

## ENGENHARIA DE PRODUÇÃO E OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NO MERCADO CONTEMPORÂNEO.

Ayla Gabrielle de Oliveira Costa (UnP) aylagaby2007@hotmail.com

Kleber Jacinto (UnP) kleber.jacinto@unp.br

Maria da Conceição Pereira Mota (UnP) ceicinha.motta@hotmail.com

Talita Katusse de Moura (UnP) talita.2@outlook.com

**Resumo:** A globalização trouxe para a sociedade uma grande facilidade de acesso a informações e manipulação destas. No entanto, o mau uso disto trouxe vários prejuízos, por exemplo: a quebra de sigilo de informações privadas, a utilização de dados de terceiros e a invasão a propriedades cognitivas pertencentes a outras pessoas ou a empresas. Nesse âmbito, a proposta aqui exposta, buscou elencar dados que confirmem a necessidade do profissional de engenharia de produção para uma melhor gestão no tratamento dado a proteção da informação. Para isso realizaram-se pesquisas que demonstram a dimensão dos impactos causados pela má gestão nessa área, as leis e órgãos que protegem a propriedade do autor e dos dados. O foco foi estabelecer a partir de pesquisas quantitativas, a base para fomentar a credibilidade da ideia de que o engenheiro de produção, com sua graduação sendo dirigida a um alto grau de gestão, possui plena capacidade para manipular dados, verificar graus de confidencialidade, e o mais importante, saber distribuir entre todos os colaboradores de uma empresa o nível de acesso à essas informações. Em fechamento os dados orientam ao longo do trabalho aqui descrito, a carência existente nesse mercado e propõe incorporação do profissional de engenharia de produção para melhor atender a essa necessidade.

**Palavras-chave:** Segurança da Informação. Engenharia de Produção. Tecnologia da Informação.

## 1. Introdução

Diante da competitividade exacerbada do mercado atual, a informação vêm sendo um dos principais ativos das empresas, com o seu volume e grande concentração nos ambientes organizacionais, cresce a preocupação com a proteção destas, pois a sua veiculação por meio de redes locais, microcomputadores e a internet fragilizam a sua proteção. De acordo com o cenário, surgiu a necessidade de gerenciamento da segurança da informação, visto que o surgimento de novas ameaças é cada vez mais frequente, pois além da intervenção humana, agora também, estão disponíveis altas tecnologias.

A informação pode ser vista como qualquer conjunto de dados ou conteúdo, que possua grande valia para organizações ou indivíduos, com algum propósito. A informação digital é uma das mais ameaçadas hoje e tornou-se um produto do nosso século. Com a necessidade de proteção desenvolveu-se um novo ramo, chamado de segurança da informação.

As primeiras normas de proteção de dados surgiram em meados de 1987, com a união entre a indústria do Reino Unido (DTI) e o departamento de comércio, onde resultou a criação do Centro de Segurança da Informação (*Commercial Computer Security Centre- CCSC*). Estes, tinham como finalidade, a criação de um código de segurança para usuários e o desenvolvimento de normas de segurança para empresas britânicas que comercializavam produtos para segurança de T.I (Tecnologia da Informação). As normas desenvolvidas foram adotadas por várias organizações e sofreram várias revisões pela ISO, a parte 1 foi homologada em 01 de dezembro de 2000, como ISO/IEC 17799:2000.

Segundo a Rocha de Carvalho (2003), em seu estudo de caso com a aplicação da ISO/IEC 17799:2000, a segurança da informação é caracterizada pela preservação dos atributos de: confidencialidade, integridade e disponibilidade e é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades. Partindo da necessidade de gerenciamento desta, surgem os seguintes questionamentos: a manutenção da segurança da informação é uma tarefa só das equipes de T.I? Não é também uma atividade de gestão? Sendo esta, uma atividade de gestão, não caberia também ao profissional de engenharia de produção trabalhar nesta área?

## **2. Justificativa**

Em artigo publicado para a Revista Security em maio de 2017, Rogério Reis diretor da Arcon, divulgou uma pesquisa feita pelo Instituto Ponemon (Centro de pesquisa preeminente dedicado à política de privacidade, proteção de dados e segurança da informação), onde observa-se que o custo anual com cibercrime só aumenta. Os números do nosso país são surpreendentes, chegando a US\$ 154 em média, por cada dado roubado e relatou ainda que a porcentagem de dados roubados cresceu para 2100%. Estamos falando de uma pesquisa efetuada há mais de um ano, seguindo a tendência, é provável que já tenham crescido.

A medida que a tecnologia avança para o bem da sociedade, desenvolve-se com mais afinco o que é mau, principalmente, quando este, gera um lucro tão alto para os atacantes. Com o aumento dos ataques, o ideal seria, que as organizações investissem mais ainda na segurança das suas informações, mas que o investimento seja feito de forma correta, ou seja, investir em segurança é mais do que investir em tecnologia da informação, é antes de tudo, reconhecer a necessidade de uma gestão de pessoas, o perigo muitas vezes está onde menos se espera: a falta de conscientização dos colaboradores, a falta de confiança nestes, pode ser o agravante invisível e precisa ser controlado.

A tecnologia da informação já é uma cultura e um setor indispensável dentro de qualquer organização, porém, como exposto antes, as ameaças exigem mais do que isso: gestão. A sociedade ganhou há poucos anos um profissional que traz em essência a gestão, principalmente, a gestão de riscos a cada passo que uma empresa planeje andar, este profissional é o engenheiro de produção. Por ser uma profissão recente e devido a tantas engenharias já disponíveis no mercado, estes profissionais ainda são pouco conhecidos e explorados.

O engenheiro de produção é uma forte arma competitiva dentro de qualquer organização e objetivo deste trabalho é mostrar que a segurança da informação pode ser gerenciada por este profissional, a estatística de danos causados pela falta de segurança pode ser reduzida, por ter ligação direta com custos e lucros da organização, a área já é parte intrínseca do leque de funções do engenheiro de produção e só tem a ganhar com a interferência multidisciplinar deste profissional.

## **3. Fundamentação Teórica**

Hoje as equipes de T.I, atuam constantemente, em busca de manter seguras as informações lançadas no sistema computacional das organizações, afim de identificar o local e as pessoas apropriadas para acessá-las, assim também como entram na área de proteção os indivíduos que possuem informações sigilosas do negócio, as empresas consideram hoje, a propriedade intelectual, uma preciosa arma competitiva.

Definida pelo INPI (Instituto Nacional de Propriedade Intelectual), propriedade intelectual é a capacidade inventiva ou criadora do homem (conhecimento, tecnologia e saberes), falar este termo, é o mesmo que falar sobre: direitos autorais, marcas e patentes, a propriedade intelectual é considerada um ativo inatingível, na obra: Inovação e propriedade intelectual: guia para o docente, de Jungmann e Bonetti (2010).

O direito a proteção da criação é um assunto bastante discutido, porém, suas discussões possuem repercussão recente, no entanto, a proteção da propriedade intelectual é garantida pela Constituição Federal desde 1988, prevista no artigo 5º:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XXVII - aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar.

XXVIII - são assegurados, nos termos da lei:

- a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;
- b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de participarem aos criadores, intérpretes e às respectivas representações sindicais e associativas.

XXIX - a lei assegurará aos autores de inventos industriais privilégio temporário para sua utilização, bem como proteção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e econômico do País. (CONSTITUIÇÃO FEDERAL, 1988, ART. 5º, INCISOS XXVII, XXVIII E XXIX, EDIÇÃO 2016, PAG. 14)

Em fevereiro de 1998, foi decretada a Lei de Direitos Autorais nº 9.610, atualizando e dando outras providências a legislação. A propriedade intelectual vai muito além do que se expõe, podemos atribuir também, a este termo, todas as informações adquiridas pelo tempo, relativos a estratégias e funcionamento de cada empresa, e afirmar que os ativos das empresas são compostos principalmente por pessoas.

### **3.1 Segurança da Informação e seus impactos**

Com a crescente competitividade, a informação passou a ser o principal ativo das organizações contemporâneas. Ativos empresariais, são todos os elementos manipuladores de informação, como: sistemas, infraestrutura e pessoas. A facilidade trazida pelas altas tecnologias, desenvolvidas com afincamento a partir dos anos 90, trouxeram consigo uma grande fonte de armas maliciosas e disto, surgiu a necessidade de proteção constante de todos os ativos. Estes, quando desprotegidos podem causar uma perda financeira intangível, englobando a isto, a perda de credibilidade e confiança dos clientes, domínio intelectual, informações de clientes, descontinuidade de serviços e o custo de reparação de todo o dano.

O objetivo constante é garantir que os negócios não sejam expostos a ameaças e possam ter continuidade, para assegurar isto, desenvolveu-se um elemento indispensável para sucesso de qualquer empresa ou organização, a área da segurança da informação.

Santos Abreu (2011), afirma que para a construção de uma política de segurança existem alguns fatores que devem ser considerados, como: riscos, benefícios, custos e esforços de implementação de mecanismos. Além disso, as organizações devem garantir uma perspectiva geral do negócio, um conhecimento técnico e gerencial impecável, capazes de identificar ameaças e suas fontes. As

iminências nem sempre estão ligadas a softwares, podem se esconder por trás de fatores não tecnológicos e quando inicialmente não identificadas, o armazenamento e exposição tomam rumos inadequados. Dessa vulnerabilidade, podem surgir pequenos incidentes que causam grandes impactos no negócio.

O cenário, no que se refere a segurança da informação, vêm recebendo mudanças revolucionárias, pelo grande número de ataques tecnológicos sofridos desde o surgimento dos microcomputadores, existia uma crença nas sociedades corporativas, de que somente a área de tecnologia da informação necessitava de armas para combater invasores capazes de corromper sistemas e processos e com isso afetar a lucratividade. Em uma nova perspectiva, as organizações, pressionadas pela chamada “Era da Imitação”, reconhecem que a gestão é que ganha destaque, principalmente, a gestão de pessoas e das políticas de acesso, principais veiculadores da arma do século: a informação.

A “Era da Imitação” citada acima, deriva da necessidade de domínio de mercado, isto é conhecido como espionagem industrial, arma utilizada planejamento estratégico das organizações e também um dos principais motivadores de ataques. Sabemos que os ataques aos sistemas empresariais são muitos e ocorrem por diversos motivos, mas a espionagem industrial ganha destaque pois afeta diretamente a propriedade das empresas em cima de alguma ideia ou produto, para este tipo de ataque temos a Lei da Propriedade Industrial nº 9.279 de 1996, esta, busca impedir casos como os mencionados nos incisos XI e XII, artigo 195 da lei, por exemplo:

XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude. (LEI DA

PROPRIEDADE INDUSTRIAL N° 9.279, 1996, INCISOS XI E XII, ART. 195).

### **3.1.1 Surgimento do Agente de Segurança da Informação**

Devido a demanda crescente, surge o profissional conhecido como Agente de Segurança da Informação. Advindo da necessidade de que as organizações possuam estruturas consolidadas de disseminação e fiscalização das políticas de segurança, este, profissional busca unir a estratégia a tática, com um conhecimento primordial, o conhecimento da implementação de funções tecnológicas com especialização em estratégia e gestão de negócios, afim de monitorar e proteger-se das espionagens das grandes indústrias. Este profissional, cresce em cima das metodologias e disciplinas dos profissionais mencionados na introdução deste trabalho.

### **3.1 Normatização da Segurança da Informação**

Devido a proporção de problemas surgidos pelos falhos sistemas de Segurança da Informação nas empresas, surgiu a necessidade de normatização, desse modo foi criada a ISO 27001, com o objetivo de determinarem uma série de requisitos e procedimentos de controle, personalizados para cada organização, afim de gerar uma gestão mitigadora de riscos. Esta, é uma versão melhorada de práticas de segurança surgidas em 1992, em uma publicação de um código de práticas preventivas do governo britânico, podendo ser aplicada em qualquer tipo de organização, independentemente das suas particularidades. Hoje, algumas organizações já exigem certificação nessa área, afim de garantir para si e para seus parceiros um alto nível de segurança.

A Norma ISO 27001, introduziu a sua abordagem no modelo PDCA (*Plan- Do- Check- Act*), afim de construir um planejamento eficiente, com foco nos objetivos e política da organização, definindo as declarações de aplicabilidade do Sistema de Gestão da Segurança da Informação (SGSI) em questão. A partir disto, implementar os procedimentos, com medições periódicas, afim de dispor rapidamente de resultados para análise crítica e aplicação de medidas corretivas. Em resumo o SGSI, assim como qualquer outra área funcional, necessita manter-se em melhoria contínua.

Inicialmente, a mesma trata de uma autoanálise da organização, ou seja, os seus objetivos globais e específicos devem ser identificados, só com esta perspectiva holística das atividades é que os

riscos podem ser controlados, e isso nem sempre quer dizer exclusivos, alguns devem ser aceitos por fazerem parte da política. Toda análise efetuada e procedimento aplicado, deve ser documentado, com resultados reproduzíveis, para fins de comparação e garantia da eficácia das correções posteriores. O que diz a Norma quanto a documentação:

A documentação do SGSI deve incluir:

- a) declarações documentadas da política e objetivos do SGSI;
- b) o escopo do SGSI;
- c) procedimentos e controles que apoiam o SGSI;
- d) uma descrição da metodologia de análise/avaliação de riscos;
- e) o relatório de análise/avaliação de riscos;
- f) o plano de tratamento de riscos;
- g) procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles;
- h) registros requeridos por esta Norma; e
- i) a Declaração de Aplicabilidade. (NORMA ISO 27001, 2005)

Todos os documentos os documentos mencionados acima, antes de serem providenciados, também passam por uma análise crítica, afim, de identificar a sua real pertinência, seu período de atualização e valia. Já os registros de tudo que ocorre devem ser mantidos, ou seja, todas as decisões tomadas, mesmo que tenham sido modificadas ao longo do tempo, todo e qualquer procedimento conforme ou não-conforme dentro da organização.

Afim, de facilitar a separação de registros e garantir que as informações recebam proteção adequada, foi designado um item para a classificação da informação, item A.7.2 da Tabela A.1, o que diz a norma:



A.7.2.1- Recomendações para classificação: A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização;

A.7.2.2- Rótulos e tratamento da informação: Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização. (NORMA ISO 27001, TABELA A.1, 2005).

Para assegurar o comprometimento da empresa e a garantia de que o SGSI vai funcionar como necessário, é pertinente um comprometimento de toda a direção, garantindo também uma impecável estrutura física e de softwares, item A.9 da Tabela A.1, juntamente com o item A.10, com foco no planejamento e aceitação de sistemas e a proteção contra códigos maliciosos, mencionados nos itens A.10.3 e A.10.4. Garantir um corpo de funcionários devidamente treinados, com boa índole e que já conheçam as suas responsabilidades com todo o patrimônio utilizado para cumprir suas tarefas, desde o momento da contratação, item A.8 da Tabela A.1, tudo isso garantindo o cumprimento das exigências dos itens introduzidos no tópico A.11, tratando sobre o controle de acessos.

Com base na exigência do cumprimento das exigências mencionadas anteriormente, são normatizadas auditorias internas agendadas, com orientação da ABNT NBR ISO 19011:2002 que trata de Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental. A análise da continuidade do negócio também é exigida em Norma, mencionado no item A.14, afim de assegurar que uma falha em algum processo, seja mitigada habilmente e não venha afetar outros. Com tudo isso funcionando, deve-se garantir também a conformidade com as leis externas e internas, discriminados no item A.15.

A ISO 27001, traz em anexo a Tabela C.1, onde mostra correspondências desta, com a ABNT NBR ISO 9001:2000 e a ABNT NBR ISO 14001:2004. Onde, destaca-se a comum necessidade de implementar o que foi planejado e garantir mensuração e monitoria, para garantir reavaliações constantes e melhoria contínua, capacidade buscada através do modelo PDCA, citado no início desta Norma e na Tabela B.1.

Além da Normatização todas as organizações ou instituições que utilizem qualquer tipo de dados pessoais de terceiros, devem estar em cumprimento da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção dos dados pessoais. O tema foi tratado pelo senado após o vazamento de informações do Facebook e utilizado nas últimas eleições dos Estados Unidos. A atualização feita este ano na mesma, trata da proibição do uso ilícito de dados de usuários para cruzamento de informações e obtenção de informações a partir dela para determinar ofertas para aquele perfil, ou de subsidiar decisões comerciais para aquele grupo específico de perfil, dessa forma, possibilita aos cidadãos um maior controle sobre seus dados pessoais, atribuindo somente a ele a opção de consentir, explicitamente, o uso de seus dados para qualquer tipo de manipulação por outras pessoas, empresas ou órgãos governamentais. A lei prevê ainda a criação de um órgão regulador, a ANPD – Autoridade Nacional de proteção de dados, que estará vinculada ao ministério da justiça, as punições de infração para aqueles que descumprirem a lei, variam de advertência até multas de até 50 milhões de reais, bem como o bloqueio da atividade com o uso dos dados tratados indevidamente e sem consentimento legítimo. O seu cumprimento é solicitado também a empresas internacionais, desde que a coleta e tratamento sejam feitas com dados do território nacional brasileiro.

## **4. Metodologia**

A presente proposta, busca comprovar que a Gestão da Segurança da Informação deve ser feita por gestores em parceria com a Tecnologia da Informação, pois tão importante quanto o conhecimento tecnológico é a pré-avaliação de riscos e fragilidades frente as ameaças que surgem, cada vez mais imprevisíveis e inteligentes.

### **4.1 Delineamento Produtivo**

#### **4.1.1 Explorando o assunto**

Afim de atingir o objetivo exposto acima, iniciou-se o processo de pesquisa bibliográfica, com o intuito de conhecer e entender o que é de fato a segurança da informação, verificar como anda a disseminação dos estudos nessa área e compreender a o porquê, desta, ser uma arma competitiva indispensável no cenário atual, no intuito, de utilizar o conhecimento absorvido, para expor de forma explicativa as particularidades do assunto.

#### **4.1.2 Pesquisa Descritiva**

Foram desenvolvidos dois tipos de pesquisas, com perguntas extraídas em sua globalidade da pesquisa exploratória, as entrevistas foram destinadas a públicos específicos, mencionados abaixo:

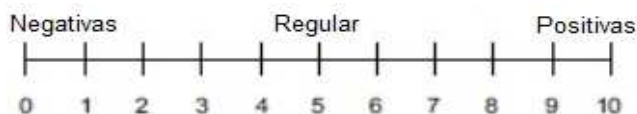
- a) Profissionais da Tecnologia da Informação: em busca de conhecer como anda o cenário da profissão diante da responsabilidade, cada vez maior, que lhes é atribuída e questionar a opinião dos mesmos relativa a proposta do trabalho.
- b) Engenheiros de Produção: estagiários do setor de Tecnologia da Informação com a finalidade de conhecer a experiência da parceria entre os profissionais de T.I e da engenharia de produção, e engenheiros formados, para com isto dispor de dados estatísticos para afirmação da nossa proposta.

As pesquisas foram efetuadas com intuito de expor quantitativamente os dados e facilitar uma análise estatística destes. A entrevista foi feita através de um questionário montado nos Formulários *Google* e foi encaminhada a um público intencionalmente selecionado, composto por profissionais das áreas envolvidas e citadas anteriormente, capazes de contribuir de forma significativa para o desenvolvimento deste trabalho.

### **5. Resultados e análise quantitativa**

As técnicas utilizadas para análise do material coletado, foram apenas observações comparativas, entre a realidade exposta pelo percentual obtido nas entrevistas e o cenário mercadológico atual. A partir disto, reafirmaram-se algumas ideias que estavam inicialmente em foco e desenvolveu-se uma nova perspectiva do assunto, levando em consideração as individualidades de cada profissional.

A métrica utilizada na maioria das perguntas foi uma escala de 0 a 10, que tem para sua legenda atribuímos: respostas abaixo de 5 são consideradas negativas para o questionamento, 5 seria regular, ou seja, o meio termo formado pelas pessoas que possuem dúvidas sobre o assunto, e para respostas acima de 5 consideramos respostas positivas, que favorecem o tema em foco.



**Figura 1-** Métrica de análise utilizada nas pesquisas em escala.

### 5.1 Exposição de dados, resultados e análises

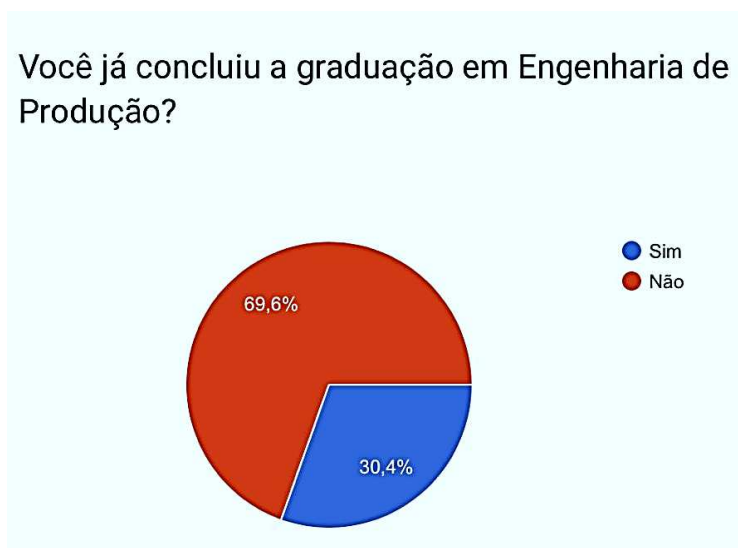
Na Tabela 1, dispomos do banco de questões múltipla escolha utilizadas, onde as três primeiras perguntas foram aplicadas ao público da engenharia de produção e a última pergunta aplicada aos profissionais de T.I, cada pergunta está exposta com o resultado obtido ao lado.

Tabela 1- Questões múltipla escolha das duas pesquisas.

| Questionário  | Percentual da resposta |       |
|---|------------------------|-------|
|   | Não                    | Sim   |
| Você já concluiu a graduação de engenharia de produção?             | 69,6%                  | 30,4% |
| Você trabalha atualmente?   | 39,1%                  | 60,9% |
| Você já estagiou, ou estageia na área da tecnologia da informação?  | 82,6%                  | 17,4% |
| Você já trabalhou, ou trabalha na área da tecnologia da informação? | 78,3%                  | 21,7% |
| Você já trabalhou com engenheiros de produção?                      | 82,6%                  | 17,4% |

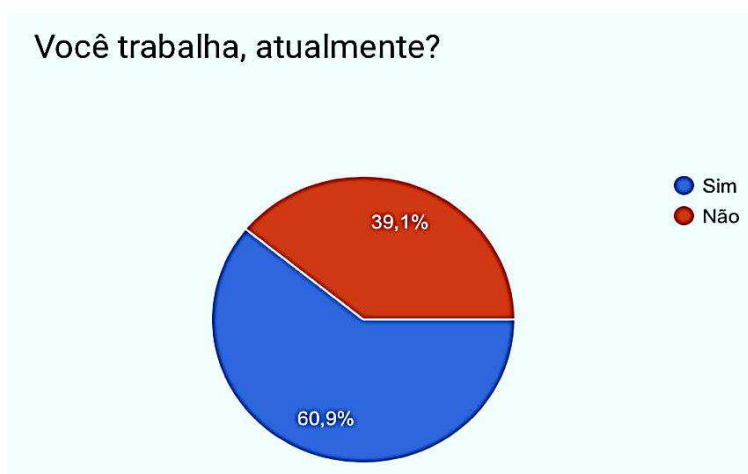
Iniciamos as pesquisas identificando o percentual do público que ainda está em processo de graduação na engenharia de produção e os já formados, afim, de identificar se a segurança da informação já tem importância reconhecida mesmo na vida acadêmica.

Como pode-se observar no Gráfico 1, nas pesquisas voltadas para estudantes e engenheiros de produção, obteve-se um uma amostra de 45 pessoas, onde 69,6% desta é composta por estudantes e apenas 30,4% já são formados, ou seja, maior parte da amostra está em fase de amadurecimento, e possibilitará identificar a sua posição sobre o assunto.



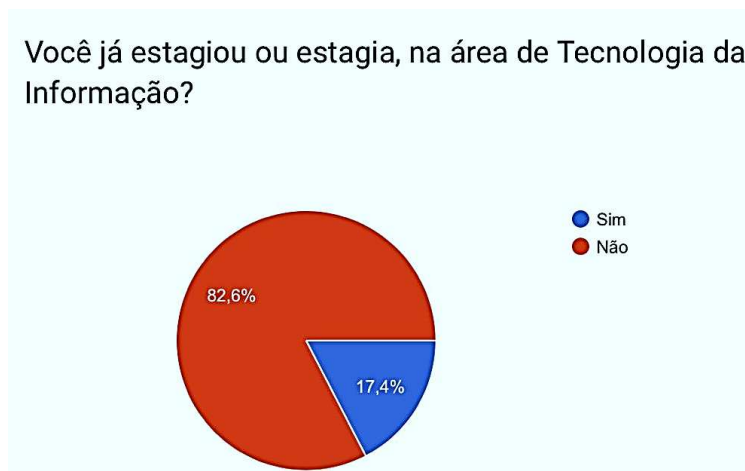
**Gráfico 1-** Pesquisa realizada com estudantes e engenheiros de produção.

De acordo com o Gráfico 2, 60,9% das pessoas estão trabalhando atualmente e somente 39,1% não trabalham, com os dados desse questionamento espera-se que a parte da amostra que já trabalha tenha conhecimento da importância da segurança da informação no ambiente de trabalho.



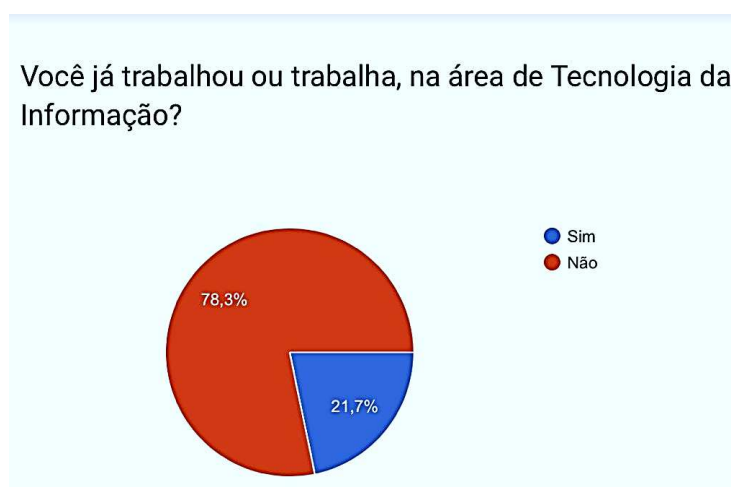
**Gráfico 2-** Pesquisa realizada com estudantes e engenheiros de produção.

As pessoas que estagiaram na área, representam 17,4% da amostra e através dos dados que foram expostos anteriormente, percebe-se que houve uma variação no cenário, algumas pessoas não tiveram contato com a área de T.I durante o período de estágio e mesmo assim, encontraram esse mercado em um momento posterior.



**Gráfico 3-** Pesquisa realizada com estudantes e engenheiros de produção.

O percentual de pessoas que trabalham na área de T.I é de 21,7%, o que nos permite concluir que das 27 pessoas que trabalham, aproximadamente 10 delas trabalham com T.I, quantidade expressiva, considerando o tamanho da amostra.



**Gráfico 4-** Pesquisa realizada com estudantes e engenheiros de produção.

Os questionamentos posteriores foram desenvolvidos com o intuito de identificar como o profissional da engenharia se reconhece dentro da área de segurança da informação, se reconhece a sua importância e se compreende a necessidade e riqueza da parceria com os profissionais de T.I.

Tabela 2- Banco de questões em escala, aplicadas a estudantes e engenheiros de produção.

| Questão  | Número da questão |
|--|-------------------|
| De 0 à 10 Indique o quanto considera produtiva a parceria entre engenheiros de produção e profissionais da tecnologia da informação, para gerir a segurança da informação nas organizações:              | <b>01</b>         |
| De 0 à 10, indique o quão adequado você se considera para fazer a segurança da informação em uma organização. Onde “ 0 significa não adequado” e “ 10 muito adequado”.                                   | <b>02</b>         |
| De 0 à 10, o quanto a falta de procedimento de segurança da informação, colocaria em risco o trabalho que desenvolve(eu) atualmente na organização em que trabalha.                                      | <b>03</b>         |
| De 0 à 10, indique o quão importante seria, dispor de um profissional de T.I. para fazer a gestão de segurança da informação, onde “0 significa nenhuma importância” e “10 significa total importancia”. | <b>04</b>         |
| De 0 à 10, o quanto você considera que o crescente aumento de ataques pela má gestão da segurança da informação nas organizações, de deve pela falta de investimento em gestão de acessos e de pessoas.  | <b>05</b>         |
| Indique de 0 à 10, o quanto você considera que o crescente aumento de ataques, pela má gestão da segurança da informação nas organizações, se deve pela falta de investimento em T.I.                    | <b>06</b>         |

Na Tabela 2, dispõe-se do banco de questões utilizadas, com identificação numeral ao lado, afim de esclarecer a Tabela 3 que expõe todo o resultado percentual ao lado da questão referida.

Tabela 3- Resultados das pesquisas realizadas com estudantes e engenheiros de produção.

| Nº da<br>questão | Resultado da Pesquisa em percentual (%): |     |     |     |     |      |      |      |      |      |      |
|------------------|--|-----|-----|-----|-----|------|------|------|------|------|------|
|                  | Notas do grau de relevância de 0 à 10    |     |     |     |     |      |      |      |      |      |      |
|                  | 0  | 1   | 2   | 3   | 4   | 5    | 6    | 7    | 8    | 9    | 10   |
| <b>01</b>        | 2,2                                      | -   | -   | -   | -   | -    | 4,3  | 6,5  | 19,6 | 21,7 | 43,5 |
| <b>02</b>        | 8,7                                      | 2,2 | 8,7 | 8,7 | 6,5 | 8,7  | 10,9 | 13,0 | 17,4 | 2,2  | 13,0 |
| <b>03</b>        | 4,3                                      | -   | -   | 2,2 | 2,2 | 6,5  | 4,3  | 6,5  | 28,3 | 19,6 | 26,1 |
| <b>04</b>        | -  | -   | -   | 2,2 | -   | 2,2  | -    | 13,0 | 17,4 | 19,6 | 45,7 |
| <b>05</b>        | 2,2                                      | -   | -   | 2,2 | -   | 15,2 | 4,3  | 10,9 | 23,9 | 26,1 | 15,2 |
| <b>06</b>        | -  | -   | -   | 2,2 | -   | 4,3  | 2,2  | 10,9 | 26,1 | 28,3 | 26,1 |

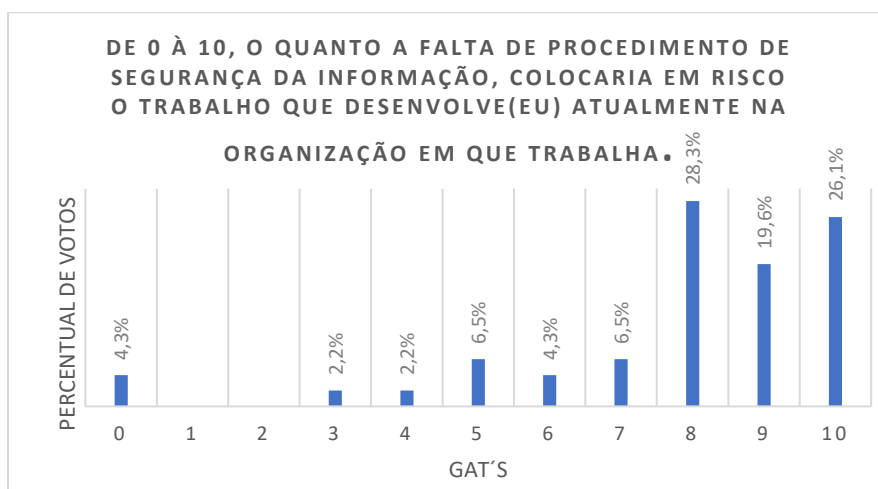
Fonte: Os autores (2019).

Nos Gráfico 5, a pesquisa foi feita com métrica em gat's de 0 a 10, onde grande maioria dos entrevistados reconheceu que a falta de procedimentos em segurança da informação colocaria em risco a atividade na qual desenvolve na organização em que trabalha ou na atividade que desenvolveu quando estagiou, chegando a um percentual de 74,0%, considerando as marcações dos gat's entre 8 e 10.

Aproxima-se do resultado esperado, visualizando que o maior percentual foi de respostas positivas, acima de 5, porém, as respostas para este questionamento deveriam ser unânimes nos maiores gat's, visto que, um engenheiro de produção estuda gestão de riscos e tem obrigação de identificar ameaças em qualquer processo produtivo ou de prestação de serviços.



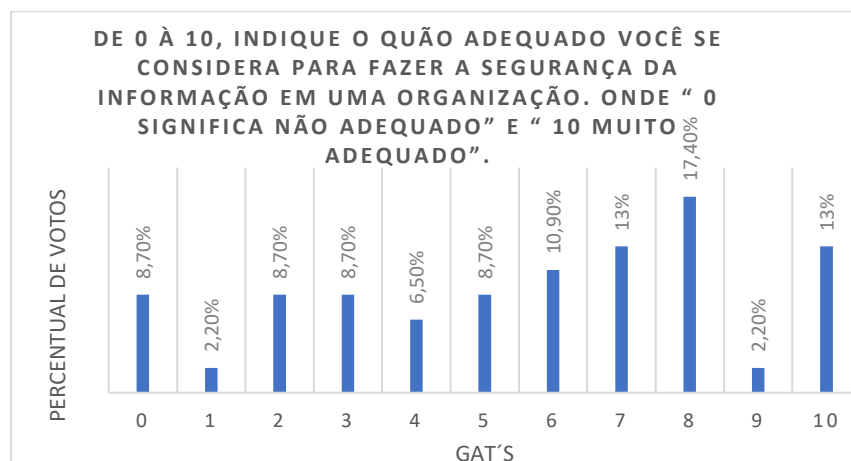
**Gráfico 5-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

Quanto a aptidão para gerenciar a segurança da informação de uma organização todos os gat's foram marcados, 56,59% marcaram acima de 6 e 32,6% indicou entre 8 e 10, é um resultado positivo, porém, não se pode ignorar o percentual expressivo de pessoas que marcaram abaixo de 5. A variação permite especular que as pessoas que marcaram abaixo de 5 consideram que a grade curricular de formação não lhe dá subsídios pra isso e que as pessoas que se consideram aptas fariam alguma especialização na área para assumir essa tarefa.

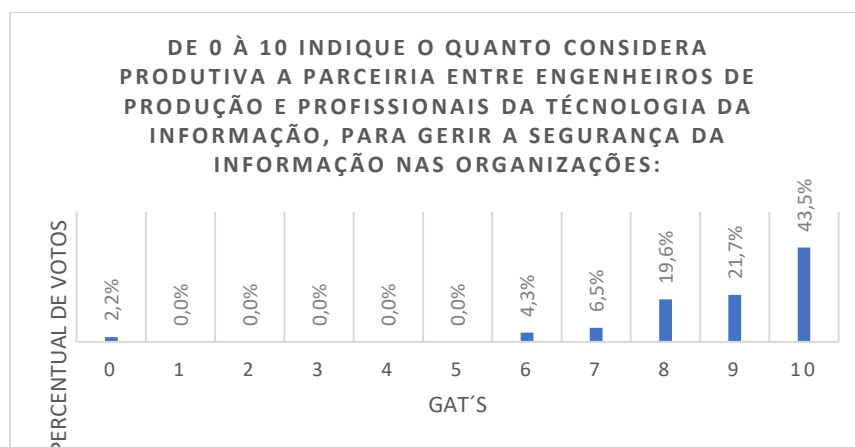
**Gráfico 6-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

No Gráfico 7, 83,8% dos entrevistados marcaram entre 8 e 10, considerando que a parceria entre engenheiros de produção e profissionais de T.I é interessante para melhorar o desenvolvimento da área, o que indica bastante coerência em reconhecer que os profissionais farão um melhor trabalho juntos.

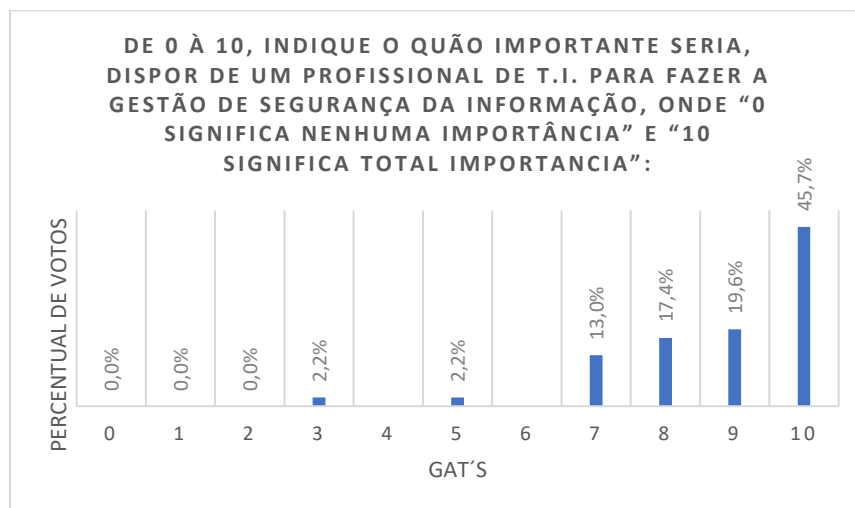
**Gráfico 7-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

Reafirmando isso, temos o resultado exposto no Gráfico 8, onde, 82,7% dos entrevistados consideram de suma importância dispor de um profissional de T.I para gerir a segurança da informação, indicando os gat's entre 8 e 10.

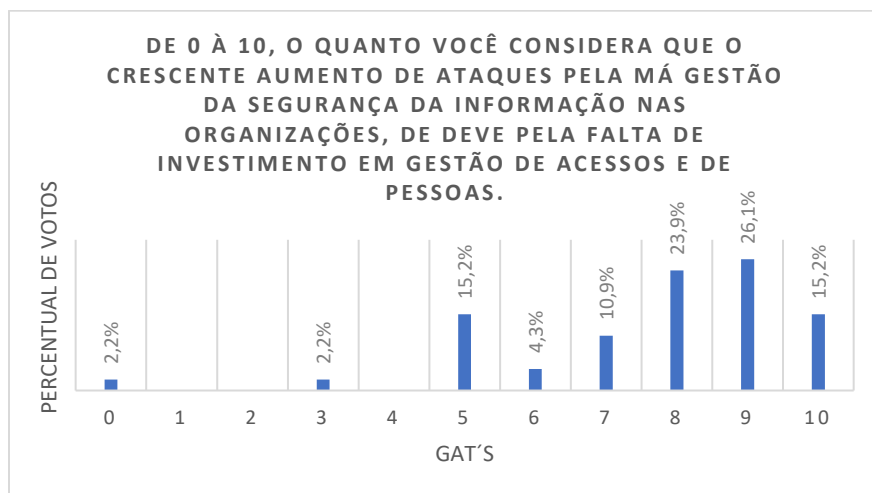
**Gráfico 8-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

No Gráfico 9, 65,20% dos entrevistados marcaram os gat's entre 8 e 10, grande parte dos entrevistados acreditam que as ameaças estão crescendo por falta de investimento em gestão.

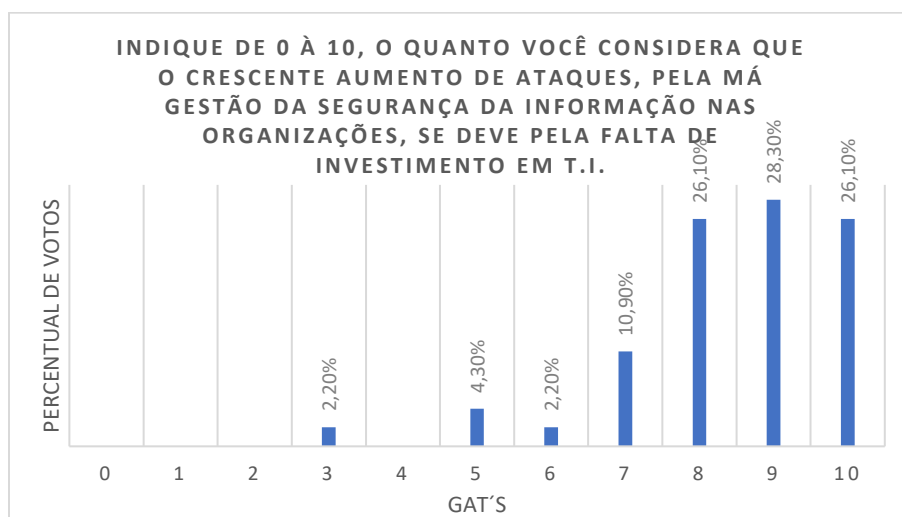
**Gráfico 9-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

Quando indagados se o aumento se decorria por falta de investimento em T.I o percentual dos mesmos gat's foi bem maior, chegando a 80,5%, observa-se que nem mesmo os profissionais de gestão reconhecem e equiparam a importância da gestão de pessoas com o conhecimento tecnológico dentro da segurança da informação. É uma cultura que vem sendo quebrada, mas ainda precisa ser bem difundida, sem o reconhecimento dos próprios profissionais é inviável para as organizações admiti-los.

**Gráfico 10-** Pesquisa realizada com estudantes e engenheiros de produção.



Fonte: Os autores (2019).

## 5.2 Exposição de dados e análises finais

As questões abaixo, foram desenvolvidas para profissionais de T.I, afim de detectar como eles se veem na área de segurança da informação e saber a sua opinião quanto a introdução do engenheiro de produção nesse ramo.

Tabela 4- Banco de questões em escala, aplicadas aos profissionais de T.I.

| Questão   | Número da questão |
|---|-------------------|
| Indique de 0 à 10, o quanto você considera que o crescente aumento de ataques, pela má gestão da segurança da informação nas organizações, se deve pela falta de investimento em T.I.                 | <b>01</b>         |
| De 0 à 10, indique o quão adequado você se considera para fazer a segurança da informação em uma organização. Onde “ 0 significa não adequado” e “ 10 muito adequado”.                                | <b>02</b>         |
| Indique de 0 à 10, o quanto você considera que o aumento de ataques pela má gestão da segurança da informação nas organizações, se deve pela falta de investimento em gestão de acessos e de pessoas. | <b>03</b>         |

De 0 à 10 indique o quão importante seria dispor de um engenheiro de produção para fazer a gestão da segurança da informação, onde: “0 significa, nenhuma importância” e “10 total importância”. **04**

Indique de 0 à 10, o quão essa parceria multidisciplinar entre engenheiros de produção e os profissionais de T.I., melhoraria na qualidade da segurança da informação nas organizações, onde: “0 significa, nenhuma melhoria” e “10 melhoraria consideravelmente”. **05**

Indique de 0 à 10, o quanto a falta de procedimentos de segurança da informação, colocaria em risco o trabalho que desenvolve atualmente na organização em que trabalha. **06**

Fonte: Os autores (2019).

Na Tabela 4, dispõe-se do banco de questões utilizadas, com identificação numeral ao lado, afim de esclarecer a Tabela 5 que expõe todo o resultado percentual ao lado da questão referida, agora voltada para resultados da pesquisa aplicada aos profissionais de T.I.

Tabela 5- Resultados das pesquisas realizadas com profissionais de T.I

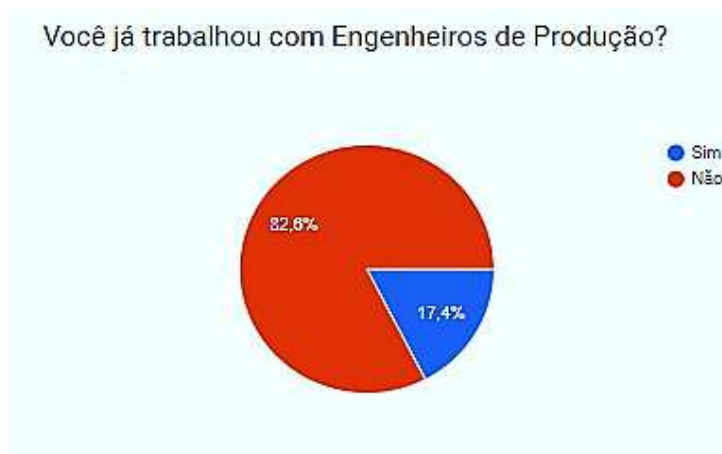
| Nº da<br>questão | <b>Resultado da Pesquisa em percentual (%):</b> |          |          |          |          |          |          |          |          |          |           |
|------------------|---|----------|----------|----------|----------|----------|----------|----------|----------|----------|-----------|
|                  | <b>Notas do grau de relevância de 0 à 10</b>    |          |          |          |          |          |          |          |          |          |           |
|                  | <b>0</b>  | <b>1</b> | <b>2</b> | <b>3</b> | <b>4</b> | <b>5</b> | <b>6</b> | <b>7</b> | <b>8</b> | <b>9</b> | <b>10</b> |
| <b>01</b>        | -   | -        | -        | -        | -        | 8,7      | 2,2      | 17,4     | 23,9     | 10,9     | 37,0      |
| <b>02</b>        | 6,5   | -        | 8,7      | 2,2      | 4,3      | 8,7      | 8,7      | 13,0     | 28,1     | 8,7      | 13,0      |
| <b>03</b>        | -   | -        | -        | 2,2      | -        | 8,7      | 4,3      | 4,3      | 23,9     | 10,9     | 45,7      |
| <b>04</b>        | 13,0  | 6,5      | 2,2      | 6,5      | 6,5      | 8,7      | 10,9     | 17,4     | 10,9     | 4,3      | 13,0      |

|           |     |     |      |     |     |     |     |      |     |      |      |
|-----------|-----|-----|------|-----|-----|-----|-----|------|-----|------|------|
| <b>05</b> | 6,5 | 4,3 | 10,9 | 6,5 | -   | 8,7 | 4,3 | 19,6 | 8,7 | 13,0 | 17,4 |
| <b>06</b> | -   | -   | 4,3  | 2,2 | 6,5 | 4,3 | 4,3 | 8,7  | 4,3 | 15,2 | 50,0 |

Fonte: Os autores (2019).

A segunda parte do questionário, foi aplicado a uma amostra de 46 profissionais de T.I, onde 82,6% do público comentou nunca ter trabalhado com Engenheiros de Produção, resultado esperado de acordo com o cenário.

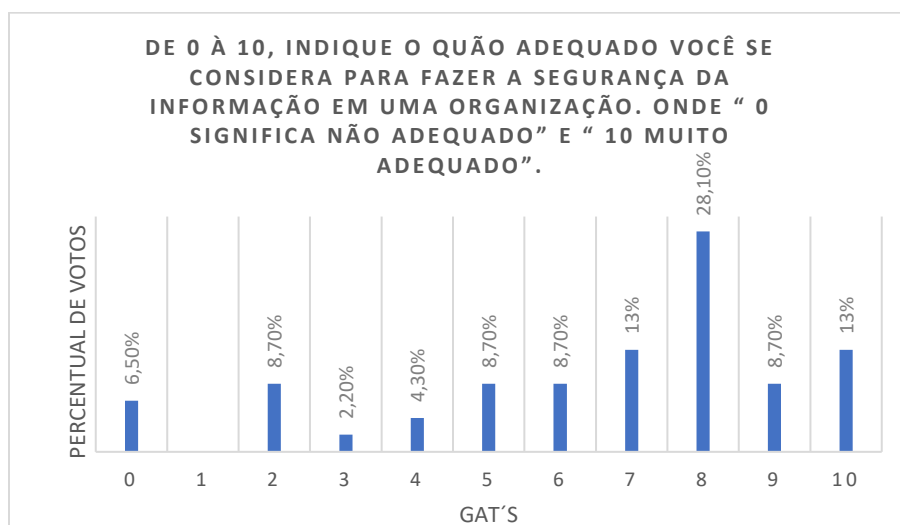
**Gráfico 11-** Pesquisa realizada com profissionais de Tecnologia da Informação.



Fonte: Os autores (2019).

Foi questionado também, quanto a aptidão desses profissionais para fazer a gestão da segurança de informação na empresa em que trabalham, o que foi interessante perceber que há uma insegurança, até mesmo entre eles que são comumente indicados a esse cargo, as respostas foram bastante dispersas, no entanto, 49,8% ainda indicaram opções entre 8 e 10.

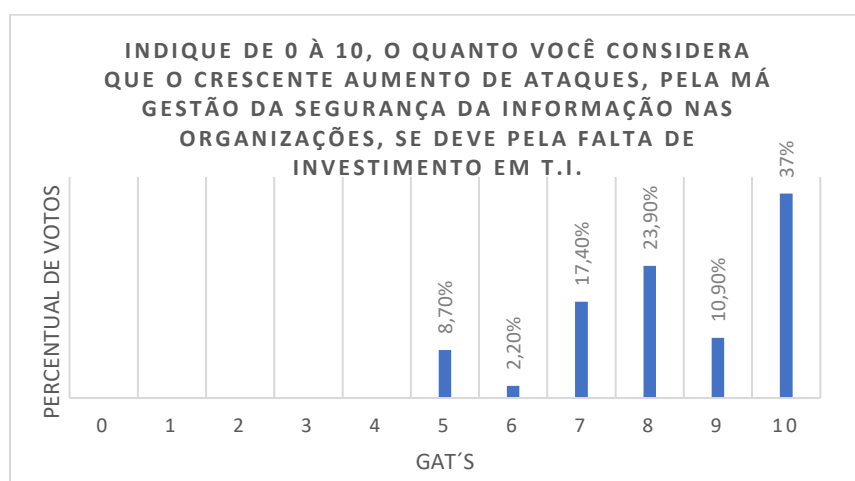
**Gráfico 12-** Pesquisa realizada com profissionais de Tecnologia da Informação.



Fonte: Os autores (2019).

Quanto ao aumento dos ataques nas organizações, foram questionados se os mesmos consideravam que tinha relação ao pouco investimento em T.I, e 100% da amostra indicou na escala os gat's de 6 acima, com 71,8% da amostra marcando entre 8 e 10., percebe-se que os profissionais reconhecem a carência na área e acreditam que as empresas deveriam dar uma maior importância.

**Gráfico 13-** Pesquisa realizada com profissionais de Tecnologia da Informação.

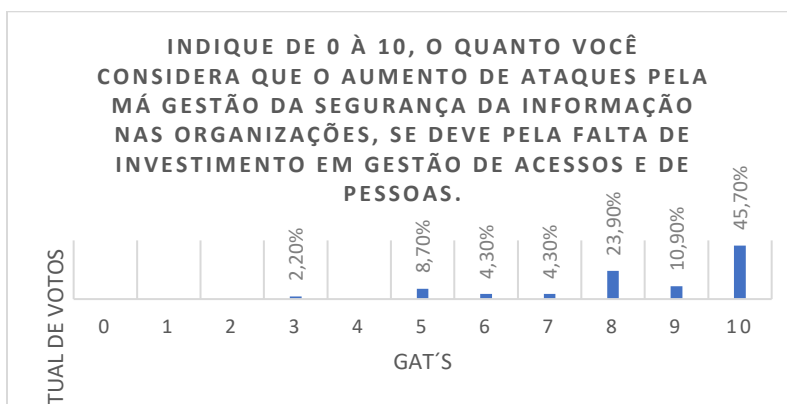


Fonte: Os autores (2019).

Se questionados se o aumento dos ataques era por falta de investimento em gestão de acessos e de pessoas, o resultado foi bastante expressivo, 80,5% indicaram entre 8 e 10.

Fazendo uma ligação entre os resultados da pesquisa com engenheiros, identificamos que o pessoal da T.I, geralmente os mais envolvidos na área de segurança, reconhecem bem mais a necessidade e a importância da gestão, pelo simples fato, de manipular bem as técnicas sistemáticas, mas que não são suficientes pra suprirem todos os canais de ameaças, além disso dividem o seu tempo com outras funções na organização.

**Gráfico 14-** Pesquisa realizada com profissionais de Tecnologia da Informação.

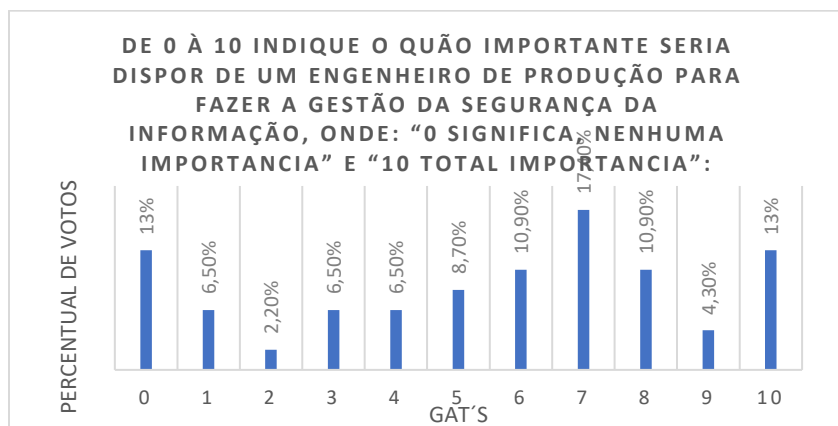


Fonte: Os autores (2019).

Quanto a importância de dispor de um engenheiro de produção para assumir o papel de gerir a informação, os resultados não foram muito convictos e apenas 56,5% marcaram de 6 acima, as respostas não têm um percentual significativo nos números maiores, entre 8 e 10, por exemplo, aparentam ter sido marcados com incerteza. Percebe-se que os profissionais entrevistados não consideram ideal ser tarefa do engenheiro de produção, mesmo considerando que falta investimento em gestão.

**Gráfico 15-** Pesquisa realizada com profissionais de Tecnologia da Informação.

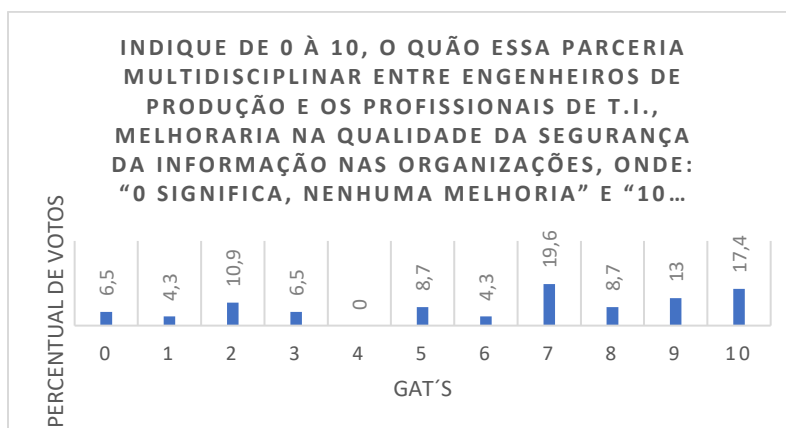




Fonte: Os autores (2019).

Dispomos no Gráfico 16, do resultado que se refere a opinião quanto a parceria entre engenheiros de produção e profissionais de T.I, e obtivemos 71,7% das respostas de 6 acima, com foco nos gat's 7 e 10. Para os dois perfis de entrevistados obteve-se um resultado melhor que o esperado, é interessante reconhecerem que para um gerenciamento eficaz precisam caminhar em paralelo.

**Gráfico 16-** Pesquisa realizada com profissionais de Tecnologia da Informação.

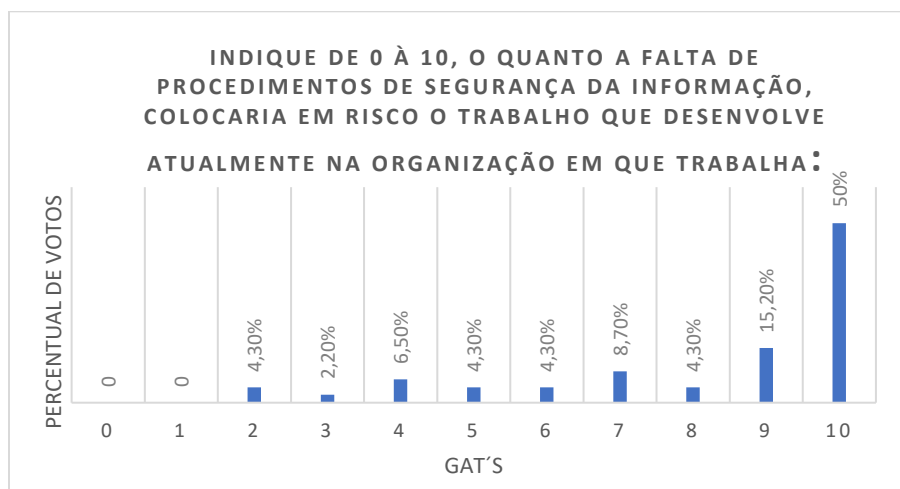


Fonte: Os autores (2019).

O resultado não saiu como esperado na questão, onde indaga-se quanto ao risco que a falta ou a má gestão da segurança da informação seria para atividade exercida atualmente na organização em que trabalha, pois 69,5% indicou entre 8 e 10, 50,0% indicou 10 e os outros resultados variaram muito, a maioria dos números foram indicados.

O que preocupa é saber que diante do cenário muitos colaboradores ainda não reconheçam a segurança da informação como algo indispensável e que influencia qualquer atividade, mesmo que não envolva a utilização de softwares e hardwares, a segurança da informação, anda mal reconhecida entre as pessoas, o que é preocupante, pois qualquer colaborador deve ter conhecimento de riscos.

**Gráfico 17-** Pesquisa realizada com profissionais de Tecnologia da Informação.



Fonte: Os autores (2019).

### 5.3 Comparando os perfis

Abaixo, veremos uma tabela que expõe os questionamentos que eram semelhantes aos dois públicos, os percentuais utilizados consideram sempre as indicações entre 8 e 10, que são os gat's mais satisfatórios.

Ressalta-se novamente que os dois profissionais precisam melhorar a sua avaliação quanto ao perigo que é não dispor de uma ótima gestão da segurança, como comentado, esperava-se que as respostas fossem unânimes nos gat's mais altos. Observa-se, que os profissionais de T.I possuem maior segurança para gerenciar a área, como já era esperado, pois há uma forte cultura de que segurança da informação é assunto técnico e nos dados coletados, o sentimento de aptidão destes, comparado ao engenheiro é significativamente mais alto.

Quanto a parceria dos profissionais, os engenheiros de produção tiveram percentual maior, resultado esperado sim, o que ressalta mais uma vez a insegurança do mesmo quanto a essa

atividade, que é reafirmada na pergunta posterior, onde se indagam sobre a importância de ter um profissional de T.I, com um resultado bastante alto, já quando foi o inverso, os profissionais da T.I não consideram algo tão importante, de acordo com o resultado exposto. Porém, mesmo com esse resultado os profissionais de T.I consideram que falta mais investimento em gestão do que em T.I, o que não aconteceu com os engenheiros de produção, pois indicaram um resultado bem acima para o investimento em T.I.

Tabela 6- Exposição de resultados para perguntas semelhantes entre os públicos.

|   |  |
|---|--|
| Indique de 0 a 10, o quanto a falta de procedimentos de Segurança da Informação, colocaria em risco o trabalho que desenvolve(eu) atualmente na organização em que trabalha.  |  |
| Engenheiros de Produção   | T.I  |
| 74,00%  | 69,50%   |
| De 0 a 10, indique o quão adequado você se considera, para fazer a gestão da Segurança da Informação em uma organização, onde: "0 significa, não adequado" e "10 muito adequado".                                   |  |
| Engenheiros de Produção   | T.I  |
| 32,60%  | 71,80%   |
| De 0 a 10, indique o quanto considera produtiva a parceria entre Engenheiros de Produção e profissionais da Tecnologia da Informação, para gerir a Segurança da Informação nas organizações.                        |  |
| Engenheiros de Produção   | T.I  |
| 83,80%  | 71,70%   |
| De 0 a 10, indique o quão importante seria, dispor de um Profissional de T.I para fazer a gestão da Segurança da Informação, onde: "0 significa, nenhuma importância" e "10 total importância".                     | De 0 a 10, indique o quão importante seria, dispor de um Engenheiro de Produção para fazer a gestão da Segurança da Informação, onde: "0 significa, nenhuma importância" e "10 total importância". |
| Engenheiros de Produção   | T.I  |
| 82,70%  | 28,20%   |
| Indique de 0 a 10, o quanto você considera, que o o crescente aumento de ataques, pela má gestão da Segurança da Informação nas organizações, se deve pela falta de investimento em T.I.                            |  |
| Engenheiros de Produção   | T.I  |
| 80,50%  | 71,80%   |
| Indique de 0 a 10, o quanto você considera, que o o crescente aumento de ataques, pela má gestão da Segurança da Informação nas organizações, se deve pela falta de investimento em gestão de acessos e de pessoas. |  |
| Engenheiros de Produção   | T.I  |
| 65,20%  | 80,50%   |

Fonte: Os autores (2019).

## 6. Propostas para continuidade do trabalho

Este trabalho, surgiu através da necessidade de falar mais sobre segurança da informação, principalmente, dentro das salas de engenharia de produção, como uma busca de alertar os estudantes e profissionais para um fato burocrático e importante que que é o alicerce de qualquer

organização. Que este trabalho possa ter continuidade, pois a partir das pesquisas efetuadas e expostas acima são criadas novas pautas, algumas delas ficam como sugestão:

- Analisar a trajetória de engenheiros de produção que já integram a área de segurança da informação;
- Estudar casos de empresa que possuem uma fraca gestão da segurança da informação e descobrir os motivos;
- Verificar em quais tipos de negócios a espionagem industrial é mais ativa;
- Criação de uma metodologia conjunta, integrando a gestão e o T.I, afim de formar agentes de segurança.

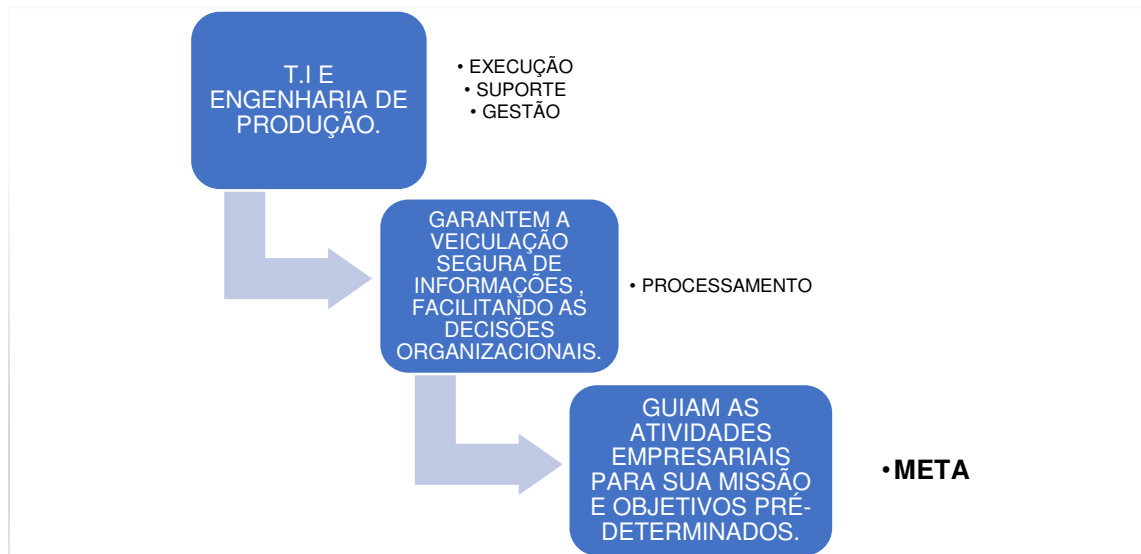
## **7. Considerações finais**

Através dos resultados com esses dois públicos, pode-se perceber que os profissionais ainda não reconhecem de fato o impacto que a má gestão da segurança da informação causa em um ambiente, principalmente, quando este, luta pra manter uma boa posição competitiva no mercado.

Os dois perfis sentem-se inseguros quanto a sua aptidão para gerir a segurança da informação sozinhos, o que é muito importante, para que consigam entender o impacto positivo que a união das competências dos dois profissionais traria. Embora, a maioria das organizações optem pelo profissional conhecido como agente de segurança, é interessante dispor do mesmo serviço com profissionais que já estão inseridos no mercado e que possuem participam e são extremamente úteis para outras atividades exercidas no local, o empirismo adquirido em todas as faces da organização, é um forte aliado no combate a espionagem industrial e ataques virtuais.

### **7.1 Proposta**

**Fluxograma 1-** Simulação do desempenho da proposta.



Fonte: Os autores (2019).

Sabe-se que o mercado é composto por vários profissionais de gestão, porém, o Engenheiro de Produção seria um dos mais adequados, por dispor de áreas que são indispensáveis na segurança da informação, como: Logística, Engenharia da Sustentabilidade, Engenharia de Operações e Processos de Produção, Pesquisa Operacional, Engenharia da Qualidade, Engenharia do Trabalho, Engenharia Organizacional, Engenharia Econômica, Engenharia do Produto e a Educação em Engenharia de Produção.

Nas dez áreas citadas acima, ressaltam-se algumas que têm influência direta na implantação e manutenção da segurança da informação, mas a maioria delas são dependentes totais da segurança, como é o caso da engenharia do produto, que pode ser vítima de roubo, cópias, fraudes no desenvolvimento e lançamento do produto, além de todas as demais áreas, que quando não influenciam, são dependentes totais de um bom gerenciamento em segurança. Assim, conclui-se que o Engenheiro de Produção ao adentrar essa área, teria uma melhor gestão de riscos e consequentemente melhoraria o desempenho de áreas adjacentes, devido ao conhecimento global do sistema no qual está envolvido.

As ameaças empresariais funcionam como oportunidades para profissionais que enxergam além do que lhe é proposto, ser multidisciplinar é o maior diferencial.

## REFERÊNCIAS

ABNT NBR ISO/IEC 17799:2005, **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.**

**Constituição da República Federativa do Brasil.** Brasília, edição 2016.

DE CARVALHO, DENIS ROCHA. **Segurança da informação: estudo de caso da aplicação da Norma NBR ISO/IEC 17799.** 2003.

JUNGMANN, Diana de Mello; BONETTI, Esther Aquemi. **Inovação e propriedade intelectual: guia para o docente.** Brasília: Senai, 2010.

Nº, L. E. I. 9.610, DE 19 DE FEVEREIRO DE 1998. **Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.**

Nº, L. E. I. 9.279, DE 14 DE MAIO DE 1996. **Regula direitos e obrigações relativos à propriedade industrial.**

Nº, L. E. I. 13.709, DE 14 DE AGOSTO DE 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.**

REIS, Rogério; **O alto custo causado pela falta de investimento em segurança da informação.** Revista Security. Brasil, 2017.

Site do Instituto Nacional de Propriedade Intelectual (INPI) - **A Propriedade intelectual e o comércio exterior- Conhecendo oportunidades para seu negócio.** Disponível em: < <http://www.inpi.gov.br/> > Acesso em 25 de outubro de 2018.