainda segundo a NBR ISO/IEC 27005, os controles são delineados como parte do processo de identificação de riscos a serem usados para evitar que tornem-se incidentes (ABNT, 2011). Portanto, controle é qualquer mecanismo administrativo, físico ou operacional, capaz de tratar os riscos de ocorrência de um incidente de segurança.

Assim tem a finalidade modificação do risco dentro das opções técnicas e orçamentárias feitas pelas organizações, são “ações tomadas para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco” (BEZERRA, 2013, p. 4) e pretendem reduzir os riscos a níveis aceitáveis (BEZERRA, 2013, p. 111).

Os tipos existentes de proteção são: correção, eliminação temporal, prevenção, minimização do impacto, detecção, recuperação, monitoramento, e conscientização (ABNT, 2011).

No entanto, é importante notar que aqui tratamos o termo como uma medida pró-ativa para salvaguardar uma vulnerabilidade, porém “nem sempre conseguem exercer o efeito de modificação pretendido ou presumido” (ISO 27005, 2011, p. 15), sendo muitas vezes um paliativo ou medida temporária até que se elimine o risco quer por um controle mais eficiente, quer pela eliminação total do risco por substituição do ativo. Tudo isto fica a cargo da organização determinar segundo o que pode dispender de recursos financeiros para garantir a proteção segundo o que entende por seus ativos mais valiosos (ISO 27005, 2011, p. 77). Na aplicação de um processo de Gestão de Riscos, tal definição de valor faz parte do processo de Definição de Contexto, e compreende todo o inventário de ativos e a Análise de Riscos.

No conceito de controle temos também os aspectos reativos, aos quais determinamos como Plano de Contingência, e consiste em controles aplicados após o sinistro, quando um incidente já ocorreu (ABNT, 2011).

1.1.7. Incidente

Sêmola afirma que é o “fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da SI: confidencialidade, integridade e disponibilidade” (2006, p. 50). Assim, um incidente é o evento em que um risco torna-se concreto, quando uma vulnerabilidade é efetivamente explorada por uma ameaça.

“Um incidente gera impactos aos processos de negócio” (SÊMOLA, 2006, p. 50) interrompendo a entrega de valor, isto é, os resultados que os clientes e usuários esperam dos serviços.

A análise de um incidente é feita em termos quantitativos e qualitativos (SÊMOLA, 2006, p. 50), por meio de uma variedade de ferramentas disponíveis, e sendo presumido pela probabilidade e medida pelo impacto.

1.1.8. Probabilidade

A ABNT ISO GUIA 73 define a probabilidade como a “(...) chance de algo acontecer, não importando se de forma definida, medida ou determinada ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (...)” (2009, p. 5).

Isto é, significa tão somente a chance de algo acontecer. Neste contexto, a chance de um risco tornar-se um incidente real..

1.1.9. Impacto

Impacto é a “mudança adversa no nível obtido dos objetivos de negócios. Consequência avaliada dos resultados com a ocorrência de um evento em particular, em que determinada vulnerabilidade foi explorada, uma ameaça ocorreu e o risco se concretizou (BEZERRA, 2013, p. 4).

Para sabermos o impacto da exploração de uma vulnerabilidade por uma ameaça precisamos responder algumas perguntas: “Qual foi o impacto deste evento nos negócios? Quanto se perdeu? A organização será responsabilizada? Haverá multas? Ações legais serão impetradas? Haverá danos de imagem?” (BEZERRA, 2013, p. 4). Isto

tudo representa danos causados sobre os ativos e têm consequências na entrega de valor.

A norma ABNT NBR ISO/IEC 27005 estabelece alguns pontos críticos a respeito deste elemento, e determina que “convém que os critérios de impacto sejam desenvolvidos e especificados em função do montante dos danos ou custos à organização, causados por um evento relacionado com a segurança da informação” (2011, p. 27). Uma vez que o risco se torna um incidente e gera um impacto ao negócio, temos uma geração de prejuízos que, embora abarquem várias questões de cunho distintos, reflete-se muitas vezes em perdas financeiras, como nos diz Bezerra: “Os critérios de impacto servem para mensurar o montante dos danos ou custos à organização causados pela ocorrência de um evento de SI. Geralmente estão relacionados a perdas financeiras” (2013, p. 28).

Para tanto, este autor ainda nos sugere que os critérios de impacto devem considerar os seguintes aspectos:

- O comprometimento das operações;
- O descumprimento de prazos;
- Os danos de reputação e imagem;
- Violações de requisitos legais e regulatórios;
- Severidade e criticidade;
- O comprometimento da confidencialidade, integridade e disponibilidade;
- Outros, de acordo com a organização e escopo (BEZERRA, 2013, p. 28-29).

Sendo assim, podemos citar como exemplos de impacto a interrupção de um processo produtivo de uma organização, por exemplo, por inoperância de centrais computadorizadas, afetando suas vendas e lucros; a paralisação de serviços essenciais, como abastecimento de energia elétrica; a perda de confiança, como ocorreria a um banco que permitisse vazamento de dados de cartão de seus clientes, entre outras possibilidades.

1.2. Contextualizando

Neste trabalho buscamos levantar informações sobre o contexto de SI da prefeitura do município estudado, analisar os riscos existentes, e propor caminhos para soluções dos problemas encontrados. Será tratado aqui o dito pilar humano da SI; porém, se faz necessário, para dar sustentação teórica a este aspecto disciplinar, tratarmos do

meio em que tal pilar se insere, para isto, contextualizando tanto os aspectos gerais da SI, como anelando explicar aspectos mais particulares, ora da Engenharia Social, ora da sociologia. Assim também se buscará reproduzir os tópicos mais relevantes para este fim presentes nos *frameworks* de SI da série ABNT ISO/IEC 27000, em específico aqueles conteúdos que mostrem ser adequados a oferecer um método de elaboração de planos de salvaguarda e proteção contra riscos e contingência para mitigação de vazamentos de informação, isto é, que se atentem mais aos planos tático-operacionais da governança – e aqui falamos mais especificamente da norma ABNT NBR ISO/IEC 27005.

No entanto, não apenas os aspectos gerenciais relativos à TI deverão ser tomados por sustentação teórica, mas, indo mais longe, lembraremos também dos aspectos de governo, para tanto necessitaremos entrar nos meandros da Governança de TI, e sua superior, a Governança Corporativa. É importante levar em consideração ainda estes aspectos, uma vez que este trabalho tem por objetivo prover uma visão parcial e inicial sobre o contexto de SI a que está sujeito seu objeto de estudo, e oferecer um caminho para elaborar um conjunto de boas práticas que possam ser usadas pela organização efetivamente, dentro das suas limitações.

Habitualmente, na SI, fala-se em tecnologias e processos, geralmente respaldados por planos gestores, estabelecidos pelo próprio departamento de TI das organizações. Em tempos atuais, com a definição cada vez mais clara do valor da informação, e a exposição ainda maior aos riscos provenientes sobretudo da internet, há uma crescente preocupação em definir melhores rumos para a SI.

A informação é o mais valioso ativo de que dispõem as organizações. Segundo a NBR ISO/IEC 27002 (ABNT, 2005, p. 9), a informação "é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida". Caruso e Steffen reforçam esta ideia:

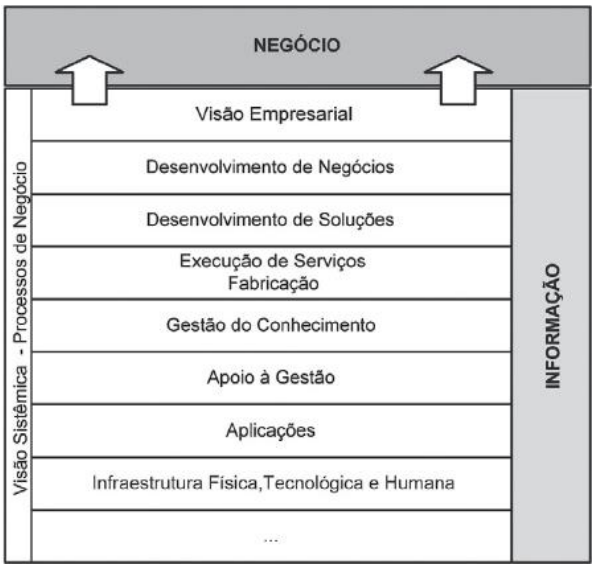
> (...)as informações envolvem os três fatores de produção tradicionais: capital, mão-de-obra e processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento físico-contábil que os outros ativos, do ponto de vista do negócio, elas são um ativo da empresa e, portanto, devem ser protegidas" (2006, p. 25).

Assim como a informação é um ativo importante ao negócio, ela não deve ser tratada exclusivamente como um aspecto informático e relegada ao completo controle do departamento de TI. Ademais, a NBR ISO/IEC 27005:2011 também versa que um ativo

é “qualquer elemento da organização que possui valor para o negócio e necessita ser protegido”.

Para Sêmola (2006, p. 2) a informação acompanha todos os ativos, e está ao lado de todos os processos de negócio, como exemplifica a figura 1:

Figura 1: Onipresença da informação nos principais processos de negócio



Fonte: (SÊMOLA, 2006, p. 2)

Podemos, assim, abstrair da imagem vários ativos, mas especificamente alguns que nos são mais pertinentes relacionados aos processos físicos (Infraestrutura), de gestão do conhecimento (Propriedade Intelectual), humanos, e de TI. A informação está em todos estes recursos e muitos mais, e podemos concluir enfim que é o mais importante elemento organizacional.

Para nos adiantarmos, notamos então que não estamos tratando somente de um aspecto de governo de TI, quiçá de sua gestão, mas de governo corporativo, daí a necessidade de se entender como a TI, em seus aspectos técnicos, deve estar em concordância e alinhamento ao plano de negócio da organização. Esta é a responsabilidade da Governança de TI, e a SI, por sua vez, deve prover todas as garantias possíveis para que o sangue da organização, isto é, a informação, nas palavras de Sêmola (2006), continue fluindo adequadamente.

Desdobrando a SI para seu foco no fator humano, saímos do campo técnico e passamos a tratar de áreas intimamente relacionada aos aspectos psicossociológicos do homem dentro das culturas organizacionais. O fator humano na Gestão de Riscos

também é parte da disciplina da Gestão de TI, e portanto está inserida no escopo da Governança de TI e, portanto, é subsidiária da Governança Corporativa (ABNT NBR/ISO 38500, 2009, p. 9). Assim, para tratarmos do assunto do Fator Humano na gestão da segurança dos sistemas de informação, precisamos antes de tudo dar algumas definições e localizá-lo neste meio.

1.3. Governança Corporativa

A Governança Corporativa diz respeito às estratégias gerais pelas quais as organizações são regidas e à forma a qual presta contas às partes interessadas em seus rumos. A governança rege os relacionamentos entre as partes interessadas no negócio e os processos, internos e externos, aos quais estão sujeitos. Isto envolve uma ampla gama de questões, desde políticas, legais, procedimentais, de relacionamentos interpessoais, até questões tecnológicas.

Para o Instituto Brasileiro de Governança Corporativa, a governança é o

> sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (IBGC, 2016, p. 20).

Isto significa que a Governança tem por objetivo propor estratégias e alavancar táticas que guiem as organizações para que convertam princípios em recomendações a fim de alinhar os interesses das partes envolvidas no negócio, otimizar o valor da organização, e facilitar seu acesso a recursos, contribuindo para a qualidade da gestão da organização (IBGC, 2016).

1.4. Governança de TI

A governança de TI é, por sua vez, a área da Governança Corporativa que se encarregará de alinhar os recursos de TI para atingir os fins almejados pelas partes interessadas no negócio. Para a NBR ISO/IEC 38500, a Governança de TI é o meio pelo qual o uso atual e futuro dos recursos de TI são dirigidos e controlados (ABNT, 2009, p. 3) e acrescenta: “(...) significa avaliar e direcionar o uso da TI para dar suporte à

organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização" (ABNT, 2005, p. 3).

Isto significa que a Governança de TI é o modo pelo qual o plano de negócios da organização é alcançado através de um alinhamento estratégico do departamento de TI aos rumos traçados na Governança Corporativa, por meio de processos e serviços que estejam pautados pelas boas práticas de governança.

As boas práticas, por sua vez, são aquelas que, como resultado de experiências empresariais e organizacionais já consagradas, se mostraram eficazes em estabelecer as diretrizes táticas dentro das organizações, a fim de alcançar os objetivos almejados pela administração, com o alinhamento do setor de TI ao plano de negócios e às perspectivas estratégicas. Estas boas práticas são as formas pelas quais a Governança se apresenta com recomendações para alcançar seus fins, e nas diferentes experiências geraram conjuntos distintos de práticas as quais, organizadas, deram origem aos chamados *frameworks* de governança.

Entre os mais populares e utilizados *frameworks* de governança estão as normas ISO, entre as quais está a série ISO 27000 das quais neste trabalho utilizaremos algumas como referencial, e das quais buscaremos obter as melhores práticas de gestão de riscos de SI, abordando essencialmente o aspecto humano da gestão de SI.

1.5. Segurança da Informação

Segundo a NBR ISO/IEC 27002, a SI consiste na preservação da confidencialidade, integridade e disponibilidade da informação. Mais especificamente, nos diz que a

> 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 (ABNT, 2005, p. x).

Ou seja, a SI tem, por fim, garantir a continuidade de negócios de uma organização através de controles adequados, se utilizando de políticas, processos e procedimentos, implementados, monitorados, e analisados criticamente (ABNT NBR ISO/IEC 27002, 2005, p. x).

Nos aspectos mais gerais, a gestão da SI constitui-se de um tríplice pilar formado pelas tecnologias empregadas, pelos processos, e pelas pessoas.

Uma vez que se entende que a informação não é um domínio computacional, mas que transcende todo o departamento de TI, e alcança os meios de suporte, isto é, todo o ambiente de informações (CARUSO; STEFFEN, 2006, p. 25), fica claro que passamos a lidar com um aspecto mais geral da informação.

Segundo a NBR ISO/IEC 27002,

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado (ABNT, 2005, p. 9).

Aqui não tratamos senão com aqueles responsáveis por fazer uso da tecnologia, bem como de todos os processos envolvidos, falamos claramente do fator humano. O usuário, em sua individualidade, com suas fraquezas, deve ser considerado um ativo da organização (PEIXOTO, 2006). Portanto, o ser humano é o fator que constitui o elo mais fraco da corrente da SI.

1.6. O tamanho do problema

De acordo com a teoria aristotélica, na concepção sobre o teleologismo, tudo o que há cumpre determinada função, ou seja, está destinado a um fim. Todos os direitos são exercidos em uma dimensão social, isto é, estão associados às relações humanas. O que cumpre uma função social é, portanto, aquilo que é designado a um fim para mediar as relações humanas.

O bem público cumpre uma função social, em sentido estrito, é a própria coisa pública, a serviço do bem comum, a justiça. Todo dano aos recursos públicos recaem necessariamente sobre toda a sociedade, uma vez que a coisa pública é de sujeição a todos. Trata-se de um desvio de finalidade, ou seja, de função social.

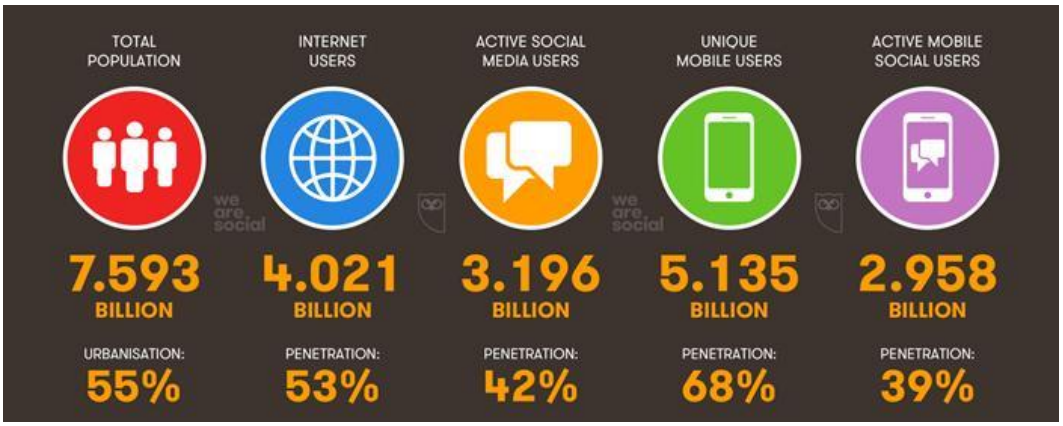
O problema com que trabalhamos, no sentido de riscos, ao passo que podem ser igualmente considerados para entidades públicas e privadas, tendem a ser agravadas na extensão dos danos causados segundo o alvo de uma ameaça. Ora, o mal causado a uma entidade privada é privado, embora, a depender do tamanho e da importância do

alvo para o bem comum, é diferente de um mal que é causado a uma entidade pública, cujos danos são socializados. Ainda se pode considerar a importância e as extensões dos danos e das organizações afligidas, certamente uma prefeitura de cidade interiorana não terá o impacto, na quebra de um ou mais dos pilares da SI, que terão os incidentes causados a uma grande organização privada cuja confiança de seus acionistas é crítica para a estabilidade econômica de todo um país. Este assunto, no entanto, sai do foco deste trabalho, e invade outros temas que poderiam ser explorados em outras pesquisas.

No entanto, mesmo quando voltado ao serviço público, os danos possíveis não se limitam àqueles causados à coisa pública e aos valores financeiros e estruturais decorrentes dela, mas estendem-se, outrossim, aos próprios cidadãos em seus direitos, e a valores ainda mais importantes, garantidos por nossa Constituição de 1988, que declara em seu artigo 5º, a privacidade, com a exposição de dados de documentos, endereço, registros de impostos; a integridade moral e da imagem, como decorrente do acesso indevido ao conteúdo de processos e requerimentos particulares, o uso de dados privados para abertura de empresas ou para gerar boletos para pagamentos falsos, por exemplo (SEBRAE, 2015); e até mesmo da propriedade, a depender das modificações possíveis, como acesso a projetos civis de construção, escrituras de imóveis, etc.

A internet ainda inicia sua disseminação. A TI, como a conhecemos atualmente, não tem muito mais que meio século de existência. Ainda assim, a conectividade global já alcança mais de 4 bilhões de pessoas no mundo todo de acordo com o relatório *Digital in* 2018, dos serviços *Hootsuite* e *We Are Social*. Assim, estamos em uma situação em que uma rede privada está acessível a todo este contingente populacional. Não apenas isto, todos os usuários de serviços *online* destas redes estão expostos. O mesmo relatório nos aponta que são cerca de 3,2 bilhões de usuários de redes sociais, ou seja, quase a metade da população mundial, compartilhando todo tipo de informação, e gerando um imenso volume de dados.

Figura 2 – *Digital around the world in* 2018



Fonte: (HOOTSUITE, 2018, p. 7)

Adicione a este fato a projeção de dispositivos conectados à internet para o ano de 2020 que será de 50 bilhões considerando a nova tendência da chamada Internet da Coisas (*IoT* na sigla em inglês). Não obstante já se discutia inicialmente a SI para estes dispositivos, não sabemos como será tratada a questão objetivamente, que só recentemente vem recebendo maior atenção de organizações (PROOF, 2017).

Esta imensa quantidade de dispositivos e pessoas conectadas à internet, com uma governança *online* que ainda se desenvolve, gera uma situação de quase anomia na rede mundial de computadores. Há um esforço de Governos, instituições, Empresas e pessoas para dar regras à internet, e resolver certas questões relacionadas sobretudo à privacidade, mas somente neste ano de 2018 entrou em vigor, na Europa, a chamada Lei Europeia de Proteção de Dados (UNIÃO EUROPEIA, 2018), e igualmente no Brasil foi sancionada sua Lei de Proteção de Dados (BRASIL, 2018).

No entanto, por mais que se legisle, leis são eficazes para controlar organizações e demais pessoas que, de fato, se sujeitem a elas, mas não para barrar a totalidade dos criminosos virtuais. Para tanto, há de se estar preparado para viver em um mundo em que eles são a realidade.

Há inúmeros casos de incidentes sendo noticiados todos os dias, embora quase metade não seja relatada sabe-se que, segundo relatórios da Kaspersky Lab (2017), quase metade (46%) dos incidentes de segurança são causados por funcionários da própria organização, sendo que 38% são de ataques maliciosos direcionados por *insiders* numa forma de ataque que envolve o recrutamento destes por agentes externos (KASPERSKY LAB, 2016).

Há de se levar em consideração, no momento de se analisar os riscos, todas as relações possíveis entre ameaça e vulnerabilidades de ativos, em cada uma de suas nuances. Ora, estar preparado significa conhecer a si mesmo e às suas fraquezas, conhecer ao seu terreno, o contexto informacional, e seu inimigo, ou ao menos como eles podem agir.

1.7. Fatores humanos: insatisfação, ignorância e sedição

Quando tratamos de ameaças não naturais, a partir dos dados obtidos em nossa pesquisa, podemos separar em duas as formas possíveis de ocorrência: aquelas que levam em consideração os meios processuais e tecnológicos, foco dos chamados *hackers*, e aquelas quais são o foco deste trabalho, relacionadas ao fator humano, as pessoas, no que pode constar tanto ameças acidentais, quanto intencionais, e podem ser realizadas por ameças exteriores, os *outsiders,* ou internas, os *insiders*.

Sendo assim, as duas formas em que o interno da organização contribui para exploração de uma vulnerabilidade, gerando um incidente de segurança são, como dito, acidentais ou intencionais. Sendo acidental, pode ocorrer por ignorância e desconhecimento do melhor procedimento em um processo, pelo mau uso de uma tecnologia. Sendo intencional, pode envolver inúmeros fatores psicológicos que não podem ser tratados objetivamente, devendo ser analisado caso a caso, sendo possível à organização, somente tentar garantir ao menos a mínima satisfação de seu usuário pelo meio em que está.

Como vimos nos relatórios da Kaspersky Lab (2017), Os *insiders* são compostos tanto por atores acidentais, como por pessoas maliciosas. Porém, ainda de acordo com o relatório Kaspersky Lab (2016), vimos que, embora haja uma grande participação de *insiders* nas ameaças aos ativos, apenas uma pequena parcela é de fato maliciosa.

1.7.1. *Insiders* maliciosos

Quando falamos em recursos humanos incluímos nestes os aspectos psicossológicos que tratam de uma ampla gama de fatores de manutenção de satisfação e motivacionais e incluem, além de tudo, questões tão humanas quanto códigos

particulares de moral e psicologia comportamental. São muitos os fatores causadores de insatisfação para os funcionários de uma organização, levantados e tratados em inúmeros artigos e trabalhos acadêmicos. Se antigamente o trabalho era considerado degradante e desagradável, e para continuidade exigia-se estímulos positivos, como melhores condições de trabalho e ordenados em dia para que fosse efetuado, agindo assim apenas num aspecto neutro, chamado higiênico (CHIAVENATO, 2014, p. 333), em que o cumprimento apenas garante a não-insatisfação, hoje muitas organizações têm passado a oferecer condições especiais de trabalho e ambiente aos seus funcionários na tentativa de permitir a eles um maior controle sobre a atividade que desempenham, uma tentativa de garantir-lhes sua autorrealização, são os chamados fatores motivacionais e costumam afetar diretamente na produtividade, envolvendo sentimentos de crescimento individual, afetando diretamente a autoestima do colaborador (CHIAVENATO, 2014, p. 334).

Marisa Eboli, em seu livro “Educação Corporativa no Brasil: Mitos e verdades”, nos diz que “Parece inquestionável a relevância que as áreas de T&D (Treinamento e Desenvolvimento) estão adquirindo sobre as demais funções da gestão de pessoas. A migração do T&D tradicional para a educação corporativa ganhou foco e força estratégica, evidenciando-se como um dos pilares de uma gestão empresarial bem-sucedida” (EBOLI, 2004, p. 38).

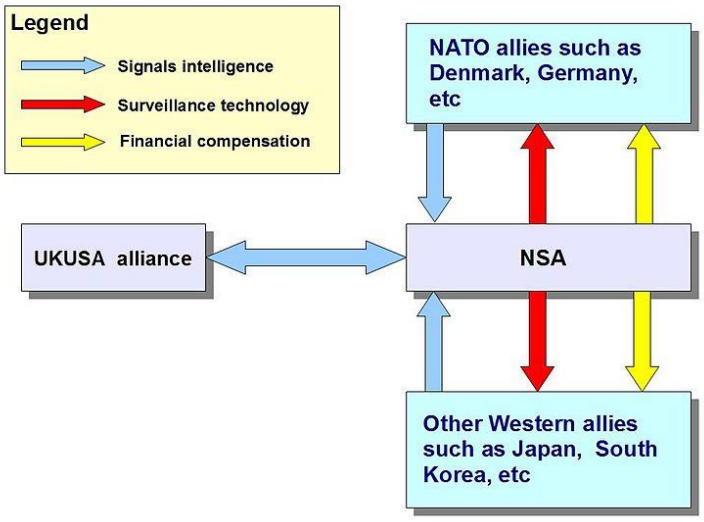
Ora, ainda assim, não se trata de prática disseminada, sobretudo no setor público, dada sua natureza burocraticamente engessada, a preocupação com a autorrealização e a autonomia do colaborador, ficando restrito à satisfação do fator motivacional ao “comportamento pró-social, lealdade e prazer com o trabalho, comprometimento com objetivos institucionais, senso de dever, de autonomia e responsabilidade de servir à sociedade e ao interesse público” (KLEIN; MASCARENHAS, 2015, p. 20). Desta forma fica claro que o fator da moralidade pessoal é que garante a integridade do colaborador do setor público. Ora, quando tal moralidade não supre a necessidade dos fatores higiênicos, ou quando é confrontada, temos uma situação de insatisfação no trabalho. Podemos considerar que isto é um dos motivos responsáveis pelos chamados *insiders* em seu aspecto malicioso.

É necessário considerar o fator humano como variável ao se elaborar a gestão de riscos da SI. Pessoas podem ser as maiores aliadas da organização, por toda sua disposição e criatividade na hora de pensar soluções, porém, podem se tornar ameaças à SI, pela mesma disposição e criatividade.

Algumas ações possíveis de *insiders* dentro das organizações incluem, tais como furto de dados para usos particulares, uso indevido de recursos para ganho de privilégios, vazamento de dados para terceiros entre outros; e as motivações podem incluir desde a mera vingança por alguma sanção sofrida, como os ganhos financeiros, motivações morais e político-ideológicas, ou curiosidade e o desejo de aventurar-se, entre outras possibilidades.

Um famoso caso de atuação de *insider* ocorreu em 2013. Um técnico terceirizado trabalhando a serviço da NSA e da CIA dos Estados Unidos da América, foi o responsável por tornar público o maior esquema de vigilância social e espionagem por um Estado até então visto. Seu nome é Edward Snowden, e tão logo o vazamento se tornou público, não demorou para que se tornasse um inimigo nacional e passasse a ser caçado pelas autoridades signatárias do "Tratado de Segurança UK-USA", tendo Snowden escapado de sua nação a fim de evitar sanções.

Figura 3: Relação entre a NSA e as chamadas "segundas" e "terceiras" partes



Fonte: (WIKIMEDIA COMMONS, 2013)

O esquema denunciado incluía vários programas secretos que o compunham. Esta rede veio a ser chamada Echelon (LIECHFIELD, 2000), liderada pelos Estados

Unidos da América. na figura da NSA, e composto pelos demais países do Tratado, as "segundas partes", principais países da *Commonwealth* de Nações do Reino Unido (Canadá, Austrália e Nova Zelândia) e as "terceiras partes", membros da OTAN e aliados do Ocidente, exemplificado no diagrama da Figura 3, logo acima.

O Tratado, em si, existe desde a Segunda Guerra Mundial, com seu desenvolvimento ao longo da Guerra-fria (ESTADOS UNIDOS DA AMÉRICA, 1940-1961), mas foi após os ataques de 11 de setembro de 2001, que passou a atuar de forma mais ostensiva, espionando a todos os cidadãos americanos, como relatado por William Binney, no documentário *Citizenfour* de Laura Poitras (2014), para levar adiante a chamada "Guerra ao Terror".

Um dos programas que compunham o *Echelon* tinha a finalidade de filtrar metadados de serviços *web* fornecidos por empresas como Apple, Facebook, Google, Yahoo! e Microsoft. Este programa fora conhecido com Prism, em "alusão ao prisma, um sólido transparente utilizado em Redes de Computadores para separar os feixes de luz em conteúdos diferentes, tais como vídeo, voz e imagem" (LOPES, 2015, p. 262).

A ação de Snowden revelou este enorme programa de espionagem, e criou uma situação de tensão para as relações internacionais dos Estados Unidos, gerando protestos por parte de países espionados, entre eles o Brasil (PORTAL G1, 2013).

As motivações de Snowden, de certa forma, podem ser obtidas a partir de suas próprias palavras, nas comunicações trocadas com a documentarista Laura Poitras. Em um de seus *e-mails*, Snowden alega "Estamos construindo a maior arma de opressão na história da humanidade, e os seus responsáveis se isentam de responsabilidade. O diretor da *NSA* Keith Alexander mentiu ao congresso, o que eu posso provar"[2]. Adicione a isto sua declaração ao periódico *South Chine Morning Post* em que confessa ter buscado uma vaga na Booz Allen Hamilton, a empresa terceirizada que prestava serviço técnico à NSA, com a finalidade de conseguir evidências sobre atividades de espionagem do governo estadunidense (LAM, 2013). Assim, temos uma situação de infiltração premeditada a fim de se vazar dados de uma organização. Não entraremos aqui nos

2 "We are building the greatest weapon for oppression in the history of man, yet its directors exempt themselves from accountability. NSA director Keith Alexander lied to congress, which I can prove" *Tradução nossa!* (WIRED, 2013).

méritos das partes envolvidas, nos aspectos constitucionais do governo dos Estados Unidos da América, se se permitiria ou não que a agência agisse desta maneira, mas fica clara a motivação político-ideológica de Snowden.

Em suma, esta variável do fator humano exige que se considere na estratégia de elaboração de controles, respostas às necessidades psicossociais dos funcionários da organização, bem como que se adote meios tecnológicos como ferramentas de monitoramento e controle de uso de recursos de TI, embora estas sejam insuficientes (MITNICK; SIMON, 2003, p. 7), e segurança física do ambiente, como sistemas de vigilância, para dificultar o acesso e vazamento de informações; além de campanhas que visem trabalhar a lealdade do funcionário. Também é necessário atenção da equipe responsável pela segurança de TI aos aspectos comportamentais dos usuários, com análises psicossociológicas, pesquisas constantes e observação de contexto (BADDELEY, 2010).

A importância do fator no setor público, no entanto, pode depender do tamanho da cidade administrada, e dos interesses envolvidos. Ataques de Engenharia Social podem ocorrer independentemente disto, e basta o desejo de aventurar-se de um hacker para explorar esta modalidade de crime. A depender do tamanho dos interesses envolvidos, sejam políticos ou financeiros, o envolvimento de grandes organizações criminosas pode ser possível, embora não seja possível verificar de fato que isto está acontecendo atualmente. Apesar de tudo, conforme dados obtidos em nossas pesquisas, as prefeituras ainda não são alvos preferenciais de ataques. Poder-se-ia dizer que estão sujeitas mais a ataques eventuais para exploração financeira por meio de sequestro de dados, ou ataques políticos locais, que aos grandes ataques coordenados. No entanto, ainda são possíveis ataque de criminosos comuns e isto de qualquer forma demanda cuidado com a segurança. Identificar todos os ataques em tempo real e responder às ameaças de forma efetiva é tarefa quase impossível, mas há diversos processos que podem ajudar a melhorar a eficiência da segurança da TI.

Neste trabalho não trataremos de buscar conhecer as teorias que embasam as motivações e insatisfações dos usuários de TI da organização. As motivações dos *insiders* maliciosos no contexto da SI podem ser o tema para uma pesquisa futura.

Exporemos agora a parcela maior dos *insiders*, os bem-intencionados, porém descuidados.

1.7.2. Uso negligente dos recursos

Outro dos aspectos que podem significar a exposição de um ativo a um risco, ou fraqueza nos processos de SI, é o mau uso dos recursos. A negligência, imperícia, falta de instrução e o desconhecimento técnico com o trabalho estão entre as maiores causas de exposição ou perda de informação. Como vimos anteriormente, mais da metade dos incidentes de informação, são causados por usuários de recursos de TI mal preparados para lidar com a tecnologia (IBM, 2017).

Em geral, os desafios de gestão de TI no setor público são semelhantes aos da iniciativa privada, e estão sujeitos às mesmas circunstâncias às quais estes estão sujeitos. A evolução das tecnologias, têm exigido adaptação de todos, porém, um plano de governança de TI é essencial para que as atualizações necessárias acompanhem o ritmo de mudanças no desenvolvimento da tecnologia. No entanto, até mesmo a iniciativa privada, mesmo dispondo de menor burocracia, e podendo tomar decisões que demandem respostas a um número menor de partes interessadas, tem dificuldades em se adaptar.

Em nossa pesquisa, encontramos uma vasta bibliografia a respeito das dificuldades enfrentadas pelo poder público municipal em adaptar-se às evoluções tecnológicas. Podemos citar, por exemplo, Sousa (2013), no artigo “A gestão da TI dentro do serviço público” para o X SEGeT (Simposio de Excelência em Gestão e Tecnologia), e também Oliveira, Cunha e Sausen (2013), no artigo “A mudança organizacional em uma administração pública por meio de um processo de informatização da gestão” para o IV Seminário Internacional sobre Desenvolvimento Regional, sobre a resistência interna ao processo de informatização. No entanto, por não ser objeto de nossa análise apenas consideraremos as informações seguintes.

Disto decorre a dificuldade em dar ao usuário o treinamento e instrução de uso adequado das ferramentas que possui, bem como de programas de conscientização para lidar com pessoas maliciosas.

Assim, como nos sugere Mitnick e Simon (2003) para evitar que acidentalmente o usuário de recursos de TI se torne a ameaça aos ativos, serão necessários programas de capacitação e conscientização. Capacitação para uso correto de recursos lógicos e físicos, conscientização sobre segurança lógica e física, já que muito mais do que uma inabilidade técnica para uso de sistemas de informação, há também as fraquezas ou condições humanas que tornam o usuário uma potencial vítima de exploração pelos fatores de ameaças externos à organização, os chamados engenheiros sociais.

1.7.3. Agentes externos e a Engenharia Social

Aos riscos exteriores a serem considerados nos aspectos humanos temos a Engenharia Social. Quando o inimigo é exterior à organização e não possui meios tecnológicos para explorar seu alvo, se valerá de técnicas que explorem o elo que está mais diretamente à sua disposição, que são as pessoas e suas fraquezas. Segundo o Relatório da Internet Society (2016) o fator humano é o meio mais fácil de se quebrar o tripé da SI.

As técnicas que uma ameaça exterior a uma organização dispõe para buscar vulnerabilidades em um sistema de informação de uma organização alvo da qual não tem os meios tecnológicos para explorar, compõe um conjunto de métodos que se convencionou chamar Engenharia Social. Podemos separar a convenção nas palavras que a compõe e tentar o explicar cada palavra ao seu modo, e daí formar um conceito.

Engenharia é a

> arte de aplicar conhecimentos científicos e empíricos e certas habilitações específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao entendimento das necessidades humanas (FERREIRA, 1995, 687p. *apud* PEIXOTO, 2006, p. 4)

Social, por sua vez, significa algo “da sociedade, ou relativo a ela. Sociável. Que interessa à sociedade” (FERREIRA, 1995, 687p. *apud* PEIXOTO, 2006, p. 4)

Compondo livremente, Engenharia Social, conforme dados obtidos, é a arte de aplicar conhecimentos específicos a fim de se produzir formas à sociedade. Noções semelhantes existem na psicologia, na sociologia e na ciência política, onde são definidas por inúmeros autores. Tratamos aqui do chamado construtivismo. Ora, iniciou-se o construtivismo no entendimento da psicologia, por Thorndike (1905), com contribuições

de John B. Watson, com o condicionamento clássico, e B. F. Skinner, com o condicionamento operante, o que deu origem à chamada escola behaviorista, ou comportamental, de psicologia.

A Escola Behaviorista nasce da psicologia científica, que expressou um ramo da psicologia que, se afastando do modelo especulativo de até então, se ocupava essencialmente um processo de aplicação de técnicas desenvolvidas pela Fisiologia em seu tempo a questões que ocuparam, por séculos os filósofos, a saber, a natureza da consciência e de seus processos, a percepção, a sensação, as emoções, em suma, os processos psicológicos (SAMPAIO, 2005, p. 371-372).

Segundo B. Skinner (2003) o comportamento humano é um reflexo do ambiente social ao qual o indivíduo está inserido, no qual este reage conforme os estímulos que recebe, e responde segundo reforços positivos ou negativos. Ora, estando associado ao ambiente, então temos que o comportamento humano é essencialmente social e insere-se em uma cultura, de onde decorre a conclusão de Skinner: "Nossa análise do ambiente social, entretanto, fornece uma explicação dos aspectos essenciais da cultura do esquema de referência de uma ciência natural" (SKINNER, 2003, p. 455). Ainda acrescenta: "No sentido mais amplo possível, a cultura na qual um indivíduo nasce se compõe de todas as variáveis que o afetam e que são dispostas por outras pessoas" (SKINNER, 2003, p. 455).

Notamos que a psicologia comportamental em Skinner se propõe a ser uma metodologia para uma ciência natural, segundo um modelo imanente[3], isto é, empirista. Tal método pretende tomar seu objeto de estudo de maneira isolada, identificar suas características e, por todo um ferramental, buscar meios de induzi-lo a uma resposta esperada.

Por tal natureza a escola comportamental da psicologia está na raiz do planejamento do comportamento, portanto da Engenharia Social. Os conceitos definidos por esta escola ainda são adotados em outras áreas do conhecimento, desde a educação até a ciência política, por meio da qual o conceito de Engenharia Social se faz presenteo,

3 "Pode-se dizer que as bases fundamentais que norteiam a obra de Skinner estão vinculadas a sua pretensão de fazer da Psicologia uma ciência e, para compreender essas bases filosóficas, precisamos identificar os modelos de ciência que ele adota" (MICHELETTO, 2001, p. 31 *apud* SAMPAIO, 2005, p. 372).

sobretudo quando se fala em planejamento estatal da sociedade. Neste ponto também alimentou a análise crítica sobre o construtivismo político, isto é, a Engenharia Social aplicada ao planejamento da sociedade, por F. A. Hayek (GRAY, 1998).

Porém, ainda que não definida cientificamente antes dos nossos tempos, a Engenharia Social já existia como prática constante entre os seres humanos. Para Mitnick e Simon, também a sujeição dos filhos aos pais está condicionada a uma forma de Engenharia Social que molda o caráter dos filhos. Dizem os autores:

> Cada leitor terá sido manipulado pelos maiores especialistas de todos os tempos da Engenharia Social — seus pais." Eles encontraram maneiras de fazer com que você — "para o seu próprio bem" — fizesse aquilo que achavam ser o melhor (MITNICK; SIMON, 2003, p. 9).

É possível notar que, para estes autores, a Engenharia Social, portanto, tem uma finalidade de condicionamento e persuasão. E continuam:

> Os pais tornam-se os grandes contadores de histórias da mesma forma que os engenheiros sociais desenvolvem com habilidade cada uma das histórias plausíveis, dos motivos e das justificativas para atingir seus objetivos. Sim, todos fomos moldados por nossos pais: benevolentes (e, às vezes,nem tanto) engenheiros sociais (MITNICK; SIMON, 2003, p. 9).

Assim, vemos que o caráter da Engenharia Social é essencialmente relacionado ao poder. No século XVI, durante a Renascença na península itálica, Maquiavel foi, se não o primeiro, o mais notável dos estrategistas políticos. Em sua obra "O Príncipe", traça uma série de recomendações às elites nobiliárquicas para auxiliá-las nos assuntos de poder, ora determinando quais seriam as características mais notáveis a um soberano para conquistar a lealdade de seus súditos, ora como se portar em assuntos de guerra e ocupação de territórios conquistados (MAQUIAVEL, 2010). Uma forma de Engenharia Social, embrionária, é verdade, mas que viria no futuro a servir de inspiração para o desenvolvimento da teoria política moderna (GRAMSCI, 2004).

Embora se relacionem os conceitos, a definição sociológica não nos é suficiente. A definição ao tema que tratamos aqui tomamos de maneira bastante específica, não como uma metodologia, mas como uma ação específica tomada pelo engenheiro social. No entanto, seu caráter de busca de poder, mantém-se.

Poder é, em essência, a possibilidade de agir conforme o arbítrio, isto é, agir sem ser questionado, exercendo sua soberania e, no sentido sociológico, impondo sua vontade sobre os outros. A palavra poder vem do latim *possum* que significa "ter permissão ou autorização para", "ter capacidade de", "ter autoridade para tomar uma

decisão"[4]. Conclui-se, assim, que o engenheiro social busca se passar por alguém que possui certa soberania, autorizada a algum fim, sendo este fim orientado, claramente, a obter vantagem a partir desta situação.

Segundo Malcolm Allen, no *paper Social Engineering: A Means To Violate A Computer System* da *SANS Institute*, a Engenharia Social segue um ciclo de quatro passos:

> - Aquisição de Informação: o atacante busca informações de seu alvo, lançado mão de uma variedade de técnicas e recursos. Uma vez que tenha informações suficientes, passa para o passo seguinte, onde buscará iniciar uma relação com a vítima;
> - Desenvolvimento de Relações: é essencial que a vítima tenha certa importância para o sucesso do ataque. O agressor cria um vínculo de confiança com a vítima, para explora sua boa vontade;
> - A execução da relação: uma vez estabelecida a relação e conquistada a confiança da vítima, o atacante buscará manipular sua vítima a fim de obter as informações que necessita, como usuários e senhas.
> - A exploração da vulnerabilidade: uma vez completos os passos anteriores, e em posse de todas as informações e dados que necessita, o atacante poderá explorar seu alvo (ALLEN, 2007, p. 5).

O comportamento humano é o centro das atenções quando tratamos da Engenharia Social. Compreender este aspecto humano é essencial para entender as motivações, como já abordamos anteriormente. Há inúmeras motivações possíveis, e cabe à equipe responsável pela SI conhecer estas possibilidades. Ainda Malcolm Allen nos dá alguns exemplos diretos destas possibilidades: ganhos financeiros; interesses particulares; vingança; ou pressão externa (ALLEN, 2007, p. 6). Podemos ainda considerar como fatores motivacionais para ataques de Engenharia Social aqueles relacionados a motivações políticas e ideológicas, e aqui entramos num campo mais a fim com o setor público.

Certamente, o mais famoso Engenheiro Social é o especialista em segurança Kevin Mitnick. Desde a juventude, ainda nos anos 1970, já mostrava sua malícia e curiosidade por invasões, tendo acedido aos computadores de sua escola onde ficavam armazenadas as notas, alterando-as.

Seu debut como engenheiro social se deu ao invadir as instalações da empresa *Pacific Bell* a fim de roubar manuais técnicos de telefonia, um exemplo do chamado

4 "po·der vtd 1 Ter permissão ou autorização para. vtd 3 Ter capacidade de. Vtd 11 Ter autoridade para tomar uma decisão. Sm 4 Imposição de obediência. 6 Grande influência. 7 Domínio exercido sobre algo. 8 Total superioridade para governar" (MICHAELIS, 2018).

dumpster diving, intento do qual acabou capturado - devido a sua idade à época, 17 anos, não pode ser punido. Em 1992, então considerado o hacker mais buscado dos Estados Unidos, após violar os termos de sua prisão condicional, devido à invasão aos sistemas da empresa de softwares DEC, em 1988, e ser novamente condenado, não se entrega às autoridades e dá-se início a uma intensa perseguição pelo FBI que duraria três anos.

Durante suas férias, em 1994, o especialista em segurança do Centro Nacional de Supercomputação em San Diego, na Califórnia, Tsutomu Shimomura, teve seu computador pessoal invadido. Após receber uma mensagem de Mitnick na caixa postal de seu telefone, acusando-se, com sua reputação e seu orgulho feridos, resolve juntar-se à caçada do hacker.

Após publicar a mensagem recebida na internet, e aguardar um novo contato, passa, junto ao FBI e a NSA, e com um monitoramento constante destes, a trabalhar em um meio de capturar Kevin Mitnick, até que, após um último contato, em 15 de fevereiro de 1995, e coma ligação rastreada, finalmente Shimomura consegue localizar o hacker, preso no estado da Carolina do Norte.

Após cumprir sua pena por cinco anos, passa à liberdade condicional – não deveria se aproximar de dispositivos tecnológicos até o ano de 2003, neste ano conseguiu uma permissão para escrever seu livro "A arte de Invadir", publicado no mesmo ano. Hoje é consultor de segurança, escreve artigos e ministra palestras sobre o tema por todo o mundo (LITTMAN, 1996).

Além de conhecer os aspectos motivacionais humanos, precisamos entender os meios pelos quais agem os engenheiros sociais, e aí entramos numa área de maior especialização, que tratam das técnicas utilizadas para se obter as vantagens indevidas. Algumas técnicas de Engenharia Social, obtidas por meio de Granger (2001), Elledge (2004), Manjak (2006) e Alexander (2016), além de documentos da |CERT.br (2012), são:

> - *Shoulder surfing* ou, literalmente, "surfar ombros", consiste em prestar atenção diretamente a informações sensíveis usadas pelo alvo, como digitar senhas, exibir informações na tela do computador, ou deixar anotações sobre a mesa.[5] O *shoulder surfing* não mais se limita à presença física do intruso. Esta técnica foi aprimorada com o advento tecnológico, sobretudo da imagem digital

5 "The term shoulder surfing refers to any direct observation of sensitive information such as individuals keying in passwords or PINs, the display of information on computer monitors, or simply personnel forms with SSNs left exposed on someone's desk." *Tradução nossa!* (MANJAK, 2006, p. 9, *In*.: SANS INSTITUTE, 2006)

(como por exemplo, o uso de equipamentos equipados com câmeras como celulares, que podem ser usados para se espionar).[6]

- *Eavesdroping* significa literalmente "ouvir". Segundo o *Glossary of Security Terms*, da *SANS Institute*, "é simplesmente ouvir uma conversa privada que pode revelar informações que possibilitem acesso a uma instalação ou rede"[7] No contexto da segurança da infomação, é definido como escutar conversas entre indivíduos associados a uma organização alvo. Em sua forma mais básica, trata-se de se manter próximo a uma conversa entre duas outras pessoas, embora na TI isto possa se estender ao uso de dispositivos de escuta e gravação remotos, incluindo a interceptação de chamadas telefônicas, transmissões de fax, e e-mails, transmissões de dados, escopo de dados e até mesmo escaneamento de rádio para comunicações móveis[8]
- *Dumpster diving* ou, literalmente, "revirar lixo", consiste em se aproveitar do fato que as pessoas dão pouca importância àquilo que descartam no lixo, muitas vezes podendo jogar informações confidenciais que podem ser facilmente acessadas pode alguém mal-intencionado. *Dumpster diving* é a arte de coletar informações (pré-*hacking*). É comum fazer esta pesquisa de forma a pré determinar o alvo e as melhores oportunidades de exploração (GRANGER, 2001, *In*.: SYMANTEC, 2001).
- *Hoaxing*, ou boato consiste em uma mensagem de conteúdo alarmante porém falso, utilizando-se de autoria forjada, geralmente de instituição, organização ou pessoa a quem se dá fé (CERT.br, 2012, p. 15), aproveitando-se do fato de que as informações da internet podem se propagar rapidamente, atingindo inúmeras pessoas em pouco tempo (CERT.br, 2012, p. 2), para influenciar comportamentos. *Online* ocorre por meio de *spam*, e pode ser encaminhados acompanhando *softwares* de códigos maliciosos, pode ainda visar espalhar desinformação ou comprometer a reputação de organizações e pessoas entre outros (CERT.br, 2012, p. 15).
- *Impersonation*, ou, na expressão latina "quid pro quo", significa literalmente "tomar uma coisa por outra". Consiste numa pessoa que se faz passar por outra, geralmente alguém da área de TI, oferecendo ao alvo alguma assistência em troca de acesso ao seu equipamento, no qual poderá, por exemplo, instalar um *malware* (ALEXANDER, 2016 In. SANS INSTITUTE, 2016).
- *Pretexting* consiste em uma técnica em que o atacante cria um pretexto ou fabrica um cenário que pode utilizar para tentar furtar as informações privadas de suas vítimas.[9]

6 "Shoulder surfing is no longer limited by the physical presence of the intruder. This technique has been significantly enhanced with the advent of digital imaging using charged coupling devices (CCDs) (RW, what is a CCD? Use it in full with the acronym after then you can use the acronyms safely.) and cell phones equipped with photographic capabilities" *Tradução nossa!* (MANJAK, 2006, p. 9, *In*.: SANS INSTITUTE, 2006)

7 "Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network" *Tradução nossa! Glossary of Security Terms: Easvesdroping* (SANS, 2018)

8 "Eavesdropping in the context of information security is defined as listening in on conversations among individuals associated with the target organization. In its most basic form, it amounts to one person keeping within earshot of a conversation between two other persons, but in the security and IT worlds it extends to remote listening and recording devices, including the interception of telephone calls, fax transmissions, e-mails, data transmissions, data-scoping, and even radio scanning for mobile communications." *Tradução nossa!* (MANJAK, 2006, *In*.: SANS INSTITUTE, 2006)

9 "Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information." *Tradução nossa!* (ALEXANDER, 2016, *In*.: SANS INSTITUTE, 2016.).

> - *Tailgating* consiste num ataque que envolve uma pessoa não autorizada seguir um funcionário ou outra pessoa autorizada para conseguir acesso a um local restrito.[10]
> - *Phishing* é um termo usado para descrever várias armadilhas envolvendo principalmente mensagens de *e-mail* fraudulentas enviadas pelos criminosos a fim de enganar suas vítimas, fazendo-as ceder suas informações pessoais. Os criminosos usam estas informações para roubar sua identidade, contas de banco, ou tomar controle de seu computador pessoal. [11]
> - *Baiting* é, em muitos aspectos, similar ao *phishing*, no entanto, o que os distingue é a oferta de algum bem ou item para atrair a atenção da vítima, como o *download* gratuito de uma música ou um filme caso cedam login e senha para algum site ou aplicativo. [12]
> - *Reverse Social Engineering (RSE),* em português Engenharia Social inversa, consiste no atacante induzir a vítima a uma posição em que necessite de sua ajuda, uma vez identificado como alguém capaz de resolver o problema do alvo. Ocorre em três etapas: a) Sabotagem: Tendo acesso ao ambiente, o atacante forja alguma situação de erro, corrompendo a estação de trabalho ou fazendo parecer que há problemas nesta, ou quaisquer situações semelhantes, a fim de induzir a vítima a recorrer a si, fazendo o usuário do sistema descobrir o problema procurar ajuda. b) Propaganda: a fim de garantir que o agressor recorra ao engenheiro social, o engenheiro social se apresenta como quem é capaz de resolver possíveis problemas, inclusive o problema forjado. c) Auxílio: finalmente o engenheiro social ajuda a vítima com o problema, garantindo que a vítima não suspeite de nada, e obtendo as informações desejadas.[13] (ALLEN, 2007, p. 7, *In*.: SANS INSTITUTE, 2007).

São muitas as técnicas disponíveis para Engenharia Social, e elas dispõem enormemente dos aspectos psicológicos e comportamentais dos seres humanos, e a aliança entre a criatividade do engenheiro social e seus conhecimentos técnicos sobre

10 "This type of attack involves an unauthorized individual following an employee or other authorized individual into a restricted area." *Tradução nossa!* (ALEXANDER, 2016, *In*.: SANS INSTITUTE, 2016).

11 Phishing, also known as "brand spoofing" or "carding", is a term used to describe various scams that use (primarily) fraudulent e-mail messages, sent by criminals, to trick you into divulging personal information. The criminals use this information to steal your identity, rob your bank account, or take over your computer. *Tradução nossa!* (ELLEDGE, 2004, p. 2, *In*.: SANS INSTITUTE, 2007).

12 Baiting is in many ways similar to phishing attacks. However, what distinguishes baiting from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads if they provide their login credentials to a certain application or website. *Tradução nossa!* (DeWolf, 2013 *apud* ALEXANDER, 2016, p. 9, *In*.: SANS INSTITUTE, 2016).

13 "Reverse Social Engineering (RSE): a legitimate user is enticed to ask the aggressor questions to obtain information. With this approach, the aggressor is perceived as being of higher seniority than the legitimate user who is actually the target. A typical RSE attack involves three parts:

a) Sabotage: after gaining simple access, the aggressor either corrupts the workstation or gives it an appearance of being corrupted. The user of the system discovers the problem and tries to seek help;

b) Marketing: in order to ensure the user calls the aggressor, the aggressor must advertise. The aggressor can do this by either leaving his business cards around the target's office and/or by placing his contact number on the error message itself;

c) Support: finally, the aggressor would assist with the problem, ensuring that the user remains unsuspicious while the aggressor obtains the required information" *Tradução nossa!* (Cf. ALLEN, 2007, p. 7, *In*.: SANS INSTITUTE, 2007).

as fraquezas de seu alvo são essenciais para explorar estes aspectos, tal qual ocorre com aqueles especialistas em tecnologia chamados *hacker*.

Importante notar, no entanto, que, de acordo com Peixoto (2006, p. 17), a distinção entre um *Hacker* e um Engenheiro Social se dá por aquele agir sobre vulnerabilidades técnicas, enquanto este atua sobre vulnerabilidades humanas. Porém, várias das técnicas de Engenharia Social, quando necessário dispor de equipamentos, muitas vezes, no entanto, demandam conhecimentos tecnológicos, embora isto não seja uma regra.

Enfim, quando entramos especificamente no campo da ação humana, lidamos com inúmeros fatores que direcionam as inteligências, vontades, comportamentos e demais aspectos psíquicos, morais e sociológicos, e isto nos força a olhar para todas as subdisciplinas que se relacionam a estes temas dentro da administração e gestão de uma organização. Isto significa que um grande foco deve ser dado ao ponto crítico do tripé da gestão de SI, os seres humanos (MITNICK, 2003), a fim de se conhecer e neutralizar as vulnerabilidades e minimizar os riscos, e isto envolve necessariamente uma equipe que envolva todos as áreas de interesse do negócio, e que considere no estabelecimento de políticas de SI, uma vez que a SI é um domínio multidisciplinar das ciências sociais (MARCIANO, 2006).

1.8. A Gestão de Riscos

Ao tratar de gestão de riscos precisamos levar em consideração as incertezas: “nas fases do ciclo de vida de qualquer atividade humana planejada, convivemos com duas certezas básicas: daquilo que deve acontecer (os objetivos) e o que pode acontecer (as incertezas)” (BEZERRA, 2013, p. 1). Estas incertezas envolvem os ativos e as ameaças circundantes a estes, e devem ser considerados ao se desenvolver o plano de negócio – e daí a importância dada pela Governança de TI, de tornar a informática como um departamento estratégico da organização –, e determinar como estes riscos podem ser eliminados, reduzidos ou contingenciados.

Um risco nem sempre é óbvio e claro em qualquer situação. Para evitar que ele seja explorado por uma ameaça antes que identificado pelo detentor do ativo é

necessário uma política ostensiva para sua identificação, e assim dispor de metodologias e modelos de análise que permitam ao gestor de SI, identificar, quantificar e qualificar seus ativos quanto às suas vulnerabilidades e controles. Na Análise e Gestão de Riscos de SI inclui-se uma vasta gama de ferramentas e recursos, para se alcançar o conhecimento dos riscos, algumas oferecendo ciclos de vida completos para o seu tratamento, como é o caso ABNT NBR ISO/IEC 27005:2011. Cabe às organizações implementarem, segundo suas particularidades, as ferramentas necessárias para adaptarem-se a um modelo de gestão de riscos.

A Gestão de Riscos é um processo cíclico que se retroalimenta. Exige constante atualização, tanto devido às trocas dos ativos quanto pela descoberta de novas vulnerabilidades que se fazem públicas. Segundo a norma ISO 27005, a Gestão de Riscos é conjunto de “atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos” (ABNT, 2011, p. 19).

Bezerra, neste sentido, complementa

> A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho, referente à segurança e saúde das pessoas, à conformidade legal e regulatória,à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação (2013, p. 5).

Neste contexto tratamos da Gestão de Riscos relacionados à informação. Embora o conceito abarque todos os ativos da organização, não o tratemos de maneira que saia deste aspecto informacional, desconsideremos, portanto, outras possibilidades de riscos, como por exemplo, os laborais, exceto quando associados à informação. Como já vimos, quando tratamos da gestão de segurança na TI, orientamos ela para a governança de TI, cuja finalidade é conformar o departamento de TI aos planos de negócio traçados pela organização, e considerar todos os aspectos organizacionais, tornando a informática parte estrutural de todos os negócios internos, assim como a informação está em todos os processos e ativos (SÊMOLA, 2006).

CAPÍTULO 2 - DIMENSÕES PREVENTIVAS

Embora não seja do interesse deste trabalho explorar profundamente a norma ISO/IEC 27005, é possível obter dela um itinerário adequado para uma análise e avaliação de riscos preliminar, para os fins a que este trabalho de graduação se destina, e aplicá-lo ao pilar do fator humano na gestão de SI de nosso objeto de estudos. Pretendemos, outrossim, oferecer uma visão de um ciclo completo de gestão de riscos, e recomendá-lo como ferramenta a ser adotada em um processo mais minucioso de gestão de riscos.

2.1. ISO 27005: uma norma para gestão de riscos

A NBR ISO/IEC 27005 não estabelece métodos para realização do escopo, estabelecendo apenas um layout sobre o qual o processo de gestão de riscos se desenvolverá. Cabe ao realizador do ciclo de vida proposto por ela trabalhar neste ponto (ABNT, 2011, p. 26).

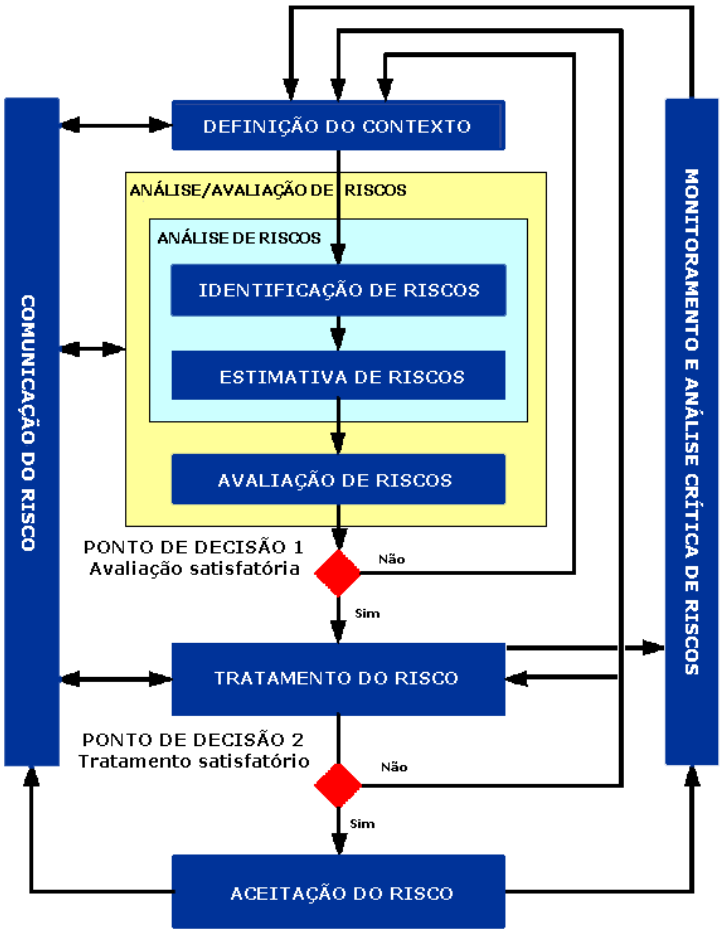
Como se trata de uma norma cuja finalidade é fornecer um processo de gestão de riscos de SI, não entra em detalhes normativos que poderiam desconsiderar as particularidades dos negócios. No entanto, fornece as diretrizes para o gerenciamento dos riscos de SI, e nos propõe um ciclo de vida para o processo de gestão de riscos, sustentando conceitos especificados na norma ISO/IEC 27001, norma de requisitos de sistemas de gestão da SI, a qual se faz necessária para adoção desta norma ISO 27005.

Nesta NBR ISO/IEC 27005, uma série de propostas nos é dada a fim de qualificar os ativos da organização por suas vulnerabilidades e possível exploração por ameaças, permitindo que a organização possa avaliar os riscos e priorizar os investimentos de segurança para aqueles que têm maior valor.

É verdade que todos os ativos têm sua importância, maior ou menor, para organização, e cabe a ela determinar os graus de proteção para cada um destes ativos a fim de estabelecer suas prioridades de proteção. Uma vez que a informação trafega por todos estes ativos, a preocupação com eles se faz essencial para segurança.

Há que se definir o valor dos ativos a fim de se chegar a um meio de estabelecer o nível de proteção necessário para eles, e as políticas de segurança pertinentes a cada, e especificar as definições de níveis de proteção adequados aos ativos de acordo com sua importância aos objetivos de negócio, isto é, a classificação de ativos de acordo com as valorações específicas de cada organização, para estes fins, ou a aceitação dos riscos existentes para cada ativo. Abaixo, podemos observar o formato cíclico desta norma com mais atenção:

Figura 4: Processo de gestão de riscos de segurança da informação



Fonte: (ABNT NBR ISO/IEC 27005, 2011, p. 13)

Estas etapas mostradas na Figura 4, acima, serão explicadas a seguir.

2.1.1. Definindo o contexto

O primeiro passo para se começar a trabalhar não apenas nos graus de proteção para os recursos, mas também para toda a gestão de riscos, é estabelecer o contexto do ambiente (BEZERRA, 2013, p. 21). Compreender o contexto significa conhecer o máximo de circunstâncias às quais a organização, com seus ativos, está inserida.

Ora, é este contexto, com a descrição da organização, documentação, levantamento de ativos, e tudo o mais que se puder obter de informações sobre a estrutura da organizacional, que permitirá a valoração de seus bens dentro de uma escala quantitativa posteriormente, e subsequente qualificação dos riscos envolvidos no plano de negócio. Para facilitar tal processo podemos adotar uma lista de questões a serem respondidas.

Bezerra (2013, p. 23), citando a norma, sintetiza os pontos principais da elicitação de contexto da norma ISO 27005, sendo eles a apresentação da organização, as entrevistas e os questionários. A fim da definição de tal contexto, a NBR ISO/IEC 27005 define tanto um ambiente externo, quanto um interno, sendo que o ambiente externo pode incluir:

> - O ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;
> - Os fatores-chave e as tendências que tenham impacto sobre os objetivos da organização; e
> - As relações com partes interessadas externas e suas percepções e valores (ABNT, 2011, p. 16).

Ao passo que o ambiente interno pode incluir:

> - Governança, estrutura organizacional, funções e responsabilidades;
> - Políticas, objetivos e estratégias implementadas para atingi-los;
> - Capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
> - Sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);
> - Relações com partes interessadas internas, e suas percepções e valores;
> - Cultura da organização;
> - Normas, diretrizes e modelos adotados pela organização; e
> - Forma e extensão das relações contratuais (ABNT, 2011, p.16).

A norma adiciona que, caso a organização deseje impor algum limite ao estabelecimento do contexto, convém (não se trata de determinação) que forneça uma justificativa. Trata-se, claramente, de um procedimento de auditoria interna, onde o

escopo é dado pela própria organização. Este escopo do processo de gestão de riscos de SI precisa ser, como dita o texto da norma:

> O escopo do processo de gestão de riscos de segurança da informação precisa ser definido para assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos. Além disso, os limites precisam ser identificados (…) para permitir o reconhecimento dos riscos que possam transpor esses limites (ABNT NBR ISO/IEC 27005, 2011, p. 28).

Este levantamento de ambiente, como parte do contexto é importante para que compreenda sua relevância no processo de gestão de risco. Neste trabalho o escopo compreenderá o ambiente corporativo relacionado ao fator humano no uso dos recursos de TI, e os dados recolhidos em observações, entrevistas e questionários deve responder a estes aspectos da elicitação de contexto.

O passo seguinte à definição de contexto, é a identificação dos ativos (BEZERRA, 2013, p. 44). Neste ponto será feito o levantamento de todos os ativos da organização, por meio de inventário. Convém considerar também os ativos humanos.

Após identificados os ativos, procedemos com a detecção das vulnerabilidades e o levantamento de ameaças correntes possíveis sobre cada um (BEZERRA, 2013, p. 41), que exigirá conhecimento técnico sobre o ativo em que se trabalha; procede-se à valoração dos ativos, que deve levar em consideração as especificações da organização (BEZERRA, 2013, p. 28), considerando-se o plano de negócio, e calculando riscos, probabilidade de ocorrência e impacto que cada risco representa para organização e, a partir dos valores quantitativos obtidos, traçar a qualificação do risco ao qual está sujeita a organização (BEZERRA, 2013, p. 83), para proceder com a elaboração dos controles existentes e tratamento do risco.

2.1.2. Análise de Risco

Aqui serão identificados os eventuais riscos (Identificação de Riscos) que possam se desdobrar em incidentes e causar um desvio do plano de negócios da organização, aos quais, posteriormente, serão estimados valores de risco (Estimativa de Risco), quantitativamente, para sua priorização no tratamento na etapa de avaliação de risco. Desta forma aqui também são identificados os controles existentes para cada uma das ameaças e suas relações com as vulnerabilidades, a fim de mitigá-las ou extingui-las. Tendo em mãos as ameaças e vulnerabilidades, podemos identificar os riscos. Com a

informação das ameaças e da efetividade dos controles podemos quantificar um nível de risco o qual poderá ser avaliado (ABNT NBR ISO/IEC 27005, 2011).

2.1.3. Avaliação de Risco

A avaliação do risco define, após elaborada a lista de riscos, as valorações quantitativas e qualitativas de cada risco, bem como a priorização de cada um destes riscos para tratamento. A avaliação do risco deve levar em conta as particularidades do negócio, cabendo a este definir segundo seus objetivos definidos em seu plano de negócios, mas considerando suas limitações sejam elas orçamentárias, legais, culturais, ou quaisquer sejam. A norma ISO 27005, define algumas abordagens para o processo de tratamento de risco, são elas as avaliações segundo a probabilidade, e segundo o impacto.

Avaliação do risco segundo o critério Probabilidade considera a facilidade que uma vulnerabilidade tem de ser explorada, considerando seus controles. A avaliação segundo o Impacto, é assim definida pela ABNT NBR ISO/IEC 27005: "convém que os critérios de impacto sejam desenvolvidos e especificados em função do montante de danos ou custos à organização" (2011, p. 18). Nesta elaboração a norma também nos recomenda considerar alguns pontos:

- Nível de classificação do ativo de informação afetado;
- Ocorrências de violação da segurança da informação (por exemplo: perda da disponibilidade, da confidencialidade, e/ou da integridade);
- Operações comprometidas (internas ou de terceiros);
- Perda de oportunidades de negócio e de valores financeiros;
- Interrupção de planos e o não cumprimento de prazos;
- Dano à reputação;
- Violação de requisitos legais, regulatórios ou contratuais (ABNT NBR ISO/IEC 27005, 2011, p. 18).

Assim concluímos que considera a priorização de ações quanto aos riscos levando-se em consideração o impacto que cada um pode significar à organização, possibilitando a priorização segundo o que mais afeta o plano de negócios, neste quesito, o primeiro risco a se considerar será aquele que impede a organização de atingir os seus objetivos, além de considerar os custos envolvidos.

2.1.4. Tratamento de Risco

Uma vez que os riscos são ordenados segundo a sua prioridade para a organização, procede-se em seguida, ao tratamento do risco. Segundo a ISO GUIA 73 O tratamento de risco pode envolver:

- Assumir ou aumentar o risco, a fim de buscar uma oportunidade;
- A remoção da fonte de risco;
- A alteração da probabilidade (ou *likelihood*);
- A alteração das consequências;
- O compartilhamento do risco com outra parte ou partes;
- A retenção do risco por uma escolha consciente (ABNT ISO GUIA 73, 2009, p. 7).

Podemos condensar em quatro pontos principais (ABNT NBR ISO/IEC 27005, p. 31): modificação do risco, retenção do risco, o ato de se evitar o risco, e o compartilhamento do risco.

A Modificação do Risco consiste em remover ou mitigar um risco por alteração de consequência ou de probabilidade. Isto ocorre pela adoção de controles (2011, p. 34). Após a análise dos riscos os controles mais apropriados devem ser selecionados a fim de se modificar tais riscos, levando-se em conta custos e prazos para sua implementação (ABNT NBR ISO/IEC 27005, 2011, p. 34). Ora, como vimos, um risco pode ser avaliado pela probabilidade de uma vulnerabilidade ser explorada. Mudando-se esta probabilidade, altera-se o risco pela probabilidade. (*likehood*), e assim o mesmo é válido para a alteração das consequências.

Aceitação, ou Retenção (ABNT NBR ISO/IEC 27001, 2006), do Risco, segundo Bezerra, “assegura os riscos aceitos pela organização, ou seja, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente. São os chamados riscos residuais, cujo enquadramento nesta categoria deverá ser justificado” (2013, p. 14). Risco Residual é o risco que ainda resta em um ciclo até que se providencie uma decisão a seu respeito pela organização.

A norma ISO/IEC 27005 diz que “convém que os critérios para a aceitação do risco sejam desenvolvidos e especificados. Os critérios de aceitação do risco dependem frequentemente das políticas, metas e objetivos da organização, assim como dos interesses das partes interessadas” (ABNT, 2011, p. 18). Sendo assim, portanto, cada organização, de acordo com seu plano de negócios, estabelece e elabora segundo suas prioridades sua escala de níveis de aceitação de riscos (ABNT NBR ISO/IEC 27005, 2011, p. 18).

A ação de evitar um risco se expressa na norma ISO 27005 no enunciado: “Convém que a atividade ou condição que dá origem a um determinado risco seja evitada” (ABNT, 2011, p. 35). Ou seja, trata-se simplesmente de não expor determinado ativo a uma ameaça prevista, optando por resguardar-se, ou seja, optando por remover a fonte de risco (ABNT ISO GUIA 73, 2009, p. 7).

O Compartilhamento de Risco consiste no “compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco” (ABNT ISO 27005, 2011, p. 94). Um exemplo de compartilhamento de risco é a adoção de planos de seguro, onde as consequências de um risco têm sua cobertura por uma entidade externa.

Na figura abaixo vemos a esquematização do processo de Tratamento do Risco.

Figura 5 - Atividade de tratamento do risco

Fonte: (ABNT NBR ISO/IEC 27005, 2011, p. 32)

2.1.5. Execução, verificação e ação

Consiste na realização das etapas finais do ciclo, em que se implementa o plano de tratamento do risco, procede-se pelo monitoramento e análise crítica dos riscos

remanescentes, e reiniciando o ciclo sempre que necessário, e tudo enquanto comunica-se o que se obteve às partes interessadas.

A diretriz de implementação para comunicação do risco é dada pela ISO 27005, parcialmente, da seguinte forma

> A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas (ABNT, 2011, p. 37).

Nos diz Bezerra que “durante todo e qualquer tipo de trabalho, a comunicação é uma atividade de grande importância. É através dela que são transmitidas informações sobre o desenvolvimento das atividades e os resultados alcançados” (BEZERRA, 2013, p. 121). Trata-se de uma troca interativa, documentada formalmente, contínua e intencional de informações que serão utilizadas para determinar a forma como os riscos deverão ser gerenciados.

Também se deve notar a importância do processo constante de monitoramento e análise crítica, responsável por manter a gestão de riscos atualizada e continuamente evitar o surgimento de novas vulnerabilidades.

É possível notar que a ABNT NBR ISO/IEC 27005:2011 segue um modelo de ciclo de melhoria contínua PDCA. E como tal, portanto, requer-se entre os requisitos para a Gestão de Riscos com ISO 27005, a implantação de um SGSI, como o definido pela norma ISO 27001.

Logo abaixo vemos uma tabela que mostra em detalhes os passos tomados dentro de um ciclo PDCA:

Tabela 1: Alinhamento do processo do SGSI e do processo de gestão de riscos de SI

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Fonte: (ABNT NBR ISO/IEC 27005, 2011, p. 16)

Importante notar que a ABNT NBR ISO/IEC 27005:2011 indica um caminho a ser seguido, mas cabe a cada organização implantá-la da maneira que seja a mais conveniente. Além disto, embora apresentemos aqui como uma possibilidade, existem outras formas de se aplicar a gestão de riscos, como por exemplo as apresentadas pela COBIT, Risk IT, também da ISACA como o COBIT, no ITIL, no PMBOK entre outros *frameworks*.

CAPÍTULO 3 - ESTUDO DE CASO

Para melhor conhecermos o objeto de estudos a partir da perspectiva do ofertante de serviços de TI, elaboramos algumas questões. São questões de respostas objetivas, como fosse um *checklist*. Como o contexto mais geral será obtido pela visão dos usuários dos serviços, aqui nos limitamos a algumas poucas questões. Este procedimento tomaremos semelhantemente ao processo de levantamento de contexto dentro da norma ISO 27005, embora não tenha a pretensão de servir para uma adequação profunda. São três fontes de informações as quais buscamos: por meio de observações e levantamento de documentação, uma entrevista realizada com o departamento de TI e a última e mais importante para este estudo de caso um questionário aplicado aos usuários de recursos de TI. Para os fins que almejamos identificamos alguns dos ativos com os quais estes usuários precisam trabalhar a fim de que possamos identificar as vulnerabilidades, reconhecer os riscos envolvidos e concluir os pontos críticos.

3.1. Definição de contexto

A definição de contexto na gestão de riscos, nas palavras de Bezerra é a

> totalidade de circunstâncias que possibilitam, condicionam ou determinam a realização de um texto, projeto, atividade ou mesmo de um evento de segurança da informação. Em outras palavras, contexto é o conjunto de circunstâncias que se relacionam de alguma forma com um determinado acontecimento. É a situação geral ou o ambiente a que está sendo referido um determinado assunto (2013, p. 22).

Desta forma podemos dizer que a análise para definição de contexto determina o mapeamento de área em que a organização atua, bem como suas disposições particulares, como vimos anteriormente, se segue em dois aspectos: externo e interno. Uma vez estabelecido o contexto e inventariados os ativos da organização, é possível avaliar e analisar os riscos com os quais está envolvida e elaborar o tratamento e a aceitação destes.

3.1.1. Escopo

Antes de tudo definiremos o escopo deste projeto: segundo Bezerra “é a maneira como são descritos os limites do projeto, sua abrangência, seus resultados e suas entregas. É a finalidade, o alvo, o intento ou propósito da gestão de riscos” (2016, p. 27).

Neste trabalho, nosso escopo são os recursos humanos, as pessoas que lidam com os ativos de TI. Podemos estabelecer, portanto, como limite de atuação a este âmbito, não chegando em detalhes outros da organização que não dizem respeito a este assunto. Por isto não detalharemos a rede interna, nem o funcionamento de seus servidores, sistemas internos, e processos, exceto naquilo em que se relacionam com os usuários.

Dentro dos documentos a que tivemos acesso estão definidos os objetivos da organização, bem como sua estrutura organizacional. A partir da prospecção de informações com o setor de TI conseguimos informações sobre alguns processos de negócios e ativos de informação.

A definição do escopo e dos limites deste trabalho incluem o acesso somente ao material de acesso público, devido às limitações legais de um projeto não contratado. Um projeto de gestão de riscos, ao tratar de seu escopo ainda deve considerar as restrições orçamentárias, técnicas e temporais, consideremos estas restrições, sem no entanto entrar em detalhes destes tópicos, que devem ser considerados na elaboração de um projeto como o que este trabalho de graduação tenta mostrar a necessidade. Em resumo, nosso escopo mais específico, e aqui acessível, como dito, é o fator humano em sua relação com os ativos informacionais: aplicações, infraestrutura, processos, e segurança física, SI, e intranet.

3.1.2. Contexto externo

Trata-se de uma prefeitura municipal, inserida em um contexto político particular. A Constituição é dada pela Lei Orgânica Municipal, de 1990, na qual está sua estruturação e delegação de deveres. Isto será tratado como parte do contexto interno à organização.

A história política recente da cidade aponta eventos de incidentes de segurança, alguns consumados, outros contidos em sua origem. Segundo tratado com o administrador da rede, a organização sofreu tentativas massivas de acessos indevidos às contas de *e-mail* de seu servidor Zimbra no mês de outubro de 2018, o que pode ser reflexo das eleições gerais no Brasil neste período. Houve, segundo relatado pelos funcionários de TI, há poucos anos, ataques com disseminação de *softwwares* em que se disparava, internamente, *jobs* nas impressoras com propaganda eleitoral de um candidato a prefeitura da cidade, tendo se iniciado a disseminação do *malware* pelo recebimento de *e-mail*, com a possível abertura de arquivo malicioso (*phishing*) anexo, e alastramento pela rede na forma de *worm*, um tipo específico de *malware* auto-replicante. Isto denota, à altura, um comportamento pouco engajado dos usuários com a segurança, possível fruto da ausência de orientações quanto ao recebimento de *e-mails* e arquivos não requisitados.

Há também entre as dimensões que exigem uma gestão de riscos adequada a uma organização, neste caso pública, a necessidade da conformação legal às demandas quanto à privacidade e acesso à informação. Quanto à privacidade, conforme a Lei de Proteção de Dados, as responsabilidades legais se definem pela Lei Nº 13.709 de 14 de agosto de 2018, que versa em seu artigo 1º:

> Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Adendo a isto, com base na Constituição Federal de 1988 e nos direitos por ela firmados, a Lei de 2018 assegura em seu artigo 2º o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O Capítulo IV da Lei nº 13.709 de 14 de agosto de 2018, no artigo 23, disserta sobre

> O tratamento de dados pessoais pelas pessoas jurídicas de direito público, como referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (BRASIL, 2018)

Estabelece, esta mesma lei, a proibição de transferência de dados pessoais para a iniciativa privada, e toda transferência de dados pelo poder público "devem atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas" (BRASIL, 2018).

Já a referida Lei Nº 12.527 de 18 de novembro de 2011, por sua vez assegura os termos do direito ao acesso à informação no serviço público, um direito fundamental garantido em nossa Constituição Federal em seu artigo 5º, inciso XXIII, aos cidadãos, Lei à qual também estão sujeitas as prefeituras dos municípios. Uma ressalva importante a se notar, o inciso citado do artigo da constituição federal assegura o sigilo de dados que sejam imprescindíveis à segurança da sociedade e do Estado.

Portanto, vemos que há um conjunto de regras às quais os dados e informações de guarda da prefeitura municipal devem estar conformes, e devem ser considerados no momento de se realizar a elaboração das ameaças, vulnerabilidades e riscos a que estão sujeitas.

3.1.3. Contexto interno

Analisando o aspecto interno, finalmente enquadramos o nosso objeto de estudos, sua estrutura organizacional, atribuições e especificamente seus recursos de TI e seus operadores. São 221 funcionários trabalhando em horário comercial, fazendo uso contínuo de microcomputadores, impressoras e *scanners* conectados à rede.

Como parte dos levantamentos de informações para definição de contexto interno, por meio de documentos e observações obtivemos uma visão do ambiente, também buscamos responder algumas questões mais gerais a este respeito. Elaboramos uma série de questões cujas respostas devem ser colhidas diretamente com o departamento

de TI e, sequencialmente, um questionário aplicado aos usuários de recursos de TI. Segue-se cada um com seus desdobramentos:

Do levantamento feito por observação do local e pela leitura de documentos públicos, possibilitados pela investigação *in loco* deste pesquisador, a respeito do propósito e da finalidade da organização pública municipal, observou-se que, de acordo com a Lei Orgânica do município de 1990, a sua finalidade é buscar a integração econômica, política, social e cultural com demais municípios da região, garantindo a preservação dos valores culturais e naturais e a existência de um meio ambiente ecologicamente equilibrado.

Ademais, tem como competência, segundo o artigo 5º da mesma Lei Orgânica do município, legislar sobre assuntos de interesse local, cabendo ainda a este:

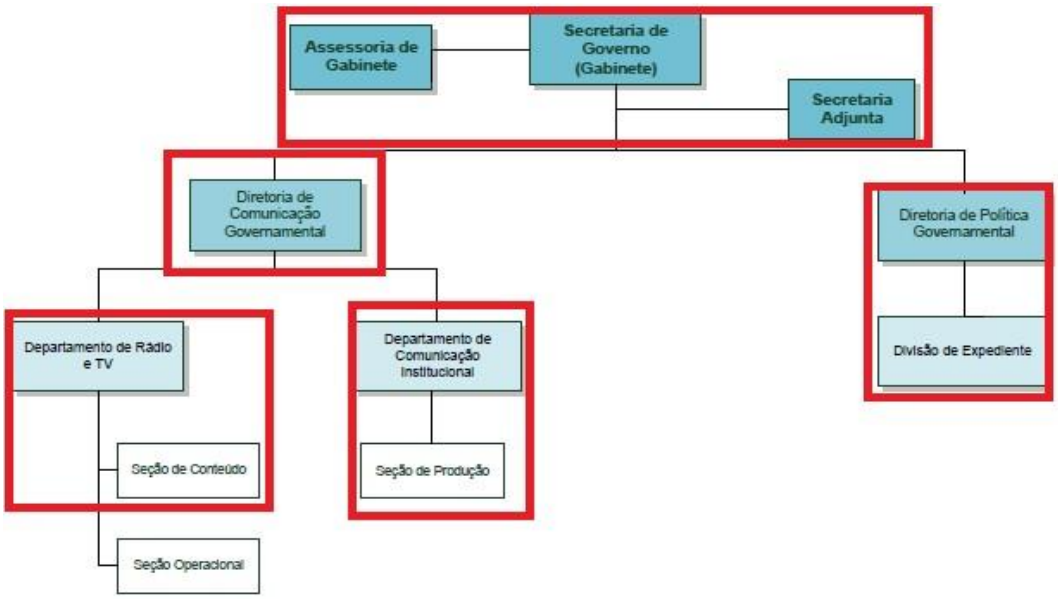
- A arrecadação de tributos;
- Fixação de preços públicos, bem como de aplicação de suas rendas;
- Organizar a execução de serviços públicos;
- O seu quadro de funcionários;
- Dispor sobre administração;
- Aquisição, utilização e alienação de seus bens; Elaborar seu plano diretor; Dispor qual o perímetro urbano do Município;
- Estabelecer normas de edificação, de loteamento, de arruamento e de zoneamento urbano, bem como as limitações urbanísticas;
- Regulamentar a utilização dos logradouros públicos;
- Organizar e dispor o transporte coletivo;
- Fixar e sinalizar os limites das “zonas de silêncio”, e de trânsito e tráfego em condições especiais;
- Disciplinar os serviços de carga e descarga e fixar a tonelagem máxima permitida a veículos que circulem em vias públicas municipais;
- Disciplinar, através de Lei, os serviços de guinchamento, transporte e guarda de veículos retidos.

Ainda de acordo com o artigo 6º da mesma Lei Orgânica, cabe ao município:

- Cuidar das questões relativas à saúde, higiene, segurança pública, educação, cultura e a assistência social;
- Defender a flora e a fauna nativas, assim como os bens e locais de valor histórico, artístico, turístico ou arqueológico;
- Prover a extinção de incêndios;
- Licença ou para abertura e funcionamento de estabelecimentos industriais e comerciais;
- Promover e executar programas de construção de moradias populares e garantir a dignidade humana, com condições habitacionais, de saneamento básico e acesso ao transporte;
- Fiscalização dos locais de venda direta ao consumidor, as condições sanitárias dos gêneros alimentícios;
- Fazer cessar, com o uso do poder de polícia administrativa, atividades que violarem as normas de saúde, sossego, higiene, segurança, funcionalidade, estética, moralidade e outras de interesse do bem comum.

A respeito da estrutura organizacional desta instituição pública, por meio de coleta de dados junto do Departamento de Recursos Humanos, obtivemos os seguintes organogramas.[14] [15]

Figura 6: Organograma da Secretaria de Governo



Fonte: Autoria própria (2018): Dados da pesquisa.

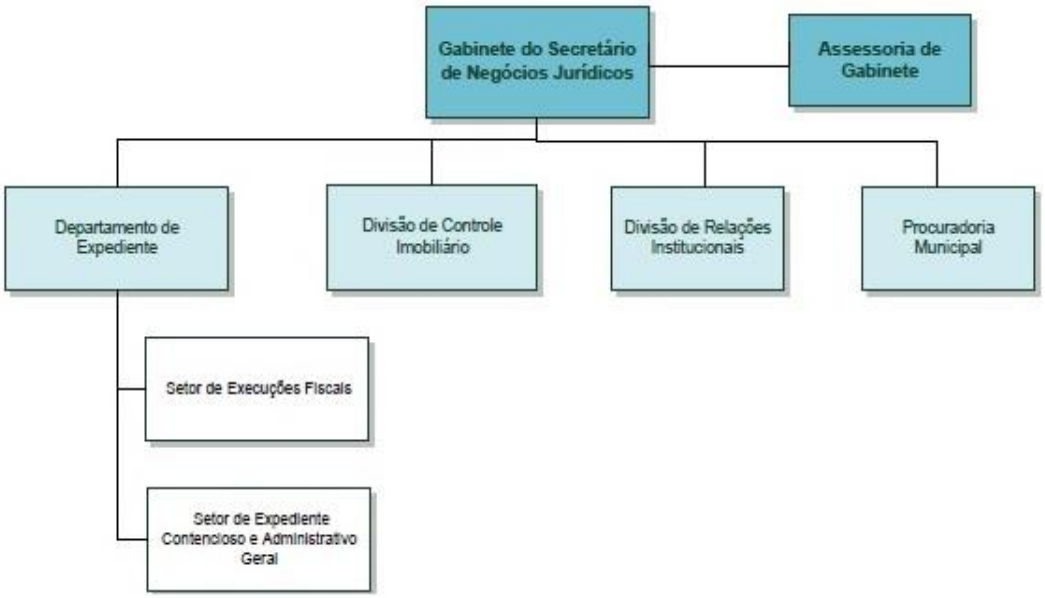
Estão no Paço do município o Gabinete da secretaria e sua assessoria; a Diretoria de Política Governamental e sua divisão de expediente; da Diretoria de Comunicação Governamental está no Paço a Seção de Conteúdo do Departamento de Rádio e TV; e o Departamento de Comunicação Institucional com sua Seção de Produção. No Paço municipal estes setores estão alocados no 7º andar.

A Secretaria de governo é a responsável por gerir o andamento das pautas que cabem à prefeitura do município, bem como relacionar-se com vereadores e imprensa, por meio de sua Assessoria de Imprensa. O Departamento de Comunicaçao Institucional é o responsável por desenvolver a apresentação publicitária dos programas da prefeitura.

Figura 7: Organograma da Secretaria de Negócios Jurídicos

14 Observe que em destaque estão os departamentos que fazem parte deste Paço Municipal, nosso objeto de estudos. Quando não destacados, é porque a Secretaria está em sua totalidade no Paço.

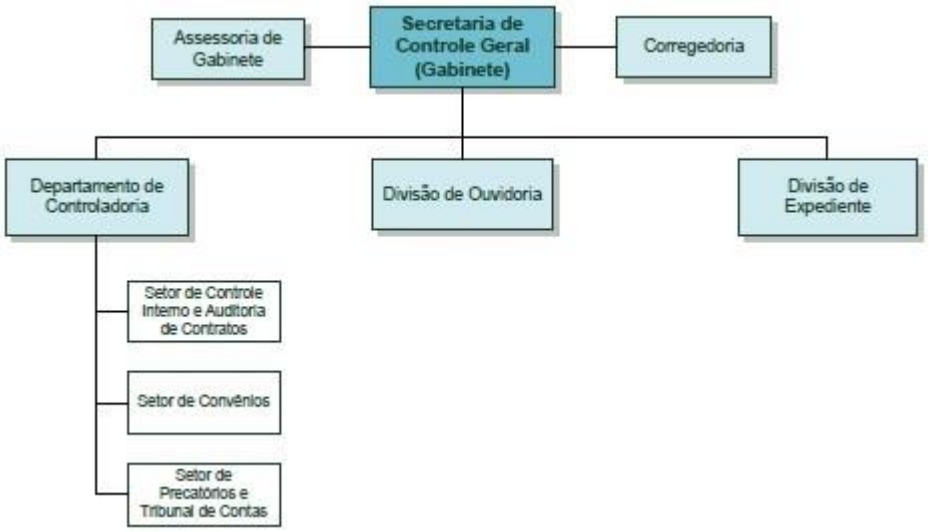
15 Para nota, aqui nos atemos aos setores do paço municipal que fazem parte de uma mesma rede interna.



Fonte: Autoria própria (2018): Dados da pesquisa.

Todas as divisões desta Secretaria estão lotadas no Paço, no 6º andar. É a secretaria responsável pelas questões jurídicas da prefeitura, seja a organização a litigante ou a litigado, atua como advocacia ou procuradoria para organização. Faz uso de peticionamentos e processos digitais, com uso de identitades e certificados digitais.

Figura 8: Organograma da Secretaria de Controle Geral

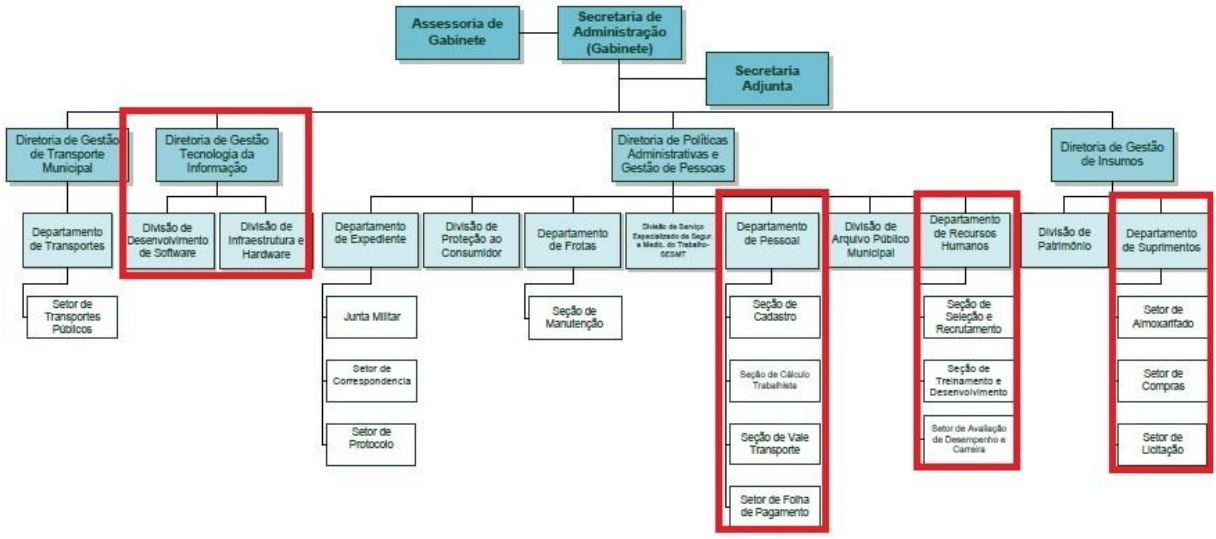


Fonte: Autoria própria (2018): Dados da pesquisa.

Todas as divisões desta Secretaria estão lotadas no Paço, no 5º andar. Trata-se da controladoria interna, move os processos disciplinares relacionados aos usuários, bem

como recebe, dos munícipes, por meio da Ouvidoria, reclamações diversas sobre a organização.

Figura 9: Organograma da Secretaria de Administração



Fonte: Autoria própria (2018): Dados da pesquisa.

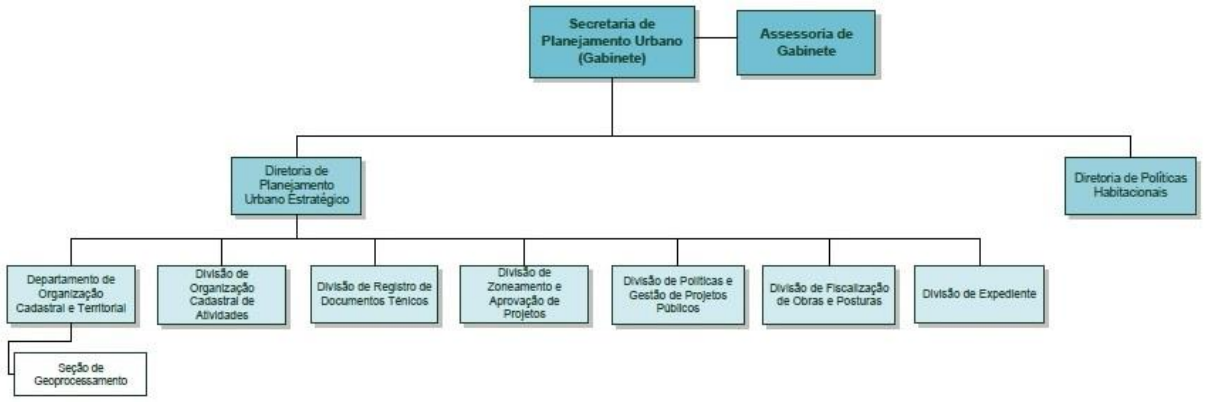
Todas as divisões desta Secretaria estão lotadas no Paço, no 4º andar. A Divisão de Informática será tratada mais adiante.

O Departamento de Pessoal é o responsável por gerir registro de ponto, folha de pagamento e direitos de funcionários contratados, além de operar as questões trabalhistas.

O Departamento de Recursos Humanos é o responsável pela elaboração de provas de concursos e contratação de novos funcionários, estabelecendo as médias salariais e outros assuntos pertinentes a registro de empregados.

O Departamento de Suprimentos conta, no Paço, com as Seções de Compras e Licitações, responsáveis por todo o processo de compras, desde pesquisa de preços, contatos com potenciais fornecedores, promoção de pregões de licitações ou compras diretas de equipamentos e insumos.

Figura 10: Organograma da Secretaria de Planejamento Urbano



Fonte: Autoria própria (2018): Dados da pesquisa.

Esta Secretaria, à exceção da Divisão de Organização Cadastral de Atividades, que fica em outro endereço, tem seus setores divididos em entre o Térreo e o 2º andar do Paço Municipal, sendo que o gabinete da Secretaria de Planejamento e sua assessoria, bem como a Diretoria de Planejamento Urbano Estratégico estão lotadas no 2º andar. Todas as divisões, à exceção da Divisão de Fiscalização de Obras e Posturas, que fica fora deste Paço, estão no Térreo.

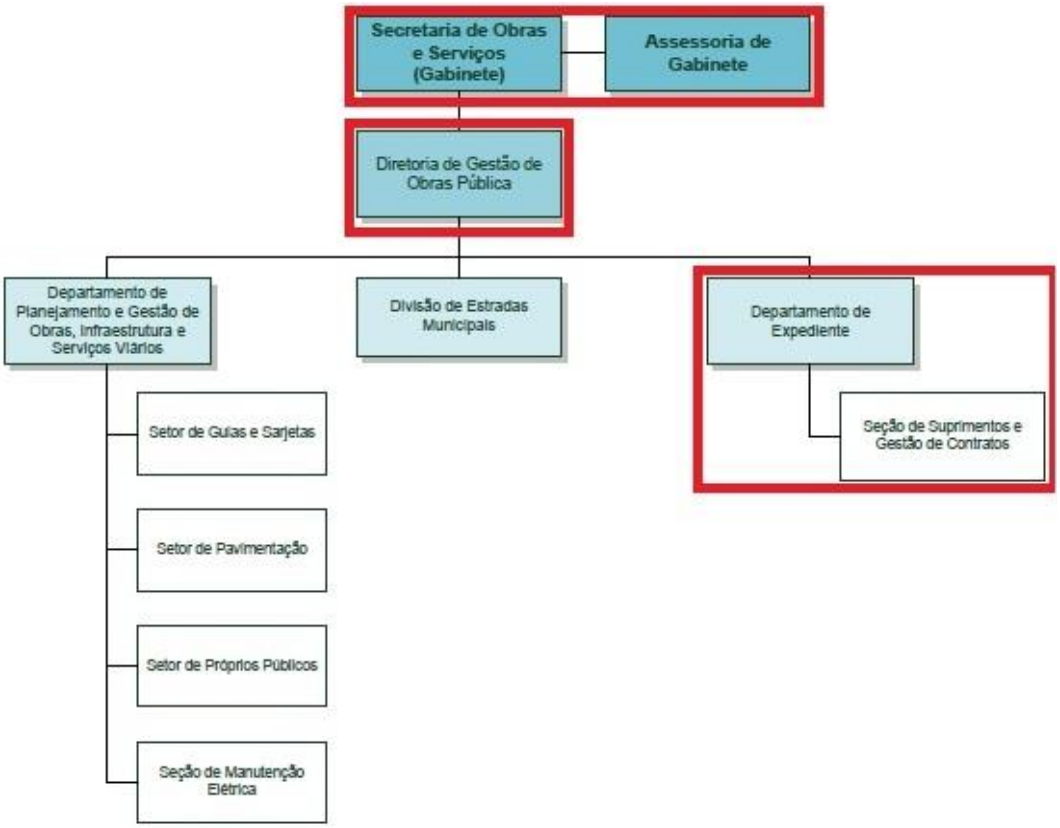
A Divisão de Organização Cadastral e Territorial é a responsável pela gestão urbanística da cidade, traçando terrenos e cadastrando novos empreendimentos imobiliários.

A Divisão de Registro de Documentos Técnicos é a responsável pela guarda de documentos de escritura, bem como a liberação de documentações diversas sobre demolição, construção, certidões de reforma, alvarás, etc.

A Divisão de Zoneamento e Aprovação de Projetos é a responsável por analisar os projetos recebidos dos munícipes ou empreendimentos a fim de aprová-los, ou solicitar adequação às determinações legais. É esta divisão que emite o Habite-se para que uma obra terminada possa ser utilizada.

A Diretoria de Planejamento, como um todo, estabelece os projetos arquiteturais das obras municipais. Bem como os desenhos de design e distribuição dos setores internos da prefeitura.

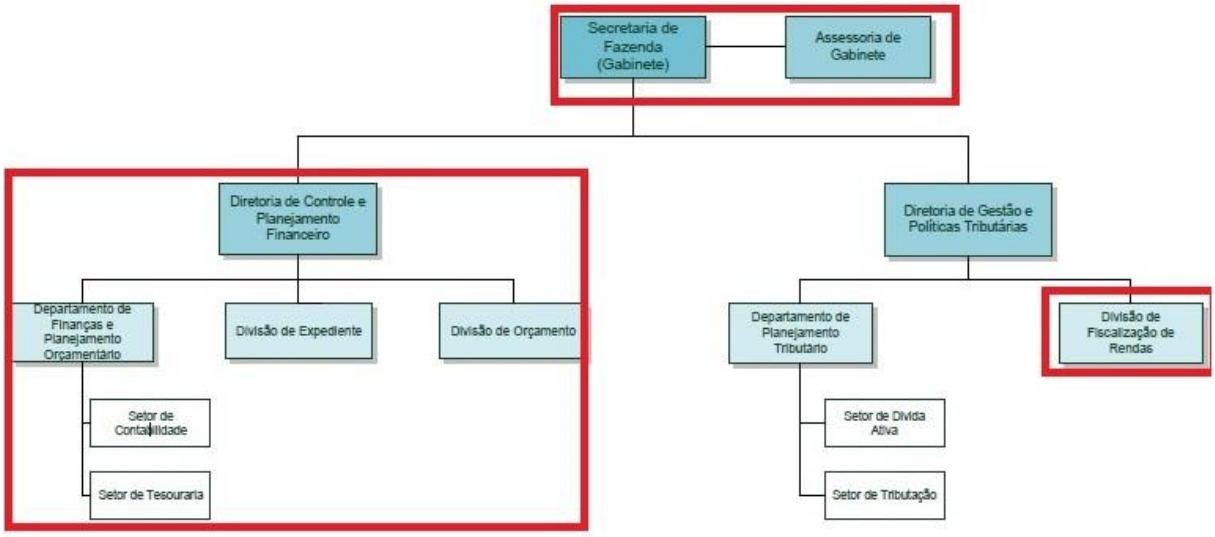
Figura 11: Organograma da Secretaria de Obras e Serviços



Fonte: Autoria própria (2018): Dados da pesquisa.

Estão no Paço do município o Gabinete e sua assessoria; A Divisão de Gestão de Obras Públicas e o Departamento de Expediente bem como sua Seção de Suprimentos e Contratos. No Paço municipal estes setores estão alocados no 2º andar. Os projetos de obras da prefeitura municipal são geridos todos por esta secretaria, desde a pavimentação de uma rua até a construção de uma nova unidade básica de saúde, tudo passa por esta Secretaria.

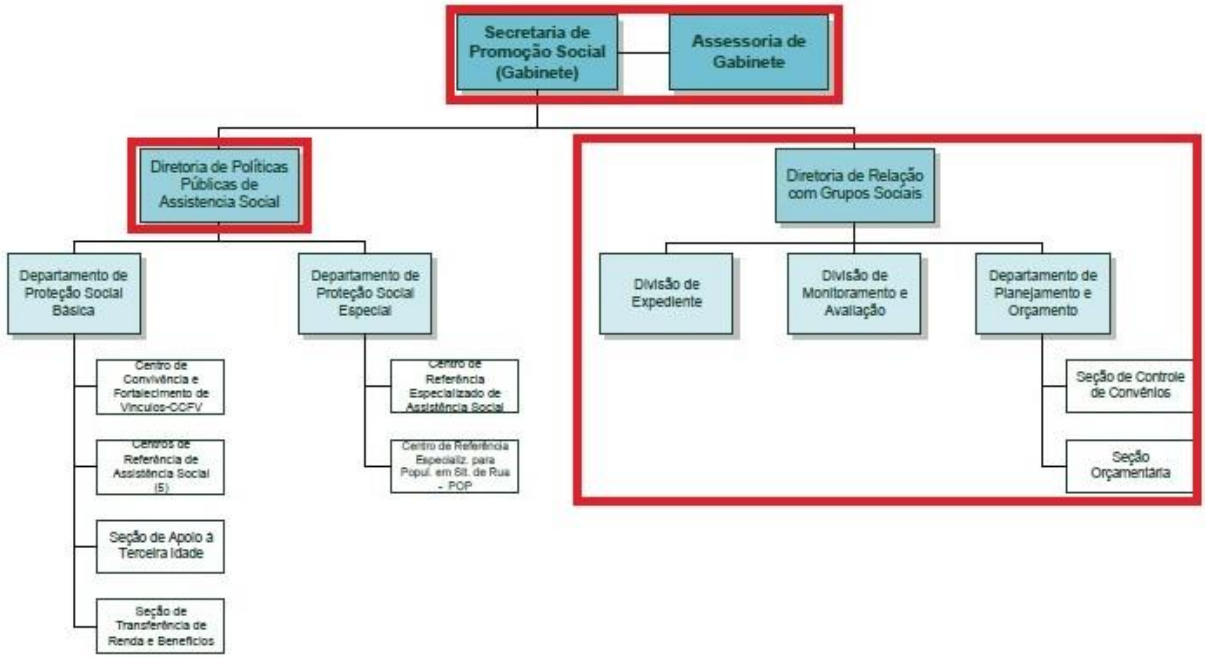
Figura 12: Organograma da Secretaria de Fazenda



Fonte: Autoria própria (2018): Dados da pesquisa.

No Paço do município é alocada no 1º andar, é a responsável pelas atividades financeiras da prefeitura, seja na fiscalização, cobrança e recebimento de impostos e taxas, seja na liberação de pagamentos para os contratos firmados pela organização, além da contabilidade oficial e prestação de contas financeiras às entidades governamentais fiscalizadoras de contas. A Secretaria detém e manipula as contas bancárias da prefeitura.

Figura 13: Organograma da Secretaria de Promoção Social



Fonte: Autoria própria (2018): Dados da pesquisa.

Está alocada em prédio anexo à prefeitura, mas dentro da mesma rede. Esta secretaria é a responsável pelos programas de inclusão social e amparo e proteção aos mais pobres.

Acerca da estruturação do departamento de TI e da SI, cujas análises foram possibilitadas por meio da análise técnica dos organogramas obtidos junto ao Departamento de Recursos Humanos, pudemos avaliar que o departamento de TI é subsidiário direto da Secretaria de Administração.

A respeito dos processos de informação na organização pública municipal e suas respectivas operacionalizações, foi possível constatar que todo o Paço é ligado a uma única rede física, sem quaisquer divisões virtuais, exceto àquelas relativas a permissões especiais para cada diretório ou servidor de serviço.

O Sistema de Protocolo reúne as principais necessidades administrativas da prefeitura, é onde estão centralizados os processos abertos, tanto de iniciativa dos munícipes quanto os trâmites internos, e toda formalização de relações entre setores ou entre munícipes e prefeitura ocorre por este meio.

O sistema de gestão, terceirizado, inclue módulos de sistema de controle de estoque e requisição de materiais, contabilidade, e recursos humanos.

O sistema de ponto digital é de domínio do departamento pessoal e a entrada é feita por relógio ponto biométrico no portão dos fundos do paço municipal, local guardado, normalmente, por um guarda-civil e uma câmera de vigilância em horários de entrada e saída, mas cuja porta fica trancada em demais horários, sendo possível o acesso pela entrada principal do paço que dá acesso ao saguão principal, guardado por guarda-civil municipal, porém de local de grande movimentação, acessando uma entrada lateral aos elevadores. Os dois monitores das câmeras de vigilância estão localizados um no saguão do paço, outro na entrada de serviço, nos fundos.

O sistema de *e-mail* é acessível via *web*, bem como as aplicações de uso público. As notícias do site são enviadas por um *link* de conhecimento exclusivo da assessoria de imprensa, mas que exige login e senha.

Os arquivos dos setores são guardados primeiramente no disco local, mas recomenda-se, para que tenham *backup* feito regularmente, que guardem nos diretórios comuns em servidor de dados. Os privilégios de acesso onde cada setor acesso seu próprio diretório é controlada por GPO. Pelo grande volume de dados produzido, a Assessoria de Imprensa possui ainda um servidor QNAP destinado aos seus trabalhos.

Somando-se a esta descrição, e respeitado o devido limite de exposição, os principais ativos inventariados a serem considerados neste trabalho de graduação são os que seguem adiante. Os principais softwares, serviços e equipamentos oferecidos no Paço são

- Sistema de Protocolo;
- Sistema de Gestão Municipal, com módulos de Suprimentos, Contabilidade e Recursos Humanos;
- Sistema de Ponto, cujo acesso é restrito ao Departamento Pessoal;
- Sistema de *e-mail*;
- Aplicações *Web* de uso público;
- Sistema de atualização de notícias para *website* para Assessoria de Imprensa;
- Sistema de câmeras de vigilância com 2 monitores de vigilância em locais públicos;
- 221 computadores;
- Sistemas Operacionais Windows;

- Acesso a contas bancárias;
- Acesso a sites de peticionamento jurídico;
- Identidades e Certificados Digitais;
- 42 impressoras, sendo 34 multifuncionais de rede;
- Relógio de ponto biométrico;
- Servidor de Dados, de acesso comum de todos os setores e seus usuários e restrito por permissões associadas aos GPO em Servidor AD;
- Servidor de dados QNAP para vídeos e imagens.

Algumas questões objetivas foram dirigidas ao departamento de TI para se somar ao contexto que estamos levantando. Foram formuladas por este pesquisador e respondidas pelo responsável pelo departamento de TI desta prefeitura e pelo administrador da rede. Foram as seguintes questões, em relação à Gestão e Governança:

1. O departamento de TI é guiado por meio de Governança de TI?

Resposta: Não.

2. O departamento de TI possui um plano de Gestão de Riscos de TI?

Resposta: Não.

3. Como funciona o Plano de Resposta a Incidentes? Há um plano prévio e formal quanto às formas de se enfrentar os possíveis incidentes?

Resposta: Ele é reativo, depende do incidente relatado. Não há um plano definido.

4. Como os ativos de informação são inventariados? O processo é automatizado e o inventário é atualizado com frequência?

Resposta: Todo a geração de inventário é manual e guardado em planilhas.

5. Como são avaliados os ativos de acordo com sua importância para organização? Existe um estabelecimento formal de prioridades de proteção para cada um?

Resposta: Não existe um estabelecimento formal de prioridades. Os servidores são o ponto central de toda operação de tecnologia da informação, mas orientado para os serviços *online* mantidos pelo município. O tratamento ao público recebe prioridade

contra indisponibilidade, sendo essencial mantê-lo funcionando. Tudo o mais é contingencial.

6. Quanto às pessoas, como elas são compreendidas do ponto de vista do serviço de TI? São usuários, são ativos...?

Resposta: Considera-se operadores de recursos, não necessariamente ativos.

Em relação à Operação, as questões e respostas obtidas junto dos mesmos responsáveis, pelo departamento de TI desta prefeitura e pelo administrador da rede, foram as seguintes:

1. Os usuários possuem algum tipo de privilégio administrativo?

Resposta: Normalmente não, porém há algumas exceções.

2. Eles receberam treinamento para uso de suas ferramentas?

Resposta: Em alguns casos, mas nada generalizado. Normalmente para ferramentas terceirizadas.

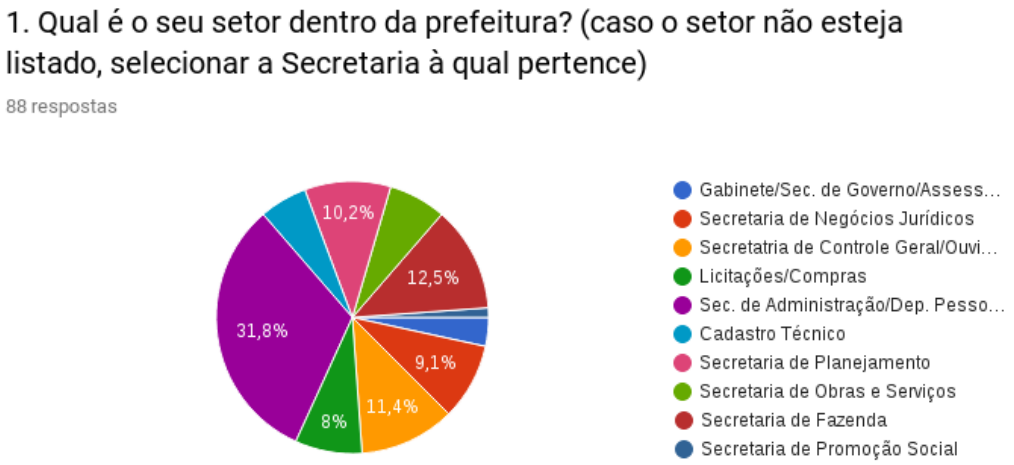
Constatação: não há a conformação da TI a um plano de Governança de TI, e nem mesmo um plano de Governança Corporativa. A prefeitura é regida pela Lei Orgânica do Município e, dentro dos organogramas das secretarias municipais, estabelece que o Departamento de TI é um subsidiário da Secretaria de Administração, como não mais que um departamento de prestação de serviços de infraestrutura, não sendo considerado parte ativa no estabelecimento das diretrizes estratégicas. Não há a orientação do departamento ao objetivo do negócio, de forma que não se estabelecem as relações das informações, as quais guarda, ao desenvolvimento das políticas municipais de maneira dinâmica, as informações são de uso particular de cada setor.

Além disto, o departamento não possui um plano gestor de riscos. Não há a previsão dos riscos existentes, nem oferecimento de controles normatizados. Todas as suas respostas a incidentes são contingenciais, isto é, reativas, o que expõe enormemente a prefeitura às incertezas.

A seguir, por meio das análises efetuadas por este pesquisador, graças às respostas alcançadas, e por meio dos documentos públicos deste Paço Municipal avaliado, apresentaremos as seguintes questões encaminhadas aos usuários dos recursos de TI, enviadas por *e-mail* no dia 14 de outubro de 2018, à meia-noite, por meio de formulário *online* da ferramenta Google Forms, na qual constava 31 perguntas, com múltiplas respostas. Dos 221 funcionários, retornaram até a meia-noite do dia 25 de outubro de 2018, 88 respondentes. As questões encaminhadas estão disponíveis em Anexo.

O primeiro gráfico apresenta os setores dos respondentes das questões:

Gráfico 1 – Setor de trabalho de pertença do funcionário público

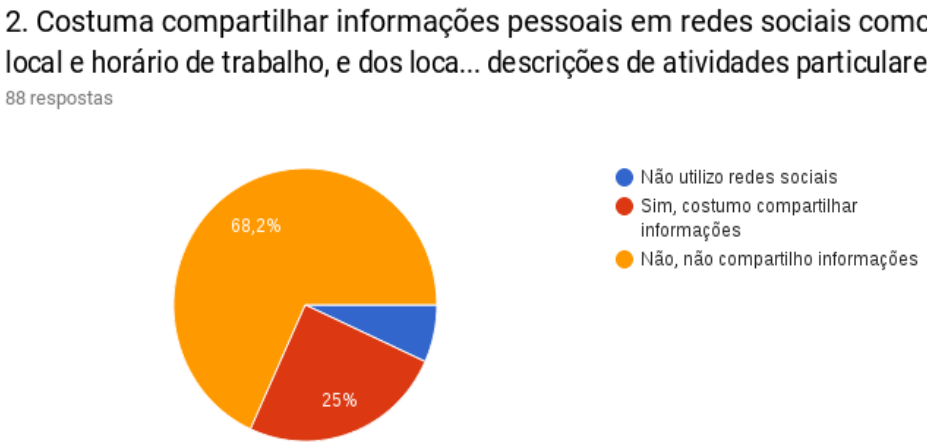


Fonte: Autoria própria (2018): Dados da pesquisa.

Estão todos discriminados de acordo com sua secretaria ou departamento de atuação. O número total de respondentes foi de 88, de um total de 221 usuários de recursos de TI, o que corresponde a uma participação de 40% dos funcionários. A maior parte dos respondentes corresponde à Secretaria de Administração, são 31,8% do total de respondentes. Como observamos no organograma da secretaria, trata-se da secretaria com maior número de setores no paço municipal, e também com maior número de funcionários. Se considerarmos ainda os setores de Licitações e Compras como parte desta Secretaria, o percentual será de 39,8% dos respondentes. Neste caso mantivemos separados por sua separação também física no prédio do paço municipal.

O primeiro grupo de questões é referente à socialização de informações. E levanta questões sobre uso e compartilhamento de dados e informações pessoais e profissionais por meio de redes sociais. Como "Redes sociais" entendemos todo site ou portal que proporcione grande número de interações entre pessoas ou organizações em uma relação de um para vários indivíduos, ou de muitos para muitos indivíduos. Inclui-se aqui tecnologias de mensagens instantâneas capazes de agregar grande quantidade de pessoas em um mesmo grupo, como o *Facebook Messenger*, *Whatsapp* e similares.

Gráfico 2 – Compartilhamento de informações pessoais em redes sociais



Fonte: Autoria própria (2018). Dados da pesquisa.

Esta questão foi levantada pelo risco de se revelar informações pessoais que possam ser exploradas por criminosos para se aferir costumes e comportamentos de suas possíveis vítimas. Segundo os resultados obtidos, 68,2% dos respondentes dizem não compartilhar informações pessoais na internet, o que pode revelar uma preocupação já estabelecida com o que estes dados podem proporcionar a pessoas mal intencionadas. É comum a exposição de dados pessoais em redes sociais, como nos mostra o relatório *Digital In* 2018 (HOOTSUITE, 2018), de forma que aqui estes números podem ser observados de maneira otimista.

Gráfico 3 – Compartilhamento de informações profissionais em redes sociais

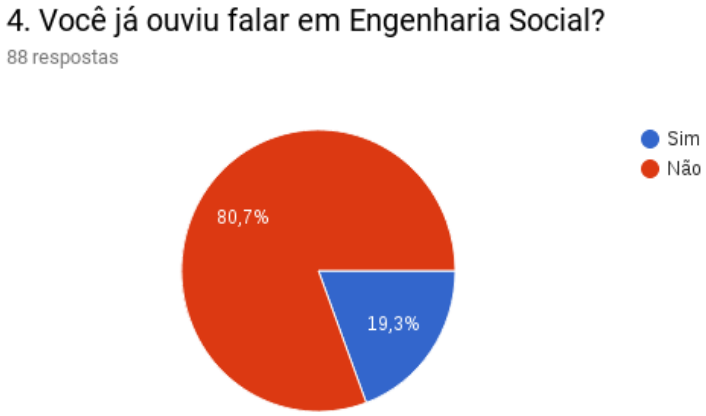
Fonte: Autoria própria (2018). Dados da pesquisa.

Adicionalmente ao gráfico 2, neste gráfico 3, os números são ainda mais conservadores no referente à exposição de informações da prefeitura. Neste gráfico, pudemos observar que 73,9% dos usuários dizem não compartilhar informações relacionadas às rotinas de trabalho em suas redes sociais, o que mostra que, de certa forma, a maioria deles não expõe dados da organização em locais não oficiais. Por outro lado, o valor correspondente àqueles que compartilham informações da organização (18,2%), ainda que bastante reduzido em relação ao primeiro valor citado, pode ser considerado alto, especialmente por não se poder aferir o que é compartilhado, quanto é compartilhado, e com quem é compartilhado. Isto pode ser considerado uma abertura a fim de comprometer a confidencialidade das informações pertinentes à organização, a depender do quão privativas são estas informações, e quão exploradas foram, se o foram, por *outsiders*.

Há de se ter um padrão de uso e de liberação de informações por parte da organização como garantia que apenas informações aprovadas, por vias aprovadas, sejam entregues aos munícipes. Faz-se necessário a conscientização destes usuários, sobre normas de compartilhamento de dados e informações que sigam requisitos estabelecidos pela prefeitura.

O grupo de questões seguintes é a respeito de conhecimentos gerais sobre SI.

Gráfico 4 – Conhecimento sobre Engenharia Social

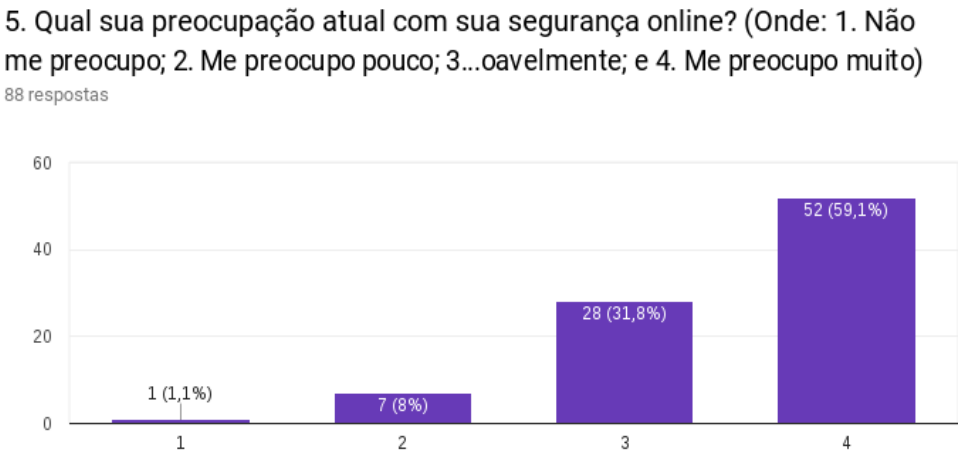


Fonte: Autoria própria (2018). Dados da pesquisa.

Como se pode observar pelas respostas à questão do gráfico 4, apenas 19,3% dos usuários da organização já ouviram falar de Engenharia Social e, portanto, podem estar cientes do que representa. Considerando que mesma uma exposição primária ao conceito não é suficiente para garantir o conhecimento dos usuários, temos aqui uma área importante para conscientização.

Daqui concluímos que, ao menos da parte da organização, não há um programa de conscientização sobre o tema. Há de se aplicar políticas neste campo para que usuários tomem conhecimento sobre o que é a Engenharia Social, quais suas técnicas, os riscos envolvidos e como evitá-la.

Gráfico 5 – Preocupação com segurança *online*

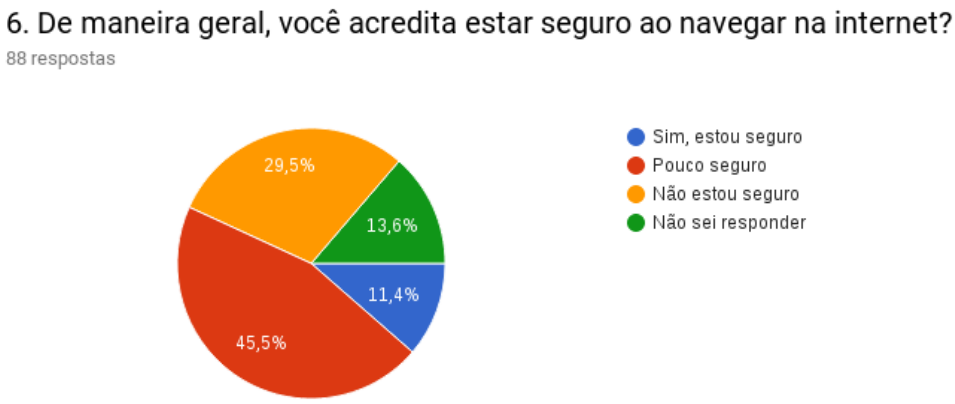


Fonte: Autoria própria (2018). Dados da pesquisa.

Podemos observar no gráfico 5 que a maioria dos usuários se considera preocupada com sua segurança *online*. Cinquenta e dois respondentes, isto é, 59,1% disseram se preocupar muito com sua segurança *online*, e vinte e oito, ou 31,8%, disseram se preocupar razoavelmente com sua segurança *online*, o que nos garante um universo de 90,9% dos respondentes preocupados em nível consideravelmente bom com sua segurança. No entanto, há de se considerar o quê estes consideram uma preocupação razoável ou importante.

A questão seguinte pode dar uma dimensão desta questão.

Gráfico 6 – Sentimento de segurança *online*



Fonte: Autoria própria (2018). Dados da pesquisa.

Um dado bom para firmar a preocupação apresentada no gráfico referente à questão número 5 está presente neste, referente à questão 6. Aqui vemos que apenas 11,4% dos usuários dizem se sentir seguros ao navegar. Ora, consideremos necessário o sentido de alerta àqueles que querem estar seguros na *internet*, uma vez que, como se sabe, a desconfiança é essencial para se buscar a segurança. Aqui vemos que 75% dos usuários se sentem pouco seguros (45,5%) ou não seguros (29,5%) ao navegarem.

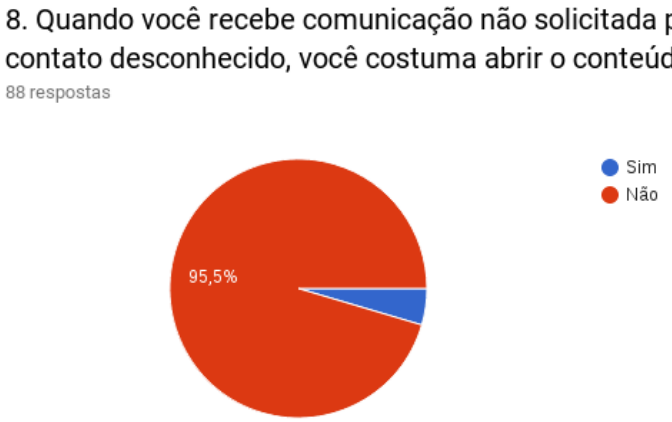
Gráfico 7 – Comportamento frente a mensagens não solicitadas de *e-mail*

Fonte: Autoria própria (2018). Dados da pesquisa.

Constatamos certa consistência nos números ao verificarmos que, relacionado à questão apresentada no gráfico 7, 75% dos usuários consultam os remetentes ao receberm comunicação não solicitada, buscando confirmar sua procedência.

É essencial a comunicação interna entre colaboradores, um senso de pertença estreitará relações e incentivará no desenvolvimento de uma cultura interna de segurança. Além de afugentar investidas exteriores.

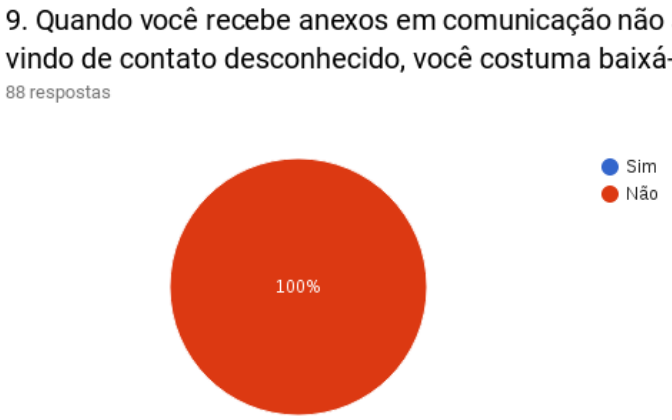
Gráfico 8 – Comportamento frente a mensagens desconhecidas *e-mail*



Fonte: Autoria própria (2018). Dados da pesquisa.

Na questão do gráfico 8, perguntados quanto a quando comunicação não solicitada é recebida por *e-mail* vindo de contatos desconhecidos, 95,5% dos respondentes, dizem não abrir a mensagem de *e-mail* recebida.

Gráfico 9 – Comportamento frente a anexos de mensagens desconhecidas de *e-mail*

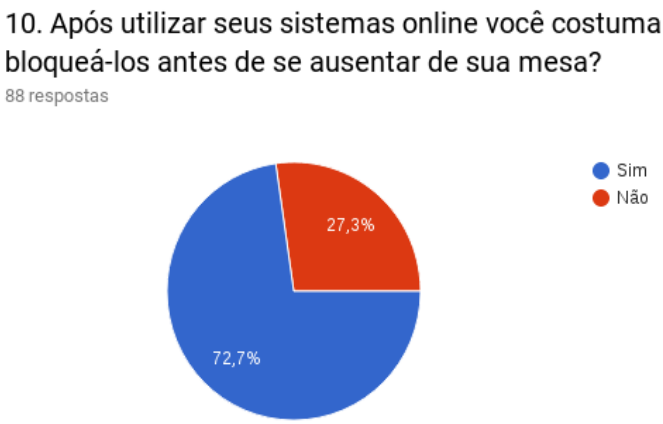


Fonte: Autoria própria (2018). Dados da pesquisa.

Ainda mais otimista que a questão do gráfico 7, somada às respostas relatadas no gráfico 8, e corroborando ao que podemos concluir então, vemos que todos os usuários, isto é 100% dos respondentes, evitam abrir conteúdo de *e-mail* ou anexos quando não

há solicitação do *e-mail*. Isto pode ser reflexo de ações tomadas no caso de *phishing* relatado anteriormente no contexto.

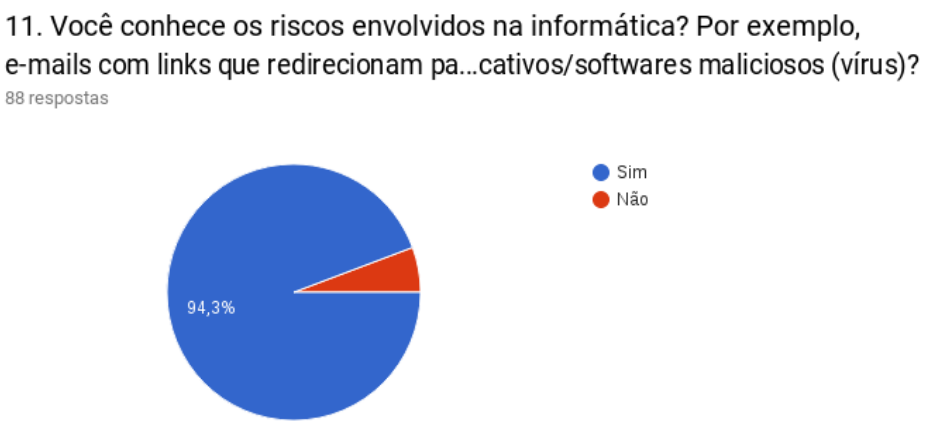
Gráfico 10 – Preocupação com segurança em sistemas *online*



Fonte: Autoria própria (2018). Dados da pesquisa.

Para evitar que invasores físicos tenham acesso às áreas de trabalho dos usuários de recursos de TI, é aconselhável que os usuários não ausentem-se de seus computadores sem antes bloquearem suas estações. No gráfico 10, vemos que 27,3% dos usuários ainda deixam suas áreas de trabalho, em seus computadores, expostas ao deixarem suas estações de trabalho.

Gráfico 11 – Conhecimentos sobre armadilhas *online*

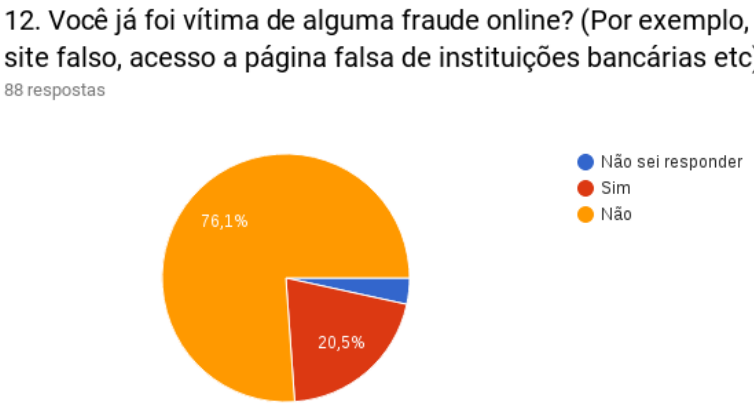


Fonte: Autoria própria (2018). Dados da pesquisa.

Grande parte dos usuários já sabem dos *malwares* e outras armadilhas e ferramentas maliciosas existentes na informática. À questão presente no gráfico 11, 94,3% dos respondentes disse estar ciente dos riscos envolvidos na informática.

É essencial mantê-los atualizados quanto às tendências atuais, com comunicados e, a depender das ameaças mais perigosas, palestras ou cursos.

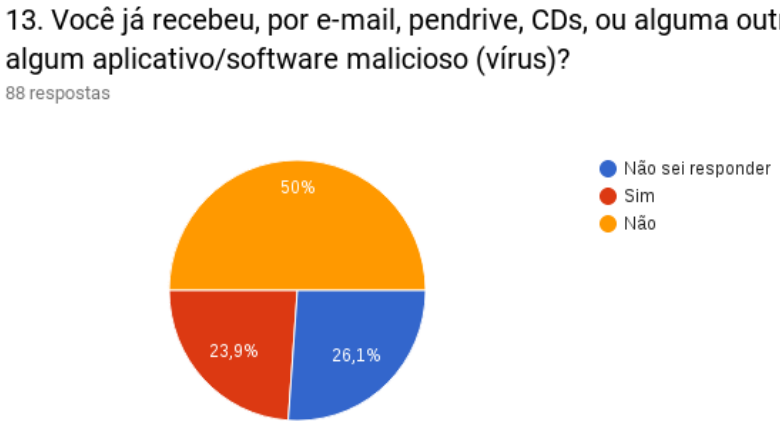
Gráfico 12 – Taxa de vitimização por fraude *online*



Fonte: Autoria própria (2018). Dados da pesquisa.

Quanto à questão do gráfico 12, a maioria dos respondentes, 76,1% diz nunca ter sido vítima de fraudes online, porém 20,5% diz já ter sido vitimada, o que configura um número consideravelmente grande. Ademais, é necessário lembrarmos que, muitas vezes, as fraudes se dão de maneira astuta a ponto de não serem notadas pelas vítimas. Um programa que explicite a forma de agir dos criminosos virtuais, bem como as técnicas utilizadas pode dar ao usuário uma dimensão maior de ação destes atacantes, para que se protejam.

Gráfico 13 – Taxa de infecção a partir de mídias

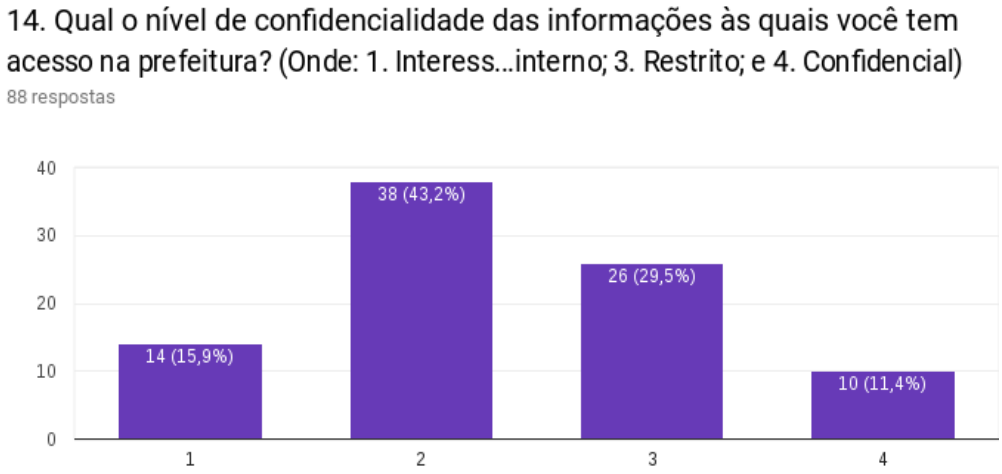


Fonte: Autoria própria (2018). Dados da pesquisa.

Apenas 23,9% assumem ter recebido aplicativo malicioso por *e-mail*, *pendrive*, *CDs*, isto significa que menos de um quarto dos respondentes podem ter sido infectados diretamente por uso de mídias, de onde podemos presumir que o uso de navegadores é a forma mais comum de infecção. Além disso, semelhantemente à análise anterior, há circunstâncias em que o usuário sequer sabe ter sido infectado.

O grupo de questões seguintes tratou da relação do usuário com a segurança lógica do patrimônio.

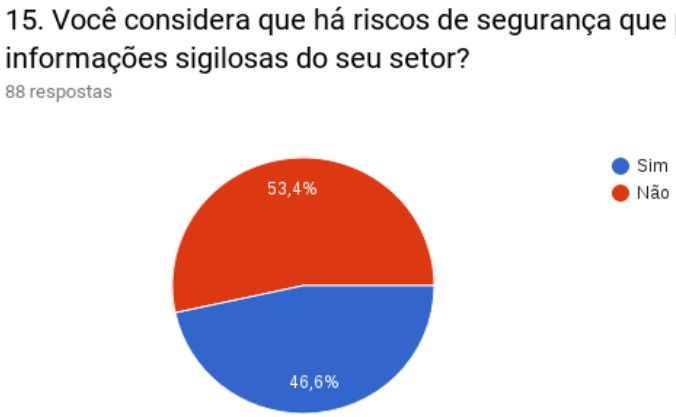
Gráfico 14 – Nível de confidencialidade com que o usuário trabalha



Fonte: Autoria própria (2018). Dados da pesquisa.

Neste histograma separamos a confidencialidade dos dados e informações da prefeitura em uma escala de quatro níveis. Para 29,5% dos respondentes as informações são de caráter restrito, isto é, de acesso exclusivo ao setor a que diz respeito, e para 11,4% são confidenciais, exclusivo para alta administração. A maior parte das informações (43,2%) diz respeito às informações de interesse interno, isto é, de rotinas processuais.

Gráfico 15 – Percepção de riscos de segurança

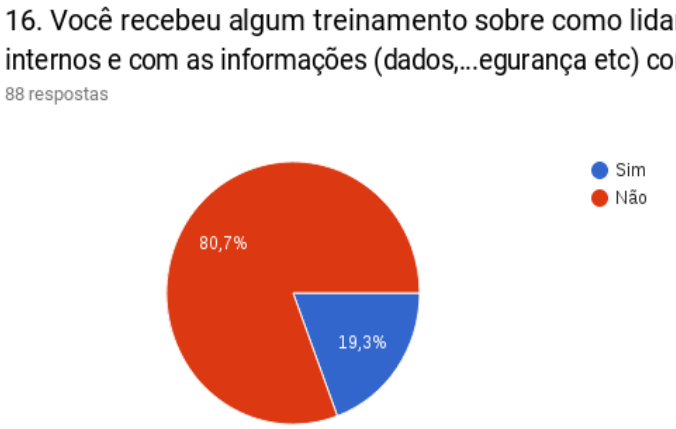


Fonte: Autoria própria (2018). Dados da pesquisa.

Como adicional ao gráfico “14”, aqui 46,6% dos respondentes alegam ver riscos que possam expor informações sigilosas de seus setores. Estes dados não incluem necessariamente todos aqueles que têm acesso a estes dados sigilosos.

Há que se identificar quais são as falhas enxergadas por estes usuários a fim de se pensar soluções. Adicionar a participação do usuário à prospecção destas falhas pode ser um meio de inseri-los a uma cultura de segurança.

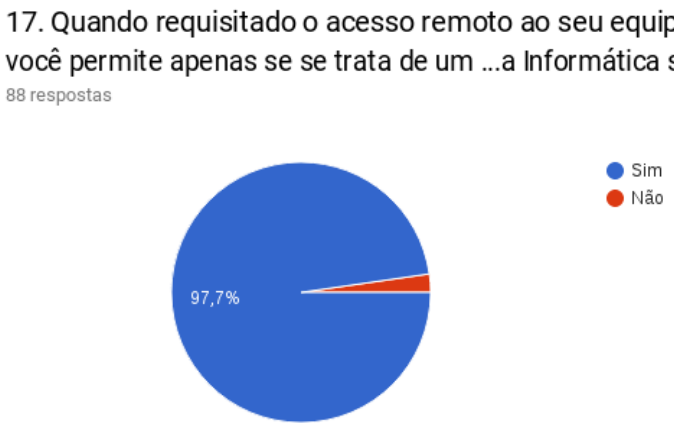
Gráfico 16 – Treinamento para processos internos



Fonte: Autoria própria (2018). Dados da pesquisa.

Aqui algo bastante preocupante e que se refere diretamente à questão do uso indevido que reflete na questão dos *insiders* não-maliciosos, em que 80,7% dos respondentes não receberam formação ou treinamento para trabalhar com os processos informatizados internos.

Gráfico 17 – Permissão de acesso remoto

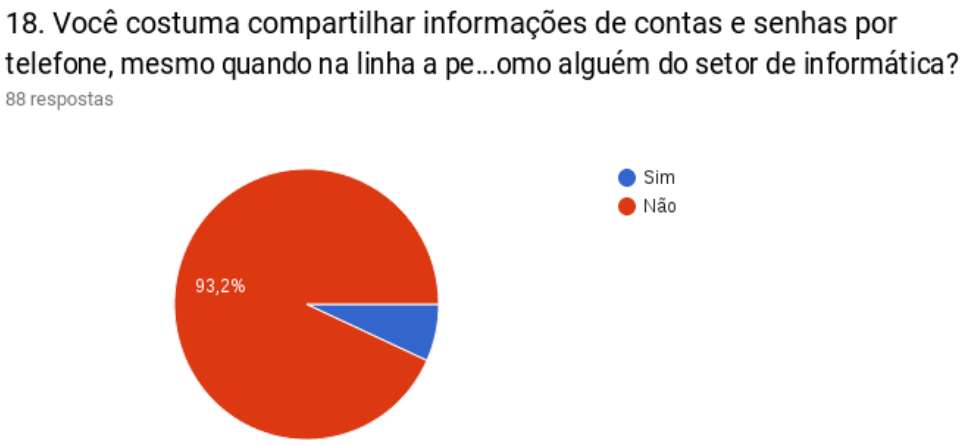


Fonte: Autoria própria (2018). Dados da pesquisa.

O acesso remoto as estações é feito por software terceiro - gratuíto. Os usuários em quase sua totalidade permitem o acesso apenas aos usuários da informática, no entanto, lembrando que, como explícito no gráfico “4” muitos desconhecem a Engenharia Social e suas técnicas, é possível que terceiros, se passando por gente da TI, consiga este acesso.

É necessário que as senhas de acesso remoto das estações sejam restritas aos responsáveis pela TI para evitar que sejam cedidas por engano a estranhos.

Gráfico 18 – Compartilhamento de informações por telefone



Fonte: Autoria própria (2018). Dados da pesquisa.

Segundo os dados obtidos na questão “18”, há aparente conscientização quanto a importância de não compartilhar informações de *login* e senha. A popularização dos acessos informatizados, especificamente os relativos a *internet banking* podem ter ajudado a espalhar esta percepção de comportamento seguro. Porém, não obstante 93,2% dos usuários aleguem não compartilhar estas informações, o meio mais comum de se obter tais informações é por meio de observação do usuário, pelo método de Engenharia Social chamado *shoulder surfing*, como relatado anteriormente.

Gráfico 19 – Tratamento com munícipes e outros terceiros

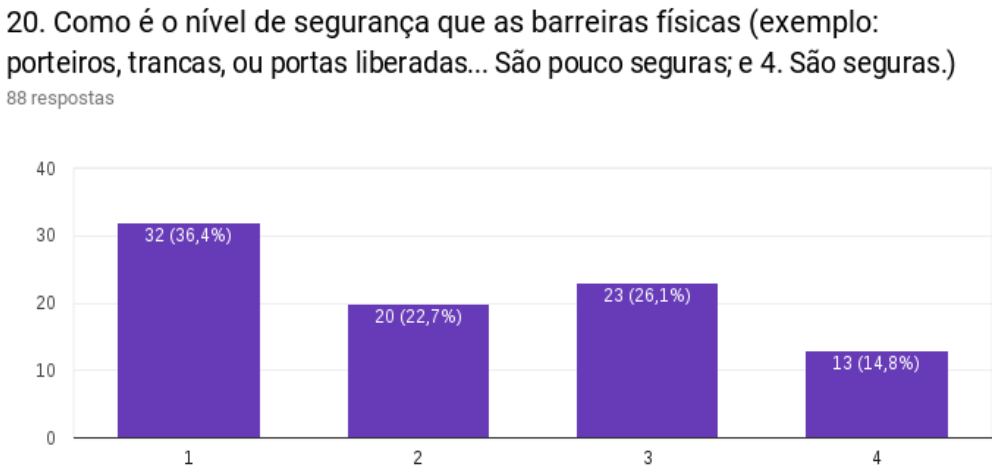
Fonte: Autoria própria (2018). Dados da pesquisa.

No gráfico “19”, 85,2% dos respondentes disse seguir o estabelecido no sistema interno de protocolo, dando formalidade aos processos. No entanto 14,8% preferem priorizar entrega de resultados de maneira informal, acreditando ser mais objetivo e rápido.

É importante, para se minimizar erros individuais a serem exploradas por terceiros, e a manutenção de uma trilha de auditoria, o registro de cada passo de um processo. Não há governança, portanto não há uma mentalidade comum quanto aos objetivos estratégicos. Porém, há a normatização do sistema de protocolo para evitar fraudes e extravio de informações. O objeto de estudos precisa estabelecer suas prioridades por meio de governança para que projetos de conscientização levem a todos um padrão de atuação segundo seus objetivos.

O grupo seguinte de questões tratou da percepção da segurança física do patrimônio.

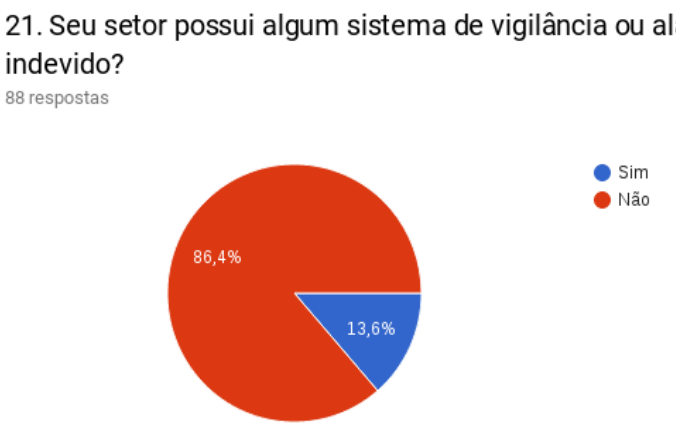
Gráfico 20 – Percepção de segurança física



Fonte: Autoria própria (2018). Dados da pesquisa.

A fim de se evitar invasões físicas há de se elaborar uma série de barreiras que dificultem ao máximo a investida de estranhos ao ambiente de negócio. No entanto, de acordo com o histograma do gráfico referente à questão “20”, apenas 14,8% considera que as barreiras existentes são seguras. Para 22,7% há barreiras insuficientes para impedir o acesso físico de estranhos aos seus locais de trabalho, sendo que para 36,4% não há barreira alguma. A julgar pelas observações dos setores há, de fato, várias vulnerabilidades, como processos e computadores acessíveis a quaisquer visitantes, pontos de rede expostos, de forma que é plausível a preocupação com segurança por parte dos usuários.

Gráfico 21 – Sistemas de vigilância ou alarme



Fonte: Autoria própria (2018): Dados da pesquisa.

Adendo ao gráfico anterior, na questão “21”, 86,4% alegam que não há sistema de vigilância contra acesso indevido em seus setores. De fato, pelas observações, os sistemas de vigilância se atém ao exterior do Paço, e às entradas, após as quais, não há mais sistema de câmeras de vigilância, alarmes ou algo semelhante.

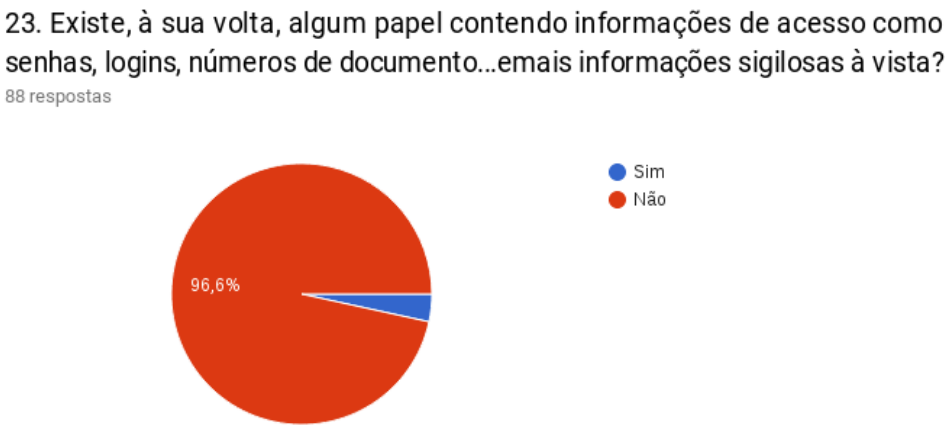
Gráfico 22 – Armazenamento de pertences

Fonte: Autoria própria (2018): Dados da pesquisa.

Seguindo a série iniciada com o gráfico “20”, na questão “22”, 86,4% alegam não possuir armários seguros para guardar pertences. A questão do furto de pertences é pertinente para este projeto da mesma forma como é a questão da exposição das vulnerabilidades particulares ou profissionais numa rede social. São meios que um engenheiro social pode se utilizar para obter acesso a informações úteis para si.

Existe a necessidade de se desenvolver um sistema de controle de acesso físico aos setores que, em maioria, estão expostos a acesso indevido por engenheiros sociais bem como um sistema de vigilância e monitoramento que coíba sua ação e a disponibilização de locais seguros para armazenamento de dispositivos pessoais.

Gráfico 23 – Atenção à exposição de dados

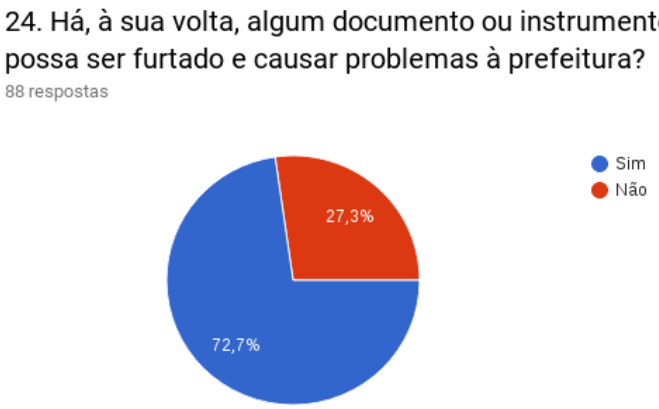


Fonte: Autoria própria (2018): Dados da pesquisa.

Segundo as respostas à questão “23”, 96,6% dos usuários dizem não manter anotações com dados confidenciais à sua volta. Aparentemente estão cientes da importância de não se deixar anotações sobre suas mesas que remetam a informações sigilosas, como senhas, *logins* e documentos.

No entanto, é importante sempre reforçar a importância deste procedimento, bem como garantir políticas que evitem que os usuários vejam neste recurso uma necessidade. Trata-se de uma vulnerabilidade a que muitos podem, por vezes, negligenciar a depender de vários aspectos, como por exemplo, a necessidade de memorizar muitos dados, ou guardar informações muito complexas, como por exemplo, quando da existência de uma política de senha bastante exigente. São práticas comuns no dia a dia e que precisam ser evitadas.

Gráfico 24 – Atenção à exposição de documentos



Fonte: Autoria própria (2018): Dados da pesquisa.

Ao contrário ao obtido na questão anterior, o gráfico da questão “24” nos relata que para 72,7% dos respondentes há processos e outros documentos em suas mesas que, se furtados, podem causar problemas à prefeitura por sua importância.

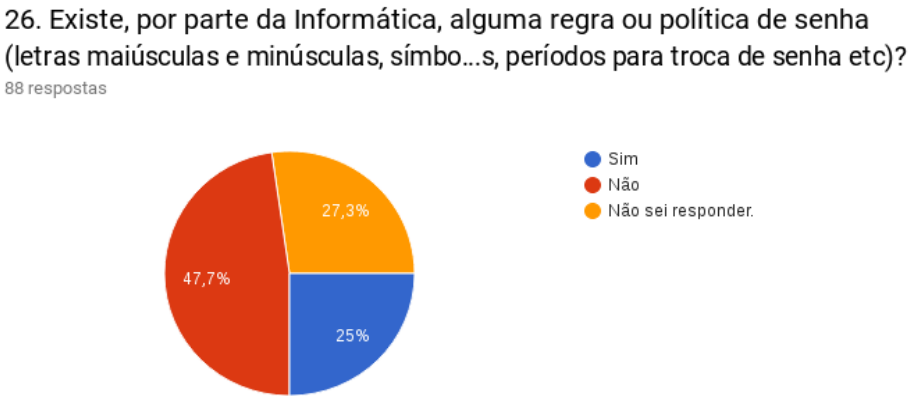
É necessário, portanto, que tais materiais sejam devidamente guardados quando não mais em uso, e que não sejam deixados ao acesso fácil para quaisquer pessoas enquanto se trabalha neles. Ora, é necessário tanto dar meios para que os usuários possam guardar com segurança estes documentos durante ou após o andamento do processo, como que ofereçam as barreiras necessárias para barrar acesso indevido.

Gráfico 25 – Complexidade das senhas usadas

Fonte: Autoria própria (2018). Dados da pesquisa.

Nenhum usuário respondeu usar a senha em branco, no gráfico “25”, no entanto, 60,2% alegam utilizar senhas formadas apenas por números, a combinação mais simples para senhas. Se tomarmos por base uma combinação de 4 caracteres para uma senha formada apenas por números, temos um total de 10.000 combinações (10^4) possíveis, algo extremamente sensível a um ataque de força bruta; a terceira combinação mais simples, com números e letras apenas em caixa alta ou baixa aumenta as combinações possíveis para aproximadamente 1.680.000 com os mesmos quatro caracteres.

Gráfico 26 – Conhecimentos sobre políticas de senha

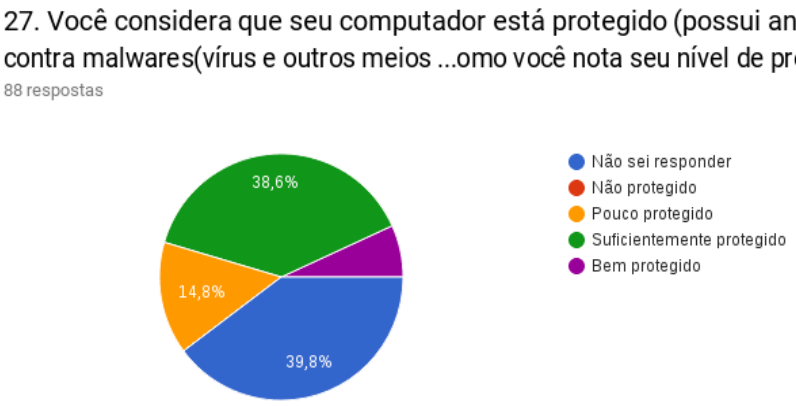


Fonte: Autoria própria (2018). Dados da pesquisa.

Do gráfico anterior decorre que, ainda que a organização não aplique uma política de senhas, como é possível notar pelo gráfico “26”, onde 47,7% dizem não seguir uma política de senha, e de fato, de acordo com o departamento de TI não há, é importante fazer com que os usuários saibam da importância do uso de senhas mais fortes, e de como isto aumenta sua segurança *online*.

Outra informação a se obter daqui, especificamente pela discordância nos números, que não há uma conversa constante entre departamento de TI e usuário, a fim de elucidar algumas questões, como a existência ou não de uma política de senha. É essencial que o departamento de TI mantenha contato com cada área do negócio, especialmente que receba destas o necessário *feedback* para suas políticas e ações. A participação do fator humano é essencial para segurança, como vimos.

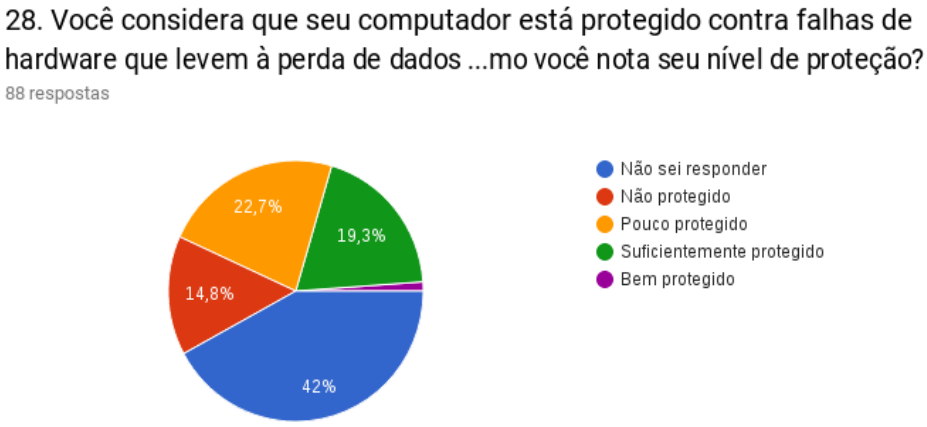
Gráfico 27 – Sensação de proteção contra *malwares*



Fonte: Autoria própria (2018). Dados da pesquisa.

Para além dos 39,8% dos usuários que não estão certos a respeito da presença de uma proteção ativa contra *malwares* em suas máquinas, outra evidência da falta de comunicação e conscientização quanto à cultura de segurança da informação necessária, a percepção de segurança dos usuários é de que estão seguros (38,6%), considerando que apenas 14,8% consideram se sentir pouco protegidos. Neste aspecto, a desconfiança do usuário não é tão produtiva, uma vez que as instalações dos sistemas antivírus dependem necessariamente do departamento de TI. Porém é necessária a confiança neste departamento para que as devidas comunicações de eventos de segurança ou incidentes sejam devidamente notificados.

Gráfico 28 – Percepção de segurança de hardware

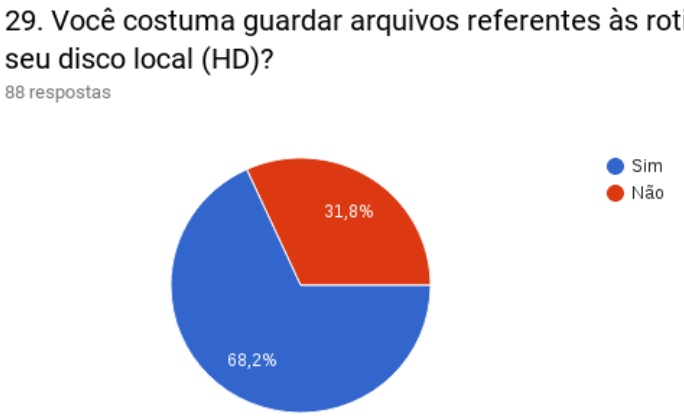


Fonte: Autoria própria (2018). Dados de pesquisa.

Muito mais do que mostrar como se sentem em relação a segurança de seus dados, esta questão mostra que os usuários em grande parte (42%) não sabem sequer responder se há proteção contra falhas. Apenas 19,3% consideram estar protegido suficientemente.

Uma política de SI que contemple uma gestão de riscos e apresente-se aos usuários por meio de programas de conscientização poderia mudar esta percepção de segurança. É importante que o usuário saiba o que é necessário para maximizar sua segurança, que ferramentas têm a disposição, e que confie no departamento de informática, ao mesmo passo que desconfie da sua efetiva segurança. Uma comunicação constante com os responsáveis por sua segurança, como notado anteriormente, reportando problemas e sugerindo melhores procedimentos para seu trabalho é essencial para melhoria contínua dos serviços.

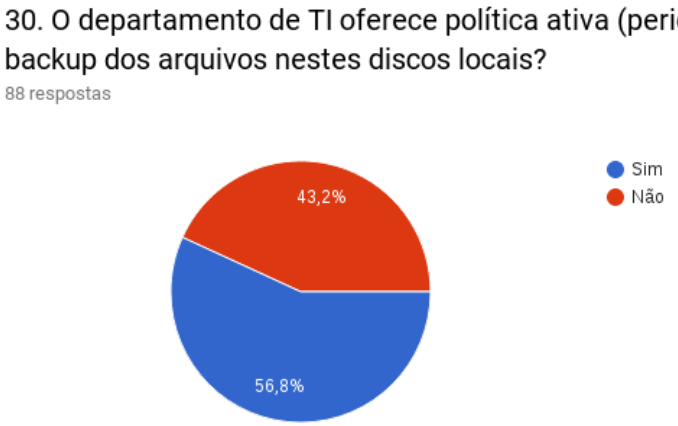
Gráfico 29 – Guarda de dados pessoais em disco local



Fonte: Autoria própria (2018). Dados de pesquisa.

Dos respondentes 68,2% dizem, no gráfico “29”, que guardam seus arquivos no disco local. O departamento de informática não garante o *backup* destes arquivos. A manutenção é a responsável por garantir a guarda dos arquivos dentro das possibilidades quando necessária manutenção dos computadores. Além disto é responsabilidade do usuário o bom uso de seu equipamento de informática.

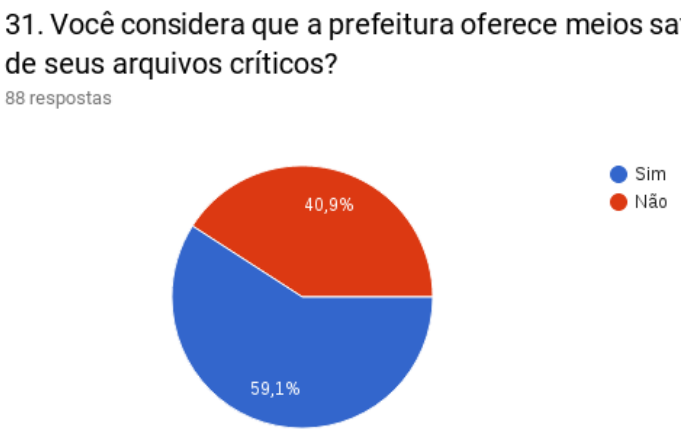
Gráfico 30 – Conhecimento sobre política de *backup*



Fonte: Autoria própria (2018). Dados da pesquisa.

Ao mesmo tempo, 56,8% dizem, no gráfico “30” que o departamento de TI oferece uma política de backup dos arquivos.

Gráfico 31 – Percepção sobre política de *backup*



Fonte: Autoria própria (2018). Dados da pesquisa.

Completando esta série desde o gráfico “29”, no gráfico “31”, 59,1% considera que os meios de *backup* são satisfatórios.

Ora, segundo apurado com a organização, os *backups* são feitos apenas dos dados guardados em servidor, não sendo estendidos aos discos locais dos computadores, sendo que, referente ao gráfico “29”, apenas 31,8% guardam os dados nas pastas protegidas por backup, ou seja, aqueles que não guardam representam um número crítico a depender do nível de importância das informações com as quais lidam.

3.1.4. Alguns riscos relatados

A partir dos dados obtidos de nosso questionário, tomando os ativos inventariados, fizemos a identificação de vulnerabilidades e ameaças, bem como dos riscos existentes nestas relações, a seguir estes riscos foram colocados em tabelas para leitura.

Tabela 2 – Tabela de Riscos 1: Sistema de Protocolo

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Intranet: Sistema de Protocolo	*Insider:* Erro Humano	Falta de treinamento de funcionários	Inserção errônea de dados	Inconsistência da informação	Máscaras de entrada de dados	Possibilidade de desativar um processo sem exclusão. Manter trilha de auditoria
Intranet: Sistema de Protocolo	*Insider:* Erro Humano	Falta de treinamento de funcionários	Movimentação imprópria de processo	Extravio de documentação	Trilha com registro de atividades (Auditabilidade)	
Intranet: Sistema de Protocolo	*Insider ou Outsider: A*cesso Indevido	Quebra de senha por força bruta	Acesso indevido	Modificações indevidas nos andamentos dos processos, exclusão ou inclusão indevida.	Limite de tentativas de login até bloqueio de conta	
Intranet: Sistema de Protocolo	*Insider: V*andalismo	Multiplas inserções por usuário, gerando muitos protocolos	Criação de informação inútil. Lixo digital	Números de protocolo são limitados, e as buscas podem retornar informações irrelevantes	Trilha de auditoria. Reativamente é possível bloquear usuários	
Intranet: Sistema de Protocolo	*Outsider: D.D.o.S.*	Sistema localizado em servidor próprio. Não possui serviço anti-D.D.o.S.	Inúmeras requisições ao sistema de busca pública	Instabilidade ou parada de serviços.	[não há]	Identificação pessoal para busca de protocolo. Sistema anti-D.D.o.S.

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 3 – Tabela de Riscos 2: Sistemas de Gestão

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Intranet: Sistemas de Gestão	*Insider* ou *Outsider*: Engenharia Social - *Impersonation*	Identificação forjada como suporte da empresa terceirizada	Exposição de informações de senhas ou logins	Acesso indevido. *Hacking*	[não há]	Alertar sobre práticas de Engenharia Social e solicitar que sempre se busque a TI como mediador de sistemas de terceiros
Intranet: Sistemas de Gestão	*Insider* ou *Outsider*: Corrupção	Privilégio cedido por funcionário	Assédio de concorrência por vantagens em contratos de licitações	Adulteração de valores em sistema de licitações	Trilha de auditoria	

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 4 – Tabela de Riscos 3: Vários ativos 1

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Intranet: Sistema de Ponto	*Insider* ou *Outsider*: fraude	Adulteração de entradas de registro de ponto	Alteração em valores de ponto eletrônico	Fraude nos horários de trabalho bem como na folha de pagamento	Câmera de vigilância sobre relógio ponto	Localizar o sistema de ponto em local cujo acesso físico seja mais difícil ou controlado
Intranet: atualização de notícias no *website*	*Outsider*: Adulteração	*Não possui detecção ou bloqueio de contas por tentativa de acesso por força bruta*	Inserção indevida de informações comprometedoras	Credibilidade da prefeitura e questões políticas	[não há]	Associar conta ao usuário de AD, procedendo no bloqueio de conta ao se tentar acesso múltiplas vezes
Câmeras de vigilância	*Outsider*: Vandalismo	Câmeras de vigilância estão expostas do lado exterior da prefeitura	Podem ser danificadas por motivações torpes, ou políticas, ou ainda serem roubadas	Financeiras e possível quebra de segurança física.	Guardas-civis municipais fazem a segurança patrimonial em tempo integral	
Monitores de vigilância	*Insider*: uso negligente	Está em local público	Ação de curiosos ou manipulação incorreta durante limpeza ou outro procedimento de manipulação	Danos físicos ou desconfiguração.	Guardas-civis municipais fazem a segurança patrimonial em tempo parcial	Alocar em posição de difícil acesso a curiosos e orientar pessoal de limpeza sobre correta manipulação
Acesso a Contas Bancárias	*Insider* ou *Outsider*: Fraude	Sistemas Operacionais desatualizados não oferecem segurança devida a *internet banking*	Acesso indevido a contas da prefeitura e seus recursos financeiros	Movimentação, espionagem e alterações indevidas em valores e informações financeiras, etc.	[não há]	Alerta sobre riscos em uso de sistemas desatualizados. Upgrade e update de equipamentos que fazem uso de sistemas críticos

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 5 – Tabela de Riscos 4: *Webmail*

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Webmail	*Outsider*: Engenharia Social - *Baiting*	Usuário não conhece ataques desta natureza	Ataque por *ramsonware*	Perda de dados e informações de maneira irreversível	*Software* antivírus	Avisos frequentes sobre os riscos de *e-mails* e anexos não solicitador. Conscientização sobre riscos e treinamentos para uso da ferramenta.
Webmail	*Outsider: phishing*	Usuário não conhece ataques desta natureza	Aplicação de fraude: p.ex. Captura de senhas	Exposição de senhas de uso particular da organização	*Antispam*	Programa de conscientização sobre práticas de criminosos e suas técnicas, bem como atualizações frequentes sobre tendências e ameaças atuais. Treinamento sobre identificação de sites falsos.
Webmail	*Outsider: baiting*	Usuário acidentalmente clica em link	Infecção por *malware*	Infecção de computador ou rede por *malware* nocivo	*Software* antivírus	Conscientização e alertas constantes para riscos de *e-mails* não solicitados
Webmail	*Insider* ou *Outsider*: Vandalismo	Senha pessoal de baixa complexidade	Exposição de informações pertinentes à prefeitura	Acesso indevido por quebra de senha por meio de força bruta	[Não há]	Conscientização sobre práticas seguras e riscos envolvidos
Webmail	*Outsider*: Engenharia Social - *phishing*	Falta de conscientização de funcionários.	Exposição a práticas de *phishing*	Infecção por *malware*	Comunicações eventuais por *e-mails*	Conscientização sobre práticas seguras e riscos envolvidos
Webmail	*Insider* ou *Outsider*: Vandalismo	Uso de conta de e-mail com senha em branco	Acesso indevido e uso abusivo	Exposição de informções pessoais ou da prefeitura, comunicações falsas. Recolhimento de informações que eventualmente encontrar para outros fins quaisquer	[Não há]	Conscientização sobre práticas seguras e riscos envolvidos
Webmail	Engenharia Social: *eavesdroping* ou *shoulder surfing*	Terceiros que tenham acesso ao interior da prefeitura podem observar comportamentos ou anotações que entreguem informações	Aquisição de informações privilegiadas e indevidas	Furto de dados, logins, senhas ou segredos da prefeitura.	[Após acesso garantido, praticamente não há]	Conscientização sobre práticas seguras: observar ao redor quanto a pessoas que estejam transitando por perto. Conscientizar usuário para que não mantenham anotações sobre as mesas com senhas e *logins*

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 6 – Tabela de Riscos 5: Vários ativos 2

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Relógio-ponto biométrico (Toda a prefeitura)	*Insider ou Outsider:* Vandalismo - motivação política	Entrada não autorizada. Fácil acesso a depender das circunstâncias.	Dano proposital	Paralisação do registro de ponto dos funcionários	[Não há dispositivo reserva]	Troca das portas de vidro por outro formato mais seguro ou guarda-civil em tempo integral.
Identidade/ Certificado Digital (Sec. Jurídico)	*Insider ou Outsider:* Furto (*pretexting, tailgating, RSE*)	Setores não oferecem locais seguros para guarda de pertences	Objeto deixado sobre a mesa pode ser furtado durante expediente	Uso em sistema de peticionamento para fins escusos / Forjamento de direitos	[não há]	Conscientização sobre riscos de guarda negligente
Sistema de peticionamento	*Insider* ou *Outsider:* Forjamento de direitos	Uso irrestrito de identidade	*Uma vez em posse de identidade digital furtada, e disponto do PIN, é possível fazer uso irrestrito do documento*	Movimentação e alterações indevidas em processos judiciais, espionagem, etc.	[não há]	Conscientização sobre riscos de guarda negligente de pertences críticos

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 7 – Tabela de Riscos 6: Computador pessoal

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Computador Pessoal	*Insider:* Erro Humano	Remoção acidental de arquivo	Remoção de arquivos críticos	Perda de dados e informações	Backup de arquivos em diretório comum	Instrução sobre uso ideal
Computador Pessoal	*Insider*: Mau uso	Danos ao Disco Rígido	Danos ao disco após batidas ou quedas	Perda de dados e informações	[não há]	Alertar usuários para que guardem seus arquivos no diretório comum
Computador Pessoal	*Outsider*: Engenharia Social – *pretexting*	Falta de conscientização de funcionários	Outsider se apresenta como sendo novo funcionário da TI	Acesso garantido a equipamento de TI	[não há]	Apresentação de cada novo funcionário aos setores como medida cultural a se adotar. Alertar para que se desconfie de quem não foi apresentado.
Computador Pessoal	*Outsider*: Uso não autorizado	Acesso às portas USB	Instalação de *keylogger*	Furto de dados	[Uma vez quehá acesso aos computadores, não há]	Melhores meios protetivos físicos. Bloqueio de portas USB

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 8 – Tabela de Riscos 7: Sistema Operacional

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Sistema Operacional	*Insider*: Erro Humano	Tela desbloqueada	Abertura para ação de curiosos	Possibilidade de exploração	[não há]	Conscientização quanto ao risco
Sistema Operacional	*Outsider*: Engenharia Social - *impersonating*	Acesso remoto por terceiro	Acesso ao interior da rede da prefeitura	Possibilidade de exploração da rede, cópia de dados e informações, furto de *hashes* de senhas, etc.	[não há]	Conscientização quanto ao risco
Sistema Operacional	*Outsider*: Uso não autorizado	Acesso indevido de recursos	Acesso ao interior da rede da prefeitura. Possibilidade de uso pessoal de recursos para quaisquer fins possíveis	Possibilidade de exploração da rede, cópia de dados e informações, furto de *hashes* de senhas, etc.	[Uma vez quehá acesso aos computadores, não há]	Conscientização quanto ao risco de ausentar-se de seu computador sem bloqueá-lo

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 9 – Tabela de Riscos 8: Diretórios compartilhados

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Diretórios compartilhados	*Insider*: Erro Humano	Arquivos podem ser apagados ou movidos por quaisquer usuários com permissão ao diretório	Remoção de arquivos críticos	Perda de dados e informações	Política de *backup* regular	Instrução sobre uso ideal
Diretórios compartilhados	*Insider*: Erro Humano	Alteração de dados por *insider* negligente	Quebra de consistência de dados. Adulteração de informação.	A depender da informação: financeiras, contabilisticas, sociais, etc.	Política de *backup* regular	Instrução sobre uso ideal
Diretórios compartilhados	*Insider*: Vingança	Acesso permitido a quem possua *login* ativo a todos os diretórios do setor	Remoção, alteração e vandalismo de arquivos críticos	Perda de dados e informações	Política de *backup* regular	Conscientização e participação em comunidade. Criar cultura de segurança com comunicação entre setores, especialmente RH e TI. Bloquear acesso de ex-funcionários imediatamente.

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 10 – Tabela de Riscos 9: Documento e *Hardware*

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Hardware – Discos Rígidos	*Outsider*: Engenharia Socia - *Dumpster diving*	Reconhecimento de informações privadas em Discos Rígidos	Acesso a Hds descartados inapropriadamente	Furto de dados	[Não há política de descarte]	Elaborar normas para descarte de documentos e equipamentos
Documentações	*Outsider*: Engenharia Socia - *Dumpster diving*	Reconhecimento de informações privadas em Documentos	Acesso a documentos descartados inapropriadamente	Furto de dados	[Não há política de descarte]	Elaborar normas para descarte de documentos e equipamentos
Documentações	Engenharia Social: *tailgating*	Acesso físico a local restrito	Furto de informações sigilosas	Exposição de documentação interna sobre locais de trabalho. Furto de informações de munícipes, dados de projetos, etc	Alguns locais possuem barreiras físicas	Implementação de barreiras físicas e procedimentos de segurança padrão que coíbam este tipo de ação.

Fonte: Autoria própria (2018). Dados da pesquisa.

Tabela 11 – Tabela de Riscos 10: Ativos intangíveis

Ativos de Informação	Ameaças	Vulnerabilidades	Descrição do Risco	Consequências	Controles	Medidas possíveis
Informações sigilosas específicas	Outsider: Engenharia Social – *pretexting*	Falta de conscientização de funcionários.	Furto de informações sigilosas	Acesso indevido a dados, informações.	[não há]	Conscientização e orientação aos usuários para que não forneçam quaisquer dados por *e-mail*, telefone, etc
Informações sigilosas específicas	*Outsider: RSE*	Obtenção de informação de maneira sistemática	Um ataque planejada e direcionado a uma informação de valor político	Informações que venham a causar impacto político afetando a reputação de pessoa pública, do governo ou da prefeitura.	[não há]	Conscientização e treinamento sobre técnicas de Engenharia Social
Informações sigilosas específicas	*Insider:* Erro Humano	Exposição pública de informação em redes sociais ou outros meios	Exposição de informações pertinentes à munícipe	Quebra de confidencialidade. A depender da importância da informação pode configurar grande prejuízo financeiro ou social para prefeitura ou para munícipes	[não há]	Padrão de uso e de liberação de informações da organização. Conscientização de usuários quanto a estas usos.
Colaborador	*Outsider*: Engenheiros Sociais	Fraquezas humanas diversas	Exploração de pessoas para obter informações privilegiadas dentro da organização	Acesso indevido a dados, informações, documentos, equipamentos etc	[Varia de usuário para usuário]	Treinamento e conscientização frequente abordando temas a respeito de Engenharia Social e *hacking*

Fonte: Autoria própria (2018). Dados da pesquisa.

Aqui relatamos alguns riscos, sem discriminar necessariamente os setores e processos a que se referem cada ativo. Para tal será necessário uma análise ainda mais aprofundada dos processos internos, bem como um detalhamento maior de cada um.

Ademais, um projeto que contemplo tal nível de detalhe demanda ainda mais tempo e recursos, e certamente sairia do escopo deste trabalho de graduação, pretendemos dar uma dimensão preliminar dos riscos existentes e de algumas possíveis medidas.

A partir deste ponto, a ISO 27005 tomaria os riscos encontrados e os submeteria ao seu tratamento, como mostramos. Tal procedimento se retroalimenta continuamente, gerando um ciclo de melhoria contínua.

CONCLUSÃO

Como parte do processo de adaptação a uma gestão de riscos, sugere-se a adequação da prefeitura a um modelo de governança, com investimento em pessoas, adoção de uma política de SI e entrada na governança, tanto de TI quanto corporativa, atendendo-se, claro, às particularidades da coisa pública. Considerando as pessoas, isto é, o fator humano, sugere-se a adoção de uma "cultura de SI", em que os usuários sejam ativamente conscientizados sobre os riscos existentes, e os meios adequados para se manterem seguros contra investidas exteriores. Sugere-se ainda, formas de gestão de pessoas que garantam ao usuário sua satisfação e contínua inserção na comunidade local formada pelos colaboradores da organização. Um norte pode ser o que escreve o Nobel em literatura de 1981, Elias Canneti, em seu "Massa e poder":

> A massa necessita de uma direção. Ela está em movimento e move-se rumo a alguma coisa. A direção comum a todos os seus membros fortalece o sentimento de igualdade. Uma meta exterior aos indivíduos e idêntica para todos soterra as metas particulares e desiguais que significam a morte da massa. A direção é imprescindível para sua durabilidade. (CANNETI, 1995, p. 16 *apud* MORGENSTERN, 2015)

Entenda a massa, aqui, como a comunidade, os funcionários. Ora, isto o que fala Canneti é a Engenharia Social em ação, uma Engenharia Social usada para o bem da organização, em combate aos engenheiros sociais *outsiders,* a quem o poder é visado para seus próprios fins escusos.

Um modelo de gestão de TI maduro deve alicerçar-se pela governança, e isto envolve uma abordagem holística da gestão de riscos de SI, isto é, que contemple, sim, os pilares dos processos e tecnologias, mas que não negligencie o fator humano. E quando tratamos de questões relacionadas ao fator humano, não podemos usar da mesma abordagem técnica de que dispomos para tratar os equipamentos de informática.

As pessoas, como mostrado, são o elo fraco na segurança, e a solução passa primordialmente pelos métodos sociológicos e educacionais para contornar suas falhas. Segundo nos recomenda a Internet Society em relatório devemos:

- Colocar os usuários sempre no centro de todas as soluções;
- Aumentar a transparência a respeito de violação de dados e divulgação;
- Segurança da Informação deve ser prioridade e as organizações devem possuir altos padrões de práticas e segurança;
- Organizações devem se responsabilizar por suas violações; e
- Aumentar incentivo de mercado para o desenvolvimento de métodos de segurança. (2016, p. 19).

Complementar a isto, segundo Josué das Chagas Menezes relata em seu livro "Gestão da Segurança da Informação", o Decreto Nº 3.505 de 13 de junho de 2000, do Governo Federal brasileiro, que estabelece a criação de um Comitê Gestor de Segurança da Informação (CGSI), e que institui sua Política de Segurança da Informação definindo como pressupostos básicos alguns métodos de prevenção de incidentes dos quais dois nos são particularmente úteis:

- Criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
- Conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade;
(MENEZES, 2006, p. 49).

É o que defendemos aqui: é preciso convencer os órgãos públicos, especificamente nosso objeto de estudos, sobre a necessidade de um projeto de gestão de riscos alinhado a uma governança de TI, e a abordagem especial sobre o fator humano na elaboração de políticas de SI e sua propagação. Assim, também nos diz Marciano:

> não se vê uma discussão adequada sobre o grau de receptividade a estas políticas, nem se apresentam, de modo metódico, questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir (2006, p. 109)

Portanto, resumimos assim: a prefeitura deve adaptar-se à governança de TI, gerir a TI com foco nos riscos ao negócio, e focar nos riscos sobre o fator humano. Marciano, ainda nos recomenda assim proceder sobre a adaptação da cultura organizacional às práticas seguras, e políticas de segurança, ainda acrescenta: "quanto mais rapidamente a prática se torna um ritual, mais facilmente a norma é obedecida, evitando assim o individualismo e os comportamentos aversivos às práticas prescritas como adequadas" (2006, p. 190).

A cultura deve ser desenvolvida e pautada em princípios de negócios que envolvam toda as lideranças. Uma recomendação de abordagem sobre como olhar para o desenvolvimento desta cultura de segurança, nos é deixada por Peixoto:

> Se todo funcionário fosse tão questionador como uma criança, demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo à sua volta, e principalmente fazendo o uso dos poderosos "por quês", com

> certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes de segurança da informação (2006, p. 20).

Há a necessidade de se adequar nosso objeto de estudos a práticas seguras, porém nem um *firewall*, um sistema de detecção de invasão, dispositivos avançados de autenticação, ou criptografia são capazes de garantir a segurança. “A verdade é que não existe uma tecnologia no mundo que evite o ataque de um Engenheiro Social” (MITNICK; SIMON, 2003, p. 195).

Como dito, entre as necessidades mais urgentes dentro da SI está elaborar uma política abrangente que envolva uma visão completa do negócio (SÊMOLA, 2006). Uma documentação que estabeleça todas as responsabilidades e normativas, estabelecendo limites e modelos de uso, mas que afinal contemple inclusive o preparo dos usuários para lidar com estas normativas e com os riscos que os envolve vindos do exterior da organização. Além disto, a fim de coibir a ação de *insiders* há a necessidade de uma gestão de pessoas em que passe a incluí-las dentro de uma comunidade. Isto se faz necessário a fim de se estabelecer uma diretriz no desenvolvimento da gestão de riscos, especificamente relacionadas ao fator humano.

O objetivo deste Trabalho de Graduação é mostrar às lideranças municipais a existência de vulnerabilidades nos seus processos internos de informação, com especial atenção ao fator humano, seu ponto fraco a fim de servir como um movimento inicial para um processo de adaptação de um Sistema de Gestão de Segurança da Informação orientando-se pela Gestão de Riscos.

Não pretendemos fazer neste trabalho de graduação uma aprofundada análise dos riscos aos quais o objeto de estudos está sujeito, senão servir de alerta para existência deles, e a necessidade de se adequar ao atual contexto de insegurança na rede mundial de computadores, especialmente quando o objeto de estudos, por sua natureza política, ser um alvo em potencial para ataques.

Neste trabalho analisamos criticamente os aspectos técnicos do negócio no que se refere aos seus recursos humanos, levando em consideração as questões de conhecimentos, treinamento e o preparo para o uso dos recursos de TI por estes segundo a preocupação com a SI. Oferecemos como dimensão protetiva um modelo de ciclo de vida para gestão de riscos como o proposto pela ABNT NBR ISO/IEC 27005:2011 sem, no entanto, nos aprofundarmos nela. A proposta é dispormos de conteúdo suficiente para

mostrar às lideranças as fragilidades a que está sujeita a TI na prefeitura, para que procedamos com seu convencimento da necessidade de tomar iniciativa de preparar o negócio à adaptação de um modelo de governança que contemple a gestão de riscos, oferecendo como modelo a norma supracitada.

Esperamos com este trabalho vislumbrar o atual estado das coisas, expor algumas das vulnerabilidades dos ativos da organização, e saber como se relacionam às ameaças, e como isto se reflete em riscos para organização, para conscientizar a administração da necessidade de um projeto de gestão de riscos baseado em governança corporativa, com estabelecimento de objetivos de longo prazo para adaptação a uma gestão madura de TI.

REFERÊNCIAS

ALEXANDER, Michael. Methods for Understanding and Reducing Social Engineering Attacks. *In*.: **SANS Institute**. Disponível em: <https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>. Acesso: 15 out. 2018

ALLEN, Malcolm. Social Engineering: A means to violate a computer system. *In*.: **SANS Institute**. 2007. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso: 15 out. 2018

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO GUIA 73:2009.** Rio de Janeiro, 2009.

_____. **ABNT NBR ISO/IEC 27001:2009.** Rio de Janeiro, 2009.

_____. **ABNT NBR ISO/IEC 27002:2009.** Rio de Janeiro, 2009.

_____. **ABNT NBR ISO/IEC 27005:2011.** Rio de Janeiro, 2011.

_____. **ABNT NBR ISO/IEC 38500:2009:** O que é segurança da informação? Rio de Janeiro, 2009.

BADDELEY, Michele Catherine. Herding, social influence and economic decision-making: Socio-psychological and neuroscientific analyses *In*.: **Philosophical Transactions of The Royal Society B Biological Sciences.** January 2010. Disponível em: <https://www.researchgate.net/publication/40756996_Herding_social_influence_and_economic_decision-making_Socio-psychological_and_neuroscientific_analyses> Acesso em 13 out. 2018

BEZERRA, Edson Kowask. **Gestão de Riscos de TI**: NBR 27005. Rio de Janeiro: Escola Superior de Redes, RNP, 2013 Disponível em: <https://pt.scribd.com/doc/55387254/Gestao-de-Riscos-de-TI-NBR-27005> Acesso em: 3 out. 2018

BRASIL. **Decreto Nº 3.505, de 13 de junho de 2000**. Presidência da República. Brasília/DF, 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 20 nov. 2018

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Presidência da República. Brasília/DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 8 out. 2018

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 8 out. 2018

CARUSO, Carlos A. A; STEFFEN, Flavio D. **Segurança em informática e de informações.** 4. ed.[rev] São Paulo: Senac, 2006.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES NO BRASIL. **Cartilha de Segurança para Internet**. 2a ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 140p. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 24 out. 2018

CHIAVENATO, Idalberto. **Teoria Geral da Administração**. Rio de Janeiro: Manole, 2014

CITIZENFOUR. Direção e Produção: Laura Poitras. Estados Unidos: Praxis Films, 2014, *online*.

EBOLI, Marisa. **Educação corporativa no Brasil**: mitos e verdades. São Paulo: Editora Gente, 2004

ESTADOS UNIDOS DA AMÉRICA. **UKUSA Agreement Release1940-1956** Disponível em <https://www.nsa.gov/news-features/declassified-documents/ukusa/> acesso em 12 out. 2018

FACHIN, Odília. **Fundamentos de Metodologia.** 5. ed.[rev]. São Paulo: Saraiva, 2006.

FERREIRA, Aurélio Buarque de Holanda. **MICHAELIS**. Dicionário Brasileiro da Língua Portuguesa**.** Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/poder/> Acesso em 7 out. 2018

GRAMSCI, Antonio. **Cadernos do Cárcere**. Rio de Janeiro: Civilização Brasileira, VOL.III, 2004.

GRANGER, Sarah. Social Engineering Fundamentals, Part I: Hacker Tactics. *In*.: **Symantec**. 18 dez. 2001. Disponível em:<https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em: 20 out. 2018.

GRAY, John. **Hayek on Liberty** 3.ed. Routledge, 1998. 186 p.

HOOTSUITE. **Digital in 2018**. Disponível em: <https://hootsuite.com/pt/pages/digital-in-2018> acesso em 1º out. 2018

HOSS O. *et al*. **Gestão de Ativos Intangíveis**. São Paulo: Atlas, 2010

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das Melhores Práticas de Governança Corporativa**. 5a edição, São Paulo, 2015. Disponível em: <http://www.ibgc.org>.

INTERNATIONAL BUSINESS MACHINES (IBM). **IBM X-Force Threat Intelligence Index 2017**. Disponível em: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN> Acesso em: 14 out. 2018

INTERNET SOCIETY. **Global Internet Report 2016**. Disponível em: <https://www.internetsociety.org/globalinternetreport/2016/wpcontent/uploads/2016/11/ISO C_GIR_2016-v1.pdf>. Acesso em: 20 ago. 2018

KASPERSKY LAB. **Em 40% das empresas do mundo todo, funcionários escondem incidentes de segurança de TI**. Disponível em: <https://www.kaspersky.com.br/about/press-releases/2017_em-40-das-empresas-do-mundo-todo-funcionarios-escondem-incidentes-de-seguranca-de-ti> Acesso em 7 out. 2018

KASPERSKY LAB. **Cybercriminals recruit insiders to attack telecoms providers.** Disponível em: <https://www.kaspersky.com/about/press-releases/2016_cybercriminals-recruit-insiders-to-attack-telecoms-providers> Acesso em 7 out. 2018

KLEIN, Fabio Alvim; MASCARENHAS, André Ofenhejm. Motivação, satisfação profissional e evasão no serviço público: o caso da carreira de especialistas em Políticas Públicas e Gestão Governamental. **Revista de Administração Pública.** 2016, Vol.50, n.1, p. 20. Disponível em: < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-76122016000100017&lng=pt&tlng=pt> Acesso em: 1º set. 2018

LAM, Lana. Snowden sought Booz Allen job to gather evidence on NSA surveillance. I*n*.: **South China Morning Post**, 2013**.** Disponível em: <https://www.scmp.com/news/hong-kong/article/1268209/snowden-sought-booz-allen-job-gather-evidence-nsa-surveillance> Acesso em 13 out. 2018

LICHFIELD, John. **França investiga rede de espionagem eletrônica dos EUA.** Disponível em: <https://www1.folha.uol.com.br/fsp/mundo/ft0507200004.htm> Acesso em 13 out. 2018

LITTMAN, Jonathan, **O jogo do fugitivo**. Trad. Fernando Carlos Silva. Rio de Janeiro: Rocco, 1996.

LOPES, Gills Vilar. Vigilância Cibernética no Brasil: O Caso Snowden sob o PRISMa de um insider. *In*.: **Revista Eco Pós.** Disponível em: <https://docplayer.com.br/45658110-Vigilancia-cibernetica-no-brasil-o-caso-snowden-sob-o-prisma-de-um-insider.html> Acesso em 13 out. 2018

MANJAK, Martin. Social Engineering Your Employees to Information Security. *In*.: **SANS Institute**. 1 jun. 2006. Disponível em: <http://www.sans.org/reading_room/whitepapers/awareness/social-engineeringemployees-information-security_1686>. Acesso em: 10 out. 2018

MARCIANO, João Luiz Pereira. **Segurança da Informação - uma abordagem social.** 2006. 211f. Tese (Doutorado em Ciência da Informação) – Colegiado do Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciências da Informação e Documentação, Universidade de Brasília, Brasília, 2006. Disponível em: <http://repositorio.unb.br/handle/10482/1943>. Acesso em: 20 set. 2018

MAQUIAVEL, Nicolau. **O Príncipe**. Companhia das Letras: São Paulo, 2010.

MENEZES, Josué das Chagas. **Gestão da segurança da informação**. Rio de Janeiro: JhMizuno, 2006.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. Trad: Kátia Aparecida Roque. São Paulo: Makron (Person Education), 2003. 284p.

MORGENSTERN, Flávio. **Por trás da máscara: do passe livre aos black blocks, as manifestações que tomaram as ruas do Brasil**. Rio de Janeiro: Record, 2015.

NG, Reynaldo. **Forense computacional corporativa.** Rio de Janeiro: Brasport, 2007.

OLIVEIRA, Vinicios Gonchoroski de; CUNHA, Neide Ribas L. S.; SAUSEN, Jorge Oneide. A mudança organizacional em uma administração pública por meio de um processo de informatização da gestão *In*.: **IV Seminário Internacional sobre Desenvolvimento Regional**. Santa Cruz do Sul, 2013.

PEIXOTO, Mário César Pintaudi. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

PORTAL G1. **Brasil e Alemanha pedem que ONU trate de abusos na espionagem**. Disponível em: <http://g1.globo.com/mundo/noticia/2013/11/brasil-e-alemanha-pedem-que-onu-trate-de-abusos-na-espionagem.html> Acesso em 13 out. 2018

PROOF. **Internet das coisas e seus desafios de segurança.** Disponível em: <https://www.proof.com.br/blog/iot-internet-das-coisas/> Acesso em 14 out 2018

RABELO JUNIOR, Mosar R.; VIEIRA, Selma Cândida C. Aspectos Humanos da Segurança da Informação *In*. LYRA, Maurício Rocha (Org.). **Governança da Segurança da Informação.** Brasilia, 2015.

SAMPAIO, Angelo Augusto Silva. Skinner: sobre ciência e comportamento humano *In*.: **Psicologia: Ciência e Profissão**. 2005, vol.25, n.3, p. 370-383. Disponível em: <http://pepsic.bvsalud.org/scielo.php?script=sci_serial&pid=1414-9893> Acesso em: 18 out. 2018

SANS INSTITUTE. **Glossary of terms**. Disponível em: <https://www.sans.org/security-resources/glossary-of-terms/> Acesso em: 25 out. 2018

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). **Como elaborar um plano de negócios**. Brasília, 2013. Disponível em: <http://www.sebrae.com.br/sites/PortalSebrae/artigos/como-elaborar-um-plano-de-negocio,37d2438af1c92410VgnVCM100000b272010aRCRD> Acesso em: 2 set. 2018

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva da segurança da informação.** 9a ed. Rio de Janeiro: Elsevier, 2003.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS. **Sebrae alerta sobre fraude contra Microempreendedores Individuais.** Disponível em <www.rn.sebrae.com.br/noticia/sebrae-alerta-sobre-fraude-contra-microempreendedores-individuais/> Acesso em 21 out. 2018

SKINNER, Burrhus Frederic. **Ciência e Comportamento humano.** Trad: João Carlos Todorov; Rodolfo Azzi. 11a ed. São Paulo: Martins Fontes, 2003. 489p.

SOUSA, Evaldo Silva de. A gestão da TI dentro do serviço público *In*.: **X Simpósio de Excelência em Gestão e Tecnologia**. Resende, 2013.

THORNDIKE, Edward L. **The Elements of Psychology**. New York: Seiler, 1905. Disponível em: <https://archive.org/details/elementspsychol01goog/page/n0> Acesso em 06 out 2018

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados aplicável em todos os países da UE a partir de 25 de maio de 2018** Disponível em: <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=pt> Acesso em 8 out. 2018

WIRED. **These Are the Emails Snowden Sent to First Introduce His Epic NSA Leaks.** Disponível em: <https://www.wired.com/2014/10/snowdens-first-emails-to-poitras/> Acesso em 13 out 2018

ANEXO – QUESTÕES REMETIDAS AOS USUÁRIOS DE RECURSOS DE TI PARA ESTUDO DE CASO

1. Qual é o seu setor dentro da prefeitura? (caso o setor não esteja listado, selecionar a Secretaria à qual pertence). Sendo as respostas possíveis:

- Gabinete/Sec. de Governo/Assessoria de Imprensa;
- Secretaria de Negócios Jurídicos;
- Secretaria de Controle Geral/Ouvidoria;
- Licitações/Compras;
- Sec. de Administração/Dep. Pessoal/Recursos Humanos;
- Cadastro Técnico;
- Secretaria de Planejamento;
- Secretaria de Obras e Serviços;
- Secretaria de Fazenda;
- Secretaria de Promoção Social.

2. Costuma compartilhar informações pessoais em redes sociais como local e horário de trabalho, e dos locais que frequenta, fotos pessoais, descrições de atividades particulares? As respostas possíveis são:

- Não utilizo redes sociais;
- Sim, costumo compartilhar informações;
- Não, não compartilho informações.

3. Costuma utilizar as redes sociais para fins profissionais pertinentes à prefeitura, realizando contatos e compartilhando informações da organização? As respostas possíveis são:

- Não utilizo redes sociais;
- Sim, costumo compartilhar informações;
- Não, não compartilho informações.

4. Você já ouviu falar em Engenharia Social? As respostas possíveis são:

- Sim;
- Não.

5. Qual sua preocupação atual com sua segurança online? Primeira questão gradativa, aqui a escala vai de 1 a 4 para:

- 1. Não me preocupo;
- 2. Me preocupo pouco;
- 3. Me preocupo razoavelmente;
- 4. Me preocupo muito.

6. De maneira geral, você acredita estar seguro ao navegar na internet? As respostas possíveis são:

- Sim, estou seguro;
- Pouco seguro;
- Não estou seguro
- Não sei responder

7. Quando você recebe comunicação não solicitada por e-mail, vindo de contato conhecido, você costuma consultar o remetente para se certificar de sua procedência? As respostas possíveis são:

- Sim;
- Não.

8. Quando você recebe comunicação não solicitada por e-mail, vindo de contato desconhecido, você costuma abrir o conteúdo recebido?

- Sim;
- Não.

9. Quando você recebe anexos em comunicação não solicitada por e-mail, vindo de contato desconhecido, você costuma baixá-los?

- Sim;
- Não.

10. Após utilizar seus sistemas online você costuma fazer logoff ou bloqueá-los antes de se ausentar de sua mesa?

- Sim;
- Não.

11. Você conhece os riscos envolvidos na informática? Por exemplo, e-mails com links que redirecionam para sites falsos para captura de dados, ou com anexos executáveis para instalação de aplicativos/softwares maliciosos (vírus)? As respostas possíveis são:

- Sim;
- Não.

12. Você já foi vítima de alguma fraude online? (Por exemplo, compra em site falso, acesso a página falsa de instituições bancárias etc)

- Não sei responder;
- Sim;
- Não.

13. Você já recebeu, por e-mail, pendrive, CDs, ou alguma outra forma, algum aplicativo/software malicioso (vírus)?

- Não sei responder;
- Sim;
- Não.

14. Qual o nível de confidencialidade das informações às quais você tem acesso na prefeitura? Outra questão gradativa, com uma escala variando de 1 a 4 onde:

- 1. Interesse público;
- 2. Interesse interno;
- 3. Restrito;
- 4. Confidencial.

15. Você considera que há riscos de segurança que podem expor informações sigilosas do seu setor? As respostas possíveis são:

- Sim;
- Não.

16. Você recebeu algum treinamento sobre como lidar com os processos internos e com as informações (dados, softwares, melhores práticas de segurança etc) com as quais trabalha? As respostas possíveis são:

- Sim;
- Não.

17. Quando requisitado o acesso remoto ao seu equipamento de trabalho você permite apenas se se trata de um funcionário da Informática solicitando tal acesso? As respostas possíveis são:

- Sim;
- Não.

18. Você costuma compartilhar informações de contas e senhas por telefone, mesmo quando na linha a pessoa se identificou como alguém do setor de informática? As respostas possíveis são:

- Sim;
- Não.

19. Qual características você considera mais importantes ao tratar com pessoas de fora da prefeitura? As respostas possíveis são:

- Sim;
- Não.

20. Como é o nível de segurança que as barreiras físicas (exemplo: porteiros, trancas, ou portas liberadas para entrada somente com identificação como por uso de crachás magnéticos, biometria, senhas etc) existentes para acesso em seu setor representam para se impedir a entrada de pessoas não autorizadas? Outra questão gradativa de 1 a 4, onde:

- 1. Não há barreiras;
- 2. Não são seguras;
- 3. São pouco seguras;
- 4. São seguras.

21. Seu setor possui algum sistema de vigilância ou alarme contra acesso indevido? As respostas possíveis são:

- Sim;
- Não.

22. Existe no setor algum local para armazenamento seguro de pertences (celulares e demais dispositivos eletrônicos pessoais)? As respostas possíveis são:

- Sim;
- Não.

23. Existe, à sua volta, algum papel contendo informações de acesso como senhas, logins, números de documentos e demais informações sigilosas à vista? As respostas possíveis são:

- Sim;
- Não.

24. Há, à sua volta, algum documento ou instrumento de trabalho, que possa ser furtado e causar problemas à prefeitura? As respostas possíveis são:

- Sim;
- Não.

25. Qual a complexidade de sua senha para login em seu computador? (Lembrando que toda resposta é anônima) As respostas possíveis são:

- Utilizo senha em branco;
- Utilizo apenas números em minha senha;
- Utilizo apenas letras maiúsculas ou minúsculas em minha senha;
- Utilizo letras maiúsculas ou minúsculas e números combinados em minha senha;
- Utilizo letras maiúsculas e minúsculas combinadas em minha senha;
- Utilizo letras maiúsculas, minúsculas e números combinados em minha senha;
- Utilizo letras maiúsculas, minúsculas, números e símbolos combinados em minha senha.
- Utilizo Dispositivo Biométrico (por exemplo: leitor de digitais).

26. Existe, por parte da Informática, alguma regra ou política de senha (letras maiúsculas e minúsculas, símbolos e números obrigatórios, períodos para troca de senha etc)?

- Não sei responder;
- Sim;
- Não.

27. Você considera que seu computador está protegido (possui antivírus) contra malwares(vírus e outros meios de infecção)? Numa escala, como você nota seu nível de proteção?

- Não sei responder;
- Não protegido;
- Pouco protegido;
- Suficientemente protegido;
- Bem protegido.

28. Você considera que seu computador está protegido contra falhas de hardware que levem à perda de dados críticos ao negócio? Numa escala, como você nota seu nível de proteção?

- Não sei responder;
- Não protegido;
- Pouco protegido;
- Suficientemente protegido;
- Bem protegido.

29. Você costuma guardar arquivos referentes às rotinas de trabalho em seu disco local (HD)? As respostas possíveis são:

- Sim;
- Não.

30. O departamento de TI oferece política ativa (periódica e pró-ativa) de backup dos arquivos nestes discos locais? As respostas possíveis são:

- Sim;
- Não.

31. Você considera que a prefeitura oferece meios satisfatórios de backup de seus arquivos críticos? As respostas possíveis são:

- Sim;
- Não;