LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

O DESAFIO DA SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA INDÚSTRIA 4.0

SANDRA CRISTINA FERREIRA ROMA

OUTUBRO-2018

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

O DESAFIO DA SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA INDÚSTRIA 4.0

SANDRA CRISTINA FERREIRA ROMA

ORIENTAÇÃO:

MESTRE EDUARDO RODRIGUES

OUTUBRO-2018

Dedicatória

Às minhas filhas Filipa e Sofia. Deixei de poder disfrutar de momentos importantes com elas e de lhes dar a atenção que meninas de 12 e 7 anos exigem, principalmente quando são cheias de energia.

Não vou esquecer os momentos em que estava a trabalhar no escritório da minha casa e elas a interromperem-me constantemente, com a esperança que eu abandonasse o computador e lhes desse a devida atenção. E sim, claro que o conseguiram muitas vezes, o que originou um duplo desafio na realização deste trabalho.

Agradecimentos

Não posso deixar de agradecer aos amigos que tornaram possível a realização das entrevistas, pois sem elas, este trabalho não seria concluído.

Agradeço também toda a confiança que os entrevistados depositaram em mim, partilhando comigo parte do seu conhecimento e de informações tão particulares de cada uma das empresas.

Lista de Acrónimos

APCER-Associação Portuguesa de Certificação

B-on-Biblioteca do conhecimento on-line

EDI- Intercâmbio electrónico de dados (*Electronic Data Interchange*)

EIC- Empresa Internacional de Certificação, S.A.

ERP-Sistema integrado de gestão empresarial (*Enterprise Resource Planning*)

I4.0-Indústria 4.0

ID&T- Investigação e Desenvolvimento tecnológico

IEC-The International Electrotechnical Commission

IIoT-Industrial Internet of things

INE-Instituto Nacional de Estatística

IoT-Internet of Things

IPAC-Instituto Português de Acreditação

ISO-The International Organization for Standardization

PME-Pequenas e Médias Empresas

RFID-Identificação por radiofrequência (*Radio Frequency Identification)*

RGPD-Regulamento Geral sobre a Proteção de Dados

SGS ICS- Serviços Internacionais de Certificação, Lda.

SI I&DT- Sistema de Incentivos à Investigação e Desenvolvimento Tecnológico

TI-Tecnologias de Informação

Resumo e palavras-chave

É uma realidade a necessidade de mudança na indústria, para permitir a competitividade.

É uma realidade também, que o que justificou o aparecimento do conceito Indústria 4.0 é o que as empresas sentem: encomendas de menores lotes do mesmo produto, mais customização de produtos, *time to market* reduzido, preços mais competitivos.

Temos assistido a várias iniciativas governamentais em Portugal para fomentar a Indústria 4.0 na realidade empresarial. Muitas são as empresas que têm aderido, através de iniciativas de pacotes lançados no programa Portugal 2020.

Mas coloca-se a seguinte questão: até que ponto essas iniciativas, principalmente quando fomentadas pelas entidades governamentais, deveriam acautelar a proteção da informação das empresas, incentivando a implementação das boas práticas de segurança da informação, acima de tudo?

Recorrendo a entrevistas a especialistas em sistemas de informação e em implementação dos conceitos da I4.0 de algumas empresas portuguesas do sector industrial, foi possível evidenciar a existência de fundamento na questão colocada.

Sendo o conceito "segurança da informação" muito abrangente, limitou-se o desenvolvimento deste trabalho, à preocupação com a segurança da informação estratégica, de conceção e desenvolvimento do produto, de processos de produção (quer a nível de produto, quer a nível de processo) e de modelos de gestão.

Este trabalho foi importante para as empresas entrevistadas, na medida que as sensibilizou para a existência de uma norma, nomeadamente a ISO/IEC 27001, que as poderá auxiliar na gestão da segurança da informação.

Contribui ainda, para evidenciar a necessidade do reforço por parte das entidades governamentais, de medidas de implementação de boas práticas no âmbito da gestão da segurança da informação, no contexto de projectos financiados relacionados com a I4.0, lançando ainda a sugestão de aplicação como requisito fundamental, para a aprovação ou encerramento de projectos, a certificação na norma ISO/IEC 27001.

Palavras-chave: Indústria 4.0; segurança da informação; ISO/IEC 27001; incentivos governamentais.

Abstract and keywords

It is a reality the need for change in the industry, to enable competitiveness.

It is also a reality that what justified the appearance of the Industry 4.0 concept is what companies feel: orders for smaller batches of the same product, more customization of products, reduced time to market, more competitive prices.

We have attended various governmental initiatives in Portugal to foster Industry 4.0 in business reality. There are many companies that have joined, through package initiatives launched in the Portugal 2020 program.

But the question emerges: to what extent should such initiatives, especially when encouraged by government agencies, be concerned with protection of corporate information by encouraging the implementation of good information security practices above all else?

Using interviews with specialists in information systems and in the implementation of the concepts of I4.0 of some Portuguese industrial sector companies, it was possible to evidence the existence of a foundation in the question posed.

Since the concept of "information security" is very broad, the development of this work was limited to the concern with security of strategic information, product design and development, production processes (product and process level) and management models.

This work was important for the companies interviewed, as it made them aware of the existence of a standard, namely ISO / IEC 27001, which could help them in the management of information security.

It also contributes to highlight the need for government bodies to reinforce measures to implement good practices in the area of information security management in the context of funded projects related with I4.0. It also proposes the application of ISO / IEC 27001 as a fundamental requirement for the approval or closure of projects.

Keywords: Industry 4.0; information security; ISO/IEC 27001; governmental initiatives.

Índice

Índice de figuras

1 Introdução

1.1 Motivação para o tema selecionado

A experiência prática do que é numa indústria tradicional, utilizar os incentivos governamentais para tentar implementar novas tecnologias e em simultâneo, manter a vantagem competitiva dessas mesmas implementações, gerou a motivação necessária para selecionar um tema que relaciona a Indústria 4.0 com a segurança da informação.

É uma realidade que, o que justificou o aparecimento do conceito Indústria 4.0 é o que as empresas sentem: encomendas de menores lotes do mesmo produto, mais customização de produtos, necessidade de menor lead time entre a encomenda e a entrega, preços mais competitivos (Rennung et al, 2016; Gabriel et al, 2016). Há efectivamente necessidade de mudança no sector industrial, para permitir a competitividade (Rennung et al, 2016).

Hoje em dia, estamos cada vez mais interligados entre sistemas, internet, equipamentos e pessoas (Pereira et al, 2017) e quanto maior for o caminho percorrido delineado com a Indústria 4.0, mais as empresas ficarão expostas às sensibilidades dos sistemas de informação (Pereira et al, 2017).

Nesse sentido, surge a necessidade de entender a relação entre a Indústria 4.0 e a segurança da informação e o que podem as empresas fazer, para poderem percorrer o caminho necessário mas sem serem surpreendidas pelas questões críticas da segurança da informação, colocando em risco a obtenção do grande objetivo da Indústria 4.0.

1.2 Objetivo de investigação

O conceito da Indústria 4.0, centrado na utilização da internet, disponibiliza ferramentas que optimizam custos, recorrendo à partilha de ferramentas entre *stakeholders*, incluindo a partilha da informação, utilizando por exemplo, a tecnologia da cloud (Oesterreich et al, 2016; Trappey et al, 2017).

Como gestor e nomeadamente como *controller* de gestão, tendo a noção do todo de uma empresa, sabe o quanto importante é a partilha de informação entre os

stakeholders, mas tem também a noção, das consequências de partilha da informação entre os interlocutores errados ou até mesmo a partilha de informação não autorizada. A informação da empresa é um bem valioso e que muitas vezes, constitui o vector diferenciador.

Considerando o que caracteriza a Indústria 4.0, num gestor, surgem muitas perguntas e dúvidas quando pensamos neste bem precioso das empresas, a informação, o conhecimento da empresa, o *Know-How*, o seu ADN. (Pereira et al, 2017).

A Indústria 4.0 é caracterizada pela presença de redes, internet, integrando vários sistemas de TI a diferentes níveis hierárquicos, expondo ainda mais a informação das empresas, em termos de segurança (Waidner et al, 2016).

São apontados 4 pontos críticos na indústria 4.0: redes, capacidades, cultura e segurança (Jennings, 2015).

FIGURA 1 OS 4 PONTOS CRÍTICOS DA INDÚSTRIA 4.0

Figura própria

Considerando as preocupações referidas anteriormente e sendo que a segurança está relacionada com os restantes pontos críticos, este trabalho tem os seguintes objetivos:

- Evidenciar o factor crítico “Segurança da Informação” na implementação da Indústria 4.0;
- Demonstrar como se encontra desenvolvida a problemática “Segurança da Informação na implementação da indústria 4.0” em Portugal;
- Fornecer alguns conselhos a considerar na implementação da Industria 4.0, referente à segurança da Informação.

Pretende-se com este trabalho, trazer à discussão a questão de, se antes de se fomentar a disseminação dos conceitos da indústria 4.0 e sabendo o que isso implica, não se deveria primeiro fomentar as boas práticas de gestão da segurança da informação, incentivando as empresas, antes de mais, a preocuparem-se em obter a certificação da norma ISO/IEC 27001. E, se só depois de se garantir essa certificação, é que as empresas deveriam percorrer o caminho da indústria 4.0. Não sendo a certificação na norma ISO/IEC 27001 um requisito exigido pelas entidades governamentais, quando as empresas se candidatam a fundos comunitários de apoio à disseminação dos conceitos da Indústria 4.0, através de projectos enquadrados no SI I&DT, (PORTUGAL2020, 2018), não poderão estar a contribuir para o agravamento dos problemas relacionados com a segurança da informação?

Considerando que em 2016, 98% da realidade empresarial portuguesa era constituída por PME de empresas não financeiras (INE, 2018), estarão elas preparadas para mitigar os riscos quanto à gestão da segurança da informação? Se há data de 31/12/2017, existiam cerca de 5.837 empresas certificadas com a ISO 9001, com a certificação ISO/IEC 27001, existiam cerca de 46, um número efectivamente muito baixo, agravado ainda pelo facto de serem na sua maioria, empresas de tecnologias de informação e não empresas do sector industrial. (IPAC, 2018).

Hoje em dia está em voga toda a problemática dos ataques informáticos, abrangendo quer as empresas a nível internacional, quer em Portugal, sejam grandes empresas, sejam simplesmente PME’s (Rodrigues et al 2017; Yilmaz et al, 2016).

É um assunto em presença constante, tanto ao nível da comunicação social, quanto ao nível de publicações científicas ou não científicas. No entanto, as razões que despoletaram o interesse pela investigação destes temas, estão mais focadas ao nível de gestão. Não relativizando a importância dos trabalhos direccionados mais ao nível dos ataques de *hackers*, que colocam em causa não só a integridade da informação, como também poderá colocar em causa a integridade das pessoas, dentro e fora das empresas (Waidner et al, 2016), este trabalho tem como objetivo focar a problemática da segurança da informação estratégica, de concepção e desenvolvimento de produto, de processos de produção (como se faz, quer a nível de produto, quer a nível de processo) e de modelos de gestão. Não se irá focar na problemática da segurança da informação,

que coloca em causa a privacidade dos dados de cada um de nós, nem na problemática da segurança da informação que poderá pôr em causa o bom funcionamento dos equipamentos, nem na disponibilidade das bases de dados.

1.2.1 Questões de investigação

Com o intuito de se conseguir atingir os objectivos propostos, foram formuladas 2 questões de investigação, para as quais se pretende obter resposta no final deste trabalho:

- As empresas que estão a implementar conceitos no âmbito da Indústria 4.0, estão certificadas com a norma ISO/IEC 27001 ou têm implementadas as boas práticas contidas na norma?
- A implementação de conceitos da Indústria 4.0, fomentou o aumento de ocorrências de problemas relacionados com a segurança da informação no que se refere à informação estratégica, de concepção e desenvolvimento de produto, de processos de produção, de modelos de gestão?

1.3 Relevância da investigação

Embora o tema "Segurança da informação" seja abordado há muito (Yilmaz et al, 2016; Baskerville et al, 2014), no contexto "Indústria 4.0" é ainda recente, já que o próprio conceito e os principais termos com ela relacionada, também o são (Schumacher et al, 2016; Pereira et al, 2017). A maioria dos artigos que se encontram na B-on sobre a Indústria 4.0, são dos últimos 3 anos. Até 2015 surgem cerca de 2.650 artigos que referem "*Industry 4.0*". Se acrescentarmos mais um ano, são apresentados cerca de 6.400 artigos. Considerando adicionalmente o ano 2017, o número sobe para 13.000 e até 02/10/2018, já são cerca de 21.000, dos quais, aproximadamente 7.500 são em revistas académicas.

Quanto à Segurança da informação, quando pesquisado o termo em inglês "*Information security"*, registam-se cerca de 267.000 resultados a 02/10/2018, mas quando se cruza com o termo "*Industry 4.0*", só surgem cerca de 800 registos à mesma data, o que evidencia que o nível de discussão dos 2 termos em conjunto, está bem longe da grandeza de qualquer um deles em separado.

Considerando os argumentos descritos anteriormente, verifica-se que o tema investigado é um tema actual, ainda em desenvolvimento e por isso, com muito potencial de investigação.

Este trabalho fornece um contributo para esse desenvolvimento ainda necessário, na medida que faz uma compilação do conhecimento na área específica de segurança da informação no contexto da indústria 4.0, apresentando o estado da arte e relacionando com a actual realidade nas empresas portuguesas, servindo como suporte para futuras investigações do tema.

Sendo a segurança da informação apresentada como um dos factores críticos da indústria 4.0 (Tuptuk et al, 2018), este trabalho é relevante na medida que apresenta testemunhos de como se pode mitigar problemas que possam surgir no percurso da sua implementação.

Alerta ainda as entidades governamentais para a necessidade de fomentar a implementação da norma ISO/IEC 27001, tornando-a como requisito obrigatório na candidatura a fundos comunitários em iniciativas fomentadoras do conceito Indústria 4.0.

2 Revisão da Literatura

A revisão da literatura tem como objetivo situar as questões apresentadas neste trabalho de investigação, realizando-se a revisão à informação existente sobre os assuntos abordados.

Foi a primeira abordagem à revisão da literatura sobre a I4.0 que gerou o interesse pelo desenvolvimento do trabalho aqui apresentado.

Para realizar este trabalho, foram utilizadas algumas das orientações descritas no livro de Correia e Mesquita (2013), tendo sido feita uma base de dados em Excel com a referenciação dos artigos que foram lidos, efectuando-se um resumo e uma classificação dos mesmos, para auxiliar ao longo da investigação.

Foram recolhidas várias palavras-chave, provenientes das leituras efectuadas a vários artigos, combinando-se algumas delas para a obtenção de documentação mais

específica do tema apresentado, utilizando ferramentas de pesquisa como a B-on e a Schoolar Google.

4TH INDUSTRIAL REVOLUTION
ADVANCED MANUFACTURING
BIG DATA
CLOUD COMPUTING
CONNECTED INDUSTRY
CYBER PHYSICAL SYSTEMS (CPS)
DIE VIERTE INDUSTRIELLE REVOLUTION
EMBEDDED SYSTEMS (ES)
INDUSTRIAL INTERNET
INDUSTRIAL INTERNET OF THINGS (IIoT)
INDUSTRIE 4.0
INDUSTRY 4.0
INFORMATION SECURITY
INFORMATION SECURITY MANAGEMENT (ISM)
INTEGRATED INDUSTRY
INTERNET OF SERVICES
INTERNET OF THINGS(IoT)
SMART FACTORY
PME EM PORTUGAL
GRAU DE IMPLEMENTAÇÃO DA FAMILIA ISO 27000
INFORMATION SECURITY AND PERSONS

FIGURA 2 LISTA DAS PALAVRAS-CHAVE UTILIZADAS NAS PESQUISAS

Figura própria

2.1 A Indústria 4.0

As mudanças sociais, económicas e tecnológicas são a causa de todas as revoluções industriais (Nikolic et al, 2017).

O rápido crescimento das tecnologias interligadas com eletrónica e a IoT, aplicadas ao mundo do sector industrial, fizeram alterar o paradigma, despoletando o surgimento da denominada 4ª revolução industrial (Nikolic et al, 2017; Hao et al, 2017).

A Indústria 4.0 apresenta-se como a 4ª revolução industrial, sendo a evolução das 3 anteriores revoluções. (Stojkić et al, 2016; Kagermann et al, 2013; Shaabany et al, 2016).

A 1ª revolução industrial, ocorreu no final do século XVIII, caracterizando-se pela introdução do equipamento mecânico na produção, sendo exemplo disso, o tear mecânico para a fabricação de produtos. No final do século XIX, surge a 2ª revolução industrial, caracterizando-se pela introdução da maquinaria eléctrica para a produção em

massa baseada na divisão do trabalho. Já no século XX, no início dos anos 70, surge a 3ª revolução industrial, caracterizando-se pela utilização da electrónica e das tecnologias de informação, automatizando os processos produtivos (Kagermann et al, 2013; Gabriel et al, 2016).

A Indústria 4.0 é a visão do que será a indústria no futuro (Hermann et al, 2016). Esta surge com a necessidade da modernização da indústria, para possibilitar a revitalização da mesma em alguns países (Neugebauer et al 2016; Gabriel et al, 2016). É na Alemanha, em 2011, que surge pela primeira vez o conceito, apresentado pelo governo alemão, com o objetivo do reforço da vantagem competitiva das empresas (Kagermann et al, 2013; Oesterreich et al, 2016; Zhou et al, 2015).

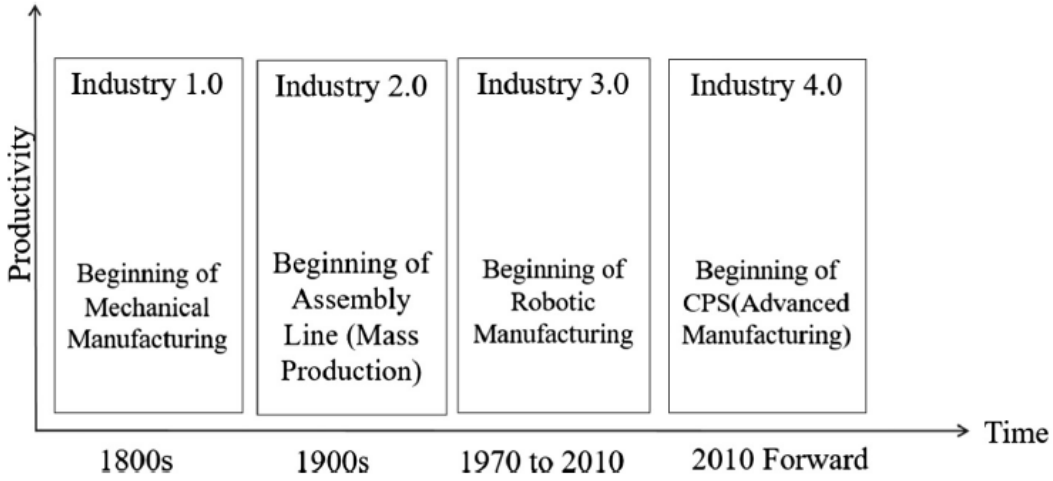


FIGURA 3- 4 REVOLUÇÕES INDUSTRIAIS
(Trappey et al, 2017)

As empresas precisam de soluções que as permitam responder em pouco tempo, com eficiência, num mercado em constante mutação, com população envelhecida e onde sofrem com a concorrência dos países em desenvolvimento (Nelles et al, 2016; Qin et al, 2016; Hofmann et al, 2017) e é nesse contexto que a I4.0 é apresentada.

O principal objetivo da Indústria 4.0 passa por fortalecer e expandir a competitividade a longo termo das empresas, aumentando a flexibilidade e eficiência da produção através da comunicação, informação e inteligência (Gabriel et al, 2016; Hermann et al, 2016; Shaabany et al, 2016; Slusarczyk, 2018).

FIGURA 4 OBJETIVO DA COMPETITIVIDADE

Figura próprio

A Indústria 4.0 caracteriza-se pela aplicação da tecnologia da internet na indústria, através de:

- **Internet of things (IoT)** - sistema global de redes de computadores ligados por IP, sensores, atuadores, máquinas e dispositivos;
- **Internet of services (IoS)** - serviços através da utilização da internet;
- **Embedded Systems (ES) -Microcomputadores-**monitorizam e controlam os processos físicos, com feedback em ciclos onde os processos físicos afectam os processos computacionais e vice-versa;
- **Cyber Physical Systems (CPS)** -convergência do mundo físico com o mundo virtual, integrações de processos computacionais e físicos. Representam o próximo patamar dos sistemas integrados e constroem a base para uma internet das coisas, que combina com a internet dos serviços para possibilitar a Indústria 4.0 (Gabriel et al, 2016; Hermann et al, 2016; Nelles et al, 2016; Stock et al, 2016; Qin et al, 2016; Slusarczyk, 2018; Hofmann et al, 2017).

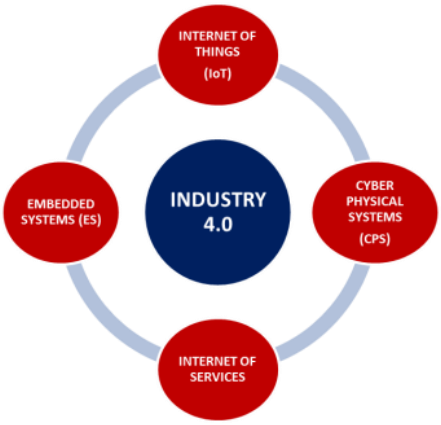


FIGURA 5 A APLICAÇÃO DA INTERNET

Figura próprio

Encontramos a Indústria 4.0 referida de forma diferente em termos mundiais, o que terá a ver com os conceitos incorporados em cada uma das regiões. Enquanto na Europa é conhecida como Indústria 4.0, do outro lado do Atlântico designa-se "*Industrial Internet*" ou "*Integrated industry*" (Gabriel et al, 2016) e na Ásia é mencionada como "*Industrial internet of things*" (IIoT), "*Intelligent Manufacturing*" ou "*Digital Industry 4.0*" (Waidner et al, 2016; Slusarczyk, 2018; Oesterreich et al, 2016). Isto ocorrerá por não haver ainda um entendimento claro do termo a utilizar (Hermann et al, 2016).

Sendo uma visão do que será a indústria do futuro, algumas empresas já estão a fazer o caminho de uma forma consciente e outras sem o saber, ao aplicar parte dos conceitos que a caracterizam. Ainda existe uma distância considerável entre a indústria actual e o que a I4.0 representa, embora exista uma convergência nas medidas tomadas pelas empresas. No entanto, ainda há muito a desenvolver. (Gabriel et al, 2016; Qin et al 2016; Yue et al, 2015).

Baseando-se na tecnologia, na digital, no imaterial, na interligação de dados, a Indústria 4.0 centra-se na fábrica inteligente, permitindo a comunicação direta entre pessoas, máquinas, sistemas de transporte e armazenamento e instalações produtivas.

Baseia-se em produtos, processos e procedimentos inteligentes e na produção descentralizada, gerando maior transparência em todo o processo do sector industrial (Gabriel et al, 2016) permitindo ganhos na eficiência, produtividade e qualidade (Preuveneers et al, 2016; Shaabany et al, 2016; Stock et al, 2016; Qin et al, 2016; Yue et al, 2015; Nikolic et al, 2017; Heikkila et al, 2016).

Toda esta tecnologia em que a I4.0 se baseia, torna-se o *driver* para a inovação da indústria (Sadeghi et al, 2015).

Mas sem a alta qualidade de padrões e dados de transacção, processos claros baseados em TI e habilidade para a complexa análise de dados, a Indústria 4.0 não é possível (Gabriel et al, 2016), sendo crítico para a implementação da indústria 4.0, as redes, as capacidades, a cultura e a segurança (Jennings, 2015).

Tem sido referido em várias publicações, os factores críticos da I4.0, apresentando -se algumas das soluções para os mitigar (Sommer, 2015; Zhou et al, 2015; Mckinsey Digital, 2016; Cheminod et al, 2013).

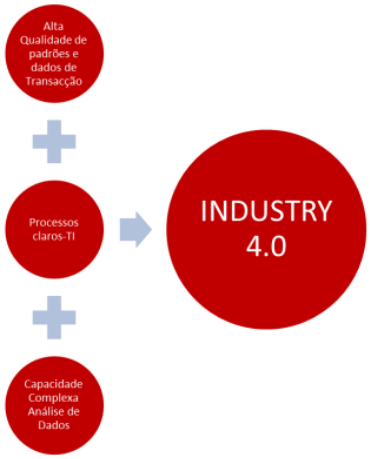


FIGURA 6 ITENS NECESSÁRIOS NA INDÚSTRIA 4.0

Figura próprio

No ambiente do sector industrial, a segurança abrange pessoas, meio ambiente, infraestruturas, máquinas, equipamentos e informação (Tuptuk et al, 2018).

A indústria tem sido alvo de sabotagem e com a integração a todos os níveis, com a utilização da internet, as indústrias ficam ainda mais expostas (Tuptuk et al, 2018; Cheminod et al, 2013).

É fundamental acautelar os requisitos de segurança em todo o ciclo dos sistemas de produção e dos produtos. A segurança terá que ser acautelada na integração horizontal, vertical e na cadeia de valor. Os requisitos de segurança devem considerar a tecnologia, verificando-se se as empresas estão a aplicar a tecnologia mais moderna existente e se essa, é adaptável aos requisitos específicos da realidade do sector industrial, onde a

disponibilidade e a fiabilidade se torna imperativo e onde existem sistemas antigos em pleno funcionamento, aumentando as vulnerabilidades quando é aumentada a conectividade (Waidner et al, 2016; Sadeghi et al, 2015).

Na indústria, a protecção do *design*, da configuração de dados e da informação de clientes, torna-se fundamental (Waidner et al, 2016). Deve-se ainda abordar a questão da segurança ao nível do comportamento humano, pois por vezes é a esse nível que surgem os factores críticos de segurança da informação (Ilie-Zudor et al, 2016; Heikkila et al, 2016).

2.2 A segurança da informação no contexto da indústria 4.0

Mesmo antes do aparecimento do conceito da Indústria 4.0, a problemática da segurança da informação já existia (Yilmaz et al, 2016; Kamal et al, 2018). A disseminação de computadores portáteis, telemóveis, *tablets*, ligação de internet aos computadores fixos, ligação de uns dispositivos aos outros, a mobilidade cada vez maior de colaboradores, em que a presença física deixou de ser uma necessidade para execução de muitas tarefas, a partilha de informação no conceito *cloud*, veio facilitar a vida das pessoas e das empresas (Zhang et al, 2015). No entanto, aumentou também a preocupação ao nível da segurança da informação (Kuyoro et al, 2011).

Os ataques informáticos e perda de dados é um problema que tem crescido de uma forma preocupante. A segurança passou a ser uma grande preocupação e o interesse por ela, tem crescido por todo o lado (Yue et al, 2015; Jansen et al, 2018; Kamal et al, 2018; Heikkila et al, 2016).

Embora as pessoas hoje em dia acedam a informação com muito mais facilidade, aumentou a exposição a ameaças. (Yilmaz et al, 2016; Baskerville et al, 2014; Tuptuk et al, 2018; Cheminod et al, 2013).

A segurança da informação é a sombra da informação e onde há informação, haverá questões com a segurança da informação (Zhang et al, 2015).

O que significa que, a segurança dos sistemas de informação tornou-se crítico num mundo em que a computação é mundial e os sistemas de informação estão interligados a nível global (Baskerville et al, 2014; Yue et al, 2015).

Tem sido recorrente notícias sobre ataques informáticos, o que tem gerado muitas preocupações nas empresas. Se por um lado é preciso garantir a segurança dos sistemas de informação, por outro lado é reconhecido que o caminho para a modernização passa pela implementação de toda a tecnologia que expõe a segurança da informação, o que significa que o caminho estará em garantir a segurança e não em deixar de aplicar toda a tecnologia existente (Zhang et al, 2015; Heikkila et al, 2016).

Com o controlo de acessos, dentro e fora da organização, pretende-se assegurar que a informação não salte as fronteiras delimitadas na empresa (Hummer et al, 2016). Mas se hoje podemos limitar mais os acessos (não significando isso que estejam totalmente protegidos), se uma das características da indústria 4.0 é a integração vertical, horizontal e a partilha da informação, ficaremos todos mais expostos, tornando-se mais crucial o correto controlo de fluxos de informação. (Tuptuk et al, 2018; Priller et al, 2014). Com toda a informação gerada num contexto de total partilha, é inevitável que surjam novos desafios ao nível da segurança da informação (Preuveneers et al, 2016). Os desafios num ambiente em que a internet tem uma aplicação alargada, exigem abordagens diferentes dos ambientes tradicionais, sendo necessário o estudo de novas abordagens (Zhang et al, 2015).

Está-se a assistir ao que efectivamente se pretendia com a indústria 4.0, está a surgir ganhos de produtividade, flexibilidade e qualidade e está-se a expandir de uma forma rápida mas, o maior risco no meio disto tudo é que a segurança está a ser considerada uma segunda preocupação em vez de ser o centro de todo o processo de desenvolvimento (Tuptuk et al, 2018).

2.3 A ISO/IEC 27001

Com a necessidade das empresas e nações protegerem a sua informação, foram desenvolvidos padrões de segurança que acabaram por se tornarem padrões a nível mundial. As empresas na sua generalidade, com o objetivo de proteger a sua informação, acabam por adoptar esses padrões e certificações. (Yilmaz et al, 2016).

Como resultado desses padrões a nível mundial, ficam disponíveis diversas abordagens de gestão, para ajudar a orientar as empresas na formulação e

operacionalidade de esforços, no âmbito da segurança da informação. Essas abordagens têm um objetivo universal e têm raízes nos princípios do controlo da qualidade.

É dentro desse processo que aparecem normas como a ISO/IEC 27001 (Baskerville et al, 2014).

A ISO/IEC 27001 é uma das 8 *standards* pertencentes à família das ISO 27000, cuja origem remonta aos anos 80, tendo sofrido várias evoluções para se adaptar às evoluções tecnológicas e ao acumular do conhecimento ao longo dos anos (ISO27001, 2017).

A série das ISO/IEC 27000 consiste em *standards* de segurança da informação publicados pela *International Standards Organization* (ISO) e pela *International Electrotechnical Commission* (IEC) com o objetivo de apresentar as melhores práticas de gestão da segurança da informação, incluindo riscos e controlos no contexto de um sistema de gestão de segurança da informação, de uma forma equivalente aos sistemas de gestão de garantia da qualidade (ISO 9000) e de protecção ambiental (ISO 14000) (British, 2017).

A ISO/IEC 27001 deriva da BS 7799 parte 2, publicada pela primeira vez em 1999.

A BS 7799 parte 2 foi revista em 2002 e é em 2005 que recebe a actual designação.

Em 2013 teve uma revisão profunda, para ficar em linha com outras ISO (ISO27001, 2017).

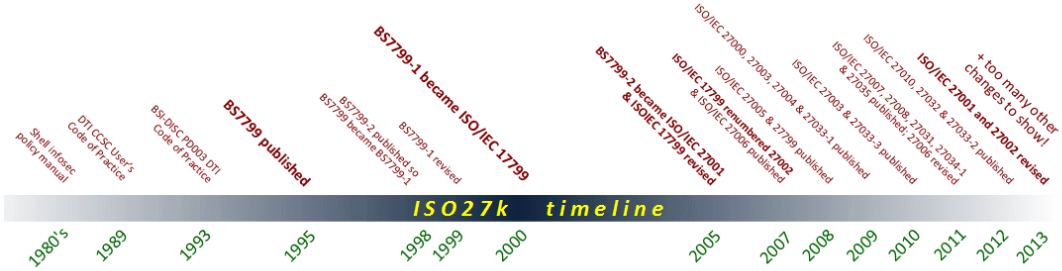


FIGURA 7 LINHA DO TEMPO DA NORMA
(ISO 27001, 2017)

A actualização visou ainda colocar a norma em linha com a realidade ao nível da segurança da informação no que se refere ao crime cibernético, conceito *cloud* e à

utilização dos *smartphones*, passando a ser reconhecida como o padrão das melhores práticas para demonstrar capacidades ao nível da segurança da informação (British, 2017).

Em 2017 surgiu uma versão europeia, denominada ISO/IEC 27001:2017, resultado de umas pequenas correcções efectuadas à versão de 2013 (British, 2017).

A norma ISO/IEC 27001 tem como âmbito, especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente, um sistema de gestão da segurança da informação no contexto de uma organização, incluindo os requisitos para levar a cabo a avaliação e tratamento do risco na segurança da informação, adaptado às necessidades da organização (ISO/IEC 27001, 2013).

Na norma, são abordados temas como o contexto da organização, os interesses dos *stakeholders*, a liderança e o comprometimento perante a segurança da informação, a politica de segurança da informação, a definição de responsabilidades, a avaliação do risco, critérios de aceitação do risco, a documentação, os objectivos e planeamento da segurança da informação, o suporte (recursos, competências, consciência e comunicação), o planeamento operacional e controle, a avaliação, as auditorias internas, a revisão da política, as não conformidades, as acções correctivas e a melhoria contínua (ISO/IEC 27001, 2013).

Resumindo, define as melhores práticas, para se gerir a segurança da informação, referindo as principais questões a considerar por todas as empresas que lidam e dependem de informação (Heikkila et al, 2016).

Embora em Portugal existam várias entidades que implementam a ISO/IEC 27001 e entidades acreditadas como a APCER, SGS IC e EIC, (IPAC1, 2018), de acordo com a base de dados do IPAC sobre entidades certificadas, esta norma ainda não tem a mesma representatividade que a ISO 9001, a norma de gestão da garantia da qualidade, nas empresas portuguesas (IPAC, 2018).

Nº Certificados	Sist.Gestão	2015	2016	2017
ISO 9001	Qualidade	5538	5589	5837
ISO 14001	Ambiente	1107	1123	1174
SST (18001&4397)	SST	568	561	734
ISO 22000	S.Alimentar	299	295	298
ISO 50001	Energia	0	0	27
ISO/IEC 27001	T.Informação	20	35	46
ISO/IEC 20000-1	S.Informação	0	0	10
NP 4457	ID&Inovação	179	170	164
NP 4406	Florestal	11	12	14
NP 4512	Formação Prof	2	1	1
TOTAL		7724	7786	8305

FIGURA 8 EMPRESAS POR TIPO DE CERTIFICAÇÃO

(IPAC, 2018)

Os registos encontrados na B-on relacionados com a ISO 9001 e com a ISO/IEC 27001, estão em sintonia com os números publicados referentes às certificações nas respectivas normas. Foram encontrados cerca de 6.000 registos até 02/10/2018 sobre a ISO/IEC 27001, enquanto sobre a ISO 9001, são encontrados cerca de 87.000 registos, o que demonstra bem a diferença do nível de discussão de cada uma das duas normas.

2.4 Os incentivos governamentais para a indústria 4.0

De acordo com as estatísticas do INE, as PME em Portugal, em 2016, representam 98% da tipologia de empresas (INE, 2018).

Tendo em conta o número de PME's existentes em Portugal e não sabendo ao certo o esforço financeiro que terão de fazer para seguirem o caminho da indústria 4.0 (Schumacher et al, 2016), as entidades governamentais, com o intuito de acelerar todo o processo relacionado com a indústria 4.0, e cientes, como em outros países, de que as PME's precisam de mais apoio para conseguirem acompanhar os desenvolvimentos já realizados por grandes empresas (Sommer, 2015), geraram diversos incentivos neste âmbito, tendo como alvo as PME's, embora os incentivos sejam também possíveis de utilizar por grandes empresas.

Neste contexto, temos assistido a várias iniciativas governamentais em Portugal para fomentar a Indústria 4.0 na realidade empresarial (IAPMEI, 2018). Muitas são as empresas que têm aderido, através de iniciativas de pacotes lançados no programa Portugal 2020 (PORTUGAL2020a, 2018).

2.5 A ISO/IEC 27001, a indústria 4.0 e os incentivos governamentais

Considerando que os incentivos governamentais têm como objetivo acelerar todo o processo relacionado com a indústria 4.0 e que são mais pensados como apoio às PME's, porque essas normalmente têm mais dificuldade em ter os recursos necessários para desenvolver a Indústria 4.0 (Sommer, 2015), então, e focando sempre no objetivo deste trabalho, até que ponto essas iniciativas, principalmente quando fomentadas pelas entidades governamentais, não deveriam acautelar também a protecção da informação das empresas, incentivando a implementação das boas práticas de segurança da informação acima de tudo, pois se as empresas não têm normalmente os recursos necessários para garantir o desenvolvimento da Indústria 4.0, não está garantido também que tenham a consciência do impacto desses mesmos desenvolvimentos no que se refere à segurança da informação.

Conhecendo alguns dos requisitos das medidas, quer na vertente da competitividade, quer na de investigação e desenvolvimento, não se identifica directamente nada que defina como requisito para a aprovação dos projectos, as boas práticas que as empresas utilizam referente à protecção dos sistemas de informação e da informação crítica das empresas. Existem algumas medidas de apoio que podem incluir consultoria na preparação da empresa para a certificação na gestão da segurança da informação mas nada é avaliado em relação a esse tema como por exemplo, em medidas relacionadas com investigação e desenvolvimento, âmbito onde normalmente se encaixam soluções relacionadas com a indústria 4.0. Não se encontra nada mencionado referente à obrigatoriedade de ter em consideração procedimentos de segurança da informação na implementação ou desenvolvimento dos projectos no âmbito do ID&T (Portugal2020b, 2018; Portugal2020c, 2018).

Mas, relembrando os conceitos que estão na base da Indústria 4.0, não será importante acautelar possíveis problemas num ambiente tão aberto quanto aquele que é apresentado? Não seria importante garantir a mitigação de riscos inerentes aos sistemas de informação num ambiente de aplicabilidade da indústria 4.0?

Até porque a segurança não é um produto que se compra e sim um processo que deve acompanhar qualquer inovação existente numa fábrica (Tuptuk et al, 2018), é algo que deve estar em processo contínuo de melhoria (Heikkila et al, 2016).

Não considerando o risco da segurança da informação, podemos estar a desenvolver algo funcional, que até responde aos objectivos que fundamentaram a Indústria 4.0 mas que está totalmente vulnerável a ataques, podendo não só não permitir atingir o que motivou o projecto mas ainda, pôr em risco informação que a empresa já detinha (Tuptuk et al, 2018).

Talvez seja interessante apercebermo-nos se as empresas que estão a trabalhar na implementação de conceitos relacionados com a Indústria 4.0, estão certificadas ou se têm como boas práticas os conceitos da ISO/IEC 27001. Sabemos que com a aplicação da ISO/IEC 27001 não se protege na sua totalidade os sistemas de informação mas mitiga bastante (ISO27001, 2017). Se estivermos a implementar conceitos da Indústria 4.0, que certamente vão influenciar as empresas na utilização de mais tecnologia, baseada na internet e muitas vezes na tecnologia *cloud*, partilha de informação entre *stakeholders*, sem termos por base numa empresa, determinados conceitos referentes à protecção dos sistemas de informação, poderemos estar a potenciar os riscos dos sistemas de informação e a transformar as vantagens competitivas que são apregoadas com o conceito Indústria 4.0, em desvantagens.

3 Metodologia

3.1 Enquadramento

Como enquadramento do tema investigado, iniciou-se o trabalho com a realização de um resumo da arte do conhecimento existente sobre os conceitos apresentados.

Utilizando como ferramentas de pesquisa a B-on e a Schoolar Google, em paralelo com as orientações assimiladas no livro de Correia e Mesquita (2013), fez-se uma viagem pela informação disponível relacionado com os diversos conceitos referidos neste trabalho. Depois de um melhor entendimento no que consiste a Indústria 4.0,

quais os benefícios, quais os principais pontos críticos apontados e considerando o que motivou a selecção do tema, foi feita uma abordagem à segurança da informação.

Conhecendo-se a existência de uma norma que releva a questão da gestão da segurança da informação, averiguou-se sobre a sua aplicação em Portugal. Verificando-se a diminuta existência de empresas certificadas na norma ISO/IEC 27001, a norma relacionada com a gestão da segurança da informação, comparando por exemplo com a norma 9001, relacionada com a gestão da qualidade (IPAC, 2018), mas sabendo que existem expectativas de grande participação das empresas em iniciativas governamentais relacionadas com a promoção dos conceitos da Indústria 4.0 (Portugal.gov, 2018), gerou alguma preocupação ao nível da gestão da segurança da informação.

Depois de uma abordagem teórica pelos diversos temas, considerando que são ainda poucas as empresas a implementar a Indústria 4.0 e algumas delas estão a implementar de uma forma inconsciente (Gabriel et al, 2016), recorreu-se à realização de entrevistas a peritos que representam as organizações (abordagem qualitativa), pois permite um diálogo com os entrevistados e esclarecimento de conceitos, nos casos necessários.

3.2 Preparação e execução das entrevistas

As entrevistas decorreram com empresas seleccionadas através de contactos com colegas, amigos, conhecidos, que permitiram obter informação de empresas completamente diferentes e de diferentes zonas do país.

As entrevistas, foram realizadas a responsáveis da segurança da informação de empresas do sector industrial. Foram entrevistadas empresas que já tenham implementado ou estejam a implementar alguns dos conceitos relacionados com a Indústria 4.0, um pouco para representarem o que se encontra actualmente ao nível de promoção desses conceitos e por outro lado, na existência de certificação na norma ISO/IEC 27001 ou em falta dela, na existência de boas práticas ao nível da gestão da segurança de sistemas de informação, no âmbito definido para este trabalho. Com as entrevistas, pretendeu-se apurar que problemas têm surgido ao nível de gestão de sistemas de informação, para que sustentem as preocupações referidas no trabalho sobre a segurança da informação no contexto da indústria 4.0.

Pretendeu-se ainda recolher com as entrevistas, algumas opiniões acerca da percepção da importância da ISO/IEC 27001 e do papel das entidades governamentais na sua divulgação.

Para a execução das entrevistas, elaborou-se um documento para a preparação da entrevista, onde se enquadrou a realização deste trabalho. Nalguns casos, esse enquadramento foi feito no momento antes do início da entrevista, de uma forma verbal e noutros casos, foi enviado para o entrevistado o documento preparado, reduzindo o tempo necessário no início da entrevista, para enquadramento do tema. Foi ainda elaborado um guião de entrevista (anexo I), considerando os pontos abordados na revisão literária e com o intuito de auxiliar na obtenção de resposta às questões de investigação. O guião de entrevista foi dividido em duas partes, a primeira parte com 3 questões a colocar aos entrevistados no âmbito da primeira questão de investigação e a segunda parte com as restantes questões a colocar aos entrevistados no âmbito da segunda questão de investigação. Foram colocadas ainda algumas questões, com o objetivo de recolher opiniões sobre o objetivo deste trabalho. O guião de entrevista foi fundamental para a realização das entrevistas, pois além de apresentar as questões para as quais se pretendia a resposta, estavam também detalhados alguns pormenores que ajudavam a esclarecer os entrevistados em caso de necessidade. Foi ainda realizado um guião esquematizado (anexo II) para auxiliar na ordem das questões a colocar aos entrevistados. A forma como as perguntas foram construídas, teve como objetivo permitir a classificação da resposta em “0” e “1”, para permitir uma análise mais objectiva. Ambos os guiões foram validados por terceiros antes de serem utilizados nas entrevistas.

Além das questões que foram colocadas aos entrevistados, foi recolhida informação sobre as empresas, nomeadamente, dimensão, local e sector de atividade.

Entrevistaram-se pequenas, médias e grandes empresas do sector automóvel, alimentar, madeira, cerâmica, metalurgia e moldes, espalhadas pelo país.

Foram realizadas 7 entrevistas. Algumas dessas entrevistas representaram mais do que uma empresa, num caso representou cerca de 5 empresas, de diferentes sectores de atividade e noutro caso, mais de 10 empresas, basicamente todas do mesmo sector de atividade. Por norma, cada entrevista foi tratada como se fosse uma só empresa mas nos

casos em que houve respostas diferentes no leque das empresas abrangidas pela mesma entrevista, houve necessidade de subdividir a análise da entrevista, o que originou 8 empresas representativas.

Considerando o conceito do método de saturação (Thiry-Cherques, 2009), e verificando-se o comportamento das respostas obtidas, decidiu-se fechar a amostra a tratar neste trabalho, com as 8 empresas representativas.

As entrevistas foram realizadas basicamente por telefone, na sua maioria com uma duração superior a 2 horas. As entrevistas basearam-se sempre numa conversa com o entrevistado, iniciando-se com os exemplos que tinham referentes ao conceito da indústria 4.0, sem colocar as questões directamente. Só quando necessário, é que foram mencionadas as questões directamente, para garantir a obtenção da resposta. Desta forma, pretendeu-se obter respostas menos pensadas. As respostas obtidas nas entrevistas foram registadas em papel e confirmadas com os entrevistados. Em alguns casos, foi efectuado mais que um contacto por telefone e foram recepcionadas respostas via *e-mail*, em simultâneo com a entrevista. Duas entrevistas foram realizadas em Setembro de 2017 e as restantes entre Setembro e Outubro de 2018. As mais antigas, foram verificadas que continuavam válidas.

3.3 Análise de dados

A informação recolhida durante as entrevistas, foi transcrita para uma folha de Excel. No anexo III deste trabalho, apresenta-se uma imagem da folha com parte das respostas às questões, tendo-se omitido o que poderia identificar as empresas, considerando que foi requisito obrigatório das entrevistas, o anonimato das empresas, entrevistados e tudo aquilo que eventualmente as poderia identificar.

Para facilitar a análise das respostas às questões, foi criada uma tabela em Excel com uma linha para cada questão e 1 coluna para cada empresa, onde se codificou as respostas em “1” e “0”, sendo que “0”, representa uma resposta “Não” ou “Antes” e “1” representa uma resposta “Sim” ou “Depois”. Para as questões não aplicáveis, não se colocou qualquer codificação.

Como algumas respostas não foram claramente respondidas com “Sim”, “Não”, “Antes” e “Depois”, recorreu-se a um segundo avaliador, que codificou também as

respostas das entrevistas em "0" e "1" numa tabela semelhante à primeira, utilizando a mesma conotação para "0" e "1" referida anteriormente, resultando nas tabelas apresentadas no anexo IV.

A utilização do segundo avaliador, teve como objetivo aferir a qualidade da codificação atribuída a cada questão, na criação da tabela com "0" e "1", recorrendo ao método de K de Cohen. Mas a verdade é que nem sequer foi necessário utilizar o cálculo para se concluir quanto à qualidade da codificação atribuída na primeira tabela, já que a codificação atribuída pelo segundo avaliador, foi exactamente a mesma. O segundo avaliador tratou-se de uma pessoa comum, ao qual foi feita uma pequena introdução sobre o âmbito deste trabalho, que lhe permitisse ter a informação suficiente para entender as questões e as repostas e poder atribuir uma codificação.

Utilizou-se o Excel como auxiliar da análise dos dados, dando uma cariz mais numérica às respostas obtidas, permitindo aferir a grandeza de cada tipo de resposta.

3.4 Conclusões

Foram analisados os resultados das entrevistas, apresentando-se as conclusões provenientes do tratamento efectuado da informação, permitindo obter respostas às questões de investigação apresentadas nesta dissertação, como ainda identificação de algumas limitações na abordagem efectuada, sugerindo ainda algumas ideias para futuras investigações referentes ao tema.

4 Análise dos resultados das entrevistas

Tal como mencionado anteriormente neste trabalho e verificado, considerando a percentagem alcançada na questão 1, 100% das empresas entrevistadas pertencem ao sector industrial e têm implementado ou estão a implementar conceitos relacionados com a Indústria 4.0. Foram mencionados conceitos como comunicação de equipamentos com telemóveis, a utilização de *tablets* na validação de informação de etiquetas, a comunicação de equipamentos com fornecedores, *sharepoint* partilhado com fornecedores e clientes, utilização de *cloud* para partilha de informação, para *backups*, para gestão de emails, conceitos de IoT implementados nos processos produtivos,

comunicação de máquinas com máquinas, robots inteligentes, visão artificial, sistemas autónomos de movimentação, impressão 3D, utilização de EDI a integrar com ERP's, leituras automáticas de RFID, utilização de tecnologia *touch* e existência de equipamento que funciona basicamente sozinho, onde o software é que dá indicação de que materiais o robot tem que ir buscar para fazer a próxima produção.

Não identificando aqui nenhuma empresa em concreto, verifica-se que existem empresas em patamares completamente diferentes de implementação de conceitos da Indústria 4.0. Uns estão a dar os primeiros passos com muito receio e outros estão a dar largos passos. Das empresas entrevistadas, verifica-se uma maior incidência destes conceitos, nas empresas relacionadas com a indústria automóvel, quer directa, quer indirectamente.

Averiguou ainda se essas empresas tinham ou estavam a ter projectos financiados no âmbito da indústria 4.0. Todas elas já tiveram ou têm actualmente projectos desse âmbito.

Quanto à questão 2, 100% das empresas não são certificadas na norma ISO/IEC 27001.

Embora pela revisão literária, se tenha verificado que são muito poucas as empresas com esta certificação, não era esperado que algumas das empresas entrevistadas, não tivessem a certificação e que nem sequer a conhecessem, resposta obtida inclusive, de alguns dos responsáveis de sistemas de informação das empresas entrevistadas.

Na questão 3, 6 empresas (75%) não têm presentes os principais procedimentos referidos na norma.

Só 25% afirmaram ter a maioria dos procedimentos contidos na norma, embora nenhuma empresa aplicasse todos os procedimentos, nomeadamente um bastante importante, as auditorias internas.

Todas as empresas têm alguma documentação, principalmente quando exigida no âmbito da norma ISO 9001. A gestão de risco da segurança dos sistemas de informação, em alguns casos nem sequer é feita, noutros é feita de uma forma não sistematizada (empresa A e B). Em outras empresas, a obrigatoriedade de cumprimento com os requisitos do RGPD, veio gerar o interesse pela possível certificação na norma ISO/IEC

27001 pois aperceberam-se que se fossem certificados com essa norma, estariam bem mais preparados para as exigências apresentadas (empresa F e G).

Na empresa C, foi referido que ao nível mais macro têm muitos procedimentos mas reconhecem que ao nível da produção ainda há trabalho a desenvolver. Na empresa D afirmaram que só têm aquilo que os clientes vão exigindo, não existe uma sistematização global na empresa desses requisitos ao nível da segurança da informação.

Foi ainda referido pela empresa A, a não existência dos meios necessários para definição, implementação, manutenção e melhoria contínua do sistema de segurança da informação.

Na empresa H sentem confiança no que têm referente à gestão da segurança da informação. Nesta empresa, os clientes também são os grandes dinamizadores das boas práticas da gestão da segurança da informação, o que obriga a empresa de uma forma regular, a rever a política da segurança da informação.

Considerando que as primeiras 3 perguntas tinham como objetivo responder à primeira questão de investigação, considerando as respostas obtidas na primeira parte do guião de entrevistas, pode-se concluir que a resposta à primeira questão de investigação é NÃO, ou seja, 100% das empresas entrevistadas (8), são empresas que pertencem ao sector industrial, que estão a implementar ou implementaram conceitos no âmbito da Indústria 4.0, não estão certificadas com a norma ISO/IEC 27001 e 75% dessas empresas entrevistadas (6) não têm implementadas as boas práticas contidas na norma, que permitam que os próprios entrevistados sintam segurança, para poderem responder que estão preparados para a implementação dos conceitos relacionados com a Indústria 4.0. Adicionalmente, verifica-se que todas elas tiveram ou têm projectos financiados no âmbito da Indústria 4.0.

Seguindo para a segunda parte do guião de entrevista, em resposta à questão 4, 63% das empresas entrevistadas (5), afirmam ter tido algum tipo de constrangimento relacionado com a segurança da informação. Algumas empresas mencionaram que tipo de constrangimentos tiveram, embora não pretendam que se refira publicamente o que foi referido em sede de entrevista e outras, simplesmente afirmaram que sim e não quiseram mencionar pormenores.

Combinando as respostas obtidas nas questões anteriores com a questão 4, verifica-se que 100% das empresas que apresentam a utilização da maioria das boas práticas contidas na norma ISO/IEC 27001 (2 empresas), não sofreram qualquer constrangimento.

Das que não apresentam a utilização da maioria das boas práticas contidas na norma ISO/IEC 27001 (6 empresas), 83% tiveram constrangimentos (5 empresas).

As empresas que não apresentaram constrangimentos relacionados com a segurança da informação, 67% (2 empresas) afirmam estar mais expostos. As duas empresas que na questão 2 apresentaram a existência da maioria das boas práticas contidas na norma ISO/IEC 27001, dizem que as têm porque sentiram necessidade de reforçar a segurança da informação, com a exposição gerada pela implementação dos conceitos da indústria 4.0.

Uma das empresas que na questão 2 apresentou a existência da maioria das boas práticas contidas na norma ISO/IEC 27001 (empresa H), afirma que sente até mais segurança com a implementação dos conceitos da indústria 4.0 pois reduziu-se nos processos produtivos a intervenção do factor humano. Estão sempre a optimizar os processos e por isso, não sentem que tenham ficado mais expostos.

100% dos entrevistados (8 empresas), depois de se explicar o que consiste a norma, o que lhe está subjacente, reconheceram encontrar vantagens em ter a certificação na norma, até porque todos os entrevistados sentem dificuldades na gestão da segurança da informação. Algumas das empresas afirmaram que estão a fazer a implementação dos conceitos da I4.0 um pouco a medo e a um ritmo inferior ao que se esperava, por estarem com alguma dificuldade em encontrar soluções para a exposição da informação.

Numa empresa, sentem que o facto de não terem algo que os ajude a medir o risco de exposição, os faz sentirem-se inseguros no trabalho que estão a realizar no âmbito da indústria 4.0.

A empresa A diz sentir ser fundamental para terem a noção das consequências da implementação dos conceitos relacionados com a indústria 4.0. A empresa B diz ser útil para a I4.0 e para o resto, ter uma certificação como a ISO/IEC 27001. A empresa C diz ser fundamental para conseguirem aferir se o que estão a fazer ou vão fazer, vai alargar

ou não o risco, tendo em conta que não fazem a avaliação do risco. A empresa D diz que se tivessem essa certificação, certamente alguns dos acontecimentos referentes à segurança da informação, não ocorreriam. A empresa E afirmou que estariam mais cientes dos riscos que estão expostos. As empresas F e G afirmam que é fundamental para controlar as situações relacionadas com a segurança da informação. Quanto à empresa H, que no início da entrevista afirmava que não tinha qualquer fragilidade quanto à segurança da informação e que não sentia qualquer vantagem na certificação na norma, após perceber o âmbito da mesma, acabou por afirmar que, se eles sentiram necessidade de implementação das boas práticas contidas na norma, então é porque talvez a certificação na norma possa trazer vantagens. No caso deles, estão a ver a certificação como uma forma de aumentar o reconhecimento da empresa perante os clientes, como uma empresa que cumpre com as melhores práticas ao nível da segurança da informação, trazendo mais credibilidade para a mesma. Afirmaram: “A segurança da informação é muito importante para que o cliente confie em nós."

A questão 7 acabou por não ter qualquer tipo de resposta, já que só seria aplicável se alguma das empresas fosse certificada com a norma ISO/IEC 27001.

Considerando as empresas que já sofreram constrangimentos no âmbito da segurança da informação, 40% (2 empresas) tiveram antes da implementação dos conceitos relacionados com a Indústria 4.0 e 60% (3 empresas), depois.

100% dos 63% que tiveram constrangimentos relacionados com a segurança da informação (5 empresas), afirmam estarem mais expostos com a implementação dos conceitos da I4.0.

A empresa B, que sofreu constrangimentos mesmo antes da implementação dos conceitos relacionados com a I4.0, está a implementar planos de contenção, por sentirem que não têm recursos com o conhecimento suficiente para mitigar riscos no âmbito da segurança da informação.

Um dos entrevistados (empresa C) afirmou que a conexão dos dados é o mesmo que deixar as portas escancaradas de uma casa e se não houver regulamentação, estamos a potenciar o risco da segurança da informação. Certamente que com as portas fechadas, a probabilidade seria menor. A empresa D sente também que não têm recursos com o conhecimento suficiente para mitigar o risco da segurança da informação.

Considerando a sua própria experiência e compreendendo o que consiste a norma ISO/IEC 27001, como resposta à questão 9, 100% das empresas entrevistadas aconselhariam as empresas a tratarem primeiro da certificação e só depois enveredarem pelo mundo da I4.0. Uns afirmam isso, considerando os constrangimentos que sofreram e outros, considerando o trabalho que foram fazendo e estão constantemente a fazer, para garantirem a segurança da informação com a implementação dos conceitos relacionados com a indústria 4.0. Um dos entrevistados (empresa H) afirma terem feito investimentos avultados na área da segurança da informação, para conseguirem evoluir consideravelmente na I4.0 sem que a segurança da informação fique em risco.

Todas as empresas, considerando as experiências vividas, aconselhariam a obter primeiro a certificação e uma refere ainda, que na pior das hipóteses, deveriam obter a certificação em simultâneo com a implementação dos conceitos relacionados com a I4.0.

A empresa C aconselha as empresas primeiro que tudo, a fazerem um levantamento das reais necessidades de implementação dos conceitos relacionados com a Indústria 4.0. Depois disso, a certificação na norma ISO/IEC 27001 e então a seguir, a implementação dos conceitos. Afirmaram que, "…as empresas, se não fazem uma análise dos processos e se não fazem uma implementação consciente do que estão a fazer, muitas vezes não estão preparados para lidar com as consequências resultantes da implementação desses conceitos."

As empresas referiram que seria mais fácil a implementação dos conceitos da I4.0, a empresa E referiu que dessa forma será certamente mais fácil avaliar os riscos da implementação, a empresa H afirmou que se eles sentiram necessidade de reforçar toda a estrutura de segurança da informação, é porque é necessário e se as empresas fizerem esse reforço logo de início, será mais fácil.

100% das empresas entrevistadas responderam à questão 10 como havendo necessidade de mais incentivos para a implementação da norma, considerando incentivos não só a ajuda financeira mas também a divulgação do que consiste a norma e que vantagens trará para as empresas, no contexto da I4.0.

A empresa A afirma que são necessários incentivos mas também obrigações de cumprimento da norma porque senão, as empresas vão continuar a investir na indústria

4.0 com o intuito de obter resultados sem se precaverem das consequências da falta de segurança da informação. Mais do que incentivos, é necessário obrigação de ter a certificação antes ou durante a implementação de projetos da indústria 4.0.

A empresa C afirma que fazer I4.0 sem gerir o risco é também um problema. Deveria ser tido em conta a gestão do risco da segurança da informação e não se falar só em I4.0. As entidades governamentais deveriam ter um papel mais formativo, mais direcionado, mais orientação.

A empresa D diz que é necessário mais vontade para implementar a norma. Os incentivos ajudam mas o que é necessário é a consciência da necessidade. Os incentivos não vão resolver o problema. É necessário compreender as vantagens de ter uma norma como esta. Se não houver essa perceção e houver só os incentivos, depois a norma pode acabar por não ser seguida e acaba por cair.

A empresa H, muito focada em tudo o que envolve o cliente, refere que deveriam existir mais incentivos pois no processo todo de I4.0 é necessário salvaguardar a confidencialidade, principalmente no que se refere aos clientes.

Como resposta à última questão do guião de entrevista, 100% das empresas entrevistadas, consideram que as entidades governamentais devem primeiro incentivar a certificação e só depois, a implementação dos conceitos da I4.0.

As empresas dizem mais ainda, que até pode ser obtida em simultâneo com o desenvolvimento dos projectos. Podem não ter a certificação aquando da candidatura mas deveria fazer parte de um requisito obrigatório para encerramento do projecto. (empresa A e C). As empresas B e D afirmam que o ideal será a implementação em simultâneo dos conceitos da I4.0 e a certificação. A empresa B e E ainda afirmam que o que constatam, é que preferem ver a funcionar do que controlar as limitações que poderão surgir na segurança da informação. A empresa E afirma que nem sequer lhes foi dado a conhecer as vantagens da certificação nessa norma, no âmbito da implementação de conceitos relacionados com a Indústria 4.0. Quanto à empresa F, afirma que já se devia ter obrigado a ter a norma e incentivado, mesmo antes da entrada em vigor do RGPD. Afirmam que a implementação até pode ser em simultâneo com a implementação dos conceitos da I4.0. Se as empresas não forem certificadas quando se

candidatam aos projectos, deveriam ser obrigadas a atingir a certificação com o encerramento dos projectos.

Quanto à empresa H, o entrevistado afirmou que, se as empresas vão iniciar o seu trajecto no mercado, se ainda não são reconhecidos no mercado, faz todo o sentido que apostem primeiro na certificação e depois então na implementação dos conceitos da I4.0. Afirmam o seguinte: "Garantidamente, é preciso cumprir com os procedimentos existentes na norma, pois temos essa necessidade e tivemos que implementar, mais importante ainda quando não se é reconhecido no mercado."

Quanto à segunda questão de investigação deste trabalho, depois de se ter analisado os argumentos de cada empresa entrevistada e considerando que 63% das empresas entrevistadas tiveram constrangimentos relacionados com a segurança da informação e que desses, mais de metade foram após a implementação dos conceitos relacionados com a I4.0, poder-se á concluir que SIM, que a implementação fomentou o aumento de acontecimentos com a segurança da informação. 88% das empresas (7 empresas) são da opinião que estão mais expostos com a implementação dos conceitos relacionados com a I4.0.

Relacionando a resposta à primeira questão da investigação com a resposta à segunda questão de investigação, pode-se afirmar que as empresas que implementaram conceitos no âmbito da indústria 4.0 e que tiveram constrangimentos após essa implementação, trata-se de empresas que não têm a certificação na norma ISO/IEC 27001 e que não têm implementado as boas práticas inseridas na norma, quanto à gestão da segurança da informação.

Com as respostas a atingir os 100% nas perguntas 9, 10 e 11, associado aos argumentos e experiências que as empresas foram detalhando, conclui-se que faz todo o sentido que as empresas primeiro se preocupem em obter a certificação na norma ISO/IEC 27001, para estarem preparadas para a implementação dos conceitos relacionados com a I4.0 e então depois sim, navegarem pela I4.0. E nisto, as entidades governamentais têm alguma responsabilidade e por isso, quando estão a aprovar a implementação de projectos relacionados com a indústria 4.0, deveriam garantir a existência dessa certificação, obrigando nos casos em que ainda não exista nessas empresas, o comprometimento em atingir esse objetivo na conclusão do projecto.

Devem as entidades governamentais, considerando as respostas obtidas nas entrevistas, fomentar a aplicabilidade da norma, informando as vantagens que a mesma traz para as empresas, principalmente no âmbito da I4.0.

Verificou-se durante as entrevistas, alguma inquietação na abordagem deste assunto, quando tomaram consciência ao longo da entrevista, que efectivamente não estavam acauteladas as necessárias seguranças relacionadas com o âmbito deste trabalho, com a implementação dos conceitos da indústria 4.0.

Em alguns casos, solicitaram mesmo mais informação sobre o tema e outros informaram que iriam passar a questão para a equipa responsável pela implementação de normas, pois apesar de terem investido muito em segurança da informação, após a entrevista, confessaram que, se existe algo que os pode ajudar a garantir a segurança da informação perante os clientes, por exemplo, deveriam investir (empresa H).

Houve outros casos no entanto que confessaram que, enquanto não fossem obrigados a implementar a norma, tal como aconteceu com a norma ISO 9001, não iriam tomar essa iniciativa.

5 Conclusões, investigações futuras e limitações

Muitas empresas já deram os primeiros passos no caminho da indústria 4.0 (Gabriel et al, 2016). A comunicação em rede é um requisito da indústria 4.0 e prevendo-se ainda um longo caminho na sua total implementação (Gabriel et al, 2016), as empresas têm que estar preparadas em vários níveis, sendo um deles ao nível da segurança da informação do âmbito desta dissertação**,** nomeadamente, no que se refere à segurança da informação estratégica, de concepção e desenvolvimento de produto, de processos de produção (como se faz, quer a nível de produto, quer a nível de processo) e de modelos de gestão.

Sendo a maioria das nossas empresas, do tipo PME, muitas com gestão familiar, com pouco conhecimento de tecnologias e dos problemas que possam advir com a implementação de tecnologias inerentes ao conceito Indústria 4.0 (Pereira et al, 2017; Heikkila et al, 2016), após a análise dos resultados das entrevistas, não parece ficarem muitas dúvidas quanto à necessidade das entidades governamentais terem que fornecer

incentivos para fomentar as certificações na norma ISO/IEC 27001. O que parece adicionalmente, considerando as respostas obtidas nas entrevistas, é que não são só as PME's que precisam desses incentivos, pois verificou-se na amostra de respostas obtidas, que as grandes empresas também não estão devidamente acauteladas quanto à problemática da segurança da informação, na implementação dos conceitos da Indústria 4.0. As empresas que foram identificadas como tendo os conceitos principais aplicados da norma ISO/IEC 27001, são PME's e as que se identificou como não tendo ocorrido constrangimentos no âmbito da segurança da informação, são também PME's. 3 das 8 empresas entrevistadas são grandes empresas e essas estão em condições inferiores no que se refere à gestão da segurança da informação.

A maioria das empresas entrevistadas, nem sequer conheciam a norma ISO/IEC 27001 ou se tinham ouvido essa referência, não sabiam exactamente no que consistia.

Tal como um dos entrevistados referiu, talvez o problema não se resolva só com os incentivos, deverá ser feito mais um trabalho de consciencialização ou como outros entrevistados referiram, de obrigação de implementação da norma ISO/IEC 27001, para que possam usufruir dos incentivos relacionados com a implementação dos conceitos da indústria 4.0.

O que se pode concluir com este trabalho é que, se não houver iniciativas no âmbito da gestão da segurança da informação que corram a par com as iniciativas da indústria 4.0, prevê-se muitos problemas de futuro relacionados com o âmbito deste trabalho, pois se algumas empresas demonstraram estarem a acautelar possíveis problemas que possam surgir com a implementação dos conceitos da indústria 4.0, outras nem por isso e todas elas assumiram que, se tivessem alguma norma implementada referente à segurança da informação, poderiam ter mais segurança no trabalho que estão a realizar, quer na mitigação de problemas relacionados com a segurança da informação, quer na implementação dos conceitos relacionados com a Indústria 4.0.

Ter a certificação na ISO/IEC 27001 por si só, não significa que uma empresa está totalmente protegida quanto aos seus sistemas de informação (Heikkila et al, 2016), principalmente no que se refere ao âmbito deste trabalho, mas certamente estarão muito mais protegidos, pois quando uma empresa apresenta uma certificação, demonstra que está a cumprir com as melhores práticas referentes ao tema (ISO27001, 2017).

Nas empresas entrevistadas, o trabalho de consciencialização já foi efectuado, pois esteve presente durante as entrevistas, a preocupação dos entrevistados quando confrontados com o assunto deste trabalho. Mas é necessário que toda esta consciencialização chegue a todas as empresas do país.

Quanto a limitações deste estudo, é de referir que a amostra das empresas entrevistadas, pode estar a influenciar os resultados obtidos pois com outra amostra, poder-se-ia obter outras conclusões, embora se tenha feito uma selecção aleatória, que acabou por abranger empresas PME's mas também não PME's, de diferentes sectores de atividade e de diferentes pontos do país.

Em futuras investigações, poderá ser interessante limitar o estudo por zona do país ou por sector de atividade, ou por tipo de dimensão de empresa, para se verificar se as conclusões se mantém ou se têm algum comportamento diferente, considerando um leque de amostra mais focado.

Referências Bibliográficas

- Baskerville, Richard; Spagnoletti, Paolo e Kim, Jongwoo (2014). "Incident-centered information security: Managing a strategic balance between prevention and response", *Information & Management,* volume 51, 1, 138– 151
- British (2017). ISO 27001 History. The British Assessment Bureau. Consultado em https://www.british-assessment.co.uk/services/iso-certification/iso-27001-certification/

  acedido em 09/09/2018
- Cheminod, Manuel; Durante, Luca e Valenzano, Adriano (2013). "Review of Security Issues in Industrial Networks", *IEEE transactions on industrial informatics*, volume 9, 1, 277- 293
- Correia, Ana M. R. e Mesquita, Anabela (2013). Mestrados & Doutoramentos, Estratégias para a elaboração de trabalhos científicos: o desafio da excelência, 2ª edição, Vida Económica
- Gabriel, Magdalena e Pessl, Ernst (2016). "Industry 4.0 and sustainability impacts: Critical discussion of sustainability aspects with a special focus on future of work and ecological consequences", *Annals of the Faculty of Enginnering Hunedoara-International Journal of Engineering*, xiv, volume 2, 131-136
- Hao, Y. e Helo, P. (2017)." The role of wearable devices in meeting the needs of cloud manufacturing: A case study", *Robotics and Computer-Integrated Manufacturing*, 45, 168-179
- Heikkila, M.;Rattyä, A. ; Pieska, S. e Jamsa, J. (2016). "Security challenges in small- and medium-sized manufacturing enterprises", *Small-scale Intelligent Manufacturing Systems (SIMS), International Symposium*, IEEE 25-30
- Hermann, Mario; Pentek, Tobias e Otto, Boris (2016). "Design Principles for Industrie 4.0 Scenarios", *49th Hawaii International Conference on System Science*, 3928-3937
- Hofmann, Erik e RüschIndustry, Marco (2017). " 4.0 and the current status as well as future prospects on logistics", *Computers in Industry*, 89, 23–34
- Hummer, Matthias; Kunz, Michael; Netter, Michael; Fuchs, Ludwig e Pernul, Günther (2016) "Adaptive identity and access management-contextual data policies", *EURASIP*

Journal on Information Security, 1-16 disponível em https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-016-0043-2 consultado em 04/10/2018

- IAPMEI (2018). Indústria 4.0 Economia Digital. Investimos com as empresas na 4ª revolução industrial. Consultado em https://www.iapmei.pt/Paginas/Industria-4-0.aspx acedido em 09/09/2018
- Ilie-Zudor, Elisabeth; Kemény, Zsolt e Preuveneers, Davy (2016). "Efficiency and security of process transparency in production networks-a view of expectations, obstacles and potentials", *Procedia CIRP*, volume 52, 84–89
- INE (2018). Empresas em Portugal 2016. Documento disponível em

  https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=318224733&PUBLICACOESstema=00&PUBLICACOESmodo=2 acedido em 09/09/2018
- IPAC (2018). Base de dados de entidades certificadas. Consultado em http://www.ipac.pt/pesquisa/pesq_empcertif.asp acedido em 09/09/2018
- IPAC1 (2018). Diretório de entidades acreditadas. Consultado em http://www.ipac.pt/pesquisa/acredita.asp acedido em 09/09/2018
- ISO27001 (2017). ISO 27K *Timeline* consultado em http://www.iso27001security.com/html/timeline.html acedido em 09/09/2018
- ISO/IEC 27001:2013(E) (2013). Information technology - Security techniques – Information security management systems – Requirements, International Standard
- Jansen, C. e Jeschke, S. (2018). "Mitigating risks of digitalization through managed industrial security services" *AI & SOCIETY*, 33(2), 163-173
- Jennings, Adrian (2015). The promise and the risks of IIoT and Industry 4.0 em www.plantengineering.com magazine june, 16-18 consultado em 05/10/2018
- Kagermann, H.;Helbig, J.;Hellinger,A. e Wahlter, W. (2013). Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative Industrie 4.0, ACATECH em

https://en.acatech.de/944/?tx_ttnews%5Btt_news%5D=916&cHash=49e3bb346e0888ce34ccf543280b08e6 consultado em 22/10/2018

- Kamal Kaur, R.; Pandey, B. e Singh, L. K. (2018). "Dependability analysis of safety critical systems: Issues and challenges", *Annals of Nuclear Energy*, 120, 127-154
- Kuyoro, S. O.; Ibikunle, F. e Awodele O. (2011). ”Cloud Computing Security Issues and Challenges”, *International Journal of Computer Networks (IJCN)*, volume 3, 5, 247-255
- McKinsey Digital (2016). Industry 4.0 after the initial hype. Where manufacturers are finding value and how they can best capture it, disponível em https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/getting%20the%20most%20out%20of%20industry%204%200/mckinsey_industry_40_2016.ashx consultado em 04/10/2018
- Nelles, Jochen ; Kuz, Sinem; Mertens, Alexander e Schlick, Christopher M. (2016). "Human-centered design of assistance systems for production planning and control: The role of the human in Industry 4.0" , *Industrial Technology (ICIT), 2016 IEEE International Conference*, 2099-2104
- Neugebauer, Reimund; Hippmann, Sophie ; Leis, Miriam e LandHerr, Martin (2016). "Industrie 4.0-From the perspective of applied research", *Factories of the Future in the digital environment - Proceedings of the 49th CIRP Conference on Manufacturing Systems*, Procedia CIRP volume 57, 2-7
- Nikolic, B. ; Ignjatic, J. ; Suzic, N. ; Stevanov, B. e Rikalovic, A. (2017). " Predictive Manufacturing Systems in Industry 4.0: Trends, Benefits and Challenges", *Proceedings of the 28th DAAAM International Symposium*, 0796-0802
- Oesterreich, Thuy Duong e Teuteberg, Frank (2016). "Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry", *Computers in Industry 83*, 121–139
- Pereira, T.; Barreto, L. e Amaral, A. (2017). " Network and information security challenges within Industry 4.0 paradigm", *Manufacturing Enginnering Society International Conference* -Procedia Manufacturing 13, 1253–1260

- Portugal.gov (2018). https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=20170130-mecon-industria-4 consultado em 09/09/2018
- Portugal2020 (2018). Formulário Portugal 2020, Página 2, declaraçõe**s,** disponível em http://www.poci-compete2020.pt/Avisos/detalhe/AAC_26-SI-2016 consultado em 08/09/2018
- Portugal2020a (2018). Lista de operações aprovadas. Consultado em https://www.portugal2020.pt/Portal2020/OperacoesAprovadas em 09/09/2018
- Portugal2020b (2018). Avisos de apresentação de candidaturas. Consultado em http://www.poci-compete2020.pt/admin/images/20161209_AAC_26_2016_CoPromocao_RCI.pdf em 22/10/2018
- Portugal2020c (2018). Avisos de apresentação de candidaturas. Consultado em http://www.poci-compete2020.pt/admin/images/20161209_AAC_25_2016_Individual_RCI.pdf em 30/09/2018
- Preuveneers, Davy; Joosen, Wouter e Ilie-Zudor, Elisabeth (2016). "Data Protection Compliance Regulations and Implications for Smart Factories of the Future", *2016 12th International Conference on Intelligent Environments*, 40-47
- Priller, Peter; Aldrian, Andreas e Ebner, Thomas (2014). "Case Study: From Legacy to Connectivity Migrating industrial devices into the world of Smart Service", *Proceedings of 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, 1-8
- Qin, Jian; Liu, Ying e Grosvenor, Roger (2016). "A Categorical Framework of Manufacturing for Industry 4.0 and Beyond", *Procedia CIRP* 52, 173 – 178
- Rennung, Frank; Luminosu, Caius Tudor e Draghici, Anca (2016). "Service Provision in the Framework of Industry 4.0", *SIM 2015 / 13th International Symposium in Management, Procedia - Social and Behavioral Sciences 221*, 372 – 377 disponível em https://doi.org/10.1016/j.sbspro.2016.05.127 consultado em 14/10/2018

- Rodrigues, Miguel Videira e Esteves, Pedro (2017). Ataques informáticos. As empresas portuguesas estão preparadas? em https://observador.pt/2017/03/26/ataques-informaticos-empresas/ consultado em 18/09/2018
- Sadeghi, Ahmad-Reza; Wachsmann, Christian e Waidner, Michael (2015). ”Security and Privacy Challenges in Industrial Internet of Things”, *Fraunhofer Institute for Secure Information Technology*, Darmstadt, Germany
- Schumacher, Andreas; Erol, Selim e Sihn,Wilfried (2016). "A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises", Procedia CIRP 52, 161 – 166
- Shaabany, Ghaidaa; Grimm, Marco e Anderl, Reiner (2016). "Secure Information Model for Data Marketplaces enabling Global Distributed Manufacturing", *26th CIRP Design Conference*, Procedia CIRP 50, 360 – 365
- Slusarczyk, Beata (2018). "Industry 4.0: are we ready?" *Polish Journal of Management Studies*, volume 17, 1, 232-248
- Sommer, Lutz (2015). "Industrial revolution - industry 4.0: Are German manufacturing SMEs the first victims of this revolution?." *Journal of Industrial Engineering and Management* , volume 8, 5, 1512-1532 em http://dx.doi.org/10.3926/jiem.1470 consultado em 30/09/2018
- Stock, T. e Seliger, G. (2016). "Opportunities of Sustainable Manufacturing in Industry 4.0", *13th Global Conference on Sustainable Manufacturing-Decoupling Growth from Resource Use*, Procedia CIRP 40, 536 – 541
- Stojkić, Željko; Veža ,Ivica e Bošnjak ,Igor (2016). “A concept of information system implementation (CRM and ERP) within industry 4.0”, *Proceedings of the 26th DAAAM International Symposium*, 912-919, disponível em http://daaam.info/Downloads/Pdfs/proceedings/proceedings_2015/127.pdf consultado em 14/10/2018
- Thiry-Cherques, Hermano Roberto (2009). “Saturação em pesquisa qualitativa: estimativa empírica de dimensionamento”, *Revista Brasileira de Pesquisas em Marketing (PMKT)*, volume 3, 20-27 disponível em http://www.revistapmkt.com.br/Portals/9/Edicoes/Revista_PMKT_003_02.pdf, consultado em 07/10/2018

- Trappey, Amy J.C. ; Trappey, Charles V.; Govindarajan, Usharani Hareesh, Chuang, Allen C. e Sun, John J. (2017). "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0", *Advanced Engineering Informatics*, volume 33, 208-229 disponível em https://doi.org/10.1016/j.aei.2016.11.007 consultado em 14/10/2018
- Tuptuk, Nilufer e Hailes, Stephen (2018). "Security of smart manufacturing systems", *Journal of Manufacturing Systems* 47, 93–106 disponível em https://doi.org/10.1016/j.jmsy.2018.04.007 consultado em 14/10/2018
- Yilmaz, Rustu e Yalman, Yildiray (2016). "A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks", *TEM Journal* – volume 5, 2, 180-191
- Yue, X.; Cai, H.; Yan, H.; Zou, C. e Zhou, K. (2015). "Cloud-assisted industrial cyber-physical systems: An insight", *Microprocessors and Microsystems*, 39(8), 1262-1270
- Waidner, Michael e Kasper, Michael (2016). "Security In Industrie 4.0 - Challenges and Solutions for the Fourth Industrial Revolution", *2016 Design, Automation and Test in Europe Conference & Exhibition*, 1303-1308
- Zhang H. G.; Han,WenBao; Lai, Xuejia; Lin, Dongdai; Ma, Jianfeng e Li, JianHua (2015). "Survey on cyberspace security", *Science China, Information Sciences*, 58, 110101:1-110101:43
- Zhou, Keliang; Liu, Taigang e Zhou, Lifeng (2015). "Industry 4.0: Towards Future Industrial Opportunities and Challenges", *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, IEEE, 2147-2152

Anexos

Anexo I

Guião de entrevista

A QUESTÕES PARA SE PODER RESPONDER À QUESTÃO DE INVESTIGAÇÃO:

-As empresas que estão a implementar conceitos no âmbito da Indústria 4.0 estão certificadas com a norma ISO 27001 ou têm implementadas as boas práticas contidas na norma?

QUESTÃO 1	**A empresa está a implementar/implementou conceitos da Indústria 4.0? Referir outras designações (Industrial Internet, Integrated industry, Industrial internet of things (IIoT), Intelligent Manufacturing, Digital Industry 4.0, caso o entrevistado não identifique o termo.** Averiguar a existência de: Conceito IoT-sistema global de redes de computadores ligados por IP, sensores, atuadores, máquinas e dispositivos; Ligação de equipamentos industriais à internet\ERP\outros Integração de sistemas em diferentes níveis hierárquicos Conceito Internet of Services-oferta de serviços através da internet Conceito Embedded Systems (ES) -Microcomputadores que monitorizem e controlem os processos físicos, com feedback em ciclos, onde os processos físicos afectam os processos computacionais e vice-versa. Conceito Cyber Physical Systems (CPS) -integração do mundo físico com o mundo virtual. Comunicação direta entre as pessoas, máquinas, sistemas de transporte e armazenamento e instalações produtivas. Se o entrevistado estiver à vontade com o termo, basta registar os exemplos que dá, senão, apresentar alguns exemplos para ajudar o entrevistado a identificar.
QUESTÃO 2	**A empresa é certificada na norma 27001? Caso o entrevistado não conheça, explicar de uma forma sucinta no que consiste.**
QUESTÃO 3- Para respostas à questão 2 = "NÃO"	**A empresa tem implementado os principais principios da norma 27001?** Se a empresa não estiver certificada na norma 27001, averiguar a existência de: Procedimentos internos que preservem a confidencialidade da informação Procedimentos internos que preservem a integridade da informação Procedimentos internos que preservem a disponibilidade da informação Procedimentos internos referentes à gestão de risco da segurança da informação Ir apresentando exemplos, para que o entrevistado possa confirmar a sua existência, caso não esteja à vontade com os conceitos. Comprometimento da gestão com a segurança da informação Procedimentos internos com a política da segurança da informação Comunicação na organização da política da segurança da informação e disponível para partes interessadas. Objetivos e planos para a segurança da informação em funções e níveis mais críticos da empresa. Competências necessárias Meios necessários para definição, implementação, manutenção e melhoria contínua do sistema de segurança da informação. Auditorias internas Utilização do conceito cloud para partilha de informação Se o entrevistado estiver à vontade com o termo, basta registar os exemplos que dá, senão, apresentar alguns exemplos para ajudar o entrevistado a identificar.

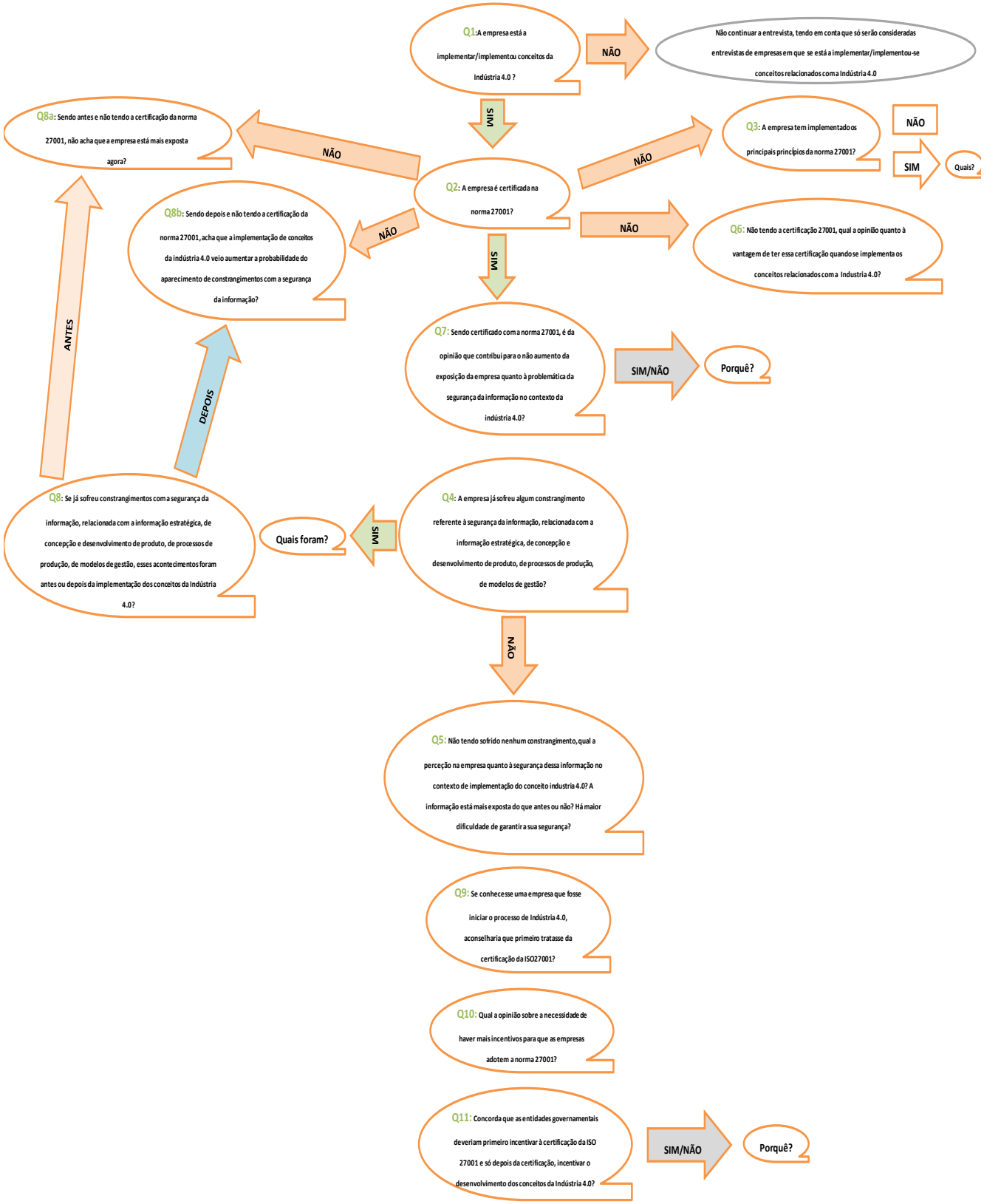
B QUESTÕES PARA SE PODER RESPONDER À QUESTÃO DE INVESTIGAÇÃO:

-A implementação de conceitos da Indústria 4.0, fomentou o aumento de acontecimentos com a segurança da informação,relacionada com a informação estratégica, de concepção e desenvolvimento de produto, de processos de produção, de modelos de gestão?

QUESTÃO 4	A empresa já sofreu algum constrangimento referente à segurança da informação, relacionada com a informação estratégica, de concepção e desenvolvimento de produto, de processos de produção, de modelos de gestão? Se sim, quais foram?
QUESTÃO 5-Para resposta à questão 4= "NÃO"	Não tendo sofrido nenhum constrangimento, qual a perceção na empresa quanto à segurança dessa informação no contexto de implementação do conceito industria 4.0? A informação está mais exposta do que antes ou não? Há maior dificuldade de garantir a sua segurança?
QUESTÃO 6-Para respostas à questão 2= "NÃO"	Não tendo a certificação 27001, qual a opinião quanto à vantagem de ter essa certificação quando se implementa os conceitos relacionados com a Industria 4.0?
QUESTÃO 7-Para respostas à questão 2= "SIM"	Sendo certificado com a norma 27001, é da opinião que contribui para o não aumento da exposição da empresa quanto à problemática da segurança da informação no contexto da indústria 4.0?
QUESTÃO 8-Para respostas à questão 4 = "SIM"	Se já sofreu constrangimentos com a segurança da informação, relacionada com a informação estratégica, de concepção e desenvolvimento de produto, de processos de produção, de modelos de gestão, esses acontecimentos foram antes ou depois da implementação dos conceitos da Indústria 4.0?
QUESTÃO 8a-Para respostas à questão 8 = "ANTES" e resposta 2 = "NÃO"	Sendo antes e não tendo a certificação da norma 27001, não acha que a empresa está mais exposta agora?
QUESTÃO 8b-Para respostas à questão 8 = "DEPOIS" e resposta 2 = "NÃO"	Sendo depois e não tendo a certificação da norma 27001, acha que a implementação de conceitos da indústria 4.0 veio aumentar a probabilidade do aparecimento de constrangimentos com a segurança da informação?
QUESTÃO 9	Se conhecesse uma empresa que fosse iniciar o processo de Indústria 4.0, aconselharia que primeiro tratasse da certificação da ISO27001?
QUESTÃO 10	Qual a opinião sobre a necessidade de haver mais incentivos para que as empresas adotem a norma 27001?
QUESTÃO 11	Concorda que as entidades governamentais deveriam primeiro incentivar à certificação da ISO 27001 e só depois da certificação, incentivar o desenvolvimento dos conceitos da Indústria 4.0?

Anexo II

Esquema do guião de entrevista



Anexo III

Folha de Excel onde foram registadas as respostas das entrevistas

EMPRESA	1- [redacted]							
EMPRESA	A	B	C	D	E	F	G	H
SECTOR	CERÂMICA	AUTOMÓVEL	AUTOMÓVEL	ALIMENTAR	MADEIRA	METALURGIA	MOLDES	MOLDES
LOCAL	[redacted]							
DIMENSÃO	[redacted]							
DATA DA ENTREVISTA	08-09-2017	09-09-2017	20-09-2018	20-09-2018	12-10-2018	10-10-2018	10-10-2018	15-10-2018
MEIO DE COMUNICAÇÃO UTILIZADO	Presencial	Telefone	Telefone	Telefone	Telefone	Telefone	Telefone	Telefone
CARGO DO ENTREVISTADO	[redacted]							
NOME DO ENTREVISTADO	[redacted]							
CONFIDENCIALIDADE NO NOME DA EMPRESA	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
QUESTÃO 1	Sim. Tem equipamentos que comunicam	Sim. Tem sharepoint com fornecedores e	Sim. Tem neste momento a decorrer	Alguma coisa mas pouco. Têm o office	Sim a empresa está a implementar	Sim. Grande parte na [redacted]	Sim. [redacted]	Têm dentro da [redacted]
QUESTÃO 2	Não	Não	NÃO, nem nunca ouviu falar.	NÃO.	Não, não somos.	NÃO	NÃO	NÃO
QUESTÃO 3	Não. Faz-se uma análisede risco muito básica e	Faz-se a análise do risco mas não de uma forma	Tem vários procedimentos ao nível da	Têm qualquer coisa, o que os clientes	Procedimentos internos que preservem a	Têm [redacted]	[redacted] RGPD, têm	Têm um termo de confidencialidade assinado pelo
QUESTÃO 4	Sim. Susceptibilidades na ligação de	Sim, internamente.A base de dados	SIM. Há uns meses, um erro de um	SIM, alguns ataques informáticos	Não	NÃO	Tiveram um ataque de ramsware a um	Não, dizem que é impossível terem ataques.
QUESTÃO 5	N/A	N/A	N/A	N/A	Sim a indústria estará mais exposta com	No caso da [redacted] muito mais expostos	N/A	Eles dizem que até sentem mais segurança, pois
QUESTÃO 6	Fundamental. Certamente iria reduzir a	Muito útil. Na I40 e em tudo. 90% era útil para tudo.	Obviamente que será a única forma de aferir se	Concerteza que há vantagens. Por	Sim, claro que sim. Teriamos mais noção dos	É fundamental. Ajuda a controlar as situações	É fundamental. Ajuda a controlar as	À primeira vista, diriam que não há vantagem pois não
QUESTÃO 7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
QUESTÃO 8	Foram depois.	Foram antes.	Depois.	Depois.	N/A	N/A	ANTES	N/A
QUESTÃO 8A	N/A	A implementação dos conceitos vai aumentar o risco	N/A	N/A	N/A	N/A	SIM	N/A
QUESTÃO 8B	Sem dúvida.	N/A	Sim. Conecção de dados, tudo aberto, é o	Acho que sim. Quanto maior a comunicação,	N/A	N/A	N/A	N/A
QUESTÃO 9	Sim. Ou então que fizesse a implementação	SIM	Primeiro as empresas devem avaliar os	Sim.	Se já tivesse a certificação seria mais fácil	Sim, era muito mais simples.	Sim, era muito mais simples.	Sim, porque se nós sentimos necessidade de
QUESTÃO 10	São necessários incentivos e obrigações	São necessários mais incentivos.	Fazer 4.0 sem gerir o risco é também um	Não diria incentivos, diria mais	Tem que haver mais para que as empresas	Não têm conhecimento sobre incentivos e aquilo	Não têm conhecimento sobre	Sim, deveria haver pois no processo todo de I40 é
QUESTÃO 11	Sim ou então em simultâneo. Podem não ter a	O ideal seria a implementação dos conceitos da	Não tem a certeza se tem que ser antes	Em paralelo o desenvolvimento dos	Se nós tivermos antes, seria mais fácil	Sim. Antes do RGPD [redacted]	Sim. [redacted] RGPD devia	Se as empresas vão iniciar o seu trajecto no

Anexo IV

Tabela com a esquematização das respostas

SIM" ou "DEPOIS"=1

"NÃO" ou "ANTES"=0

AVALIADOR 1

	EMPRESA							
Nº DA QUESTÃO	A	B	C	D	E	F	G	H
1	1	1	1	1	1	1	1	1
2	0	0	0	0	0	0	0	0
3	0	0	0	0	1	0	0	1
4	1	1	1	1	0	0	1	0
5					1	1		0
6	1	1	1	1	1	1	1	1
7								
8	1	0	1	1			0	
8a		1					1	
8b	1		1	1				
9	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1

AVALIADOR 2

	EMPRESA							
Nº DA QUESTÃO	A	B	C	D	E	F	G	H
1	1	1	1	1	1	1	1	1
2	0	0	0	0	0	0	0	0
3	0	0	0	0	1	0	0	1
4	1	1	1	1	0	0	1	0
5					1	1		0
6	1	1	1	1	1	1	1	1
7								
8	1	0	1	1			0	
8a		1					1	
8b	1		1	1				
9	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1

		2		
		SIM	NÃO	
1	SIM	57	0	57
	NÃO	0	47	47
		57	47	104

K	100%