INSTITUTO FEDERAL
SANTA CATARINA

CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM
GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

MARCELO RODRIGUES GOMES

A FORMAÇÃO PROFISSIONAL DE TI NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO:
estudo de caso em Instituições de ensino superior de Santa Catarina

Florianópolis - SC
2017

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

MARCELO RODRIGUES GOMES

A FORMAÇÃO PROFISSIONAL DE TI NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO: estudo de caso em Instituições de ensino superior de Santa Catarina

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professor Orientador:
Hamilcar Boing Dr.

FLORIANÓPOLIS - SC
NOVEMBRO/2017

Ficha de identificação da obra elaborada pelo autor.

Gomes, Marcelo Rodrigues
A formação profissional de TI no âmbito da segurança da informação : estudo de caso em instituições de ensino superior de Santa Catarina / Marcelo Rodrigues Gomes ; orientador, Hamilcar Boing, 2017.
68 p.

Trabalho de Conclusão de Curso (graduação) - Instituto Federal de Santa Catarina, Campus Florianopolis, Graduação em Gestao da Tecnologias da Informação Florianopolis, 2017.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Segurança da informação. 3. Tecnologia da informação. 4. Formação em TI. I. Boing, Hamilcar. II. Instituto Federal de Santa Catarina. Graduação em Gestao da Tecnologias da Informação III. Título.

A FORMAÇÃO PROFISSIONAL DE TI NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO: estudo de caso em Instituições de ensino superior de Santa Catarina

MARCELO RODRIGUES GOMES

Este trabalho foi julgado adequado para obtenção do Título de Tecnólogo em Gestão da Tecnologia da Informação e aprovado na sua forma final pela banca examinadora do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis-SC, 07 de dezembro de 2017.

Prof. Julio Cesar da Costa Ribas, Dr.
Coordenador do CST em Gestão da Tecnologia da Informação
Instituto Federal de Santa Catarina

Banca Examinadora:

Prof. Hamilcar Boing Dr.
Orientador
Instituto Federal de Santa Catarina

Profª. M. Sc Elenir Ap. Crestani Lisot
Instituto Federal de Santa Catarina

Prof. M. Sc Adriano Heis
Instituto Federal de Santa Catarina

“A verdadeira sabedoria consiste em se conhecer a própria ignorância.”

(Sócrates)

RESUMO

O presente estudo tem como objetivo lançar um olhar crítico sobre as necessidades do mundo do trabalho e o alinhamento da formação dos estudantes nas áreas de Tecnologia da Informação para atuar na subárea de segurança da informação. Na primeira etapa da pesquisa foram realizados estudos teóricos em segurança da informação, redes sociais, sistema de segurança, políticas de segurança e sobre os conhecimentos e habilidades dos profissionais que atuam em segurança da informação para delinear o perfil desse profissional. Na segunda parte da pesquisa foram avaliadas a matriz curricular de vinte e cinco cursos e entrevistados cento e dezessete estudantes na região de Florianópolis/SC que compõem o público-alvo. Foram levantadas informações que pudessem basear a análise crítica dos conhecimentos desenvolvidos no processo de formação acadêmica e compará-las com as necessidades do mundo do trabalho obtidas a partir da análise da literatura para o profissional atuar em segurança da informação. O questionário desenvolvido é composto por vinte e quatro questões, divididas entre quatro categorias, sendo: Carreira Profissional, Programação, Rede e Sistemas Operacionais e Pessoas. Os resultados mostram que existem lacunas na formação dos acadêmicos de TI em todas as categorias pesquisadas para atuar como profissional de segurança da informação, ocasionadas pela baixa quantidade de carga horária e conteúdo específicos nas matrizes curriculares, o que faz com que esse profissional precise complementar de forma ampla sua formação para atuar na área de segurança da informação, impactando na baixa quantidade de profissionais habilitados e altos custos para preparar esse profissional para o mundo do trabalho, impactando diretamente na segurança da informação das empresas.

Palavras-chave: Segurança da Informação. Tecnologia da Informação. Formação em TI.

ABSTRACT

The present study aims to launch a critical look at the needs of the world of work and the alignment of the training of students in the areas of Information Technology to act in the information security subarea. In the first stage of this research, theoretical studies were carried out on information security, social networks, security system, security policies and on the knowledge and skills of professionals who work in information security to delineate the profile of this professional. In the second part of this research were evaluated the curricular matrix of twenty-five courses and interviewed one hundred and seventeen students in the region of Florianópolis / SC that make up the target audience. Information was collected that could base the critical analysis of the knowledge developed in the academic training process and compare it with the needs of the work world obtained from the analysis of the literature for the professional to act in information security. The questionnaire developed is composed of twenty-four questions, divided into four categories: Professional Career, Programming, Network and Operating Systems and People. The results show that there are gaps in the training of IT academics in all the categories surveyed to act as information security professionals, due to the low amount of specific workload and content in the curricular matrices, which makes this professional need to complement has broad training in the area of information security, impacting the low number of qualified professionals and high costs to prepare this professional for the world of work, directly impacting the information security of companies.

Keywords: Information Security. Information Technology. IT Training.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

O avanço da tecnologia traz consigo o aumento na velocidade nas atividades cotidianas. Um exemplo é processo de comunicação, que evoluiu drasticamente nos últimos 20 anos, partindo de cartas que demoravam dias, às vezes semanas e até meses para serem entregues, até as mensagens instantâneas que usamos hoje em dia pelo celular. Por trás de toda esta evolução está o fato de que a informação ganhou um novo tipo de importância, principalmente para as empresas. As informações precisam chegar no lugar certo, para a pessoa certa e no tempo certo. Velocidade e qualidade da informação viraram diferencial competitivo nos negócios.

Com tantas informações importantes sendo trocadas, é despertado o interesse de pessoas com más intenções no uso destes dados. Basta acompanhar as notícias para descobrir uma nova invasão na rede de um banco ou o roubo de informações de uma grande empresa ao redor do mundo. Os c*rackers* e outras pessoas especializadas em corromper a segurança de sistemas da informação também estão avançando em suas estratégias. Por isso, a cada dia se faz mais importante para as organizações terem profissionais especializados e dedicados em proteger estas informações.

A proteção das informações estratégicas de uma empresa passa pelo profissional de segurança de informação, que deve estar preparado para desempenhar seu papel sem margens de erro. Em uma era onde quem tem a informação tem o poder, fica claro que é muito importante saber usar estas informações de maneira inteligente. Bem como, é fundamental que as informações estejam disponíveis em tempo hábil e protegidas de acordo com seu nível de sigilo.

Com o mercado aquecido em busca de profissionais das áreas ligadas à Tecnologia da Informação, nem sempre as empresas têm a escolha perante a oferta de profissionais, e muitas vezes se veem com a obrigação de treinar a mão de obra que chega ao mercado de trabalho sem o preparo necessário e cada vez mais exigido. Isso leva as empresas a terem que investir em capacitações e certificações para que garantam a qualidade de sua segurança da informação (SI). Isto requer um investimento de tempo e de dinheiro por parte das organizações, recursos estes que nem sempre estão disponíveis em abundância.

Para se pensar em soluções definitivas e de longo prazo para a questão da qualidade dos profissionais de TI para atuarem com segurança da informação, deve-

se direcionar esforços para a formação adequada desse profissional, ou seja, repensar o papel e o processo formativo nas universidades. Enquanto assuntos como inovação e novas tecnologias parecem ser a base das grades curriculares, paira a questão de se o foco apresentado na área da qualidade e segurança das informações está abrangendo a real importância deste assunto. Foi baseado nessa questão que surgiu este estudo, a fim de mapear, qualificar e discutir ações para uma melhor formação dos profissionais de TI no quesito segurança da Informação.

1.1 **JUSTIFICATIVA**

Estamos vivendo a era digital. Isso significa a virtualização de muitos processos e até mesmo, serviços que antes só conseguíamos ter acesso nos deslocando até determinado local. Bancos, universidades e, inclusive, supermercados vem apostando no atendimento digital como forma de manter os clientes fiéis ao seu negócio. Isso se traduz em mais informação circulando nas intranets e internet. Informação importante, relevante e muitas vezes confidencial. Junto a esta virtualização veio a necessidade de investimento em novos computadores, processadores e servidores. Também veio a necessidade de organizar estas informações, distribuindo-as de maneira eficiente e, principalmente, a protegendo de acessos não autorizados.

Atualmente há muitas pessoas que dedicam seu tempo em buscar formas de romper as barreiras de segurança de sistemas diversos como bancos, grandes empresas e até órgãos do governo. Um dos ataques mais recentes e que movimentou a mídia em todo o mundo foi por conta do *ransomware WannaCry*, que sequestrou os dados de várias empresas ao redor do planeta solicitando um resgate em troca da liberação das informações. Os crackers conseguiram extorquir pouco mais de sessenta mil dólares em virtude do golpe, mas o *WannaCry* teve sua fonte descoberta e foi derrubado em poucos dias pelo profissional de segurança britânico Marcus Hutchins.

Os principais motivos que podem permitir as invasões aos sistemas são fragilidades em três aspectos: falta de preparo pessoal, falhas nas redes e falhas na programação dos sistemas. O primeiro aspecto está ligado ao fato de muitas pessoas não conseguirem se enxergar como parte do processo de segurança da informação, não respeitando os protocolos de segurança da informação, adotando senhas fracas

para e-mails ou sistemas e distribuem informações confidenciais, por exemplo. Quanto às redes, ações simples como redundância, criando várias camadas de segurança com o uso de firewalls, por exemplo, dificultaria a ação de hackers. Já as falhas de programação são talvez a falha mais grave, pois indicam a baixa qualidade dos códigos produzidos – ou a falta de testes - em muitos casos.

As fragilidades que levam a problemas de segurança podem ser evitadas, ou, pelo menos, minimizadas. Este é um processo que deve ser feito em conjunto nas empresas, atuando com a capacitação e preparo dos profissionais envolvidos. Em primeiro lugar, o profissional responsável pela segurança deve saber identificar e sinalizar as falhas, sejam elas em qualquer um dos aspectos já citados (pessoas, redes ou programação). Identificadas as falhas fica mais fácil corrigi-las e trabalhar a fonte para que não se repitam os mesmos problemas.

No Brasil, a média de investimentos em tecnologia supera a de todos os países da América Latina. Segundo a Associação Brasileira das Empresas de Software (2017), “no ranking de investimento no setor de TI na América Latina em 2016, o país se manteve em 1º lugar, com 36,5% dos investimentos, somando US$ 38,5 bilhões, seguido por México (22,9%) e Colômbia (10,2%)”[1]. De acordo com a Empresa Brasil de Comunicação (2016), com o surgimento de novos negócios e empresas no setor a cada dia, há uma demanda não atendida e que busca por profissionais qualificados para atender às suas necessidades[2]. Se em um cenário de constantes mudanças o assunto segurança da informação vem sendo discutido cada vez mais e está, portanto, listado entre estas demandas da empresa, fica justificada a necessidade de rever a forma como este assunto está sendo abordado em sala de aula.

O tema da presente pesquisa foi escolhido pela grande proximidade com a área de segurança da informação, após ter sofrido ataques cibernéticos aos servidores que eu gerenciava quando trabalhei em um grande grupo empresarial do setor de comunicações nos anos de 2000 e 2001. O avanço da tecnologia, a crescente quantidade de novas modalidades de ataques e os prejuízos gigantescos às empresas vítimas desses ataques reforçam a importância da segurança da informação e o estudo do tema.

---

[1] Disponível em: http://www.abessoftware.com.br/dados-do-setor/estudo-2017--dados-2016

[2] Disponível em: http://radios.ebc.com.br/revista-brasil/edicao/2016-07/mercado-de-ti-sofre-com-falta-de-profissionais-qualificados

1.2 **DEFINIÇÃO DO PROBLEMA**

Qual a relação entre a formação acadêmica em cursos superiores de tecnologia da informação, incluindo correlatos, e a falta de profissionais habilitados para atuarem na área de segurança da informação?

1.3 **OBJETIVOS**

1.3.1 **OBJETIVO GERAL**

Avaliar as demandas de conhecimentos dos profissionais de tecnologia da informação que se inserem no mundo do trabalho para atuarem na área de segurança da informação, identificando conhecimentos em gestão de pessoas, redes de computadores e desenvolvimento de sistema e o interesse dos futuros profissionais na carreira de gestão da segurança da informação a partir da análise das habilidades e competências adquiridas na formação acadêmica em instituições de ensino superior e da comparação face as demandas reportadas pela literatura temática.

1.3.2 **OBJETIVOS ESPECÍFICOS**

a) Avaliar as matrizes curriculares de cursos superiores da área de TI no estado de Santa Catarina, identificando assim a abordagem que está sendo realizada em segurança da informação;
b) Identificar os principais conhecimentos práticos e teóricos exigidos do profissional de segurança da informação;
c) Avaliar os conhecimentos práticos e teóricos sobre questões de segurança da informação de alunos de cursos de TI;
d) Avaliar os alunos de cursos superiores de TI sobre o interesse de atuar na carreira de gestor de segurança da informação;
e) Apresentar recomendações para alinhar a formação acadêmica de profissionais de TI com as demandas do mundo do trabalho para a atuação na área de segurança da informação.

1.4 **ESTRUTURA DO TRABALHO**

No primeiro capítulo buscou-se conceituar os termos técnicos que serão utilizados no decorrer desse estudo e contextualizar a área de segurança da informação. Serão abordados conceitos como sistemas da informação, segurança da informação, e por fim, um aprofundamento do perfil do profissional de tecnologia de informação.

O capítulo dois apresenta uma revisão da literatura sobre os conceitos de sistemas da informação, segurança da informação, políticas de segurança da informação e certificações para profissionais da área.

No capítulo três são comentados os procedimentos metodológicos, definindo a modalidade de pesquisa, o campo de observação, os instrumentos de coleta de dados, os critérios para análise dos dados e a descrição das etapas de investigação.

O capítulo quatro faz a apresentação dos resultados da análise da matriz curricular de vinte e cinco cursos obtidos através de dezessete instituições de ensino superior referentes a área de TI, e mostra a contabilização das respostas referentes ao questionário aplicado a cento e dezesseis alunos de três instituições de ensino superior em Florianópolis.

O capítulo cinco traz as conclusões e recomendações dessa pesquisa, mostrando as necessidades de alinhamento do mundo do trabalho com o mundo acadêmico, além de dissertar sobre curiosidades encontradas.

2 REVISÃO DA LITERATURA

A área de segurança da informação envolve a análise e proteção de vários tipos de riscos as informações armazenadas digitalmente e é, inicialmente, embasada em conceitos de sistemas de informação.

2.1 **SISTEMAS DE INFORMAÇÃO**

A palavra sistema é definida por Lacombe (2004, p. 286) como sendo um "conjunto integrado de elementos dinamicamente inter-relacionados, desenvolvendo uma atividade ou função, para atingir um ou mais objetivos comuns ao conjunto". Já Chiavenato (2002, p. 571), discorre sobre informação sugerindo que:

> As informações podem provir do ambiente externo (de fora da organização, como o mercado de trabalho, concorrentes, fornecedores, agências reguladoras, outras organizações etc.) ou do ambiente interno (de dentro da organização, como o organograma de cargos e respectivos salários na organização, pessoas que nela trabalham homens/horas trabalhadas, volume de produção e de vendas, produtividade alcançada, etc.).

Rezende (2005, p. 34) defende que "os sistemas de informação podem se enquadrar em diversos modelos e classificações pertinentes". O autor classifica os sistemas de informação em três classes:

a) SIO – Sistemas de Informação Operacionais: controlam todos os dados relacionados às operações das da empresa, auxiliando na tomada da decisão do corpo técnico da organização.
b) SIG – Sistemas de Informação Gerenciais: Sintetizam os dados das operações para auxílio na tomada de decisão do corpo gestor da empresa.
c) SIE – Sistema de Informação Estratégicos: Trabalham com dados em nível macro, e propiciam uma visão mais abrangente para presidentes e diretores.

Os sistemas de informação avançam de maneira rápida, pois as empresas também vêm mudando a maneira de gerir seus negócios. Uma das mudanças que influenciou o amadurecimento dos sistemas de informação foi a visão sistêmica de

todas as áreas da empresa. De acordo com Rezende (2005, p. 36) “não existe mais separação formal dos sistemas de informação estratégico, gerencial, tático e operacional”.

Um sistema de informação quando aplicado às organizações é, de acordo com Laudon e Laudon (1999), a integração de três aspectos, conforme apresentado na Figura 1: as empresas/ organizações, os fatores ligados à tecnologia e as pessoas.

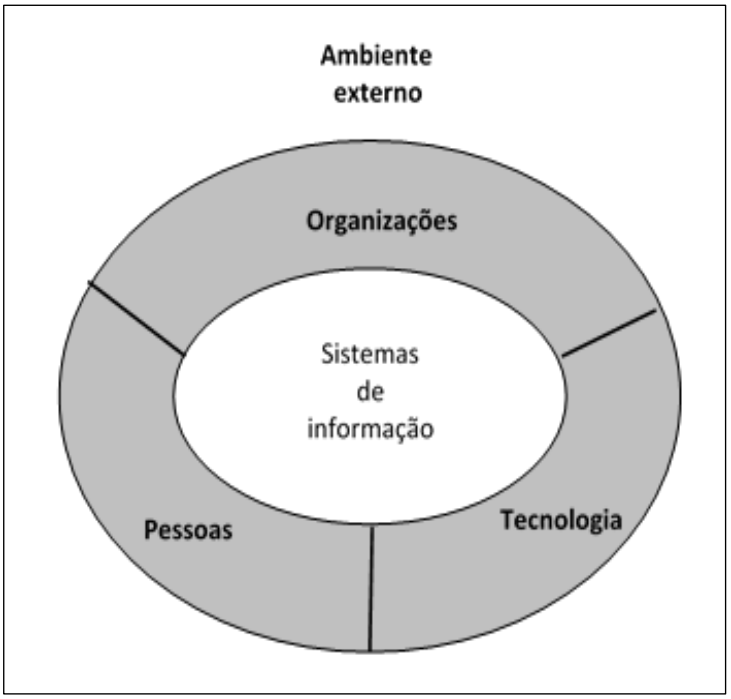


Figura 1 - Componentes de um sistema de informação
Fonte: Adaptado de Laudon e Laudon, (1999, p. 11).

Todos estes fatores recebem influência do ambiente externo, bem como exercem influência uns sobre os outros. Por isso, reafirma-se o cuidado com que a informação deve ser utilizada e principalmente armazenada, contribuindo para o alcance dos objetivos da organização e evitando problemas relacionados ao uso de informações desencontradas ou não relevantes.

2.2 **SEGURANÇA DA INFORMAÇÃO**

De acordo com Silva et al (2003), as teorias e consequente aplicação do termo segurança dos sistemas de informação iniciou-se com os próprios técnicos que, após criarem os sistemas, verificaram a transição para gestores e outros usuários e a

crescente utilização dos meios como computadores e redes, despertando a necessidade de assegurar estas estruturas. Para o autor, existem alguns princípios que devem ser buscados para satisfazer os critérios mínimos para SI, sendo eles:

a) Relação custo/benefício;
b) Concentração;
c) Proteção em profundidade;
d) Consistência do plano;
e) Redundância.

Com relação aos aspectos da SI no que diz respeito à proteção de dados e computadores, Laudon e Laudon (1999, p. 270) explica que:

> Três importantes aspectos da segurança são: garantir a segurança dos dados, proteger os PCS e redes e desenvolver os planos de recuperação dos desastres que afetam os sistemas de informação. Todos esses aspectos exigem mais atenção agora do que antes devido à crescente dependência em relação às redes e à internet.

Para Cabral e Caprino (2015, p.22) “a gestão de risco é o objetivo máximo da segurança da informação” sendo “risco, algo definido de várias maneiras, nas mais diversas disciplinas, mas podemos fazê-lo de forma genérica como ‘a probabilidade e potencial magnitude de uma perda futura’”. Os autores defendem que o primeiro passo para uma correta gestão de riscos é identificá-los. Após, deve ser analisá-los e definir qual passo tomar, entre os quais sugerem:

a) Mitigar o risco: caso o risco seja considerado muito alto pela empresa, ela pode tomar precauções para reduzi-lo, geralmente diminuindo suas vulnerabilidades. Este tipo de risco também requer um controle frequente, para que se acompanhe as probabilidades de causar algum dano à organização.
b) Aceitar o risco: é quando o risco não apresenta ameaça direta ou é aceitável pela organização. Neste passo, a empresa segue em frente sem nenhuma atitude a tomar mediante ao risco.
c) Transferir o risco: existem alguns riscos, independentemente do tamanho, que poder ser terceirizados. Uma alternativa é a contratação de seguros, por exemplo.

A SI deve ser pensada em todas as etapas que a informação percorre, seja na entrada, no processamento ou na saída das informações, pois ela estará sujeita a falhas e intervenções externas em vários momentos.

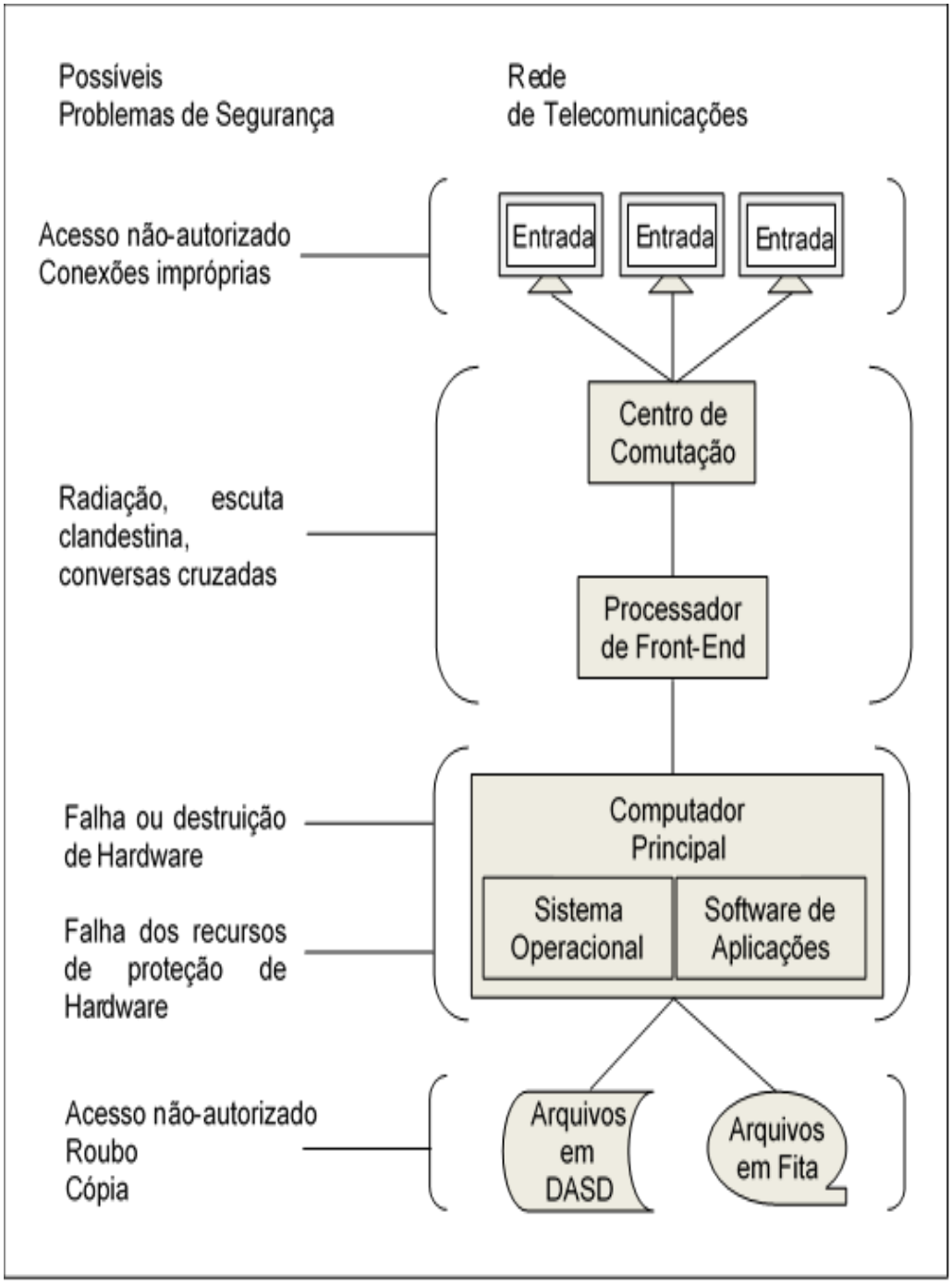


Figura 2 - Vulnerabilidades de uma Rede de Comunicação
Fonte: Adaptado de Laudon e Laudon (1999, p. 263)

Percebe-se na Figura 2 que vários riscos são apresentados em cada processo de transmissão de informação. Sendo assim, fica evidente a importância do

cumprimento de alguns requisitos básicos para garantir a segurança de toda a estrutura envolvida no processo de criação, armazenamento e distribuição das informações através do uso de sistemas. Este pode ser um problema para algumas empresas pois, segundo Cabral e Caprino (2015, p. 15) “ainda é comum observar um grande descompasso entre a segurança tradicional e a segurança de TI, devido ao fato de existir uma visão equivocada da intangibilidade desta última”.

2.2.1 **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

De acordo com Campos (2006, p. 99) a política de SI em uma organização “deve indicar como as coisas devem acontecer na organização no que se refere à segurança da informação”. O autor ainda cita como exemplo de uma política de segurança da informação, a forma como os e-mails serão disponibilizados aos colaboradores de uma organização. Em algumas empresas, o uso é livre, em outras há a restrição de que o uso seja apenas para fins profissionais.

A política de SI tem papel preventivo e é fundamental em qualquer empresa, não passando apenas pela área de TI, mas devendo abranger toda a estrutura da empresa. Para Fontes (2012, p.72) “uma segurança da informação efetiva exige o envolvimento dos executivos da organização para participar da avaliação das novas ameaças e da definição de prioridades”. Esta participação conjunta é importante, pois oferece uma visão mais ampla de quais os riscos e as possíveis soluções a serem implementadas pela organização.

Além de estabelecer padrões e propor soluções imediatas para momentos de crise, possuir uma política de SI também tem outras funções, segundo Fontes (2012):

a) Atender à legislação
b) Atender à exigência do mercado e dos próprios clientes
c) Se adequar às melhores práticas
d) Acompanhar o avanço tecnológico
e) Atender às necessidades do próprio negócio

A empresa que possui uma política bem definida apresenta várias vantagens frente a outras organizações que não a utilizam. Campos (2006, p. 100) destaca que uma das vantagens “é que todos passam a conhecer ‘as regras do jogo’, ou seja, as

pessoas sabem como se comportar em diversos temas diferentes dentro da organização. Sabem o que podem e o que não podem fazer".

Para o estabelecimento de uma política de SI eficaz, Geus e Nakamura (2007, p. 194-195) fazem considerações importantes:

a) Conheça seus possíveis inimigos: identifique possíveis ações e perigos antes que aconteçam.
b) Contabilize os valores: uma política de SI eficaz pode requerer a contratação de novos profissionais ou a compra de novos equipamentos. Todos estes valores devem ser levantados antecipadamente para evitar alterações no plano.
c) Identifique, examine e justifique suas hipóteses: qualquer aspecto que não for previamente identificado pode ocasionar uma grande mudança no escopo do plano, atrasando os trabalhos e gerando desconforto.
d) Controle os seus segredos: estabeleça quais são as informações totalmente secretas.
e) Avalie os serviços estritamente necessários para o andamento dos negócios na organização: este fator é válido para evitar conflitos com os usuários.
f) Considere os fatores humanos: muitas das falhas nos procedimentos de segurança são causados pelas pessoas. É preciso convencer os usuários de sua responsabilidade em todos os processos.
g) Conheça seus pontos fracos: seja crítico e reconheça suas fraquezas.
h) Limite a abrangência do acesso: crie barreiras como uma zona desmilitarizada, equilibrando a força entre toda a rede.
i) Entenda o ambiente: é preciso conhecer o funcionamento regular da rede para identificar de maneira rápida quando algo está fora do normal.

O local físico onde estão concentradas as informações também deve possuir um plano de SI que contemple os riscos físicos envolvidos. Tanto nas empresas que centralizam esta responsabilidade quanto em *Data Center*, os riscos abrangendo a estrutura física são diversos, porém passíveis de serem evitados com as medidas corretas. Campos (2006, p. 13) salienta três importantes riscos relacionados ao ambiente para a segurança, sendo:

a) Ausência de mecanismos contra incêndio
b) Ausência de mecanismo de prevenção à enchente;
c) Ausência de proteção contra poluentes diversos que possam prejudicar mídias e equipamentos.

Como sistemas de controle físicos de acesso podem ser utilizados crachás e a leitura biométrica. Este tipo de acesso também deve ser monitorado e atualizado constantemente para evitar a entrada de ex-colaboradores ou pessoas utilizando cartões perdidos de colaboradores. Outras ações efetivas são o uso de câmeras, catracas e a própria utilização de seguranças previamente capacitados para realizar o controle de acesso. O ideal é sempre associar duas ou mais barreiras para aumentar a efetividade do controle.

Para os riscos envolvendo ação humana, Geus e Nakamura (2007, p. 87) afirmam que o controle de acesso é o meio mais eficaz:

> O acesso direto aos sistemas é uma das facetas dos ataques físicos, os quais podem possuir dimensões ainda maiores. O controle de acesso físico, por exemplo, é uma delas, e deve ser utilizado para minimizar possibilidades de ataques físicos diretamente aos sistemas [...] O controle aos servidores têm de ser o mais restrito possível, com um sistema de identificação eficiente.

Além dos riscos de invasão e hackeamento, ocasionado por pessoas, outros riscos como incêndios, alagamentos e outros de forças maiores também precisam estar previstos, para que as pessoas responsáveis possam ter uma reação rápida e assim evitar perdas maiores. Este plano deve ser feito em conjunto com a área de segurança da empresa, e incluída no plano de segurança geral da companhia.

As políticas de SI devem estar em constante atualização, já que conforme Geus e Nakamura (2007, p. 25) o mundo da segurança “é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataque, de maneira que um ciclo é formado”. Para tentar se antecipar aos riscos, Geus e Nakamura (2007) sugerem que é necessário prestar atenção em alguns pontos:

a) É preciso entender a natureza dos ataques.
b) Novas tecnologias significam novas fraquezas.
c) Novas formas de ataque sempre surgirão.

d) Quanto mais conectado, maior o risco de ataques.
e) Existem ataques oportunistas e ataques direcionados.
f) Defender é bem mais complicado que atacar.
g) Os crimes pela internet vêm aumentando.

Tendo em conta estes aspectos as empresas podem se antecipar aos ataques ou, pelo menos, criar estratégias de reação mais rápidas para o caso de serem atingidas em algum momento. Uma das estratégias, por exemplo, pode ser uma política de senhas. De acordo com Geus e Nakamura (2007, p. 204) “a política de senhas é importante também porque diversos problemas de segurança das empresas estão relacionados a elas, o que faz com que um dos grandes desafios seja a fortificação das senhas”.

2.2.2 **REDES SOCIAIS E APLICATIVOS DE MENSAGEM**

Moraes (2011, p. 138) diz que “as redes sociais podem ser definidas como comunidades virtuais que possibilitam diversos meios de comunicação e interação com outros usuários”. As redes sociais podem ser utilizadas para diversos fins, como se comunicar com a família que está distante, passar o tempo ou até mesmo fazer negócios. O uso de redes sociais e aplicativos de mensagens vem crescendo a cada dia. Junto a este crescimento, aumenta também o universo onde se torna possível a aplicação de golpes utilizando a fragilidade dos sistemas e também a falta de informação e preparo do usuário ao fazer uso das tecnologias. Dentre as redes sociais e aplicativos de mensagens mais utilizados podemos citar o *Facebook, Instagram, Snapchat, Twitter* e *Whats App.*

De acordo com Barbosa (2013, p. 109) “o grande ativo do *Facebook* (na área do B2B), que nunca nenhuma empresa teve ou tem, é o brutal investimento que as marcas já fizeram dentro do seu perímetro.” O grande número de perfis ativos na rede chama muita atenção das empresas. A Folha de São Paulo (2017) anunciou que no dia vinte e sete (27) de junho deste ano o *Facebook* atingiu o número de 2 bilhões de usuários por mês[3]. Devido ao alto potencial de mercado da rede, as empresas vêm

[3] Disponível em: http://www1.folha.uol.com.br/tec/2017/06/1896428-facebook-atinge-marca-de-2-bilhoes-de-usuarios-anuncia-zuckerberg.shtml

criando estratégias para aparecer cada vez mais e utilizar o Facebook como meio de fidelizar os seus clientes. As estratégias são as mais diversas, passando pela geração de marketing de conteúdo até a realização de promoções pela rede.

Para Moraes (2011, p. 139) “da mesma forma que as redes sociais podem ser usadas para divulgação de conteúdo útil, ela também tem sido usada por criminosos, que induzem os usuários a clicarem em *links* e efetuar *download* de *malware”*. Quando isso ocorre, vários arquivos do computador podem ser prejudicados e até mesmo roubados, colocando em risco o usuário que pode ter informações bancárias e pessoas compartilhadas sem autorização com pessoas mal-intencionadas.

Algumas ações podem ser tomadas para evitar armadilhas nas redes sociais, de acordo com Moraes (2011, p. 140):

a) Criar senhas com no mínimo 8 caracteres, misturando números e letras, e trocar essa senha a cada 6 meses.
b) Ao aceitar algum novo amigo nas redes sociais, conferir outros dados como foto, cidade e, se possível, por telefone. Alguém pode usar a foto de um conhecido seu para aplicar golpes.
c) Não divulgar suas informações pessoais como endereço completo, número de documentos, ou data de nascimento.
d) Refletir antes de postar uma foto em uma rede social, se ela pode te comprometer ou expor de alguma maneira. Depois de postadas, as fotos estão sujeitas a cópias e dificilmente você terá acesso a apagar todas caso se arrependa.
e) Modificar as opções de privacidade, fazendo com que só seus amigos diretos visualizem seu conteúdo.
f) Nunca avisar nas redes sociais que você passará dias fora, essa pode ser a informação que falta para alguém que está planejando roubar sua casa ou apartamento.
g) Ao receber comentários com *links*, verifique se o *link* é válido. Se possível, digite-o no navegador em vez de clicar.

Moraes (2011, p. 139) reforça sobre as senhas escolhidas para acesso as redes sociais, dizendo que “o uso de senhas fracas tem sido considerado um alto fator de risco para os usuários, visto que problemas graves podem ocorrer”.

2.2.3 **SEGURANÇA NA INTERNET**

A internet é mais e mais utilizada a cada dia, e não apenas pelas pessoas, mas também pelas empresas. De acordo com Cheswick et al (2005, p. 87) “a *World Wide Web* é a coisa mais importante na Internet. Reportagens em jornais diários informam sobre novos *URL*s maravilhosos. Mesmo anúncio de filmes, *outdoors* e rótulos em garrafas de vinho apontam para *home pages*”. Ou seja, praticamente e tudo o que consumimos, lemos, vestimos e conhecemos em algum momento passará a fazer parte desta imensa rede.

Com o aumento do uso da internet para a realização das atividades do dia a dia, seja através de e-mail ou mais recentemente com a inserção das redes sociais como forma de chegar ao cliente, aumentaram também os riscos envolvidos para as empresas. Estando na rede as empresas estão expostas a pessoas mal-intencionadas, que estão atentas a todos os detalhes procurando uma brecha para roubar informação. Dentre os incidentes mais comuns e preocupantes está a invasão e roubo de dados por *hackers*, que podem trazer prejuízos milionários para as organizações.

Cheswick et al (2005, p. 87) aponta que existem, pelo menos, quatro tipos de problemas de segurança envolvidos com a internet, sendo eles:

a) Riscos para o cliente.
b) Proteção de dados durante e transmissão.
c) Riscos diretos ao servidor ao executar o software de *Web*.
d) Outros caminhos de entrar nesse *host.*

De acordo com (Knight, p. 99), “enquanto os benefícios da internet para o desenvolvimento econômico, social e político são inegáveis, ela como qualquer tecnologia pode ser usada para o bem ou para fins questionáveis, ilegais ou militares”. Um grande desafio com relação à segurança na internet, é que as mudanças ocorrem em uma velocidade muitas vezes difícil de acompanhar, por isso Cabral e Caprino (2015, p. 40) ressaltam que:

> Não adianta implementar controles e tentar resolver todos os problemas, pois eles são tão numerosos que precisamos buscar formas de priorizá-los. Além disso, o contexto muda o tempo todo: os ataques populares hoje são triviais amanhã, as tecnologias mudam de forma constante e a doutrina de entrega

> ágil faz com que iniciativas se tornem obsoletas antes mesmo de sua conclusão.

Pessoas vem usando as redes sociais, criando perfis falsos ou muitas vezes roubando identidades de outras pessoas para aplicação de golpes. Com relação a isso Cabral e Caprino (2015, p. 227) alerta que “será cada vez mais difícil identificar quem são os personagens e quem são as pessoas reais [...] tornando necessária uma capacidade, ainda não existente, de autenticar ou acreditar pessoas nas redes sociais”. Estes perfis falsos são utilizados para a aplicação de golpes e também roubo de informação, evitando ou, pelo menos, dificultando que, caso seja descoberta a fraude, o real responsável seja facilmente localizado.

Os autores também explicam que um passo muito importante é o trabalho com o usuário final, ou seja, aquela pessoa que está em frente ao computador e que decide entre clicar ou não no conteúdo mal-intencionado. Este processo pode ser feito pelo que Cabral e Caprino (2015, p.39) chamam de Campanhas de Conscientização em Segurança da Informação que “têm como objetivo principal mudar os hábitos das pessoas, incorporando precauções até então inexistentes ou deficientes à sua rotina”. Este é um processo longo e constante, que pretende criar uma consciência de uso seguro da internet, principalmente das redes sociais, que ganham milhares de novos adeptos todos os dias.

As empresas também precisam tomar muito cuidado com as informações que postam na internet, sendo os próprios sites, *blogs*, *Facebook* ou *Instagram*. Simples fotos postadas nas redes sociais podem dar informações importantes à possíveis ladrões, pois podem explicitar a localização de servidores, cofres, ou outro alvo estratégico. Diretores e gerentes de grandes organizações também podem ser alvo de espionagem, pois possuem informações importantes de como chegar nos objetivos de estelionatários e bandidos. Por isso, precisam também tomar cuidado com as informações que dividem com sua rede de contatos, que possam levar ao conhecimento dos outros a sua rotina, horários, locais que frequenta, entre outros.

Para Moraes (2011, p. 138) “a importância das redes sociais para fins profissionais (*networking*) tem despertado o interesse de invasores, que podem usar esse meio para infectar computadores e possuir o controle de atividades criminosas”. Knight (2014, p. 99) cita os maiores problemas encontrados na internet como sendo:

> *Spam, phishing*, abuso infantil, tráfico de drogas, pirataria da propriedade intelectual, invasões de privacidade, terrorismo, espionagem econômica e política (tanto por órgãos governamentais quanto por grupos privados), vigilância generalizada (como a revelada por Edward Snowden), e guerra cibernética são ameaças reais.

Para um melhor entendimento dos riscos envolvidos nas operações na internet, verifica-se a seguir alguns conceitos com base em Goodrich e Tamassia (2013):

a) *Spam* (Mensagem em massa): é considerado *Spam* qualquer conteúdo disseminado em massa via e-mail sem prévio contato. O mais comum é que contenha anúncios, mas também pode conter tentativas de perpetração para execução de fraudes.
b) *Virus* (Vírus de Computador): é um código que se multiplica através da modificação de outros arquivos e programas, inserindo códigos que possibilitam replicação posterior.
c) *Spyware* (Programa Espião): é um *software* que invade a privacidade do usuário, e é instalado sem permissão. Em geral, está relacionado ao uso de programas que permanecem em execução em segundo plano, dificultando que o usuário perceba.
d) *Adware* (Programa de anúncios)*:* é considerado como uma forma de Invasão de privacidade do usuário, pois inicialmente se confunde com as informações da página inicial de um site que o usuário está acessando, se utilizando deste disfarce para exibir conteúdo sem consentimento.
e) *Rootkit:* sua função é alterar utilitários do sistema, de forma que dificulte que seja detectado, para encobrir outras ações de *malware.*
f) *Worms* (Vermes de computador): programa malicioso que atua distribuindo suas cópias sem precisar usar de outros programas.
g) *Trojan* (Cavalo de Tróia): *malware* que engana o usuário ao demonstrar uma utilidade inicial. Podem vir junto a outros programas, ou até mesmo i instalados por um usuário ou administrador, propositalmente ou não.

Também devemos destacar um ponto alarmante para o nosso país, pois “o Brasil foi a maior fonte de *spam* na América Latina e no Caribe em 2012, dando origem

a 36,3% do spam proveniente dessa região e 58,4% das páginas *web* maliciosas". (KNIGHT, 2014, p. 100)

O Brasil é um alvo potencial de criminosos, principalmente no que diz respeito a transações bancárias via internet, já que, segundo Knight (2014, p. 102) "mais de 50% dos brasileiros usam meios eletrônicos de comunicação e computadores para os serviços financeiros, oferecendo um alvo atraente para os grupos criminosos organizados". Para Peixoto (2006, p. 18) os riscos apenas passaram do meio físico para o meio digital, conforme explica dizendo que "os perigos quanto às compras online e transações bancárias via internet mediante a disponibilização dos números de cartão de crédito existem, assim como também a utilização do seu cartão pessoalmente". Ou seja, os riscos sempre existiram, o que acontece agora é que há mais um meio por onde os golpes podem ser aplicados.

Existem várias formas pelas quais as pessoas físicas e empresas pode se prevenir de ataques externos através da internet. Oliveira (2013, p. 41-42) cita entre elas:

a) *Firewall*: em poucas palavras, o *firewall* não permite o acesso de usuários sem autorização a um determinado *host* ou ficheiro. Ele faz um exame em todo o pacote, levantando sua origem e verificando se está ou não na lista aprovada.
b) IDS (sistemas de detecção de intrusão): são criados para detectar tentativas externas de invasão, em tempo real. Além de emitir alerta caso haja invasão, ele pode ser programado para aplicar as ações necessárias automaticamente.
c) *Logs*: são registros que o sistema a respeito de todos os eventos gerados. Gerados. São considerados uma medida básica de SI, mas muitas vezes não são utilizados pelos administradores.
d) Antivírus: verificam a existência de vírus em todos as pastas do computador, e pode ser programado para efetuar limpeza quando algum vírus é encontrado.
e) *Backup:* faz cópias de segurança do sistema e suas informações, para que possam ser restauradas caso aja algum incidente com perda de dados.

Cheswick et al (2005, p.104) sugere ao profissional de segurança em tecnologia da informação que “ao utilizar a *Web*, registre tudo em *log,* verifique tudo e instale o maior número possível de camadas de defesas nominalmente redundantes. Não se surpreenda se algumas defesas falharem e planeje como você pode detectar e recuperar-se de erros”. É possível afirmar então que a redundância nas medidas de proteção aos sistemas deve ser uma prática entre os profissionais, a fim de dificultar a entrada de invasores ou *malware.*

Um fator que vem contribuindo para o aumento dos casos de invasões e roubos de informação é o aumento do número de *smartphones* ativos. Os celulares são hoje mais uma porta de entrada para os invasores, que se utilizam também deste meio para efetuar seus golpes. O uso de dados pelo celular vem aumentando a cada dia mais, conforme pesquisa realizada pela TeleBrasil (2017).

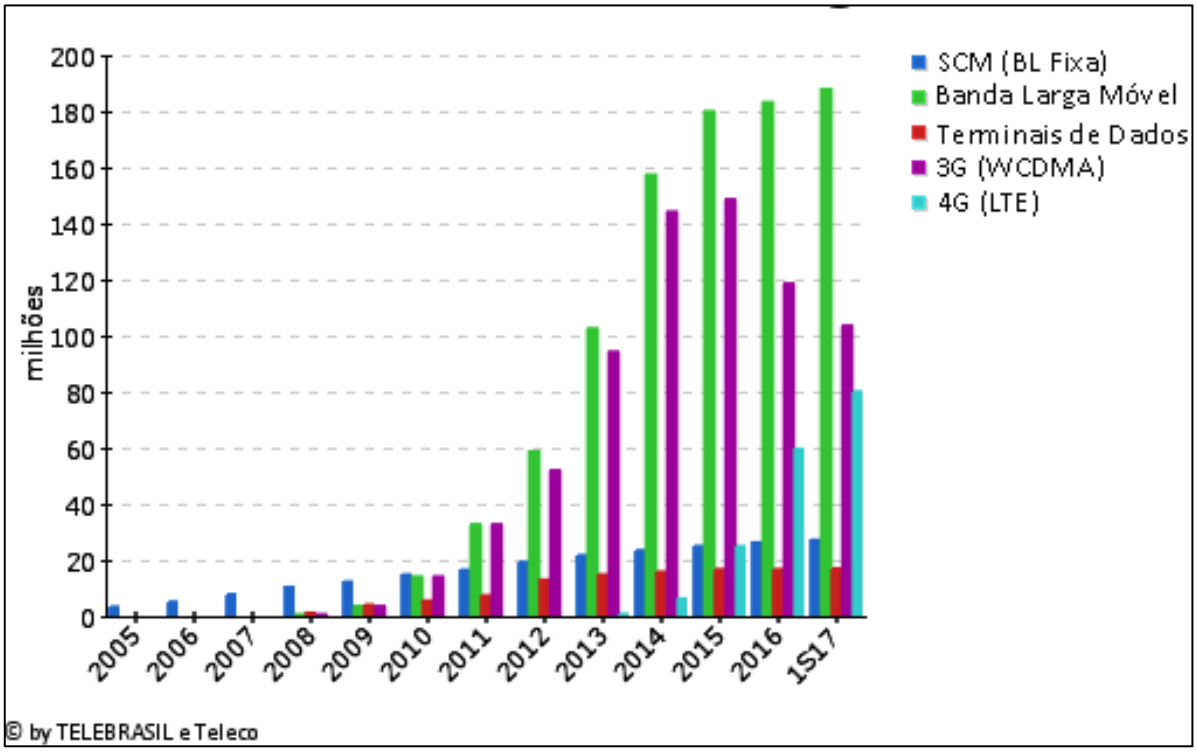


Figura 3 - Acessos SCM (Banda Larga Fixa) e Móvel
Fonte: Disponível em http://www.telebrasil.org.br/panorama-do-setor/consulta-a-base-de-dados

Na Figura 3 é perceptível o crescimento acelerado do uso de banda larga através dos aparelhos telefônicos, que aumentou mais de 80% só nos últimos 5 anos. O crescimento do uso da tecnologia 4G também é bem significativo, saindo de 0,

quando teve entrada no Brasil em 2014 e alcançando 80 milhões de acessos no primeiro semestre de 2017. No gráfico também é possível identificar a queda do uso de 3G, pois ao trocar de celular as pessoas já optam por aparelhos que usam a novas tecnologias.

O uso de celulares para o uso das redes sociais e ferramenta de organizações também chama a atenção. Pretto e Silveira (2008, p. 34 – 35, apud RHEINGOLD, 2004), citam “o caso das mobilizações convocadas por SMS contra o ex-presidente filipino Joseph Estrada, que redundou em sua queda em 2001”. O fenômeno ficou conhecido como *Smart Mobs* ou multidões inteligentes. Os autores ainda afirmam que “com a digitalização da comunicação sem fio, cada vez mais a internet poderá ser acessada pelos celulares, bem como da rede de computadores já é possível enviar mensagens para telefones móveis”. (PRETTO E SILVEIRA, 2008, p. 34)

Segundo Moraes (2011), independente do meio por onde atuarão, as pessoas que tem intenção de roubar ou sequestrar dados geralmente fazem uso do que ele chama de Engenharia Social. Peixoto (2006, p. 4) define Engenharia Social como “a ciência que o estuda o conhecimento do comportamento humano e pode ser utilizada para induzir uma pessoa a atuar segundo seu desejo”. Este método já era utilizado muito antes da internet, com golpes pelo telefone.

Utilizando as técnicas da Engenharia Social, o estelionatário consegue se aproximar da vítima de maneira a parecer familiar, se identificando como gerente do banco ou atendente de operadoras de cartão de crédito, por exemplo, para extrair informações variadas como dados de conta bancária, número de documentos pessoais, entre outros. Com esses dados em mãos, os estelionatários conseguem efetuar saques, extorquir a vítima ou até mesmo usar a identidade desta pessoa na aplicação de novos golpes.

No ano de 2017, houve um grande ataque cibernético, a nível mundial, onde um tipo de vírus que foi chamado de *WannaCry* atacou muitas empresas, desde companhias aéreas, bancos e pequenos negócios. De acordo com a Agência Brasil (2017) “só na América Latina, durante os quatro dias de atividade do *WannaCry* em maio, os *crakers* conseguiram arrecadar ilegalmente, com o pagamento de resgates, US$ 62 mil, só falando de usuários comuns”. Os ataques tiveram início em maio de 2017, e duraram apenas alguns dias. Os *crackers* entraram em contato com as

empresas exigindo um resgate de U$ 300 para que os dados que estavam em toda a rede da organização não fossem sequestrados.

O cenário na América Latina, de acordo com a Agência Brasil (2017), é que "ao menos 12 registros de invasão por programas maliciosos – os chamados *malwares* – são contabilizados, por segundo, no continente". A Agência Brasil (2017) ainda afirma que "somente com pesquisa e investimento – para estar um passo à frente dos invasores – é possível proteger a informação". Já no Brasil o cenário não é diferente, "é um dos países mais vulneráveis do mundo ao *ransonware*. Aparece em quinto lugar, à frente dos Estados Unidos, Argentina e Tailândia". Segundo pesquisas realizadas, 49% dos computadores no país que tem conexão com a internet já foram alvos de tentativas de fraudes[4].

Além do sequestro de informações com o intuito de obter um resgate em troca do desbloqueio, há também casos onde os dados são roubados, para então serem expostos e assim prejudicar a pessoa ou empresa de alguma maneira. No âmbito civil há vários casos em que pessoas tem fotos e vídeos roubados e depois expostos nas redes sociais, por exemplo. Muitas destas pessoas são escolhidas por algum tipo de vingança, ou às vezes, também são chantageadas para que as imagens ou vídeos sejam retirados da internet. O grande problema é que, uma vez na internet, se torna quase impossível retirar todo o conteúdo colocado uma vez que várias fontes podem ter feito cópias e as armazenando em locais diferentes.

No âmbito empresarial, relatórios e informações sigilosas acabam sendo postadas com o intuito de prejudicar a imagem da empresa ou de revelar alguma irregularidade. Um exemplo de como informações de empresas podem ser publicadas sem autorização ocorreu há alguns anos com o início do *Wikileaks*, site que publica informações sigilosas de diversas empresas. Um dos primeiros escândalos descobertos pelo público através do site, segundo Domscheit-Berg (2011), foi sobre a prisão de Guantânamo. Dentre outros documentos da Agência de Segurança Nacional dos Estados Unidos, foram publicados os manuais que revelavam que não eram cumpridas sequer as medidas básicas impostas pelos Direitos Humanos aos condenados. Edward Snowden, que, foi o responsável por fornecer ao site as informações, hoje é um exilado pois foi condenado pelo país acusado de ameaçar a

[4]Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016

segurança nacional. A Rússia, à época já comandada por Vladimir Putin, concedeu exilo à Snowden. (ARAN, 2016)

2.2.4 **PROFISSIONAIS DE SEGURANÇA EM TI**

Segundo o pensamento de Laudon e Laudon (1999, p. 4), se você for um profissional de alguma das áreas da Tecnologia da Informação (TI), “você deve saber como identificar problemas e oportunidades e como usar os sistemas de informação para aumentar a capacidade de reação da organização”. Podemos afirmar que este é realmente uma característica que pode definir um profissional bem qualificado nas áreas de TI.

Para Laudon e Laudon (1999, p.4) chama atenção para a necessidade de investir constantemente em sistemas, e isso inclui também os profissionais. A falta deste investimento pode trazer sérios riscos às empresas:

> Precisaremos de uma ampla compreensão sobre sistemas de informação para atingir níveis mais altos de produtividade e eficácia em nossas fábricas e escritórios nacionais. Será simplesmente impossível operar com eficiência, mesmo uma pequena empresa, sem investimento significativo em Sistemas.

Cabral e Caprino (2015, p.15) defendem que a qualificação é um fator chave para a determinação da qualidade dos profissionais, especialmente dos que irão se dedicar à Segurança em TI, afirmando que “essa é uma discussão que poderia ser bastante alongada, possivelmente levantando pontos nos quais mercados e academia poderiam interagir de forma eficiente para uma melhor definição das necessidades da formação de profissionais de segurança de TI”.

O cuidado na elaboração dos planos de ensino dos cursos relacionados à Tecnologia da Informação deve ser constantemente revisado e adequado à realidade do setor, em constante mudança, porém, também deve-se manter o foco nos conhecimentos básicos e essenciais para uma boa formação. Pode-se perceber essa dificuldade na afirmação de Takahashi (2000, p. 49):

> No nível de graduação, alguns currículos estão irremediavelmente obsoletos: por exemplo, o típico currículo de Ciências da Informação, em muitos países, reflete uma visão da área que foi atropelada em muitos aspectos essenciais

> (alguns para bem, outros para mal) pela revolução das tecnologias de informação e comunicação. [...] um reposicionamento dos Parâmetros Curriculares Nacionais deve ser considerado.

"Há argumentos no sentido de que, para países em desenvolvimento, a capacidade de absorver novas tecnologias e de colocá-las em aplicação é tão ou mais importante do que a capacidade de gerar essas tecnologias", segundo Takahashi (2000, p. 48). O autor também sugere um fluxo de como seria um cenário ideal para a capacitação de recursos humanos em Tecnologia da Informação, passando pelos três processos principais de geração, aplicação e uso do conhecimento.

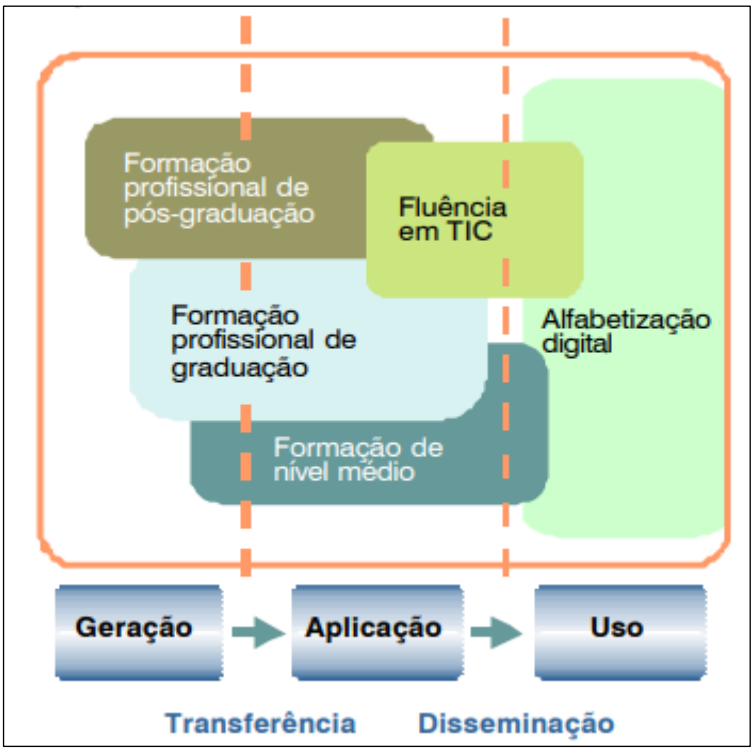


Figura 4 **- Capacitação de Recursos Humanos em TIC**
Fonte: Takahashi (2000, p. 48)

A Figura 4 mostra a relação entre o desenvolvimento acadêmico e o domínio do profissional sobre o assunto. Ou seja, enquanto avança da formação de nível médio para níveis mais altos, vai agregando o que o autor chama de alfabetização digital, atingindo aos poucos a fluência em TI.

Quanto ao ingresso destes estudantes no mercado de trabalho, Cabral e Caprino (2015, p. 15) alerta para as características que julga importantes em um profissional de segurança em TI dizendo que, "ao procurar avaliar os estudantes com potencial para se tornarem grandes analistas de segurança, costumo dividir as

características desejáveis em dois grandes grupos: atitudes e habilidades". Segundo o autor, atitudes são características próprias da pessoa, enquanto habilidades são os conhecimentos adquiridos no decorrer do tempo. O autor também levanta três características consideradas essenciais em um bom analista de segurança: curiosidade, persistência e comprometimento.

Cabral e Caprino (2015, p. 14) também fazem uma crítica sobre a forma como as empresas vêm contratando profissionais de segurança em TI:

> Trata-se do fato de as empresas raramente possuírem uma política institucional para contratação de profissionais de segurança da informação. Na maioria das vezes, o setor de RH das empresas delega essa atribuição para uma empresa de RH terceirizada, fora da organização, ou ainda recorrem a *headhunters* ou sites especializados em recrutamento. As exigências de contratação, nesses casos, baseiam-se em alguns poucos critérios de habilidades técnicas, conhecimentos de línguas estrangeiras e experiência anterior na área.

Complementando esta opinião, o autor coloca sua experiência prática como argumento, dizendo que:

> Segundo minha experiência, os analistas de segurança que acabam tendo mais sucesso profissional e que conseguem evoluir de forma mais rápida suas habilidades de *hacking* já possuem as características de atitude presentes em seu comportamento e seu caráter. (CABRAL E CAPRINO, 2015, p. 16)

Estas últimas citações confirmam o que já foi citado anteriormente, Cabral e Caprino (2015) acreditam que as habilidades ou características técnicas são muito importantes, mas o desenvolvimento de atitudes e comportamentos é fundamental para a construção de um bom profissional na área de segurança em TI. Sobre as exigências que são solicitadas hoje para contratação de um profissional de segurança em TI Cabral e Caprino (2015, p.6) ressaltam que:

> Universidades, faculdades, entidades de classe, instituições públicas ou privadas, dentre outros consultados, afirmam não possuir uma política bem estabelecida e escrita sobre o currículo mínimo exigido para avaliar formação específica que seja aplicada para contratação em segurança de TI. Também não existem políticas escritas a respeito de habilidades e personalidades a serem buscadas.

Para comprovar de alguma maneira perante o mercado as competências relacionadas à Segurança da Informação, os profissionais podem buscar as chamadas Certificações.

De acordo com Júnior (2017, p. 76 e 77), dentre as certificações mais procuradas e conhecidas no mercado estão:

a) CISM (*Certified Information Security Manager*): Certificação de Gestor em SI, é destinada àqueles profissionais que atuam com planejamento, gerenciamento, acompanhamento e execução das atividades relacionadas à segurança da informação em uma empresa.
b) CIFI (*Certified Insurance Fraud Investigator*): Certificação de Investigador em Fraudes de Segurança, desenvolvida pela IISFA, entidade americana especialista em crimes cibernéticos.
c) SSCP (Systems Security Certified Practioner): Certificação em Práticas de SI, é considerada o primeiro passo dentro da carreira em SI.
d) CISSP (*Certified Information Systems Security Professional*) Certificação de Profissional em Segurança de Sistemas de Informação. Conta com poucos profissionais certificados no Brasil, pois possui várias exigências. Entre elas, ter 3 anos de experiência na área e ser indicado por outro membro que já possui a certificação.
e) CISA (*Certified Information Systems Auditor*): Certificação de Auditor de Sistemas de Informação, é uma formação mais genérica, mas considerada uma das mais eficazes.
f) CompTIA *Security+*: é uma certificação respeitada mundialmente para validar conhecimento e competências de segurança de TI de base e neutro do ponto de vista do fornecedor.[5]

Para Oliveira (2009, p.75):

> Se uma organização estabelece uma certificação profissional como pré-requisito durante um processo seletivo, ela pode concentrar seus esforços de análise dos candidatos em aspectos comportamentais, pois o conhecimento técnico está garantido pela certificação.

[5]Disponível em: https://certification.comptia.org/pt/certifica%C3%A7%C3%B5es/security

Possuir as certificações, hoje em dia, é muito mais do que ter um diferencial, é garantir estar atualizado nos temas importantes e passar confiança para os empregadores.

3 PROCEDIMENTOS METODOLÓGICOS

Para a concretização deste estudo, foi necessária a coleta prévia de informações de campo para análise posterior. O principal instrumento de coleta de dados foi um questionário desenvolvido especificamente para essa pesquisa, fundamentado nas demandas apontadas pela literatura. As conclusões e recomendações foram alcançadas através de análise dos resultados desse questionário.

3.1 **MODALIDADE DE PESQUISA**

A pesquisa realizada para este estudo é qualitativa, pois tem como propósito levantar as informações necessárias para responder de maneira satisfatória a questão problema. A pesquisa qualitativa, de acordo com Malhotra (2006, p. 155) é uma “pesquisa não-estruturada, exploratória, baseada em pequenas amostras, que proporciona insights e compreensão do contexto do problema”.

Os dados que serão trabalhados serão coletados diretamente em universidades e locais frequentados pelos estudantes das áreas de Tecnologia de Informação, público-alvo do estudo, caracterizando também, desta maneira como pesquisa de campo.

3.2 **CAMPO DE OBSERVAÇÃO**

A pesquisa será aplicada em estudantes dos cursos na área de Tecnologia de Informação na cidade de Florianópolis.

3.3 **INSTRUMENTOS DE COLETA DE DADOS**

Através da pesquisa de campo, com a utilização de questionário desenvolvido especificamente para este fim. O questionário utilizado pode ser visualizado no apêndice A. Foram abordados estudantes dos cursos na área de Tecnologia de Informação que responderam a uma pesquisa com perguntas de múltipla escolha em formulário impresso onde não era necessária a sua identificação.

Foi desenvolvido um mini sistema web usando a linguagem PHP com o sistema gerenciador de banco de dados (SGBD) MySQL para armazenar e processar os dados da pesquisa, que está detalhado no apêndice B. A pesquisa foi realizada manualmente, com questionário impresso distribuído aos alunos presentes em sala de aula nos seus devidos cursos superiores, com autorização dos seus professores e com a supervisão do aplicante - autor deste trabalho de conclusão de curso. Após recolhido, o questionário foi digitado no sistema *web* e submetido a um processo de contabilização.

O questionário foi dividido em 4 categorias, sendo Carreira Profissional, Programação, Rede & SOs e Pessoas.

Na categoria Carreira Profissional estimou-se saber do aluno a vivência dele no mercado do trabalho e sua visão. Este item é importante para que possamos conhecer se há relação entre grupos de pessoas com a mesma visão e mesmo conhecimento técnico.

A categoria Programação avaliou o conhecimento técnico em programação do aluno, pois, de acordo Assunção (2002, p.153) “a programação é essencial no mundo da segurança, pois ela melhora o raciocínio e nos dá uma visão lógica das coisas.”.

Já na categoria Rede & SOs, Rufino (2002, p.163) alega que:

> Grande parte dos sistemas operacionais está passando por uma auditoria, buscando basicamente por problemas de estouro de pilha e tratamento de parâmetros [...] e isto é particularmente preocupante porque as equipes de desenvolvimento, tradicionalmente, não tem preocupações com a segurança, mesmo porque não são treinadas para isso.

A cartilha oficial de segurança de redes da Cert.br cita que:

> Independente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como: furto de dados, uso indevido de recursos, varredura, interceptação de tráfego, exploração de vulnerabilidades, ataque de negação de serviço, ataque de força bruta, ataque de personificação[6].

Por fim, mas não menos importante, a categoria Pessoas foi inclusa no questionário por se tratar de uma das possíveis falhas em segurança, conforme afirma Silva (2012, p.09):

[6] Disponível em: https://cartilha.cert.br/redes/

> […]a informação se tornou um dos ativos de valor mais inestimável para as empresas e que precisa, portanto, ser protegida das diversas ameaças, tais como falha humana, funcionários mal treinados ou mesmo mal intencionados, espionagem, dentre outras que poderão possibilitar a ocorrência de problemas de vazamento de importantes informações das empresas.

O questionário foi validado por Marcos Flávio Araújo Assunção, professor mestre em Sistemas de Informação e Especialista em Segurança de Redes, autor de vários livros na área, que o validou como “bem completo” para o trabalho proposto.

3.4 **CRITÉRIO PARA ANÁLISE DOS DADOS**

Os dados coletados através dos questionários serão transcritos neste trabalho através de texto, tabelas e figuras, objetivando a fácil visualização e análise das informações. Focou-se em duas áreas: habilidades e atitudes para avaliar os conhecimentos, vocação e interesse dos participantes da pesquisa na área de SI. A descrição detalhada dos critérios de análise está nos itens 4.1 e 4.2 deste trabalho.

3.5 **DESCRIÇÃO DAS ETAPAS DE INVESTIGAÇÃO**

Para a elaboração deste trabalho, é necessário o seguimento de algumas etapas, a saber:

a) Reunir bibliografia sobre o tema a fim de nortear a pesquisa;
b) Desenvolver a fundamentação teórica do tema selecionado;
c) Desenvolver um questionário para avaliar as habilidades e competências de acadêmicos de cursos superiores da área de TI e validar com um especialista de SI.
d) Coletar dados e informações através da aplicação do questionário;
e) Analisar e interpretar os dados coletados, comparando-os com os dados obtidos a partir da análise da literatura;
f) Desenvolver considerações sobre a formação dos profissionais de TI que auxiliem tanto as instituições de ensino a aperfeiçoarem as matrizes curriculares para privilegiar e integrar os conhecimentos sobre segurança da informação quanto os futuros profissionais que atuarão em SI e as empresas a definirem um itinerário formativo para complementar sua formação acadêmica e poderem atuar com proficiência na área de SI;

4 APRESENTAÇÃO DOS RESULTADOS

Os resultados estão divididos em 3 etapas. A primeira analisa o processo formativo dos profissionais de TI a partir dos PPCs de instituições de ensino superior em Santa Catarina e investiga o referencial teórico sobre o perfil e atuação do profissional de segurança da informação.

Na segunda etapa, baseada em entrevistas com acadêmicos de cursos da área de TI, avalia-se os conhecimentos e o perfil dos futuros profissionais da área de TI e o seu alinhamento com a área de segurança da informação.

Na terceira etapa, através de análise e comparação dos resultados das duas etapas anteriores, identifica-se as lacunas no processo de formação e os impactos para o mundo do trabalho, identificando um possível processo formativo para complementar a formação dos profissionais que atuam ou atuarão em segurança da informação, o qual permitirá aos profissionais e empresas mensurar as necessidades para habilitar os profissionais de TI para atuarem em segurança da informação.

4.1 **ANÁLISE DE PPC**

Foram coletados projetos pedagógicos de cursos (PPC) de dezessete instituições de ensino superior em Santa Catarina com cursos referentes a Tecnologia e Computação, sendo elas: IFSC, UFSC, UDESC. SENAI, FURB, Estácio, Católica SC, UNISUL, UNISOCIESC, UNIVALI, UnC, UNIBAVE, UNOESC, UNIPLAC, UNIDAVI, AVANTES, UNIFEBE. Os PPCs foram coletados a partir da página institucional das instituições na internet.

Os cursos superiores analisados foram: Gestão da Tecnologia da Informação, Sistemas de Informação, Ciência da Computação, Engenharia de Computação, Sistemas para Internet, Redes de Computadores e Análise e Desenvolvimento de Sistemas. A relação entre as instituições de ensino e cursos superiores resultou em vinte e cinco grades curriculares avaliadas.

A análise se baseou em 2 fatores, sendo:

a) a existência de matérias específicas sobre SI ou de sistemas na grade curricular e o tempo disponibilizado em relação a carga horária total do curso (equivalente a carga horária informada pelo projeto pedagógico do curso menos as horas complementares e a carga horária dedicada ao TCC);

b) a quantidade de matérias relacionadas com os três focos do questionário aplicado (programação, rede e pessoas).

Para o item Programação foram contabilizadas também as matérias sobre banco de dados. No quesito Pessoas foram excluídas matérias de ética e sociedade que tem a ver somente com o profissional em questão, pois o interesse era o conhecimento em gestão de pessoas, incluindo liderança de equipes. E para Redes, além das específicas, também foram inclusas as de gerenciamento de redes e computação distribuída.

INSTITUIÇÃO	CURSO	Carga Horária	Fases	Segurança (h)	Pessoas (h)	Programação (h)	Redes (h)
Estacio	sistemas da informação	2439	8	36	0	687	108
UNISUL	sistemas da informação	2580	9	60	60	720	240
UNISUL	ciência da computação	2820	10	60	0	660	240
UNISUL	gestão da TI	2070	5	60	120	60	180
UNIVALI	ciência da computação	2768	10	0	0	828	144
UNIVALI	engenharia da computação	3384	10	0	0	612	144
UNOESC	ciência da computação	2580	9	60	150	900	60
UNOESC	engenharia da computação	3195	10	120	45	630	180
UNOESC	sistemas de informação	2235	8	60	60	600	120
UNIPLAC	sistemas de informação	2340	8	60	0	480	180
UNIDAVE	sistemas de informação	3078	8	72	144	1116	144
UNIDAVE	sistemas para internet	1980	5	72	180	864	144
SENAI	redes de computadores	2160	6	160	70	150	1000
SENAI	análise e desenv. de sistemas	2100	6	70	70	770	140
FURB	sistemas de informação	3024	9	72	0	684	72
Catolica SC	sistemas de informação	2625	8	120	0	1260	120
UnC	ciência da computação	2700	8	60	120	600	180
UNISOCIESC	sistemas de informação	2920	8	60	0	560	0
UNIBAVE	sistemas de informação	2535	8	60	120	780	120
UNIFEBE	sistemas de informação	2460	8	60	90	540	90
AVANTIS	sistemas de informação	2400	8	80	300	720	80
UDESC	sistemas de informação	2610	8	72	72	666	180
UFSC	sistemas de informação	2538	8	72	0	720	270
UFSC	ciências da computação	2952	8	72	0	774	216
IFSC	gestão da TI	1944	6	108	108	342	162

Figura 5 - Relação das instituições e cursos superiores com análise de carga horária
Fonte: do autor.

Com base na análise de horas e tipos de curso conforme demonstra a Figura 5, foi constatado que quanto mais técnico o curso (ciências da computação e engenharia da computação) menos importância é dada a gestão de pessoas, chegando alguns cursos a não ter nenhuma matéria direcionada para esse sentido. Por outro lado, em cursos com visão mais gerencial, o item Pessoas pode ter importância igual ou superior ao quesito Segurança.

Averiguou-se dois cursos de bacharelado que não tinham nenhuma matéria específica do item Segurança. Apesar das poucas exceções, a média geral de horas destinadas para matérias de segurança fica entre 2% e 4% em relação a carga horária total do curso. Existe a possibilidade de haver inserções de conhecimento sobre segurança em outras matérias da grade, mas não afetará a média geral ao ponto de mudar o cenário diagnosticado.

O item Programação é o que mais se destaca em todos os cursos - com exceção de Gestão da TI na Unisul – tendo os mais altos índices de carga horária das grades curriculares. Em contraponto com o quesito Pessoas, quanto mais gerencial é o curso, menos carga horária as matérias sobre programação recebem.

Descartando o único curso que é direcionado para Redes de Computadores – SENAI, este quesito tem uma variação moderada, recebendo no geral a mesma importância nos cursos analisados.

Na avaliação final dos dados analisados, os quesitos Pessoas e Segurança ficaram com uma média de 2,835% em relação a carga horária. O ensino de Redes obteve em torno de 5,8% de importância na grade curricular enquanto Programação chega a assumir até ¼ das horas úteis totais dos cursos.

4.2 **ANÁLISE DO QUESTIONÁRIO**

A pesquisa foi baseada em cento e dezessete entrevistas de alunos de cursos superiores das instituições de ensino IFSC, SENAI e UFSC, as quais foram as únicas que permitiram a aplicação do formulário em seus campus universitários. Um dos questionários foi anulado por ter sido preenchido erroneamente de forma intencional, totalizando para essa análise cento e dezesseis alunos. As instituições pesquisadas possuem grande impacto na formação profissional e com abrangência estadual.

Do total válido dos questionários pesquisados, as mulheres atingiram 15.51% enquanto os homens ficaram com os 84.49% restantes. A maioria, 47.41%, tem idade entre 18 e 24 anos e a minoria, 4.31%, estava acima dos 45 anos. A faixa de 25 a 32 anos foi de 28.45% e a faixa dos 33 aos 45 atingiu 19.83%.

A maioria dos alunos cursavam a sexta fase, totalizando 45.69% enquanto a primeira fase foi de apenas 11,20%. O restante se dividiu entre a segunda, terceira e quarta fase dos cursos pesquisados. Não houve público na quinta fase de nenhum curso.

Os dados contabilizados pelo sistema web são apresentados apenas com as respostas selecionadas, ocultando assim as respostas do questionário que não receberam nenhuma marcação. O questionário completo pode ser visualizado no Apêndice A.

Está trabalhando atualmente?

Não (18, 15.517%)
Sim, em empresa de TI (52, 44.828%)
Sim, em outro tipo de empresa (46, 39.655%)

A área de Segurança da Informação te interessa como carreira? (vide figura 6)

Sim (44, 37.931%)
Não (26, 22.414%)
Tenho interesse, mas pouco conhecimento sobre a área (46, 39.655%)

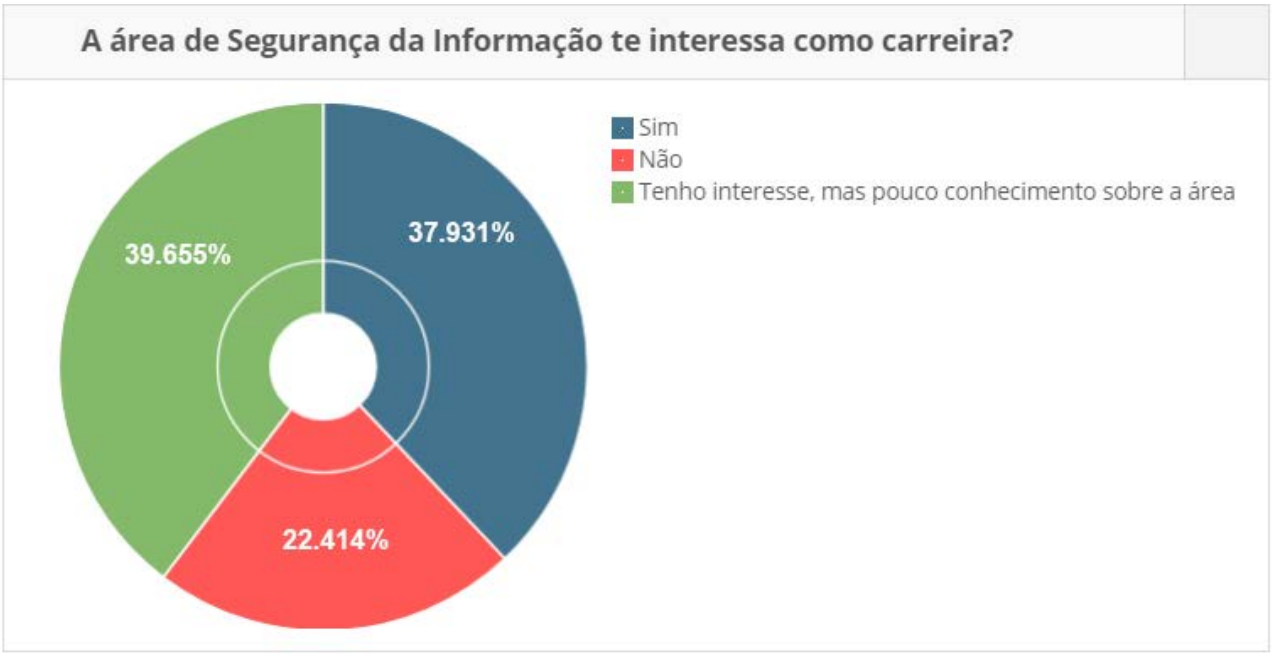


Figura 6 – Pesquisa IFSC/UFSC/SENAI – interesse na carreira de SI declarado pelos acadêmicos.

Tem interesse em fazer cursos específicos sobre Segurança em TI?

Sim (80, 68.966%)
Não (36, 31.034%)

Em qual nível você avalia o seu curso atual em termos de noções de segurança em TI?

Não informado (3, 2.586%)
Não tem (9, 7.759%)
Pouco conteúdo (52, 44.828%)
Razoável (35, 30.172%)
Bom (15, 12.931%)
Excelente (2, 1.724%)

Já fez algum tipo de hacking ou invasão anteriormente?

Sim (23, 19.828%)
Não, mas tenho conhecimento (20, 17.241%)
Não, nem tenho conhecimento (73, 62.931%)

Já sofreu algum tipo de hacking ou invasão anteriormente?

Sim (28, 24.138%)
Não sei (65, 56.034%)
Com certeza não (23, 19.828%)

Já identificou alguma falha em algum software ou sistema de terceiros?

Nunca (37, 31.897%)
Sim, mas não reportei (44, 37.931%)
Sim, reportei pra empresa desenvolvedora (35, 30.172%)

Atualmente, se a empresa que você trabalha te chamar para coordenar a Segurança da TI? (vide figura 7)

Não informado (2, 1.724%)
Eu aceito, com mesmo salário (20, 17.241%)
Eu aceito, se o salário for maior (32, 27.586%)
Eu recuso (62, 53.448%)

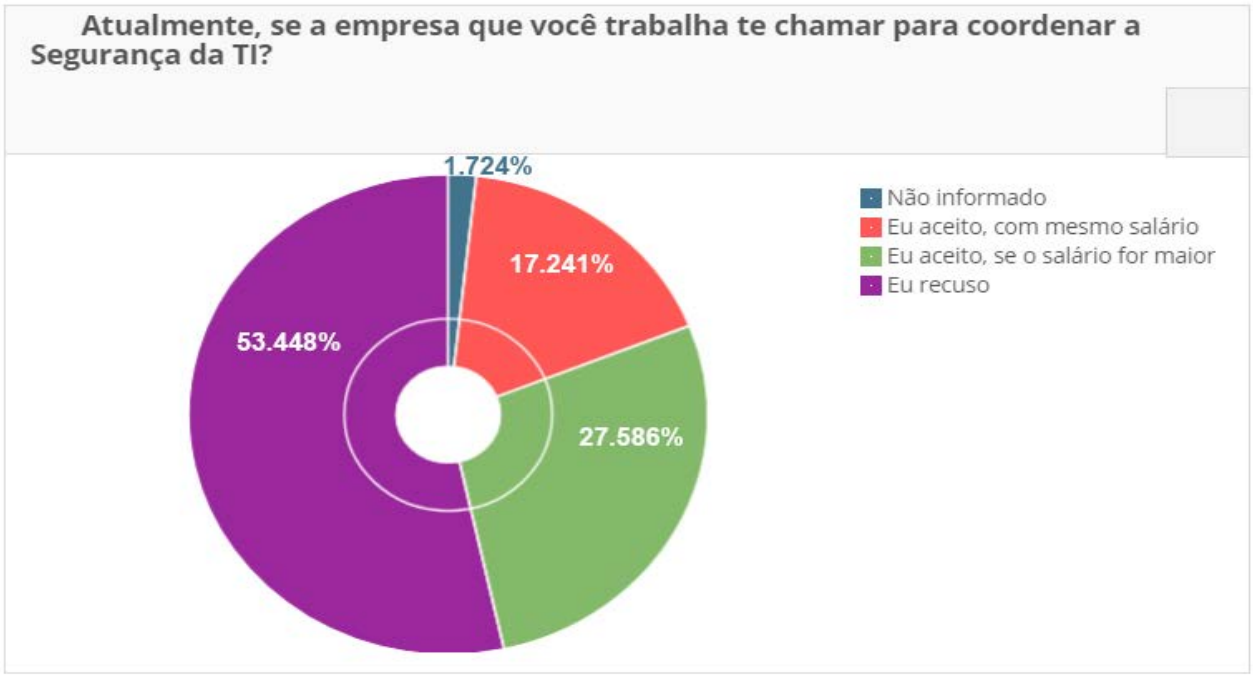


Figura 7 – Pesquisa IFSC/UFSC/SENAI – possibilidade de aceitação imediata de cargo na área de segurança da informação, com o conhecimento atual, declarado pelos acadêmicos.

Nível de conhecimento na linguagem Assembler

Não conheço (95, 81.897%)
Iniciante (21, 18.103%)

Nível de conhecimento na linguagem Bash

Não conheço (82, 70.69%)
Iniciante (15, 12.931%)
Intermediário (15, 12.931%)
Avançado (4, 3.448%)

Nível de conhecimento na linguagem C

Não conheço (28, 24.138%)
Iniciante (64, 55.172%)
Intermediário (24, 20.69%)

Nível de conhecimento na linguagem C++

Não conheço (40, 34.483%)
Iniciante (62, 53.448%)
Intermediário (14, 12.069%)

Nível de conhecimento na linguagem Java

Não conheço (17, 14.655%)
Iniciante (56, 48.276%)
Intermediário (36, 31.034%)
Avançado (7, 6.034%)

Nível de conhecimento na linguagem Perl

Não conheço (103, 88.793%)
Iniciante (12, 10.345%)
Intermediário (1, 0.862%)

Nível de conhecimento na linguagem PHP

Não conheço (40, 34.483%)
Iniciante (47, 40.517%)
Intermediário (24, 20.69%)
Avançado (5, 4.31%)

Nível de conhecimento na linguagem Python

Não conheço (55, 47.414%)
Iniciante (46, 39.655%)
Intermediário (14, 12.069%)
Avançado (1, 0.862%)

Nível de conhecimento na linguagem Oracle

Não conheço (73, 62.931%)
Iniciante (31, 26.724%)
Intermediário (12, 10.345%)

Nível de conhecimento na linguagem MySQL

Não conheço (28, 24.138%)
Iniciante (49, 42.241%)
Intermediário (33, 28.448%)
Avançado (6, 5.172%)

Nível de conhecimento na linguagem Postgre

Não conheço (76, 65.517%)
Iniciante (21, 18.103%)
Intermediário (19, 16.379%)

Nível de conhecimento na linguagem NoSQL

Não conheço (89, 76.724%)
Iniciante (23, 19.828%)
Intermediário (3, 2.586%)
Avançado (1, 0.862%)

Conhece sobre exploit Metasploitable

Não (106, 91.379%)
Sim (10, 8.621%)

Conhece sobre exploit SQL Injection

Não (63, 54.31%)
Sim (53, 45.69%)

Conhece sobre exploit Zero Day

Não (96, 82.759%)
Sim (20, 17.241%)

Conhece sobre exploit Buffer Overflow

Não (98, 84.483%)
Sim (18, 15.517%)

Conhece sobre exploit XSS Injection

Não (107, 92.241%)
Sim (9, 7.759%)

Conhece sobre exploit Heap Overflow

Não (111, 95.69%)
Sim (5, 4.31%)

Conhece sobre exploit Fuzzing

Não (113, 97.414%)
Sim (3, 2.586%)

Conhece sobre exploit Meterpreter

Não (110, 94.828%)
Sim (6, 5.172%)

Já estudou o código fonte de algum exploit para entender o funcionamento?

Não informado (1, 0.862%)
Nunca (62, 53.448%)
Sim, em curso (5, 4.31%)
Sim, sozinho (11, 9.483%)
Não, mas gostaria (37, 31.897%)

Já programou algum exploit?

Não informado (1, 0.862%)
Nunca (78, 67.241%)
Sim, em curso (3, 2.586%)
Sim, sozinho (2, 1.724%)
Não, mas gostaria (32, 27.586%)

Já programou algum bugfix?

Não informado (1, 0.862%)
Nunca (75, 64.655%)
Sim, em curso (6, 5.172%)
Sim, sozinho (4, 3.448%)
Não, mas gostaria (30, 25.862%)

Já programou utilizando Sockets?

Não informado (1, 0.862%)
Nunca (70, 60.345%)
Sim, em curso (12, 10.345%)
Sim, sozinho (9, 7.759%)
Não, mas gostaria (24, 20.69%)

Nível de conhecimento no SO Windows

Iniciante (6, 5.172%)
Intermediário (62, 53.448%)
Avançado (48, 41.379%)

Nível de conhecimento no SO Linux

Não conheço (4, 3.448%)
Iniciante (49, 42.241%)
Intermediário (48, 41.379%)
Avançado (15, 12.931%)

Nível de conhecimento no SO FreeBSD

Não conheço (92, 79.31%)
Iniciante (14, 12.069%)
Intermediário (9, 7.759%)
Avançado (1, 0.862%)

Nível de conhecimento no SO MacOS

Não conheço (47, 40.517%)
Iniciante (42, 36.207%)
Intermediário (23, 19.828%)
Avançado (4, 3.448%)

Conhece o protocolo TCP

Não (40, 34.483%)
Sim (76, 65.517%)

Conhece o protocolo DHCP

Não (48, 41.379%)
Sim (68, 58.621%)

Conhece o protocolo UDP

Não (63, 54.31%)
Sim (53, 45.69%)

Conhece o protocolo NTP

Não (104, 89.655%)
Sim (12, 10.345%)

Conhece o protocolo POP3

Não (57, 49.138%)
Sim (59, 50.862%)

Conhece o protocolo SMTP

Não (62, 53.448%)
Sim (54, 46.552%)

Conhece o protocolo HTTP

Não (21, 18.103%)
Sim (95, 81.897%)

Conhece o protocolo SNMP

Não (86, 74.138%)
Sim (30, 25.862%)

Conhece o protocolo FTP

Não (40, 34.483%)
Sim (76, 65.517%)

Conhece o protocolo XMPP

Não (111, 95.69%)
Sim (5, 4.31%)

Conhece o protocolo SSH

Não (67, 57.759%)
Sim (49, 42.241%)

Conhece o protocolo TELNET

Não (58, 50%)
Sim (58, 50%)

Conhecimento em Firewall (vide figura 8)

Não conheço (13, 11.207%)
Iniciante (69, 59.483%)
Intermediário (25, 21.552%)
Avançado (9, 7.759%)

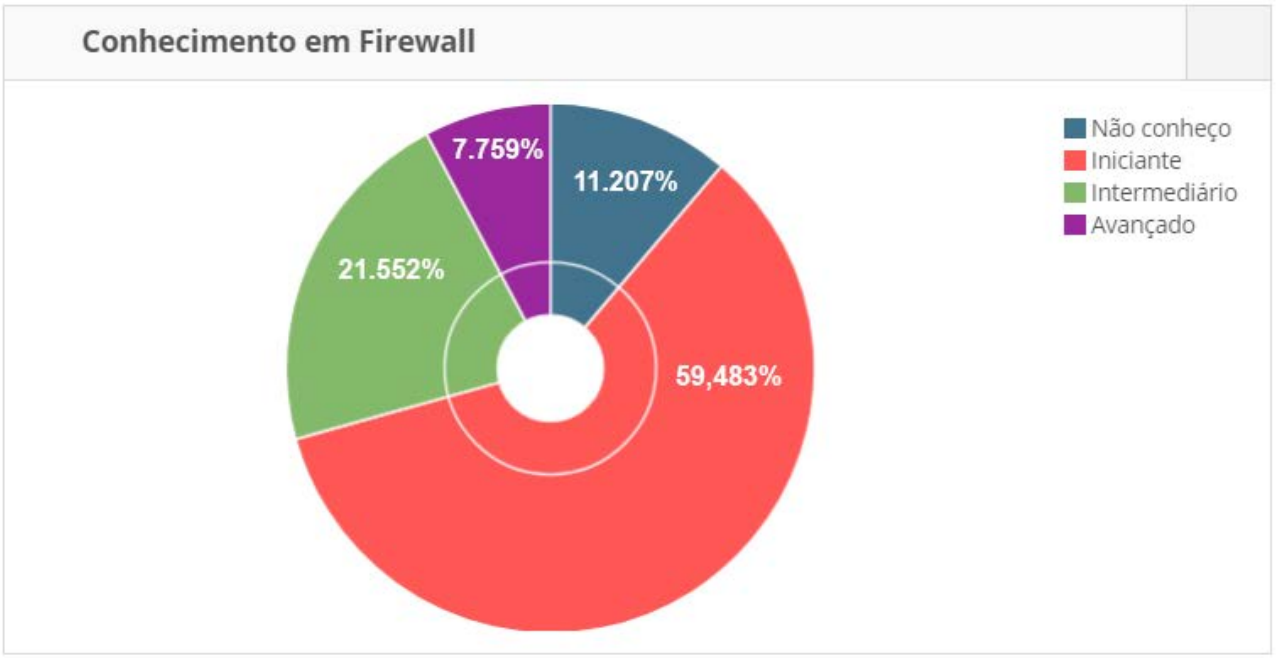


Figura 8 – Pesquisa IFSC/UFSC/SENAI - nível de conhecimento sobre firewall declarado pelos acadêmicos.

Conhecimento em Proxy

Não conheço (23, 19.828%)
Iniciante (68, 58.621%)
Intermediário (19, 16.379%)
Avançado (6, 5.172%)

Conhecimento em DNS

Não conheço (16, 13.793%)
Iniciante (57, 49.138%)
Intermediário (34, 29.31%)
Avançado (9, 7.759%)

Conhecimento em Roteamento

Não conheço (8, 6.897%)
Iniciante (61, 52.586%)
Intermediário (37, 31.897%)
Avançado (10, 8.621%)

Conhecimento em Wireless

Não conheço (4, 3.448%)
Iniciante (64, 55.172%)
Intermediário (38, 32.759%)
Avançado (10, 8.621%)

Sabe instalar Rede Cabeada

Sim (47, 40.517%)
Parcialmente (42, 36.207%)
Não (27, 23.276%)

Sabe instalar Rede Wireless

Sim (51, 43.966%)
Parcialmente (43, 37.069%)
Não (22, 18.966%)

Sabe instalar Modem ADSL

Sim (39, 33.621%)
Parcialmente (35, 30.172%)
Não (42, 36.207%)

Sabe instalar Roteador Cisco

Sim (26, 22.414%)
Parcialmente (39, 33.621%)
Não (51, 43.966%)

A empresa que você trabalha possui políticas de segurança?

Sim (63, 54.31%)
Não (11, 9.483%)
Não sei informar (27, 23.276%)
Não se aplica (15, 12.931%)

A empresa que você trabalha oferece treinamento de segurança da informação?

Não oferece (61, 52.586%)
Somente na admissão (6, 5.172%)
Eventualmente (17, 14.655%)
Frequentemente (9, 7.759%)
Não se aplica (23, 19.828%)

Grau de importância em Login ao sistema

Nenhuma (1, 0.862%)
Pouca (9, 7.759%)
Média (33, 28.448%)
Alta (73, 62.931%)

Grau de importância em Controle de acesso físico

Nenhuma (3, 2.586%)
Pouca (12, 10.345%)
Média (39, 33.621%)
Alta (62, 53.448%)

Grau de importância em Alteração regular de senha

Nenhuma (2, 1.724%)
Pouca (15, 12.931%)
Média (45, 38.793%)
Alta (54, 46.552%)

Grau de importância em Treinamento em Segurança TI

Nenhuma (5, 4.31%)
Pouca (12, 10.345%)
Média (36, 31.034%)
Alta (63, 54.31%)

Grau de importância em Vigilância por câmeras

Nenhuma (3, 2.586%)
Pouca (24, 20.69%)
Média (45, 38.793%)
Alta (44, 37.931%)

Grau de importância em Sistema de Ponto

Nenhuma (11, 9.483%)
Pouca (22, 18.966%)
Média (42, 36.207%)
Alta (41, 35.345%)

Grau de importância em Identificação por crachá

Nenhuma (10, 8.621%)
Pouca (31, 26.724%)
Média (42, 36.207%)
Alta (33, 28.448%)

Falha de segurança (importante) na empresa: Insatisfação

Não (78, 67.241%)
Sim (38, 32.759%)

Falha de segurança (importante) na empresa: Baixo salário

Não (98, 84.483%)
Sim (18, 15.517%)

Falha de segurança (importante) na empresa: Acesso irrestrito

Não (55, 47.414%)
Sim (61, 52.586%)

Falha de segurança (importante) na empresa: Virus / Malware

Não (56, 48.276%)
Sim (60, 51.724%)

Falha de segurança (importante) na empresa: Engenharia Social

Não (78, 67.241%)
Sim (38, 32.759%)

Falha de segurança (importante) na empresa: Desinformação

Não (51, 43.966%)
Sim (65, 56.034%)

Falha de segurança (importante) na empresa: Falta de Comunicação

Não (77, 66.379%)
Sim (39, 33.621%)

Falha de segurança (importante) na empresa: Phishing

Não (82, 70.69%)
Sim (34, 29.31%)

De quem deve ser o dever de educar o novo funcionário sobre a Segurança da TI da empresa?

Não informado (1, 0.862%)
Recursos Humanos (10, 8.621%)
Departamento de TI (72, 62.069%)
Gerência do Setor (31, 26.724%)
Diretoria (2, 1.724%)

Na sua visão, qual colaborador oferece maior risco? (vide figura 9)

Não informado (2, 1.724%)
Novo funcionário (16, 13.793%)
Ex funcionário (42, 36.207%)
Funcionários atuais (19, 16.379%)
Colaborador terceirizado (37, 31.897%)

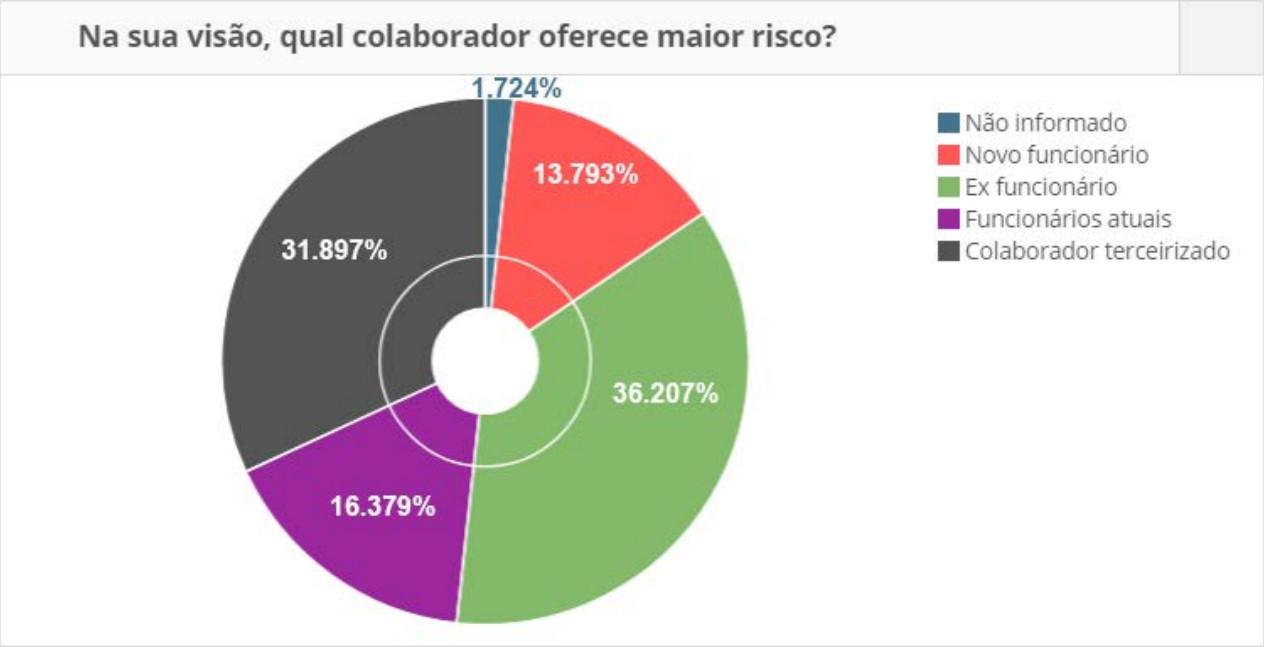


Figura 9 – Pesquisa IFSC/UFSC/SENAI – visão de maior risco por colaborador, declarado pelos acadêmicos.

5 CONCLUSÕES

Nessa pesquisa, foram avaliadas as demandas de conhecimentos para a formação de profissionais de tecnologia da informação atuarem na área de segurança da informação, as quais foram divididas em três categorias, conforme mostra a literatura, sendo Programação, Redes e SOs e Pessoas, com aprofundamento específico em alguma linguagem programação e banco de dados, conhecimento de protocolos de redes e sistemas operacionais e gestão de pessoas em ambiente corporativo.

A avaliação dos PPCs de cursos superiores de TI confrontada com as demandas apresentadas na literatura permitiram identificar lacunas no processo de formação de acadêmicos, o que, em parte, é um dos fatores que elevam os riscos de segurança da informação para a sociedade. Essas lacunas levam a falta de profissionais habilitados para atuar em segurança da informação e elevam as fragilidades de sistemas computacionais na medida que não evidenciam as necessidades de conhecimentos específicos.

Os principais conhecimentos práticos exigidos para o profissional de segurança da informação são a identificação do tráfego de dados em redes para análise de *logs*, sistemas de *firewalls* e IDS, gerenciamento de acesso de usuários em sistemas operacionais diversos e estar constantemente atualizado com informações de *bugfixes* (correção de falhas). Para os conhecimentos teóricos, o profissional precisa ser capaz de definir e implantar o plano estratégico de segurança da informação (PESI), conhecer as normas indicadas como boas práticas da área (ISO 17799 e NBR ISO 27002) e ser capaz de gerir pessoas e resolver conflitos.

A análise dos PPCs dos cursos superiores de TI demonstrou uma carência no ensino direcionado a segurança da informação, por não ter carga horária suficiente para atender aos requisitos do mercado do trabalho. Em uma visão mais aprofundada dos PPCs pode-se notar que, mesmo em matérias relacionadas, não há a presença explícita da abordagem da segurança da informação durante o ensino. Para a finalidade de habilitar profissionais para atuarem em segurança da informação, nenhum curso superior analisado oferece a capacitação necessária ao cargo. As lacunas deixadas pelo curso superior devem ser preenchidas com especializações ou cursos específicos.

Para adequação e melhoria da formação acadêmica visando a segurança da informação nas matrizes curriculares, é recomendado que haja, no mínimo, uma unidade curricular sobre segurança da informação, englobando as três principais características do setor, sendo Programação, Redes e Pessoas. Métodos de programação segura, ambientes

de pesquisa sobre *exploits* e *bugfixes*, ferramentas de *firewall* e técnicas de leitura de *logs* para identificação de tráfego de dados, modelos de planos estratégicos de segurança da informação, resumo da NBR ISO 27002 e formas de gestão de pessoas em ambiente corporativo com a finalidade de alertar para a importância da segurança da informação dentro da empresa, seriam algumas formas de melhorar a formação do aluno, tanto na unidade específica quanto disseminado em outras unidades relacionadas.

Apesar da análise dos PPCs mostrar que o quesito Programação é o mais difundido, a necessidade das instituições de estarem “atualizadas com o mercado” faz com que elas aumentem o foco no desenvolvimento *mobile* e para internet, com programações rasas e pouca prática. O mercado de SI necessita de programadores com conhecimentos profundos, não apenas em internet mas, até mesmo, em sistemas embarcados. Essa especialização de conteúdo pode ser fornecida pela empresa caso seus sistemas sejam muito específicos.

Uma situação similar ocorre na área de redes de computadores, onde atualmente não é necessário ter um conhecimento profundo dos protocolos, mas sim de como esses dados são trafegados, seja de forma aberta ou criptografada. Hoje em dia, em algum momento, alguém vai capturar os dados. Se conseguirão ler ou não, é parte do trabalho do gestor de SI e que deveria ser abordado na formação acadêmica.

Durante a análise dos questionários, notou-se algumas curiosidades nas respostas individuais fazendo cruzamento de dados, que colaboram com a visão que a formação desses profissionais possui lacunas, sendo:

- Alunos sem interesse em carreira de segurança, mas que aceitariam o cargo caso a empresa ofereça um salário maior;
- Alunos informam que conhecem o protocolo POP3 porém não tem conhecimento de SMTP;
- Alunos querem seguir carreira na segurança da informação, mas consideram que pessoas não representam risco;

Conforme as respostas dos acadêmicos apontaram, poucos se identificaram como conhecedores avançados de conhecimentos específicos nas áreas de programação, redes de computadores, SOs e gestão de pessoas, essenciais para a atuação em segurança da informação. Dos respondentes, poucos declararam que obtiveram seus conhecimentos na formação acadêmica, o que fortalece a visão da inaptidão na sua formação e para atuarem na área de segurança da informação.

Os futuros profissionais têm interesse na área de segurança da informação porém a maioria não se considerou capacitada para exercer tal função, embora alguns aceitassem um cargo no setor de segurança da informação da empresa se lhes fosse oferecido atualmente. Dos interessados na área, a maioria tem a intenção de fazer cursos específicos sobre o tema e considerou que seu curso superior atual tem pouco conteúdo específico sobre SI.

Os dados obtidos por essa pesquisa indicam que as carências no processo de formação dos profissionais de TI tem resultado direto sobre a demanda por profissionais de segurança da informação habilitados, impactando no mundo do trabalho com reflexos na propagação de riscos de segurança da informação para empresas e usuários em geral.

Ao confrontar os dados da literatura com a análise dos conhecimentos dos acadêmicos da área de TI, essa pesquisa evidenciou que o nível de informação destes para atuarem com segurança da informação adquiridos na formação acadêmica ainda é baixo, necessitando de complementação, e que esses profissionais não estão prontos para ingressarem nessa área de trabalho específica.

5.1 **RECOMENDAÇÕES FUTURAS**

Como sugestão de continuação desse trabalho, algumas empresas devem ser consultadas para determinar a necessidade de conhecimento atual do profissional de segurança da informação e o que é encontrado hoje no mercado do trabalho. Também avaliar a intenção de investimento financeiro por parte das empresas no profissional contratado para alcançar o nível técnico desejado pela empresa.

Para o aluno que se forma e tem o desejo de ser um profissional de segurança da informação no mercado do trabalho, recomenda-se o investimento (tempo x dinheiro) em cursos, formações e certificações específicas para a área. Há vários cursos no Brasil de pós-graduação (especialização) em segurança da informação, com duração variando de dez até dezoito meses e valores mensais[7] em torno de R$ 319,00 (SENAC), R$ 396,00 (UNISUL), R$ 400,00 (IGTI), R$ 658,00 (CESUSC) e R$ 987,90 (UNIP).

Fora do Brasil, podemos encontrar outros cursos, como o *Master of Science in Cyber Security and Information Assurance*, da Southern Utah *University*, com duração de dezesseis meses ao custo total de 45 mil dólares. Outros cursos fora do Brasil tem valores similares.

[7] Valores consultados ao final de novembro de 2017.

Adquirir certificações na área de segurança da informação é uma prática muito bem-vista no mundo do trabalho, pois informa à empresa que o profissional tem conhecimento e está habilitado a proteger as suas informações com um padrão de segurança testado mundialmente.

REFERÊNCIAS

ARAN, Edson. **O livro das conspiraçõe**s. São Paulo: Suma de Letras, 2016.

ASSUNÇÃO, Marcos Flávio Araújo. **Guia do Hacker Brasileiro.** Florianópolis: Visual Books, 2002.

BARBOSA, Pedro. ***The end of Facebook***. Portugal: Editorial AS, 2013.

CABRAL, Carlos; CAPRINO, William. **Trilhas em Segurança da Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

CAMPOS, Andre L. N. **Sistema de Segurança da Informação**: Controlando os Riscos. Florianópolis: Visual Books, 2006.

CERT.BR. Centro de estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha oficial de segurança de redes da Cert.br.** Disponível em: <https://cartilha.cert.br/redes/ > Acesso em 25 nov. 2017

CHIAVENATO, Idalberto. **Recursos Humanos:** edição compacta. 7. ed. São Paulo: Atlas, 2002.

DOMSCHEIT-BERG, Daniel. **Nos bastidores da *Wikileaks***. Portugal: Leya, 2011.

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

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. **Segurança de Redes em ambientes corporativos**. São Paulo: Novatec, 2007.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

JÚNIOR, Elias Daher. **A culpa é da Informática:** os desafios e caminhos para o gestor de TI. Ebook. Clube de Autores: 2005. Disponível em: <https://books.google.com.br/books?id=DQSvCQAAQBAJeprintsec=frontcoverehl=pt-BResource=gbs_ge_summary_recad=0#v=onepageeqef=false> Acesso em: 06 nov. 2017

KNIGHT, Peter T. **A internet no Brasil**: origens, estratégia, desenvolvimento e governança. Minnesota: AuthorHouse, 2014.

LACOMBE, Francisco. **Dicionário de Administração**. São Paulo: Saraiva, 2004.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação com Internet**. Rio de Janeiro: LTC, 1999.

MALHOTRA, Naresh. **Pesquisa de Marketing:** uma orientação aplicada. Porto Alegre: Bookman, 2006.

MORAES, Paulo. **Mente Anti-hacker - Proteja-se!** Rio de Janeiro: Brasport, 2011.

OLIVEIRA, Fátima Bayma de. **Tecnologia da Informação e Comunicação**: Articulando Processos, Métodos e Aplicações. Rio de Janeiro: E-papers, 2009.

OLIVEIRA, Wilson. **Técnicas para hackers**: Soluções para Segurança. Portugal: Centro Atlântico, 2013.

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

PRETTO, Nelson de Luca; SILVEIRA, Sérgio Amadeu da. **Além das Redes de Colaboração:** Internet, Diversidade Cultural e Tecnologias do Poder. Salvador: EDUFBA, 2008.

REZENDE, Denis Alcides. **Engenharia de Software e Sistemas de Informação**. 3ª ed. Rio de Janeiro: Brasport, 2005.

RUFINO, Nelson Murilo de Oliveira. **Segurança Nacional.** São Paulo: Novatec Editora, 2002.

SILVA, Antônio Everardo Nunes da. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2012.

SILVA, Pedro Tavares; CARVALHO, Hugo. TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação:** Gestão Estratégica da Segurança Empresarial. Portugal: Centro Atlântico, 2003.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

_____. **Facebook atinge marca de 2 bilhões de usuários, anuncia Zuckerberg.** Folha de São Paulo. Disponível em: http://www1.folha.uol.com.br/tec/2017/06/1896428-facebook-atinge-marca-de-2-bilhoes-de-usuarios-anuncia-zuckerberg.shtml Acesso em 07.nov.2017

_____. **Mercado de TI sofre com falta de profissionais qualificados.** Empresa Brasil de Comunicação (EBC). Disponível em: <http://radios.ebc.com.br/revista-brasil/edicao/2016-07/mercado-de-ti-sofre-com-falta-de-profissionais-qualificados> Acesso em 13. nov. 2017.

_____. **Acessos SCM (Banda Larga Fixa) e Móvel.** TELEBRASIL – Associação Brasileira de Telecomunicações. Disponível em: http://www.telebrasil.org.br/panorama-do-setor/consulta-a-base-de-dados Acesso em: 07.nov.2017

_____. **Cibercrimes causaram prejuízos de bilhões de dólares no mundo em 2016.** Agência Brasil. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016>. Acesso em: 06.nov.2017

_____. **Mercado Brasileiro de Software-Panorama e Tendência-Estudo 2017-Dados de 2016**. Associação Brasileira de Software. Disponível em: <http://www.abessoftware.com.br/dados-do-setor/estudo-2017—dados-2016>. Acesso em 13. nov. 2017.

APÊNDICE A

Carreira Profissional

1 – Está trabalhando atualmente?

( ) Não ( ) Sim, em empresa de TI ( ) Sim, em outro tipo de empresa

2 - A área de Segurança da Informação te interessa como carreira?

( ) Sim ( ) Não ( ) Tenho interesse, mas pouco conhecimento sobre a área

3 - Tem interesse em fazer cursos específicos sobre Segurança em TI?

( ) Sim ( ) Não

4 - Em qual nível você avalia o seu curso atual em termos de noções de segurança em TI?

( ) Não tem ( ) Pouco conteúdo ( ) Razoável ( ) Bom ( ) Excelente

5 - Já fez algum tipo de hacking ou invasão anteriormente?

( ) Sim ( ) Não, mas tenho conhecimento ( ) Não, nem tenho conhecimento

6 - Já sofreu algum tipo de hacking ou invasão anteriormente?

( ) Sim ( ) Não sei ( ) Com certeza não

7 - Já identificou alguma falha em algum software ou sistema de terceiros?

( ) Nunca ( ) Sim, mas não reportei ( ) Sim, reportei pra empresa desenvolvedora

8 - Atualmente, se a empresa que você trabalha te chamar para coordenar a Segurança da TI?

( ) Eu aceito, com mesmo salário ( ) Eu aceito, se o salário for maior ( ) Eu recuso

Programação

1 - Indique o seu nível de conhecimento nas linguagens abaixo:

Assembler	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Bash	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
C	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
C++	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Java	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Perl	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
PHP	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Python	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Oracle	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
MySQL	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Postgre	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
NoSQL	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado

2 - O que você conhece sobre exploits?

[ ] Metasploitable	[ ] SQL Injection	[ ] Zero Day	[ ] Buffer Overflow
[ ] XSS Injection	[ ] Heap Overflow	[ ] Fuzzing	[ ] Meterpreter

3 - Já estudou o código fonte de algum exploit para entender o funcionamento?

( ) Nunca ( ) Sim, em curso ( ) Sim, sozinho ( ) Não, mas gostaria

4 - Já programou algum exploit?

( ) Nunca ( ) Sim, em curso ( ) Sim, sozinho ( ) Não, mas gostaria

5 - Já programou algum bugfix?

( ) Nunca ( ) Sim, em curso ( ) Sim, sozinho ( ) Não, mas gostaria

6 - Já programou utilizando Sockets?

( ) Nunca ( ) Sim, em curso ( ) Sim, sozinho ( ) Não, mas gostaria

REDE & SOS

1 - Indique o seu nível de conhecimento nos SOs abaixo:

Windows	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Linux	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
FreeBSD	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
MacOS	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado

2 - Quais protocolos você tem conhecimento técnico?

[ ] TCP	[ ] DHCP	[ ] UDP	[ ] NTP	[ ] POP3	[ ] SMTP
[ ] HTTP	[ ] SNMP	[ ] FTP	[ ] XMPP	[ ] SSH	[ ] TELNET

3 - Qual seu nível de conhecimento nos itens abaixo:

Firewall	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Proxy	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
DNS	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Roteamento	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado
Wireless	( ) Não conheço	( ) Iniciante	( ) Intermediário	( ) Avançado

4 - Você sabe instalar (operacional, física e lógica):

Rede Cabeada	( ) Sim	( ) Parcialmente	( ) Não
Rede Wireless	( ) Sim	( ) Parcialmente	( ) Não
Modem ADSL	( ) Sim	( ) Parcialmente	( ) Não
Roteador Cisco	( ) Sim	( ) Parcialmente	( ) Não

PESSOAS

1 – A empresa que você trabalha possui políticas de segurança?

( ) Sim ( ) Não ( ) Não sei informar ( ) Não se aplica

2 – A empresa que você trabalha oferece treinamento de segurança da informação?

( ) Não oferece ( ) Somente na admissão ( ) Eventualmente ( ) Frequentemente ( ) Não se aplica

3 - Na sua visão, com relação aos colaboradores, determine o grau de importância:

Login ao sistema	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Controle de acesso físico	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Alteração regular de senha	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Treinamento em Segurança TI	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Vigilância por câmeras	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Sistema de Ponto	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta
Identificação por crachá	( ) Nenhuma	( ) Pouca	( ) Média	( ) Alta

4 - Marque 3 itens que considerar mais importantes para falha de segurança na empresa:

[ ] Insatisfação	[ ] Baixo salário	[ ] Acesso irrestrito	[ ] Virus / Malware
[ ] Engenharia Social	[ ] Desinformação	[ ] Falta de Comunicação	[ ] Phishing

5 - De quem deve ser o dever de educar o novo funcionário sobre a Segurança da TI da empresa?

( ) Recursos Humanos ( ) Departamento de TI ( ) Gerência do Setor ( ) Diretoria

6 - Na sua visão, qual colaborador oferece maior risco?

( ) Novo funcionário ( ) Ex funcionário ( ) Funcionários atuais ( ) Colaborador terceirizado

Sexo: ( ) Feminino ( ) Masculino **Idade**: ( ) Entre 18 e 24 ( ) 25 e 32 ( ) 33 e 45 ( ) acima de 45

APÊNDICE B

O sistema de gerenciamento e análise do questionário foi desenvolvido em PHP, com o framework CodeIgniter na versão 3, utilizando banco de dados mySQL. Foi instalado em um link provisório dentro de um domínio do autor para que pudesse ser executado.

O sistema é composto por:

- tela de login, para que apenas aluno e coordenador possam acessar as informações;
- cadastro dos usuários que podem acessar o sistema;
- tela de cadastro dos questionários aplicados, com listagem, busca, consulta, inclusão, edição e exclusão;
- dashboard com gráficos de pizza com a análise dos totais de cada pergunta.

O banco de dados é composto basicamente de duas tabelas, sendo uma tabela para os administradores que podem acessar o sistema e a outra referente ao questionário que foi aplicado aos alunos.

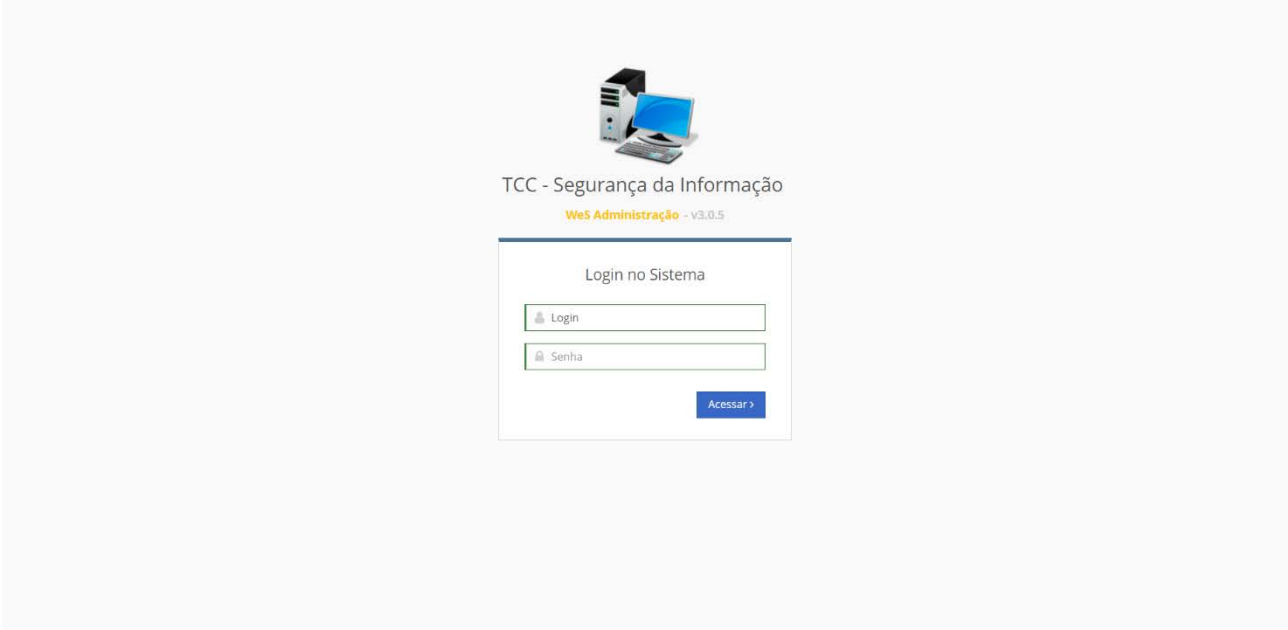
Como o objetivo do sistema é analisar o questionário, segue o código SQL de construção da tabela desenvolvida para essa finalidade:

```
CREATE TABLE `questionario` (
  `codigo` int(10) NOT NULL,
  `ativo` int(1) NOT NULL DEFAULT '1',
  `created_at` datetime NOT NULL,
  `updated_at` datetime NOT NULL,
  `deleted_at` datetime NOT NULL,
  `deleted` int(1) NOT NULL DEFAULT '0',
  `faculdade` varchar(40) NOT NULL,
  `publica_privada` int(2) NOT NULL DEFAULT '0',
  `curso` varchar(50) NOT NULL,
  `fase` int(3) NOT NULL,
  `idade` int(2) NOT NULL,
  `sexo` varchar(1) NOT NULL COMMENT 'M,F',
  `carreira_1` int(2) NOT NULL,
  `carreira_2` int(2) NOT NULL,
  `carreira_3` int(2) NOT NULL,
  `carreira_4` int(2) NOT NULL,
  `carreira_5` int(2) NOT NULL,
  `carreira_6` int(2) NOT NULL,
  `carreira_7` int(2) NOT NULL,
  `carreira_8` int(2) NOT NULL,
  `programacao_1_1` int(2) NOT NULL,
  `programacao_1_2` int(2) NOT NULL,
  `programacao_1_3` int(2) NOT NULL,
```

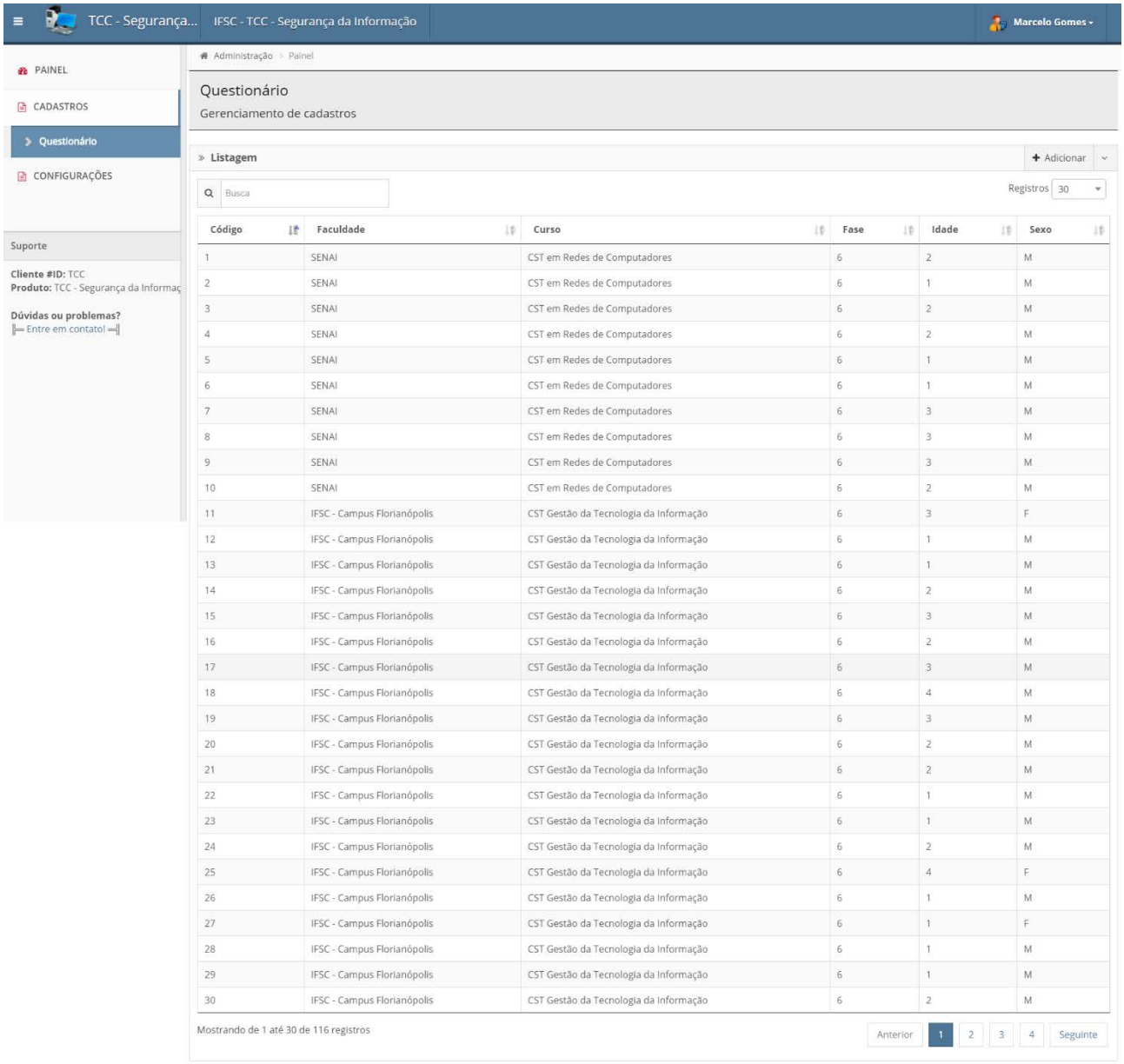
```
`programacao_1_4` int(2) NOT NULL,
`programacao_1_5` int(2) NOT NULL,
`programacao_1_6` int(2) NOT NULL,
`programacao_1_7` int(2) NOT NULL,
`programacao_1_8` int(2) NOT NULL,
`programacao_1_9` int(2) NOT NULL,
`programacao_1_10` int(2) NOT NULL,
`programacao_1_11` int(2) NOT NULL,
`programacao_1_12` int(2) NOT NULL,
`programacao_2_metasploitable` int(1) NOT NULL,
`programacao_2_sqlinjection` int(1) NOT NULL,
`programacao_2_zeroday` int(1) NOT NULL,
`programacao_2_bufferoverflow` int(1) NOT NULL,
`programacao_2_xssinjection` int(1) NOT NULL,
`programacao_2_heapoverflow` int(1) NOT NULL,
`programacao_2_fuzzing` int(1) NOT NULL,
`programacao_2_meterpreter` int(1) NOT NULL,
`programacao_3` int(2) NOT NULL,
`programacao_4` int(2) NOT NULL,
`programacao_5` int(2) NOT NULL,
`programacao_6` int(2) NOT NULL,
`rede_1_1` int(2) NOT NULL,
`rede_1_2` int(2) NOT NULL,
`rede_1_3` int(2) NOT NULL,
`rede_1_4` int(2) NOT NULL,
`rede_2_tcp` int(1) NOT NULL,
`rede_2_dhcp` int(1) NOT NULL,
`rede_2_udp` int(1) NOT NULL,
`rede_2_ntp` int(1) NOT NULL,
`rede_2_pop3` int(1) NOT NULL,
`rede_2_smtp` int(1) NOT NULL,
`rede_2_http` int(1) NOT NULL,
`rede_2_snmp` int(1) NOT NULL,
`rede_2_ftp` int(1) NOT NULL,
`rede_2_xmpp` int(1) NOT NULL,
`rede_2_ssh` int(1) NOT NULL,
`rede_2_telnet` int(1) NOT NULL,
`rede_3_1` int(2) NOT NULL,
`rede_3_2` int(2) NOT NULL,
`rede_3_3` int(2) NOT NULL,
`rede_3_4` int(2) NOT NULL,
`rede_3_5` int(2) NOT NULL,
`rede_4_1` int(2) NOT NULL,
`rede_4_2` int(2) NOT NULL,
`rede_4_3` int(2) NOT NULL,
`rede_4_4` int(2) NOT NULL,
`pessoas_1` int(2) NOT NULL,
`pessoas_2` int(2) NOT NULL,
`pessoas_3_1` int(2) NOT NULL,
`pessoas_3_2` int(2) NOT NULL,
`pessoas_3_3` int(2) NOT NULL,
```

```
  `pessoas_3_4` int(2) NOT NULL,
  `pessoas_3_5` int(2) NOT NULL,
  `pessoas_3_6` int(2) NOT NULL,
  `pessoas_3_7` int(2) NOT NULL,
  `pessoas_4_1` int(1) NOT NULL,
  `pessoas_4_2` int(1) NOT NULL,
  `pessoas_4_3` int(1) NOT NULL,
  `pessoas_4_4` int(1) NOT NULL,
  `pessoas_4_5` int(1) NOT NULL,
  `pessoas_4_6` int(1) NOT NULL,
  `pessoas_4_7` int(1) NOT NULL,
  `pessoas_4_8` int(1) NOT NULL,
  `pessoas_5` int(2) NOT NULL,
  `pessoas_6` int(2) NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

ALTER TABLE `questionario`
  ADD PRIMARY KEY (`codigo`);

ALTER TABLE `questionario`
MODIFY `codigo` int(10) NOT NULL AUTO_INCREMENT;
```

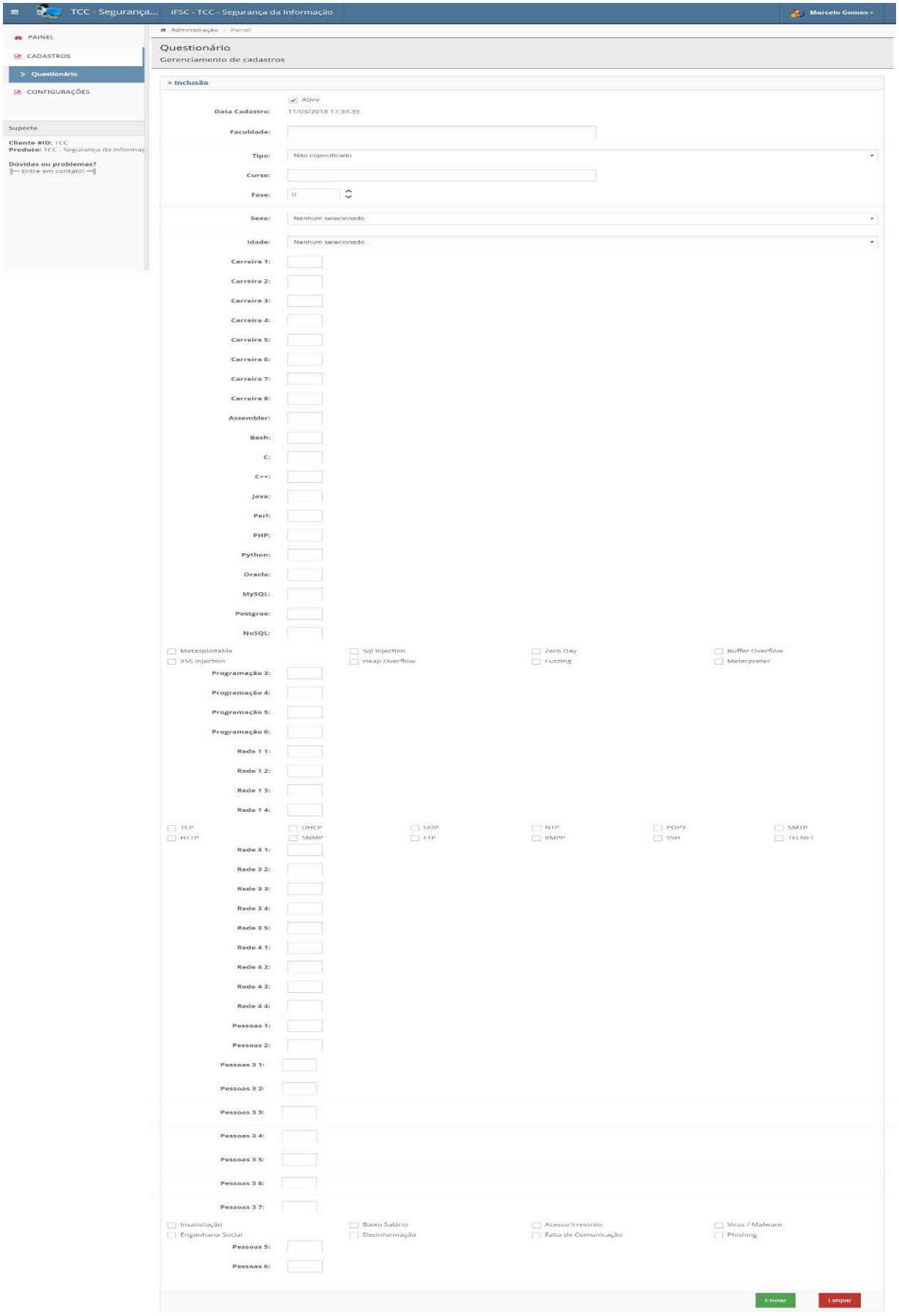
Telas do Sistema



Login do sistema



Listagem do cadastro de questionários



Cadastro individual das respostas do questionário.

Painel com todos os gráficos analíticos de todas as perguntas do questionário.