UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
SISTEMAS DE INFORMAÇÃO

TIAGO OLIVEIRA DE SOUZA

Transformação Digital e Suas Implicações na Vulnerabilidade das Organizações: Uma Revisão Sistemática da Literatura

Recife
2022

TIAGO OLIVEIRA DE SOUZA

Transformação Digital e Suas Implicações na Vulnerabilidade das Organizações: Uma Revisão Sistemática da Literatura

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Profa. Dra. Simone Cristiane dos Santos

Recife

2022

TIAGO OLIVEIRA DE SOUZA

Transformação Digital e Suas Implicações na Vulnerabilidade das Organizações: Uma Revisão Sistemática da Literatura

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Recife, 16 de maio de 2022

BANCA EXAMINADORA

_____

Profa. Dra. Simone Cristiane dos Santos (Orientador)

UNIVERSIDADE FEDERAL DE PERNAMBUCO

_____

Prof. Dr. Vinícius Cardoso Garcia (2º membro da banca)

UNIVERSIDADE FEDERAL DE PERNAMBUCO

Dedico este trabalho à Universidade Federal de Pernambuco, dela é toda a iniciativa.

AGRADECIMENTOS

Agradeço a Deus pelo seu incessante trabalho, misericórdia, amor e filho. Agradeço a professora Simone Cristiane dos Santos, pela sua orientação, compreensão e ensino. Os professores da Universidade Federal de Pernambuco, pelo seu trabalho e universidade sem o qual não poderia ter construído as fundações do meu conteúdo acadêmico, espero ter agregado em algo na jornada da graduação. Agradeço a meu pai, José Augusto Lima de Souza e minha mãe Maria Gracinda Oliveira de Souza, pelas oportunidades, amor, orientação e cuidado. Agradeço a Camila Oliveira de Souza, minha irmã, pela sua devoção e carinho. Também ao resto da minha família, amigos, RIO e Píer vocês significam o mundo pra mim. Muito Obrigado.

"When my bird was looking at my computer monitor I thought, ‘That bird has no idea what he’s looking at.’ And yet what does the bird do? Does he panic? No, he can’t really panic, he just does the best he can. Is he able to live in a world where he’s so ignorant? Well, he doesn’t really have a choice. The bird is okay even though he doesn’t understand the world.

You’re that bird looking at the monitor, and you’re thinking to yourself, ‘I can figure this out.’ Maybe you have some bird ideas. Maybe that’s the best you can do"

(Terrence Andrew Davis)

RESUMO

A transformação digital é vista como uma necessidade para pequenos e grandes negócios se manterem relevantes no mercado a partir do uso abrangente da Tecnologia da Informação e Comunicação (TIC), e também como uma melhoria para cadeias produtivas, automação, tomada de decisão e outras atividades produtivas. Contudo, essa transformação digital não é integralmente benéfica para todo caso, já que pode causar impactos negativos em muitos aspectos sociais, ambientais e tecnológicos. Nesse contexto, a seguinte questão central de pesquisa motiva este estudo: QC -Quais os impactos das vulnerabilidades trazidas pela transformação digital nas organizações, sob as perspectivas das dimensões de pessoas, processos e tecnologia? Para responder essa questão, o método de Revisão Sistemática da Literatura (RSL) de Kitchenham foi utilizado, encontrando 69 estudos primários relacionados a esse tema. A partir da análise desses estudos, este trabalho evidencia vulnerabilidades nas organizações e possíveis riscos provenientes da transformação digital em processos, pessoas e tecnologias. Assim como também, esclarece como uma organização se torna vulnerável a eventos e atores internos e externos nesse contexto de transformação, relaciona essas vulnerabilidades aos seus incidentes mais comuns e também explora definições sobre os diversos tópicos presentes neste recorrente tema.

Palavras-chave: Transformação Digital, Vulnerabilidades, Segurança Digital.

ABSTRACT

Digital transformation is seen as a necessity for small and large businesses to remain relevant in the market from the extensive use of Information and Communications Technology (ICT), and also as an improvement for production chains, automation, decision making and other productive activities. However, this digital transformation is not entirely beneficial in all cases, as it can cause negative impacts in many social, environmental and technological aspects. In this context, the following central research question motivates this study: QC - What are the impacts of vulnerabilities brought about by the digital transformation in organizations, from the perspective of the dimensions of people, processes and technology? To answer this question, Kitchenham's method of Sistematic Review of Literature(RSL) was used, finding 69 primary studies related to this topic. from analysis of these studies, This work highlights vulnerabilities in organizations and possible risks arising from digital transformation in people, processes and technologies. It also clarifies how an organization becomes vulnerable to internal and external events and actors in this transformation context, relates these vulnerabilities to the most common incidents and also explores definitions about the various topics present in this applicant theme.

Keywords: Digital Transformation, Vulnerabilities, Digital Security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
TD	Transformação Digital
RSL	Revisão Sistemática da Literatura
CS	Cadeia de Suprimentos
IA	Inteligência Artificial
IEEE	Institute of Electrical and Electronic Engineers
SD	Science Direct

SUMÁRIO

1 **INTRODUÇÃO**

Essa introdução tem a motivação de expor as principais razões pelas quais essa pesquisa foi realizada, apresentar o seu o Contexto 1.1, Motivação 1.2, Justificativa 1.3 e Objetivos de pesquisa 1.4. Também justifica a escolha do uso da RSL como método principal de pesquisa e descreve a questão central de pesquisa e seus objetivos.

1.1 CONTEXTO

O termo *"Transformação Digital"* (TD), se tornou muito popular na última década, com a necessidade da digitalização dos processos das empresas e organizações se estabelecendo cada vez mais no imaginário das pessoas. O interesse pelo termo vem crescendo vertiginosamente e se encontra em pico de popularidade nas buscas do Google (GOOGLE, 2022). A transformação digital vem à tona não apenas pelo intenso avanço da tecnologia, mas pelo novo contexto de globalização da sociedade. A tecnologia se permeia por todas as camadas da sociedade e adentra o universo das empresas e organizações com força total.

Apesar de muito se falar sobre o tema, existem diferenças sobre o que as pessoas pensam a respeito do que é de fato a transformação digital. Isso se deve às diferentes fontes de onde receberam a informação, e as opiniões socialmente pré-estabelecidas sobre o tema. Essas opiniões são formadas a partir do conhecimento sobre TD vindos da história da computação, onde as empresas passavam por dilemas de "mudar ou morrer" que ocorre até hoje (JONES, HUTCHESON e CAMBA, 2021).

A pandemia do COVID 19 criou um cenário onde a transformação digital se tornou necessária para a sobrevivência das empresas. Para que a continuidade do trabalho se desse preservando a saúde dos funcionários e clientes, vários processos precisaram passar por transformações. O trabalho remoto se tornou uma realidade não só para as empresas do ramo de tecnologia, mas também passou a permear a muitos dos outros setores.

Essa transformação pode trazer inúmeros benefícios para uma empresa. Entre elas, podemos citar uma melhor experiência, e consequentemente, melhor engajamento dos clientes, simplificação de operações gerais, inovação nos modelos de negócios, além de benefícios financeiros de longo prazo (YAMASHIRO e MANTOVANI, 2021). Porém,

apesar dos benefícios, essas mudanças também podem trazer riscos e expor as empresas a diversas vulnerabilidades. Algumas dessas vulnerabilidades são mais fáceis de serem percebidas, como por exemplo a possibilidade de crime cibernético, perda de capital e atrito dos funcionários, outras porém, são mais sutis e não muito tratadas como problemas na infraestrutura, falta de conhecimento e complexidade dos novos processos. É nesse contexto que o presente trabalho busca contribuir para trazer luz às vulnerabilidades trazidas pela transformação digital e às consequências dessas vulnerabilidades no contexto das dimensões de Sistemas de Informações (Pessoas, Processos e Tecnologia).

1.2 MOTIVAÇÃO

A transformação digital é um processo de mudanças que traz desafios às organizações e tem se tornado um tópico amplamente divulgado pelos meios de comunicação, relacionado à procura destas organizações por acessos e engajamento. Muitas vezes, porém, a abordagem rasa de alguns artigos online podem criar diferentes compreensões do que realmente é a TD. Temos também, que a imprescindível necessidade das organizações em adotarem essas mudanças traz a inevitável exposição a vulnerabilidades diversas, desde brechas vindas de aplicações de código aberto até as diversas vulnerabilidades da rede pública, incluindo ataques de atores externos, que podem trazer risco e exposição para a organização. Assim, surge, desses pontos, a necessidade de definir claramente o que é a transformação digital e os impactos causados pelas vulnerabilidades provenientes das transformações nas pessoas, processos e tecnologias nas organizações.

Se torna importante também, retratar as vulnerabilidades vindas desses processos de transformação, para saber os impactos financeiros, taxa de sucesso da organização e como elas podem influenciar as pessoas, processos e tecnologias. É diversa a variedade de vulnerabilidades existentes no meio digital, algumas vindas de mudanças de processos empresariais, relações interpessoais e ambientais, outras, vindas da parte de tecnologias, atualizações de software, rede, hardware entre outros. Se torna então relevante analisar quais dessas vulnerabilidades são mais comuns, e como elas se relacionam com os seus incidentes. O estudo em (SKRODELIS e ROMANOVS, 2021) estima uma taxa de 70% de falha nas iniciativas de transformação nas empresas, por isso é necessário uma visão clara sobre o tema.

Sem a percepção das consequências, por vezes catastróficas, das vulnerabilidades envolvidas na TD, é improvável que sejam colocados em prática mecanismos de defesa e

alocado o capital necessário para questões de segurança digital, que muitas vezes é significativo e pode ser visto por alguns gestores puramente como um custo (CULOT *et al.*, 2019). Essa visão da segurança como um custo puro é limitada, pois já é visto que um acesso seguro, uma tecnologia confiável e uma política de proteção de dados podem ser vistos como vantagem competitiva e se tornar uma parte fundamental do que é vendido pela empresa (CULOT *et al.*, 2019).

Só com o conhecimento dos possíveis riscos e vulnerabilidades aos quais uma empresa estará exposta durante e depois da transformação digital, é possível criar um plano que vá proteger a empresa e aumentar as suas chances de ter uma TD segura e completa.

1.3 JUSTIFICATIVA

Dentro desse contexto de aumento crescente do interesse pela transformação digital das empresas e organizações, e do sentimento de urgência por essa transformação trazido pela pandemia do COVID-19, faz-se necessário esclarecer que essas mudanças trazem consigo não apenas benefícios diversos, mas também inúmeros riscos associados. Esses riscos podem acarretar em consequências graves para os processos, pessoas e tecnologias dentro de uma empresa.

Tomemos como exemplo os riscos de segurança digital, conceito esse que será tratado com detalhes no Capítulo 2 do presente trabalho. Uma pesquisa realizada no Reino Unido no ano de 2020 apontou que 390 dentre 1000 negócios analisados reportaram incidentes relacionados à segurança digital (ALAHMARI e DUNCAN, 2021). Especialistas na área sugerem que os ataques cibernéticos são uma das maiores ameaças para qualquer corporação, porém gestores de pequenas e médias empresas, SMEs, ainda não acreditam que eles podem se tornar um alvo (ALAHMARI e DUNCAN, 2021). Enquanto isso, relatórios do Reino Unido apontam que acidentes cibernéticos custam em média £13400 para SMEs (ALAHMARI e DUNCAN, 2021).

É preciso deixar claro que toda e qualquer empresa ou organização está exposta a riscos quando passa por uma transformação digital. Apenas com a clareza das possíveis consequências advindas dessas mudanças, gestores e líderes dentro dessas empresas podem traçar planos para uma TD segura e colocar em prática medidas preventivas para minimizar a sua exposição a vulnerabilidades.

Esse trabalho visa, então, contribuir com a literatura sobre o tema no que se diz respeito a enumeração e avaliação das vulnerabilidades trazidas pelo processo de TD; enumeração e evidência sobre como essas vulnerabilidades podem impactar os diferentes aspectos da sociedade, tanto o trabalho, quanto o mercado; evidências do impacto quanto às novas tecnologias vindas desse processo disruptivo contínuo e; como a avaliação se os impactos das vulnerabilidades têm referências na literatura para embasar a sua infâmia.

Para isso, o presente trabalho usa o método de Revisão Sistemática da Literatura (RSL) de Kitechenham (2004), devido à possibilidade de quantificar evidências, para explorar essas vulnerabilidades, e abordar as consequências que elas podem trazer para os processos, as pessoas e as tecnologias dentro de uma organização. A avaliação dos impactos nessas três dimensões vem da importância do tripé da gestão de processos de negócios (GPN). As pessoas fazem o trabalho, processos os ajudam a ser eficientes e a tecnologia agiliza e automatiza suas tarefas. O panorama criado por essa perspectiva coopera para uma visão mais abrangente, resultando em uma pesquisa que não apenas observa problemas técnicos de TIC mas também da aos aspectos sociais e suas vulnerabilidades para as organizações sua devida importância.

Diante disso, a questão central de pesquisa escolhida para apoiar o trabalho foi:

"QC - Quais os impactos das vulnerabilidades trazidas pela transformação digital nas organizações, sob as perspectivas das dimensões de pessoas, processos e tecnologia."

Para responder esta questão central, as seguintes questões secundárias foram definidas:

- Q1: Quais são as vulnerabilidades trazidas pela transformação digital para as organizações?
- Q2: Qual o impacto dessas vulnerabilidades nas pessoas?
- Q3: Qual o impacto dessas vulnerabilidades nos processos da organização?
- Q4: Qual o impacto dessas vulnerabilidades na tecnologia?

1.4 OBJETIVOS

Este trabalho tem como objetivos:

- A realização de uma revisão sistemática da literatura sobre a transformação digital e suas implicações na vulnerabilidade das organizações;

- Elencar as vulnerabilidades trazidas pela literatura da área;
- Analisar as implicações dessas vulnerabilidades sob as perspectivas das três dimensões de Sistemas de Informação (Pessoas, Processos e Tecnologia).

Dados esses objetivos, torna-se necessário responder à pergunta central de pesquisa, se baseando na literatura existente a respeito da transformação digital e suas vulnerabilidades nas bibliotecas digitais IEEE e Science Direct.

Esse trabalho não busca desencorajar ou encorajar a transformação digital, apenas tratá-la como um processo contínuo e muitas vezes inevitável e levantando os riscos acompanhados por ela a fim de facilitar uma transformação segura e sadia, tanto para as empresas quanto para os seus funcionários.

1.5 ESTUTRURA DE TRABALHO

Para facilitar a leitura e compreensão deste trabalho, este documento foi organizado em cinco capítulos:

● Capítulo 1 – Introdução: Neste capítulo são apresentados o contexto, a motivação e a justificativa para a execução deste trabalho, além de elencar os objetivos da pesquisa e a organização do documento;

● Capítulo 2 – Referencial Teórico: Neste capítulo são trazidos os referenciais teóricos necessários para o completo entendimento do trabalho. Os tópicos aqui apresentados falam sobre a Revisão Sistemática da Literatura, a Transformação Digital e a Segurança Digital. Também são trazidos o conceito de Vulnerabilidades Digitais e uma sessão sobre os Trabalhos Relacionados;

● Capítulo 3 – Metodologia: O capítulo 3 descreve a metodologia utilizada, a partir do método de Revisão Sistemática da Literatura (RSL). São apresentados a caracterização e as etapas de pesquisa, o protocolo de busca, e a forma como foi executada a avaliação da qualidade dos artigos;

● Capítulo 4 – Resultados e discussão: Neste capítulo são apresentados os resultados da RSL e as discussões trazidas a partir dos artigos analisados. As questões de pesquisa também são comentadas nesse capítulo;

● Capítulo 5 – Conclusão: Neste capítulo, são apresentadas a conclusão do trabalho, as limitações da pesquisa e os trabalhos futuros.

2 **REFERENCIAL TEÓRICO**

Este capítulo expõe as definições dos principais temas abordados com o intuito de esclarecer seus significados no contexto desse trabalho. Os temas expostos são, 2.1 Revisão sistemática da literatura, 2.2 Transformação digital, 2.3 Segurança digital e 2.4 Vulnerabilidades digitais. Descreve também em 2.5 Trabalhos relacionados, artigos sobre esses temas para dar mais clareza ao lugar dessa revisão na literatura.

2.1 REVISÃO SISTEMÁTICA DA LITERATURA

De acordo com (KITCHENHAM, 2004), uma revisão sistemática da literatura é um meio para identificar, avaliar e interpretar todas as pesquisas disponíveis relevantes para uma pergunta de pesquisa específica, área de estudo ou fenômeno de interesse. Estudos individuais contribuindo para uma revisão sistemática são chamados estudos primários, assim, uma revisão sistemática é uma forma de estudo secundário (KITCHENHAM, 2004). Essa forma sistemática de revisão tem sido amplamente utilizada para estabelecer argumentos sólidos e quantificados a respeito de pesquisas em diversas áreas de atuação e tentar esclarecer controvérsias se apoiando nos estudos de melhor qualidade sobre o assunto.

A característica sistemática auxilia a validação da confiabilidade dos artigos e as respostas propostas pelas perguntas de pesquisa dos mesmos. Visto que o método pode ser replicado e posto à prova, essa qualidade assegura que a verificação da fidedignidade do conteúdo dos artefatos ao estado da arte da literatura pode ser feita facilmente, e artigos de baixa qualidade prontamente ignorados. A quantidade de artigos vindos de fontes e autores diferentes, também corrobora para evitar qualquer viés de pesquisa, apesar de uma característica de qualquer revisão de literatura, a RSL quantifica e qualifica os artigos de maneira sistemática, removendo espaço para conclusões precipitadas. Esses pontos são também levantados no trabalho de Kitchenham (2004) quando menciona a falta de valor científico em revisões de literatura que não são completas e justas e que pesquisadores, ao realizar uma revisão sistemática da literatura devem fazer todos os esforços para identificar e relatar pesquisas que não suporta sua hipótese de pesquisa preferida, da mesma forma que identificam e relatam pesquisas que o suportam, mantendo a imparcialidade da análise.

Revisões sistemáticas começam por definir um protocolo de revisão que especifica uma pergunta de pesquisa referenciada e os métodos que serão usados para efetuá-la. Então,

baseadas numa estratégia de pesquisa propõem-se a detectar a maior quantidade de literatura relevante possível. Documentação é utilizada para que os futuros leitores possam avaliar seu rigor e completude. Para isso, são então criados critérios de exclusão e inclusão para os estudos primários em potencial, aplicando-os à informação obtida para cada estudo primário. Em seguida, são aplicados os critérios de qualidade pelo qual cada estudo é avaliado e então, a meta-análise quantitativa.

A principal desvantagem do uso da RSL é o esforço consideravelmente maior que nas revisões tradicionais, devido a sua forma estruturada. Também é necessário que o objeto de pesquisa contenha uma quantidade significativa de trabalhos primários para que a análise dos resultados seja valorizada. Para a confecção deste trabalho, as vantagens da RSL se mostraram mais significativas.

2.2 TRANSFORMAÇÃO DIGITAL

A transformação digital é um dos principais desafios enfrentados pelas empresas contemporâneas. Esse desafio consiste em perceber e reavaliar capacidades, estruturas, e culturas existentes de maneira a identificar quais tecnologias são relevantes e como elas irão atuar nos processos organizacionais e ofertas de negócio (SAARIKKO, WESTERGREN e BLOMQUIST, 2020). Esse cenário coloca as organizações em uma posição de reavaliação constante dos seus processos e produtos, tornando-as mais propensas a aquisição de novas tecnologias para manter ou aumentar a competitividade no mercado.

Existem atualmente divisões nos artefatos acadêmicos que falam sobre transformação digital, essas divisões são na maior parte das vezes sobre as diferentes definições e conceitos que estão envoltos no tema. Essa diferença se torna evidente quando existe na literatura divisão no que se diz respeito a digitalização, transformação digital e o figital, onde, em alguns casos, esses três termos são usados como substituíveis entre si. Porém, a diferença é clara entre esses termos, digitalização se refere principalmente a automação de processos de negócio, automação de operações e processo de informações, enquanto o figital, embora associado a transformação digital, é a transformação da experiência de usuário que surge da combinação dos elementos físicos e digitais e é impelido pela mudança da cultura causada pela TD (PANGARKAR e ARORA, 2022). Por outro lado, a transformação digital é uma tendência que alcança muitos domínios sociais e industriais. Edvard Tijan e Marina Jović (2021) descrevem bem o processo de transformação digital em (TIJAN e JOVIC, 2021)

"Digital transformation in the maritime transport sector", abordam que a TD pode ser definida como:

> O uso de novas tecnologias digitais para possibilitar melhorias nos negócios, ou para inovar os modelos de negócios em termos estratégicos, táticos e operacionais. (TIJAN e JOVIC, 2021)

A transformação digital também é descrita como a adoção de novas tecnologias. Como exemplo, temos a definição de (ALDABBAS, TEUFEL e TEUFEL, 2017):

> A transformação digital geralmente se refere ao processo de mudança nos negócios e na sociedade baseado na onipresença de sensores, redes e tecnologia de informação e comunicação. (ALDABBAS, TEUFEL e TEUFEL, 2017)

Nesses casos, geralmente são citadas novas tecnologias como Aprendizagem de Máquina, Blockchain, Internet das Coisas, entre outras.

Outros casos expandem um pouco mais essa definição e colocam a adoção de novas tecnologias com o propósito de um melhor aproveitamento do "digital". Esse melhor aproveitamento pode ser entendido como aumento da competitividade de mercado e lucro, otimização de processos, adequação a normas sociais do nosso dia a dia, além da comum expectativa de digitalização de processos. Temos por exemplo o caso de (PRAMANIK, KIRTANIA e PANI, 2019) que define a transformação digital como:

> O uso da tecnologia para melhorar radicalmente a performance ou o alcance dos empreendimentos. (PRAMANIK, KIRTANIA e PANI, 2019)

A maioria dos trabalhos, no entanto, já entende a transformação digital como ato contínuo de adequar processos, pessoas e tecnologias a uma nova realidade do mercado, suportada pela adoção de tecnologias diversas. Para (DIGMAYER e JAKOBS, 2019), TD representa uma mudança de pensamento e cultura das organizações em busca de inovação e de vantagens competitivas:

> A transformação digital é caracterizada pelas iniciativas digitais que uma corporação assume, a sua adoção da tecnologia e suas características corporativas que incluem a sua cultura, seu conjunto de habilidades, objetivos, políticas, e gerenciamento de risco.

Esse tipo de definição é interessante porque não restringe a TD apenas a usar uma ou outra tecnologia. Melhorar um processo com a adoção de uma tecnologia nova como a Aprendizagem de Máquina, por exemplo, pode ser bom começo para uma empresa, mas não significa que ela passou por uma transformação digital. Para isso, é preciso o envolvimento de diversas camadas do negócio e uma mudança mais profunda na organização. As diversas tecnologias disponíveis devem ser um meio de inovar e expandir a empresa, e não um fim em si mesmas.

No contexto industrial, esse tema é muitas vezes abordado como a Indústria 4.0. Muitos estudos relatam sobre o fato de estarmos passando por uma quarta revolução industrial. A primeira revolução começou com o advento da máquina a vapor. A segunda foi marcada pela descoberta e pelo aproveitamento de novas fontes de energia. A terceira começa com a eletrônica e os semicondutores e, segundos defendem alguns autores, termina com a internet e a computação. Agora uma quarta revolução industrial está em curso, que vem com o advento de tecnologias avançadas como Inteligência Artificial, Robótica, Internet das Coisas, e Computação em Nuvem. Segundo JONES, HUTCHESON e CAMBA (2021), essa nova era traz mudanças tão dramáticas que vão forçar todas as indústrias a passarem por uma transformação digital.

Entre os principais impactos e benefícios da TD que podem ser citados, tem-se a criação de valor, a eficiência operacional, uma melhor relação e, consequentemente, um melhor engajamento dos clientes, inovação nos modelos de negócios e vantagens competitivas (JONES, HUTCHESON e CAMBA, 2021). LIERE-NETHELER (2018) entrevistou 16 indivíduos de diferentes sub-indústrias da manufatura e trouxe que os dois grandes impulsionadores da TD são a melhoria de processos e a demanda dos clientes (como por exemplo, demanda por qualidade). Um terceiro motor, porém menos citado, foi a melhoria do ambiente de trabalho.

Com todos esses benefícios, é esperado que o interesse pela TD venha crescendo e causando um efeito manada, já que uma vez que uma empresa passe pelo processo de mudança e comece a colher os seus benefícios, os competidores se sintam pressionados pelos próprios clientes e funcionários para oferecer as mesmas vantagens e oportunidades.

Por fim, alguns fatores de sucesso listados por MORAKANYANE *et al.* (2020) para guiar as organizações para uma transformação digital de sucesso podem ser citados: determinar os gatilhos para a TD; cultivar uma cultura digital, desenvolver uma visão digital,

determinar os impulsionadores da TD, estabelecer uma organização digital, determinar as áreas que serão transformadas e determinar os impactos da TD.

Como citado por MORAKANYANE (2020), determinar os possíveis impactos da TD é um dos fatores determinantes para o sucesso da empreitada. E é justamente nesse ponto que o presente trabalho busca dar a sua contribuição.

2.3 SEGURANÇA DIGITAL

A transformação digital trouxe imensos benefícios para as empresas e para a sociedade como um todo. Porém, esse nível de conectividade traz riscos próprios. Segundo a International Telecommunication Union, agência das Nações Unidas, mais de 60\% da população mundial tem acesso à internet (ITU, 2022). Essa porcentagem sobe muito para os países desenvolvidos. Todos os dias, as pessoas inserem seus dados pessoais nos bancos de dados de empresas espalhadas pelo mundo. Já as empresas, ao passarem pela TD e adotarem o uso de sistemas digitais que se conectam pela intranet (rede privada) ou pela rede pública, aumentam a sua superfície de ataque e se tornam expostas a ataques cibernéticos.

Os ataques a empresas como Sony, Facebook e Yahoo foram manchetes em todo o mundo, fazendo com que a conscientização sobre segurança cibernética atingisse um nível recorde e com que as consequências dos ataques digitais ficassem mais claras para a população em geral e para outras empresas, destacando a importância da segurança digital. A segurança digital pode ser definida como as medidas para manter a confidencialidade, integridade e disponibilidade de sistemas de informação e dados. O estudo em (TAM, RAO e HALL, 2021) corrobora também com a definição um pouco mais técnica do ISO/IEC 27032:2012, que define o termo "Cybersecurity" como "a preservação da confidencialidade, integridade e a disponibilidade de informação em ambientes complexos provenientes das interações interpessoais, software e serviços na internet usando dispositivos tecnológicos e redes conectadas (LEE, 2021)."

O custo médio de crimes virtuais para uma organização cresceu de 1.4 milhões de dólares em 2015 para 13 milhões de dólares em 2020 (LEE, 2021). Esse valor é menor para SMEs, o que não significa que ele não exista. De acordo com ROMERO (2019), riscos digitais incluem falha de tecnologias, demonstrando que todas as empresas participantes do processo de TD estão suscetíveis a riscos digitais, isso porque o desenvolvimento da TIC chegou em um ponto onde ela se torna a base para essas indústrias. Esse tipo de dependência

tecnológica apresenta riscos que devem ser atacados pela introdução de técnicas de segurança apropriadas (SKRODELIS e ROMANOVS, 2021).

É possível ver hoje em dia a imensa demanda por dados cada vez mais sensíveis, o que cria uma grande necessidade de investimento em segurança, sendo esses muitas vezes os produtos finais das organizações. O gasto anual mundial de Cibersegurança cresceu em 64\% de 75.6 bilhões de dólares em 2015 para 124 bilhões em 2020 (LEE, 2021). Esse gasto se torna necessário porque os impactos causados pela perda de dados afetam diversas áreas, como marketing, pessoas, processos e finanças. Empresas com nomes manchados por falta de segurança, são menos propícias para serem escolhidas para processamento de informações sensíveis, usuários também são mais discretos ao cadastrar dados pessoais. A melhora na segurança digital leva a níveis mais altos de confiança de clientes e mais oportunidades de receita (LEE, 2021).

Adicionando a sua importância, é conhecido também que criminosos não só roubam dados, mas também interrompem operações e serviços. Projetos de ETL e BI podem também ser interrompidos ou permanentemente desligados por problemas de segurança, gerando custo aos proprietários ou terceiros. Esses são projetos de processamento de dados que utilizam extração, carregamentos, transformações e processamentos para gerar informações relevantes ao processo decisório. Brechas de segurança em quaisquer das etapas desses processos, sejam dashboards, carregamentos ou processamento de dados podem gerar multas e custos altíssimos para a organização. É comum que nesses processos aplicações de código aberto sejam utilizadas, essas aplicações não garantem proteção de dados absoluta, sendo o código público, maior a chance de uma falha ser reconhecida. Também, a grande quantidade de usuários da mesma aplicação, torna a possível brecha ainda mais desejada.

Os ataques cibernéticos citados são ataques propositais de criminosos que visam ganhar acesso a informações privilegiadas, dados pessoais de clientes ou ainda tomar o controle de algum computador ou dispositivo eletrônico a fim de interromper ou alterar o funcionamento do mesmo. Esses ataques também podem ser chamados ao longo do texto de ataques virtuais ou digitais e eles podem causar danos imensos ao patrimônio, à imagem de uma empresa e aos processos de uma empresa. Os criminosos dessa área são conhecidos como hackers. Alguns dos tipos mais comuns de ataques virtuais são citados abaixo (HUMAYUN et al., 2020).

- **Malware**: Nesse tipo de ataque, um hacker pode implantar um programa malicioso para conseguir acesso não autorizado a um sistema privado. Os famosos "vírus" de computador são um exemplo de malware.
- **Denial of Service, DoS**: Esse ataque tem a intenção de fazer com que uma máquina ou um recurso da rede se torne inacessível aos seus usuários. É um evento que enfraquece a capacidade da rede de funcionar normalmente. Geralmente, são enviados uma grande quantidade de acessos simultâneos, quantidade essa maior do que o sistema é capaz de processar, fazendo com que ele saia do ar.
- **Phishing**: O ataque de phishing foca nos usuários de um sistema e usa de técnicas de engenharia social para enganar os usuários e ter acesso a dados confidenciais. Um exemplo clássico são e-mails que fingem ser de determinada empresa e pedem para os usuários fornecerem seus dados pessoais.
- **Ransomware**: Nesse tipo de ataque, o hacker toma posse dos dados de uma empresa com o intuito de pedir resgate para que a empresa possa reavê-los. Isso pode acontecer sem mover ou deletar os dados, apenas criptografando-os e exigindo um pagamento em troca da chave para a descriptografia.
- **Man-in-the-middle:** Quando um terceiro, não autorizado, ganha controle de um canal de comunicação de forma secreta, podendo interromper, manipular ou até substituir o tráfego normal de dados

As técnicas de segurança digitais visam então a proteção do perímetro organizacional, ou seja, a proteção da sua rede contra o acesso não autorizado. Esse não é, porém, o seu único propósito. Há muito se reconhece que a segurança cibernética é tão robusta quanto seu elo mais fraco, e, com os avanços atuais em segurança digital, esse elo mais fraco dentro de uma empresa de TI tem constantemente sido seus próprios funcionários (SIMMONDS, 2018). Portanto, é essencial não só proteger a empresa de ameaças externas, mas também definir estratégias que visem proteger os seus dados, processos e sistemas de erros internos ou de operações equivocadas dos seus usuários.

2.4 VULNERABILIDADES DIGITAIS

O instituto nacional de padrões e tecnologia americano (NIST) define vulnerabilidades digitais como *"um bug ou fraqueza em um processo de sistema de segurança, design,*

implementação ou controle interno que pode levar a brechas de segurança ou violação de uma política de sistema de segurança".

Essas vulnerabilidades podem vir de um número diverso de lugares, sistema de segurança das dependências físicas da organização, sistemas de internet internos e externos, formas como os dados são tratados dentro da organização ou políticas de segurança mal elaboradas. Essas vulnerabilidades podem ser exploradas por ameaças dentro e fora da organização, desde pessoal interno mal intencionado até sistemas inteligentes projetados para causar dano.

Ciberataques citados na Seção 2.3 tais como vírus, ransomware, esquemas de phishing, spam, ataques DoS, análise de tráfego, são algumas ameaças que exploram essas vulnerabilidades e são bastante conhecidas.

Essas e outras vulnerabilidades podem vir a aparecer do processo de transformação digital. O processo de adotar novas tecnologias, sem conhecer as repercussões de segurança da sua implementação, cria a possibilidade da exploração sem a percepção do risco em potencial. Isso cria um cenário perigoso para as corporações que adotam essa prática sem as precauções necessárias.

2.5 TRABALHOS RELACIONADOS

Outros trabalhos encontrados durante a análise da literatura, se relacionam com esse no que se refere à transformação digital e segurança. O estudo "Past, present, and future barriers to digital transformation in manufacturing: A review" (JONES, HUTCHESON e CAMBA, 2021) descreve bem os motivos pela qual a transformação digital deve ser vista como um processo contínuo em detrimento a uma única instância de automação. Este é um artigo de qualidade que consegue configurar bem o tom do estado da arte sobre TD e manufatura. Esse artigo também discute como o COVID influenciou a indústria numa nova onda de transformação, na qual as empresas de manufatura impelidas pelas forças dentro e fora da organização não tiveram escolha senão, mais uma vez, se adaptar ou sofrer as consequências. Define também as barreiras da transformação digital na literatura, declarando que as maiores barreiras dentro da manufatura percebidas pelos líderes giram em torno de financiais, logísticas e componentes técnicos do processo de transformação. E, finalmente,

define TD de maneira satisfatória, mostrando as muitas diferentes definições em diferentes trabalhos e que o sucesso organizacional não é inerente ao seu comprometimento à TD.

O estudo “Digital transformation risk management in forensic science laboratories” (CASEY e SOUVIGNET, 2020) se relaciona com este nos aspectos de segurança e transformação digital. Este estudo é uma pesquisa que demonstra como as vulnerabilidades trazidas pela transformação digital podem ser prejudiciais. No caso específico de laboratórios forenses, os autores definem riscos na Rretenção de dados, Integridade da evidência, Rastreabilidade digital, Problemas de sistemas de computadores e Armadilhas da automação. Esse trabalho demonstra a presença de artefatos na literatura que tratam das vulnerabilidades da TD em setores específicos, demonstrando a importância e validade do tópico. Além disso, mostra que a análise forense digital pode revelar fraquezas em laboratórios de operação forense, e especialistas em forense digital podem melhorar esses quadros.

3 METODOLOGIA

Este capítulo tem a motivação de expor a metodologia utilizada pela pesquisa, apresentar a Caracterização e etapas de pesquisa 3.1, seu Protocolo de busca 3.2 e sua Avaliação de qualidade 3.3 demonstrando o processo que foi usado para a coleta, filtro e análise de dados.

3.1 CARACTERIZAÇÃO E ETAPAS DE PESQUISA

Esse trabalho se iniciou com disciplina de Tendências e Desafios de Sistemas de Informação da UFPE. Onde, Durante seu desenvolvimento, a ideia principal desse artigo nasceu e foi posta em prática, resultando em uma prequela. O artigo intitulado "The inevitability of Digital Transformation and its impact on organizational processes, people and technology" teve autoria de Tiago Oliveira de Souza, João Pedro Lira dos Santos, Ricardo Ebbers Carneiro Leão e Victor Hugo Rodrigues da Cunha, sem os quais esse artefato não poderia ter o nível no qual se encontra.

O método utilizado para a coleta de artefatos para basear o trabalho atual e suas conclusões foi uma análise sistemática extensiva da literatura sobre o tema de transformação digital, que tem ganhado força e se mostrado um tema de relevância duradoura, e que também demonstra ganhar ainda mais tração nesses tempos de disrupção tecnológica. Foi selecionado um grupo seleto de bases de dados acadêmicas, IEEE, ScienceDirect, Scopus e ACM, essas quatro bibliotecas virtuais foram escolhidas por serem fontes renomadas que possuem a literatura acadêmica de mais alta qualidade no mundo. Porém devido ao escopo, apenas as bibliotecas IEEE e ScienceDirect foram utilizadas. Os motivos para a escolha dessas duas bases como foco principal da RSL foram a facilidade de busca, tamanho do acervo e familiaridade.

Na primeira fase da RSL, foram selecionadas palavras chaves que sumarizam o tema central da pesquisa. A partir dessas palavras chaves, e, levando em consideração a relação lógica entre elas, foi construída uma expressão de busca para serem usadas em ferramentas automatizadas das bases anteriormente mencionadas. Essa expressão (apresentada na Seção 3.2 – Protocolo de busca) foi então aplicada na busca automática avançada das bases de pesquisa escolhidas e geraram uma lista de possíveis artigos de interesse para o trabalho.

Durante a segunda fase, os estudos foram selecionados manualmente, após um processo de filtragem utilizando critérios específicos de inclusão e exclusão, a fim de restringir os estudos analisados àqueles dentro do escopo de interesse desta pesquisa, questão central e questões secundárias (definidas no Capítulo 1).

Os seguintes critérios de inclusão foram aplicados durante a segunda fase da RSL:

- Artigos do tipo Journal/Periodicals ou Conference papers/Proceeding;
- Artigos que abordam vulnerabilidades geradas a partir de algum tipo de transformação digital;
- Artigos completos;
- Artigos em inglês;
- Artigos entre o período de 2017 e 2021 (últimos 5 anos).

Os seguintes critérios de exclusão foram aplicados aos mesmos artigos:

- Artigos duplicados;
- Artigos secundários;
- Artigos com menos de 4 páginas;
- Artigos que fogem ao tema principal;
- Artigos fora do período estabelecido.

Numa etapa posterior, que vamos chamar de terceira fase, os artigos que continuaram como candidatos para a RSL depois dos filtros de inclusão e exclusão passaram por ainda mais um filtro: o filtro da qualidade. Os seguintes critérios foram utilizados para a análise qualitativa dos artigos:

- Contexto claro;
- Metodologia bem definida;
- Aplicação prática;
- Discussões relevantes e consistentes;
- Limitações e ameaças da pesquisa comentadas.

Os artigos com notas iguais ou superior a 50\% da maior nota na análise da qualidade passaram para a quarta fase, onde foi adotado mais um filtro, agora de acordo com o critério da responsividade. Nessa quarta fase, foi avaliado se os artigos respondiam ou não as

perguntas de pesquisa propostas, tendo as seguintes possíveis notas: "0 - Não responde", "0.5 - Responde parcialmente" e "1 - Responde totalmente". É importante ressaltar que o raciocínio utilizado para dizer que um artigo responde totalmente às perguntas de pesquisa não depende necessariamente da quantidade de perguntas que ele responde, mas também da profundidade e qualidade da resposta. Um artigo que só responde uma pergunta, mas que o faz de forma completa e satisfatória pode receber uma nota maior do que um artigo que menciona brevemente todas as respostas.

Os artigos que passaram no critério de responsividade foram utilizados para a fase de coleta de evidências e posterior análise e síntese de dados, retratados no Capítulo 4 do presente trabalho.

3.2 PROTOCOLO DE BUSCA

As fontes escolhidas foram as seguintes livrarias digitais renomadas:

- Science Direct (Site: http://www.sciencedirect.com/)
- IEEE (Site: www.ieee.org/ieeexplore)

Após a escolha das fontes de pesquisa, houve um longo processo de decisão visando analisar quais palavras chave mais se encaixam com o tema de pesquisa e as perguntas relevantes a serem respondidas ao longo do processo de análise da literatura. Cinco palavras chave foram escolhidas como os principais temas com mais relevância entre si e o tema do trabalho:

- Digital Transformation;
- Organizations;
- Vulnerability;
- Threats;
- Risks;

A expressão "Transformação Digital" foi escolhida por ser o tema principal do trabalho, ela foi utilizada para filtrar apenas artigos que contivessem menções a esse processo de reavaliação.

"Vulnerabilidades" e os seus devidos sinônimos foram também escolhidos com alta prioridade, devido ao tema do trabalho ter relação direta com a transformação digital e como ela afeta as organizações.

Em seguida, a palavra "organização" também foi escolhida, visto que o trabalho tem como objetivo entender as vulnerabilidades no contexto das organizações.

O resultado final do termo de busca foi:

("Digital transformation") ***AND*** *(Organization* ***OR*** *Company* ***OR*** *Organizations* ***OR*** *Companies)* ***AND*** *(Vulnerability* ***OR*** *Vulnerabilities* ***OR*** *Threats* ***OR*** *Risks)*

Esse termo de busca foi utilizado nas bases escolhidas com posterior aplicação de um filtro para selecionar apenas artigos relativos ao período entre 2017 e 2021.

3.3 AVALIAÇÃO DE QUALIDADE

Como já mencionado anteriormente, os seguintes critérios foram utilizados para a avaliação da qualidade de cada artigo foram:

- Contexto claro;
- Metodologia bem definida;
- Aplicação prática;
- Discussões relevantes e consistentes;
- Limitações e ameaças da pesquisa comentadas.

Para cada um desses critérios, foi dada uma nota que podia ser "0 - Não atende o critério", "0.5 - Atende parcialmente" ou "1 - Atende o critério". Isso faz com que a nota máxima possível para um artigo seja igual a 5. Como critério de corte de qualidade, o artigo precisa receber uma nota igual ou superior a metade da nota máxima (2.5) para passar para a próxima fase.

Por essa ser a fase mais subjetiva da RSL, alguns cuidados especiais foram tomados. Primeiramente, os artigos foram avaliados em lotes referentes ao número de páginas (todos os artigos de 4 páginas, depois de 5, etc.) para evitar comparações inconscientes entre a qualidade de artigos feitos para propósitos diferentes em publicações com critérios diferentes de tamanho.

Além disso, visto que alguns critérios de qualidade são bastante subjetivos, cada um deles, serão comentados para deixar clara a linha de raciocínio por trás das notas atribuídas e elencar alguns pontos que ajudaram a balizar a avaliação. No critério “Contexto claro”, foi levada em consideração principalmente a introdução do trabalho, o quanto ele consegue fazer o leitor entender o contexto em questão e o problema que o artigo está tentando tratar.

Perguntas de pesquisa são bons sinais de que o autor tem um problema claro em mente. Apesar de não estar explícito no tópico, artigos com um nível de inglês ou escrita ruins, que atrapalham a compreensão do tema foram penalizados.

Na parte de "Metodologia bem definida", foi avaliado se o artigo se preocupou em definir e passar a metodologia da pesquisa para o leitor. Seções específicas e bem estruturadas de metodologia, mesmo que curtas em artigos mais concisos, são bem vistas. O critério "Aplicação prática" levou em conta se o artigo criou algo que pode ser aplicado ou se levanta pontos ou sugestões práticas a serem aplicadas. Alguns artigos elencaram passos e utilizam gráficos/diagramas, o que torna a aplicação mais clara e didática para o leitor.

"Discussão relevante e consistente" é com certeza o critério mais subjetivo de todos. O julgamento da relevância de uma discussão é complexo e o que pode ser relevante para alguns, pode não ser relevante para outros. Apesar disso, uma coisa que pode balizar a avaliação é se o artigo é consistente enquanto discorre sobre o problema, se a sua pesquisa, referencial teórico e trabalhos citados tem a ver com o seu tema proposto e se o tema é tratado de forma séria e científica. Por fim, as "Limitações e ameaças" muitas vezes são citadas de forma bem breve na conclusão, quando o são. Artigos que trazem sessões específicas e tratam as limitações de forma séria e objetiva receberam mais pontos.

4 RESULTADOS E DISCUSSÕES

Este capítulo tem a motivação de expor os Dados gerais 4.1, os principais resultados, responder as perguntas de pesquisa por meio da RSL e apresentar discussões embasadas nos estudos primários. Responde: Q1 - Quais as vulnerabilidades mais comuns 4.2, Q2 - Qual o impacto dessas vulnerabilidades nas pessoas 4.3, Q3 - Como essa vulnerabilidades impactam os processos organizacionais 4.4 e Q4 - Qual o impacto dessas vulnerabilidades na tecnologia.

4.1 DADOS GERAIS

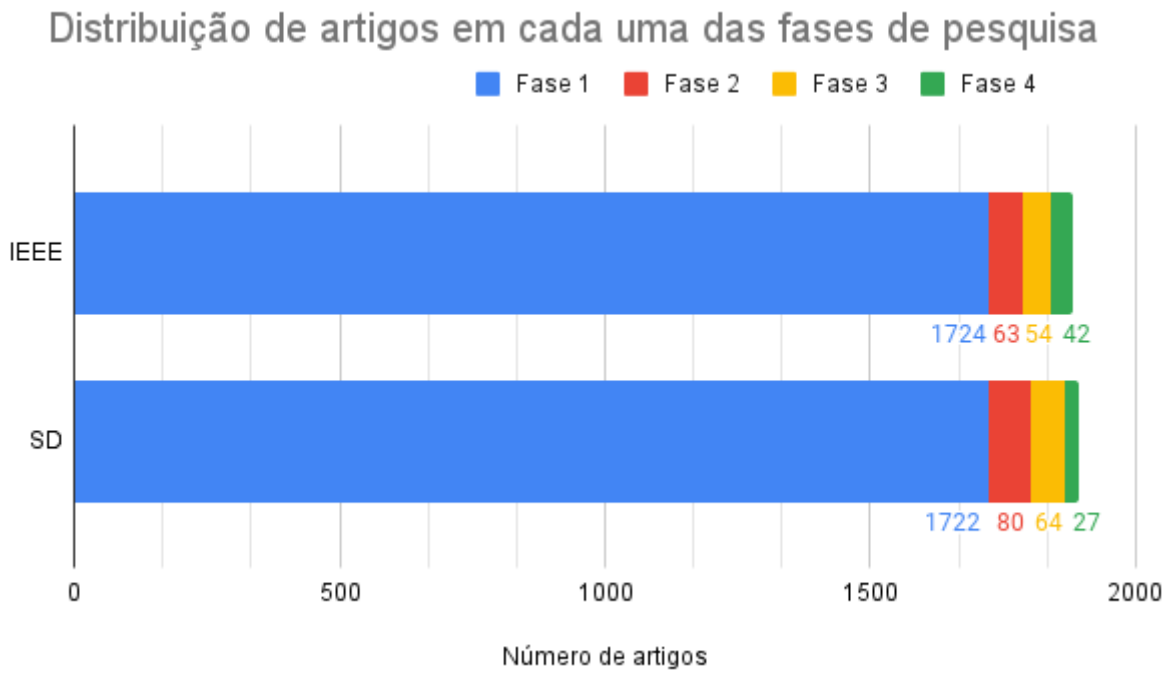
Na primeira fase da RSL, após aplicar o protocolo de busca, foram coletados um total de 1724 artigos na base IEEE e 1722 artigos na base Science Direct, SD. Após aplicar os primeiros critérios de exclusão e inclusão restaram 63 artigos na base IEEE e 80 na base SD. Em seguida, os critérios de qualidade foram aplicados, o que resultou em 54 trabalhos para o IEEE e 64 para SD. A última fase, referente ao critério de responsividade quanto às perguntas de pesquisa, resultou em um total de 42 e 27 artigos selecionados nas bases IEEE e SD, respectivamente, totalizando 69 estudos primários para a análise. Uma lista com todos os artigos selecionados após a fase 4 se encontra no Apêndice A. Os dados citados acima podem ser visualizados na Figura 1.

Etapas:

- **Fase 1**: Busca automática;
- **Fase 2**: Critérios de inclusão e exclusão;
- **Fase 3**: Critérios de qualidade;
- **Fase 4**: Critério de responsividade.
-

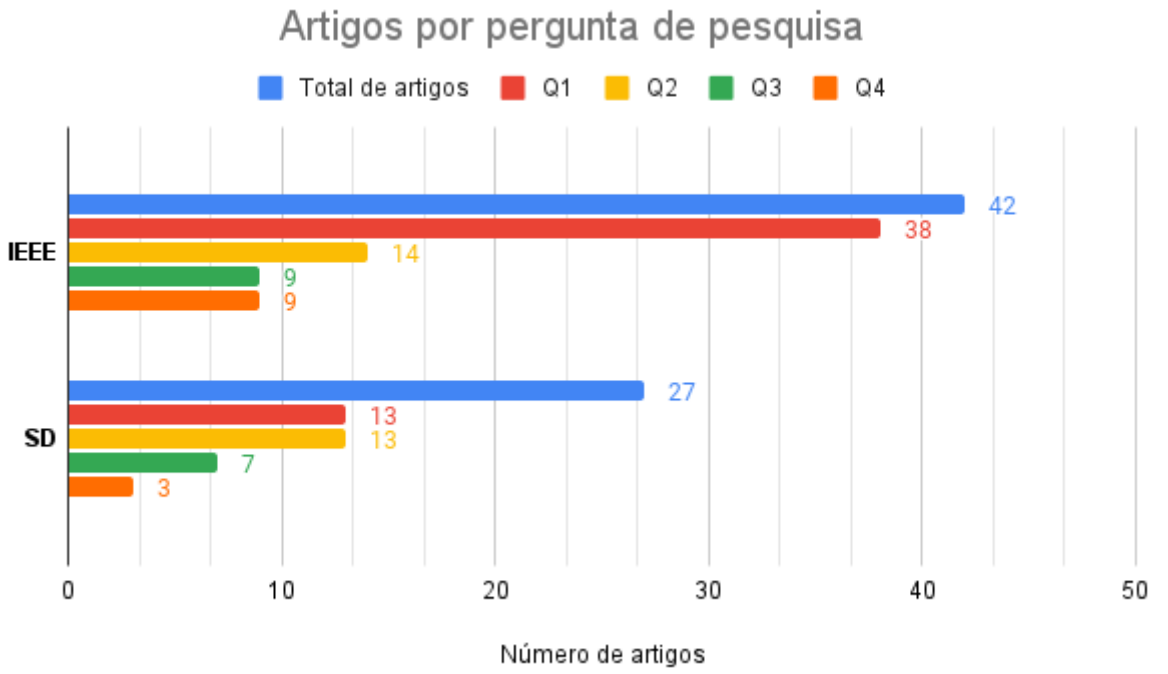
A Figura 2 mostra a quantidade de artigos selecionados por base para a análise da RSL e a quantidade de artigos que respondeu a cada pergunta de pesquisa. Vemos que a pergunta Q1 foi a mais abordada, enquanto a Q4 só foi tratada por 12 artigos no total. Para facilitar o entendimento da imagem, relembraremos nesse momento as nossas perguntas de pesquisa central e secundárias:

Figura 1 - Distribuição de artigos por base em cada uma das fases de pesquisa



Fonte: O autor (2022)

Figura 2 - Distribuição de artigos por base em cada uma das perguntas de pesquisa



Fonte: O autor (2022)

- **QC**: Quais os impactos das vulnerabilidades trazidas pela transformação digital nas organizações, sob as perspectivas das dimensões de Pessoas, Processos e Tecnologia?
- **Q1**: Quais são as vulnerabilidades trazidas pela transformação digital para as organizações?
- **Q2**: Qual o impacto dessas vulnerabilidades nas pessoas?
- **Q3**: Qual o impacto dessas vulnerabilidades nos processos da organização?
- **Q4**: Qual o impacto dessas vulnerabilidades na tecnologia?

Pode-se ainda ter uma noção do aumento do interesse pelo tema pesquisado observando a quantidade de artigos publicados em cada ano, de acordo com a Figura 3.

Destes artigos publicados, na IEEE, a maior parte foi publicada em conferências, que na SD, a maior parte foi publicada em revistas. A Figura 4 aborda essa diferença.

Figura 3 - Distribuição de artigos por base em cada ano

Fonte: O autor (2022)

Figura 4 - Distribuição de artigos por base em cada tipo de publicação

Fonte: O autor (2022)

As subseções seguintes discutirão os resultados da análise dos estudos para cada uma das questões secundárias.

4.2 Q1 – QUAIS AS VULNERABILIDADES MAIS COMUNS

A nossa primeira pergunta de pesquisa visa entender quais são as vulnerabilidades mais comuns trazidas pela transformação digital a uma empresa ou organização. Dos artigos selecionados para a RSL, 51 mencionaram algum tipo de vulnerabilidade, alguns com maior nível de detalhamento que outros. As vulnerabilidades mais citadas serão trazidas para o texto, com trechos dos artigos selecionados, como forma de evidência. Porém, as menos citadas, ou menos explicadas, serão ainda assim mencionadas na Tabela 1, que traz uma lista com todas as vulnerabilidades encontradas e os artigos que a elas se referem.

A vulnerabilidade mais comum, abordada em 9 dos artigos da RSL, são as próprias pessoas dentro da organização. O fator humano é abordado extensivamente nas pesquisas, trazendo possibilidades de erro não intencional, negligência ou sabotagem intencional. Nesses casos, os próprios funcionários são a porta de entrada para atores externos. Esses casos podem acontecer de diferentes maneiras, tais como quando processos manuais de segurança que concedem autorizações a indivíduos são feitos de maneira indevida, permitindo a um usuário acessos e privilégios que deveriam ser apenas designados para funcionários chave. Esse tipo de ocorrência pode causar, entre muitas outras consequências, perda de informações,

vazamento de dados sensíveis, mudança indevida de dados, processos de sistema sendo alterados e sabotagem.

Algumas evidências comprovam esses resultados:

"Massive numbers of cybersecurity incidents are in some way related to human mistake, despite the organizations implementing many controls to reduce this. This is despite the fact that many practical cases prove that an organization can have any suitable technological solution or properly documented policy, only a person's intentional or negligent actions can cause serious harm. [...] The motivation of the person who committed the incident can be different. Without wishing to be exhaustive the leaking person can be negligent, may seek financial gain, showcasing knowledge, advancement in the ladder, exercise of power, or can be guided by sexual motivation." [EP009]

"The primary threat to companies' data security is human error. Moreover, most IT teams lack accurate visibility of this employee vulnerability, and it is further exacerbated by the remoteness of employees and the lack of adequate cybersecurity planning for teleworkers." [EP024]

Uma outra vulnerabilidade comumente tratada é a falta de conhecimento especializado. A demanda por profissionais do ramo da segurança digital é mais alta do que a oferta desses especialistas no mercado. Fora isso, o custo de um profissional especializado é alto e nem todas as empresas podem arcar com ele, principalmente SMEs. A falta de funcionários com conhecimento na área não só diminui as chances de a empresa implementar medidas de segurança apropriadas, como também influencia na sua adesão a regulações e normas, além de dificultar o treinamento dos empregados de forma geral, que sem o conhecimento apropriado ficam mais suscetíveis a erros e a golpes do tipo phishing.

Algumas evidencias corroboram com essas afirmações:

"It is well reported that small companies are increasingly becoming major targets for cyber criminals. Major reasons for this are that small companies do not have the expert security knowledge and often cannot afford to acquire expensive security solutions." [EP027]

"With the development of technology and the digitalization of supply chains, there has also been a shortage of relevant skills in employees. About 60\% of security incidents occur

due to incompetence of employees and most often unintentionally, so employee training could solve this problem." [EP020]

Em seguida, pode-se citar um fator muitas vezes chamado de “Autenticação Vulnerável”. Aqui pode-se ter tanto falhas no desenvolvimento dos mecanismos de autenticação, como falta de autenticação mútua ou permissão de tráfego de dados na fase pré-autenticação, quanto falhas por parte do usuário, como a utilização de senhas fracas ou a não utilização de autenticação de múltiplos fatores. Esse fator se tornou ainda mais relevante depois da pandemia e do aumento de casos de trabalho remoto, visto que muitos funcionários passaram a utilizar dispositivos pessoais para trabalhar, aumentando a necessidade das empresas de autenticar os dispositivos que se conectam a sua rede de forma segura.

Evidências:

“Intruders intercepting data due to improper authentication mechanisms: The companies must adopt Multi-factor authentication mechanisms for securing their critical applications. This will help keep a track of the devices on which corporate data and applications are being accessed.” [EP021]

“With the development of technology and the digitalization of supply chains, there has also been a shortage of relevant skills in employees [9]. About 60\% of security incidents occur due to incompetence of employees and most often unintentionally, so employee training could solve this problem.” [EP020]

A falta de criptografia nos dados/comunicação, bem como a criptografia fraca também são vulnerabilidades que podem ser exploradas pelos hackers e acabar deixando as empresas expostas a crimes cibernéticos. Apesar do aumento do conhecimento sobre a segurança digital e dos relatos de várias empresas mostrando danos significativos por conta de crimes digitais, muitas SMEs ainda não acreditam que podem ser alvos desses crimes e não investem em técnicas como criptografia.[EP023] Muitos ataques que visam o roubo de dados se tornariam infrutíferos se os dados obtidos estivessem criptografados.

“It is shown that only an integrated approach implying the simultaneous use of hardware, software and cryptographic means can provide reliable information protection.” [EP033]

Por fim, pode-se citar a vulnerabilidade trazida pela colaboração com terceiros. Segundo [EP020], uma empresa é tão forte quanto a empresa mais fraca na sua cadeia de parceiros. Utilizar aplicações de terceiros, contar com outras empresas para realizar o seu armazenamento de dados na nuvem, entre outros, são exemplos desse tipo de interação.

"Smaller companies are more likely to suffer from cyber-attacks because they are the weakest link in the chain. Thus, larger companies also suffer from this interconnection. It can be said that a company is as strong as a weaker company among the business partners in the chain." [EP020]

"The companies did not have their own solutions for all requirements. So, they had to rely on third party applications for various tasks like organizing virtual meetings. This exposed the company's data on third party applications which is involves tremendous amount of risk." [EP021]

Essas são apenas algumas das vulnerabilidades encontradas na literatura. Uma lista mais extensa, juntamente com as respectivas referências, pode ser encontrada na Tabela 1.

Tabela 1 – Vulnerabilidades encontradas na RSL

Vulnerabilities	**Mentions**	**References**
Unpatched legacy systems/obsolescent software	3	EP003, EP010, EP011
Obsolete technology	1	EP013
Security failures	1	EP004
Unauthorized access/ access control violations	3	EP004, EP010, EP013
Human error/negligence	9	EP004, EP009, EP014, EP017, EP024, EP028, EP029, EP035, EP061
Lack of specialized knowledge	6	EP005, EP006, EP020, EP021, EP027, EP033, EP048
Lack of employee training	2	EP021, EP024
Lack of security	2	EP021, EP044

policies/standards		
Insider and privileged misuse	2	EP009, EP017
Lack of digital culture	1	EP013
Exposure by third parties	6	EP004, EP020, EP021, EP035, EP047, EP069
Vulnerable authentication	6	EP005, EP010, EP011, EP012, EP029, EP033
Errors in source code	3	EP005, EP010, EP026
Firmware update errors	1	EP005
Complexity of DT strategy	1	EP006
Complexity of resulting system	2	EP020, EP030
Information security	2	EP006, EP044
Weak cryptography	5	EP010, EP011, EP027, EP030, EP033
Inadequate auditing	1	EP010
Hardware/Technology specific vulnerabilities	5	EP011(Communications), EP012(APIs), EP014(Cloud storage), EP018(Containers), EP036(IA)
Unavailability of backup copies	1	EP014
BYOD/Disappearance of the enterprise perimeter	3	EP021, EP024, EP034
Use of heterogeneous devices/infrastructure	3	EP021, EP024, EP031
Ethical issues	1	EP047

Essas vulnerabilidades deixam as empresas suscetíveis a diversos riscos. O risco mais citado com certeza é o de sofrer ataques cibernéticos, mas existem outros como o risco da perda de empregos, o risco de distração do seu real negócio e até, em alguns casos críticos, como por exemplo o de dispositivos médicos, o risco de perda de vidas humanas.

É importante notar que a distinção de risco e vulnerabilidade muitas vezes é sutil e artigos diferentes podem trazer o mesmo ponto como risco ou como vulnerabilidade. Na Tabela 2 abaixo, porém, foram trazidos alguns dos riscos advindos dessas vulnerabilidades.

Tabela 2 - Riscos encontrados na RSL

Risks of Digital Transformation	**Mentions**	**References**
Cyber Security Attacks	62	See Table 3
Unauthorized access to confidential information	4	EP005, EP015, EP016, EP030
Alteration of data	1	EP036
Loss of Stored Data (Cloud)	1	EP005
Termination of Cloud Services	1	EP005
Insecure or incomplete deletion of data (Cloud)	1	EP005
Supplier Linkage (risks when changing the cloud-based service provider)	2	EP005, EP022
Talent deficit	1	EP006
Hardware failure	2	EP013, EP014
Job cuts	1	EP015
Loss of life	2	EP016, EP030
Undesirable end result	2	EP006, EP013
Cost of DT	2	EP006, EP047
Distraction from business	1	EP006

Por ser o risco mais comum, a Tabela 3 trata apenas dos ataques cibernéticos e suas variações mais comuns na literatura.

Tabela 3 - Ataques encontrados na RSL

Cyber Attacks	**Mentions**	**References**
Malware	8	EP001, EP004, EP021, EP026, EP029, EP030, EP034, EP060
Ransomware	6	EP002, EP003, EP004, EP005, EP021, EP034
Phishing scams	7	EP002, EP003, EP004, EP005, EP021, EP034, EP036
Spam/Infected email	2	EP004,EP021
Denial of Service(DoS)	13	EP004, EP005, EP012, EP017, EP019, EP021, EP029, EP030, EP037, EP042, EP058, EP062, EP066
Traffic analysis	1	EP005
Node replication attack	1	EP005
Sinkhole Attack	1	EP005
Cloning Attack	1	EP005
Wormhole Attack	1	EP005
Hello Flood Attack	1	EP005
Sybil Attack	2	EP005, EP026
Structured Query language injection attacks (SQLIA)	2	EP008, EP042
Botnets	2	EP012, EP029
Man in the middle	1	EP019
General mention on cyber crime	8	EP007, EP011, EP023, EP039, EP044, EP047, EP057, EP059
Private key attacks	1	EP037
Certificate authority (CA)	1	EP037

attacks		
Replay attack	1	EP042

4.3 Q2 – QUAL O IMPACTO DESSAS VULNERABILIDADES NAS PESSOAS

Em relação às pessoas, os impactos causados por vulnerabilidades trazidas pela transformação digital são diversos e atingem um grande espectro das suas vidas. Alguns desses podem ser privacidade, requerimentos profissionais, responsabilidades legais, saúde, segurança, etc. As esferas da privacidade e responsabilidades legais, sendo populares, amplamente discutidas e tendo impactos comumente conhecidos a seu respeito, se tornam componentes chaves dos quais discursar.

O impacto das vulnerabilidades que podem permitir acesso de dados a terceiros não apenas acendem um alarme para a segurança jurídica da organização, como influenciam também as pessoas envolvidas dentro e fora da organização. Em relação às pessoas de dentro da organização, um desses impactos é a adaptação a novas políticas e diretrizes de segurança. Medidas de segurança cibernética devem ser criadas para minimizar as chances de acidentes, reportar casos confirmados de brechas de segurança e mitigar os danos. Essas medidas afetam diretamente os funcionários. No caso da prevenção de Phishing, por exemplo, cada um dos emails externos na caixa de entrada do funcionário devem ser filtrados e avaliados por ele. Essa mudança de comportamento para acatar com as diretrizes de segurança esperadas pode não ocorrer, havendo a possibilidade do colaborador enxergar essa política como uma barreira para efetuar a sua atividade ou que não é justo ter que cumprir com essa política.

Evidências:

"Several studies on cybersecurity (Han, Kim, & Kim, 2017; Ifinedo, 2012, 2014) discovered that security policies do not always work effectively for employees. Some employees do not pay attention to their organization's information security policies, and others tend to underestimate information security risks even though these employees receive a written security policy and instructions. Individuals who have been exposed to the adequate level of information security training from their companies do not necessarily exhibit greater levels of cybersecurity behavior (Ng & Xu, 2007). As more and more organizations become increasingly concerned about the cyber risks in the workplace and have invested a huge

amount of resources to tackle this issue, they are expecting a positive return on their investment." [EP052]

"Teleworkers could ignore the policy when they feel that the restriction from BYOD policy will cause them to lose their freedom at work, and also ignore or resist the BYOD policy when the policy causes them not to work efficiently and effectively.

Teleworkers who do not know IT user's roles, may experience fear, anxiety, uncertainty, confusion, and lower self-efficacy. If an employee is facing an unclear or unfamiliar with identified threat or vulnerability will affect them to comply with a policy." [EP024]

Fora da organização, outro impacto advindo da exploração dessas vulnerabilidades é o vazamento de dados confidenciais e a preocupação com a privacidade de forma geral. A literatura mostra que vazamento de dados pode impactar indivíduos que tiveram suas informações publicadas, como também indivíduos responsáveis pelo incidente. O GDPR (regulamento geral da proteção de dados), testifica da necessidade de regulamentações da forma que empresas lidam com dados, trazendo a proteção de dados como um direito fundamental. É conhecido que os riscos à segurança de dados podem afetar a sociedade, mas as preocupações com possíveis incidentes variam entre indivíduos.

Evidências:

"This finding added up to the conclusion of his 2013 paper that the valuation of privacy is circumstantial and depends on the individual perception of how much he or she loses with the unauthorized disclosure. That perception is reinforced by his 2004 article, where he shared the understanding that:

'Privacy means different things to different people, including the scholars who study it, and raises different concerns at different levels. Hence 'protecting privacy' is a vague concept. Not only different parties might have opposite interests and views about the amount of information to disclose during a certain transaction, but also the same individual might face trade-offs between her need to reveal and her need to conceal different types of personal information.'" [EP063]

"There are various kinds of privacy risks involved, some of these risks include – collection of sensitive information, like accurate geolocation, financial account number,

issues related to healthcare like physical conditions over time, health habits. In fact, an existing smartphone sensor can be used to predict a user's mood, personality type, smoking habits, stress level, types of physical activities, sleep pattern. Such kind of critical information can be used in an unauthorized way if not properly handled. Some companies may also use such information for making crucial employment decisions, for insurance and for selling credit cards. Some insurance companies also use the driving habits of a person in order to set the insurance rate." [EP029]

O impacto na cultura organizacional também é um fator comentado nos artigos selecionados. Dentro desse tema, vemos que a transformação digital traz a necessidade de uma mudança de pensamento na liderança da empresa. A competência dessa liderança em lidar com as constantes mudanças e a sua capacidade para entender a tecnologia e conhecer as suas consequências adversas é um fator crítico para o sucesso da manutenção da transformação digital. O risco da adoção de novas tecnologias criam expectativas no trabalho e visão desses indivíduos [EP048]. Deja corrobora com essa teoria quando fala que a cibersegurança, os padrões voláteis, regras, princípios e as dúvidas decisórias, tornam a gerência da informação um verdadeiro desafio [EP045].

Evidências:

"It is not without significance that people face obstacles in information management. Theodoros Evgeniou and Phillip Cartwright distinguished three types of obstacles: 1) behavioral, 2) process and 3) organizational (Evgeniou \& Cartwright, 2005). These obstacles and the problems involved in information management systems at universities, which can include issues with cybersecurity, changing standards, rules, and principles, as well as doubts in terms of decision-making, make information management a real challenge (Musti, 2020). It also happens that the organization does not reach IT maturity, is not ready to accept the necessary changes (Turner & Stylianou, 2004), and is exposed to various adverse events (Koehler et al., 2015)." [EP045]

"Therefore, the ability of traditional organizations to cope with this change greatly depends on its people. Currently, managers often lack lucidity in regards to the various options and elements they need to take into account in their digital transformation endeavors (Hess et al., 2016). As a result, they risk failing to think about important elements of digital

transformation that could have unpredictable adverse consequences (Hess et al., 2016; Loonam et al., 2018)." [EP048]

Um caso claro de danos à integridade física das pessoas pode ser visto nas indústrias. Em um exemplo que trata de vulnerabilidades em tratamento de água com o uso de SCADA (controle supervisório e aquisição de dados), vemos que ciberataques em sistemas de tratamento podem ser perigosos. Um ataque envolvendo a operação dos componentes do tratamento de água pode resultar em super/subdosagem de produtos químicos, afetando diretamente a saúde dos consumidores daquela água.

"Unauthorized access and altering the required instructions in local processors to take control of the system, faces consequences such as overflow of sewage into public waterways, inappropriate services, water distribution or waste water collection." [EP030]

Com esse exemplo podemos ver que as consequências da vulnerabilidade cibernética não tem consequências apenas virtuais, como muitos pensam. Esse é um caso em que as consequências podem atingir a saúde e até a vida das pessoas. A Tabela \ref{tbl:impactsOnPeople} mostra os principais impactos das vulnerabilidades trazidas pela TD nas organizações, sob a perspectiva da dimensão Pessoas.

Tabela 4 - Principais impactos nas Pessoas

Impacts	**Mentions**	**References**
Adaptation to security policies and guidelines	2	EP052, EP024
Privacy concerns	2	EP063, EP029
Impact on organizational culture	2	EP045, EP048
Danger to physical integrity	1	EP030

4.4 Q3 – COMO ESSAS VULNERABILIDADES IMPACTAM OS PROCESSOS ORGANIZACIONAIS

Um dos grandes impactos vindos do processo contínuo de transformação digital encontrado durante a RSL foi nos processos de avaliação de risco das organizações, que têm

o trabalho de identificar, analisar e avaliar os riscos presentes no ambiente de trabalho. Esse aspecto impacta diretamente a gerência de risco, que é o processo de planejar, organizar, dirigir, e controlar recursos para atingir certos objetivos quando eventos inesperados, bons ou ruins, podem acontecer (HEAD, 2009).

Levando em consideração a segurança digital na administração organizacional, a necessidade de reconhecer no gerenciamento de risco toda a variedade de vulnerabilidades cibernéticas advindas da digitalização, integração, automação e sistemas conectados à rede que esse tipo de organização pode encontrar é essencial para uma administração digitalmente segura. É desta maneira que é possível encontrar medidas de mitigação, gerenciamento de segurança, segurança digital e estratégias decisórias para reduzir o risco ou aumentar a conscientização desses riscos em todos os níveis da organização.

O processo de gerência de segurança naturalmente sofre sérios impactos, a implementação de políticas de segurança da informação e estratégias organizacionais depende fortemente da administração do comportamento de segurança dos colaboradores.

Evidências:

"Additionally, the maritime cyber risk management suggested by the International Maritime Organization is also used to improve a port risk assessment process to recognize the full range of the cyber risk from digitization, integration, automation, and network-based systems that the port and data might encounter. By doing this, PAT can develop the appropriate emergency preparedness plan, mitigation measure, safety management system, cybersecurity, and strategy for reducing the cyber risk or increasing awareness of cyber risks at all levels of an organization (PAT, 2018a, PAT, 2018b, IMO, 2019a, IMO, 2019b, IMO, 2019c)." [EP051]

"The understanding of a more holistic approach toward information security management not only contributes to theory but also is important and applicable to managing employees' security behavior. A variety of technological solutions and procedures for information security have been developed in the past ten years, yet information security issues are still a great challenge to many companies and are at an intensifying level (Soomro et al., 2016). Successfully implementing information security technological solutions depends on successfully implementing information security policy and organizational strategies. In a broader sense, information security should be considered as a company's board level priority

so that cybersecurity responsibility is the commission of everyone, not just a responsibility of technical or information officers only." [EP052]

Não é só o preparo em relação a essas vulnerabilidades, processos correntes também podem ser afetados. Muitos dos impactos nos processos organizacionais vem não de uma falha no processo, mas da interrupção da operação. Ataques de DDOS e outros tipos de negação de serviço, atrapalham os processos sem a necessidade de encontrar brechas de segurança no código em si, mas na maneira que os acessos são efetuados. Processos organizacionais tem que não só se adequar a brechas de segurança em potencial mas também a interrupções de serviço.

Evidências:

"Such ransomware or DDoS attacks can lead to regular disruptions or complete interruption of business operations, as well as temporary or permanent loss of important information. Also, denial of service can reduce the network's ability to provide certain services." [EP005]

"As industrial machines are connected sequentially in the production line, the attacker can disrupt communication by targeting different equipment each time in order to avoid suspicion. The result of this type of attack would be devas- tating as production will stop, and it will be challenging to pinpoint the exact cause of the failure." [EP042]

A Tabela 5 mostra os principais impactos das vulnerabilidades trazidas pela TD nas organizações, sob a perspectiva da dimensão Processos.

Tabela 5 - Principais impactos nos Processos

Impacts	**Mentions**	**References**
Changes the risk assessment process	1	EP051
Creates the need for new security procedures	1	EP052
Interruption of operation	2	EP005, EP042

4.5 Q4 – QUAL O IMPACTO DESSAS VULNERABILIDADES NA TECNOLOGIA

As vulnerabilidades que acompanham a adequação organizacional à indústria 4.0, seus padrões ou implementações de casos de uso, também impactam as tecnologias. Mudanças nas novas tecnologias tem se tornado cada vez mais disruptivas e novos artefatos substituem outros marginalmente desatualizados a cada dia. Novas tecnologias abrem portas para novos riscos e na luz dessa mudança constante, novas tecnologias acabam tendo que se adequar a novos padrões de segurança que consideram os impactos de novas vulnerabilidades que surgem.

A correlação entre o grau de automação e a mudança na autonomia do funcionário desempenha um grande papel nisso. Considerando esta crescente falta de autonomia do funcionário, tecnologias autônomas precisam de mecanismos à prova de falhas, visto que ataques a esse tipo de sistema podem fazer grande estrago, principalmente em sistemas críticos.

Tomando o setor de saúde como exemplo, é conhecido que há a possibilidade de hackers adulterem dispositivos médicos para prejudicar indivíduos. Algoritmos de inteligência artificial podem ser usados para modificar tomográficas computadorizadas de pulmões em tempo real por wi-fi e adicionar ou remover imagens de metástase sob demanda. Já no setor de transporte, ataques cibernéticos aos trens tem o potencial de atingir sistemas críticos de segurança, como os que controlam a velocidade do trem. Para minimizar esses impactos, avanços na tecnologia devem levar em conta diversos tipos de ataques durante sua confecção e implementação, tanto hardware como software. [EP054]

Evidências:

"Another research study showed how artificial intelligence algorithms can be used to modify CT scans of the lung in real time [14]. The test was conducted in a radiology department's CT room, where a Wi-Fi port was installed that grabbed the CT datasets from the scanner to the digital picture archive. A computer was connected to the Wi-Fi network from the hospital room, and with the algorithm installed on this computer, lung metastases were added to, and deleted from, the CT datasets within seconds." [EP054]

"A cyber attack has the potential to target safety-critical systems, such as those that control the train's speed. An attack on a signaling system could cause untold disruption to train movements, leading to further safety concerns." [22]

Já vimos que, ao confeccionar um novo sistema ou adotar uma nova tecnologia, é necessário levar em consideração as vulnerabilidades em questão e implantar mecanismos de defesa. O avanço da tecnologia, porém, não para nesse momento. Com o surgimento de novas tecnologias, os ataques se tornam cada vez mais sofisticados, fazendo com que uma empresa precise estar sempre atenta e ponderar se os mecanismos de defesa implantados naquele sistema ainda são efetivos.

Evidências:

"CI-embedded malware will learn to imitate human behavior using contextualization, changing the behavior based on the current situation.

[...]The characteristics of existing malware are constantly being improved, and specialized CI learns to understand the context on-the-fly. The combination of these factors means a paradigm shift for the security industry [4, 5]. Outdated tools can no longer protect modern CDI against such serious security threats. The only thing that can withstand CI-enabled security violation is a retaining, protective CI." [EP039]

Uma vez que todas as barreiras de proteção falham e um ataque cibernético acontece, o sistema no qual o ataque foi realizado pode sofrer diversos problemas. Alguns desses problemas são silenciosos, o que é extremamente perigoso, visto que o ataque pode passar despercebido e expor a organização durante muito tempo. Outros podem ter consequências muito claras, impactando a performance ou alterando os dados de um sistema.

Evidências:

"Some of the symptoms that indicate that the system is affected by malware are slow computer speed or performance, system hang, blank screen, computer system restart continuously, erasing entire disk or drive, erratic screen behavior, browser homepage change automatically, operating system software modified." [EP001]

"SQLIA allows an attacker to interfere with the legitimate Structured Query Language (SQL) queries that an application makes to its database, where the attacker includes a malicious code which is known as injecting a malicious content. Once the SQLIA is successful, the attacker can perform operations on the database such as view, insert, delete, etc. which might require a high level of authorization generally. These unauthorized

modifications/deletions will cause persistent changes to the application’s content or behavior." [EP008]

"Li et al. has recognised that the key weak link for smart cities is the security and trustworthiness of data (Li et al., 2018). The trustworthiness of data is fundamental to a successful operation of the smart city; however a potential cyber attack could alter or generate misleading data (Li et al., 2018). As a result, falsified reports on smart grid or traffic could lead to inappropriate controls to the systems. This could have far reaching and even life-threatening implications, such as car accidents or inappropriate water treatment." [EP058]

"The maritime industry and the CI should be aware of the catastrophic result that the ship's systems were controlled by cybercriminals, which could result in collisions, pollution, grounding, the interruption of port operations or an incendiary device. At present, the authorities and the industry itself is not prepared to give an effective response to any of the threats posed. Ships in port represent another component of port infrastructures that must be protected. All coastal States must have the ability to monitor all the ships that enter its CI in order to validate whether they are cyber clean, in convergence with supply chains, port operations and information technology." [EP059]

A Tabela 6 mostra os principais impactos das vulnerabilidades trazidas pela TD nas organizações, sob a perspectiva da dimensão Tecnologia.

Tabela 6 - Principais impactos na Tecnologia

Impacts	**Mentions**	**References**
Damage to critical systems	1	EP054
Constant update of defense technology	1	EP039
Affect on system performance	2	EP001, EP059
Alteration on system data	2	EP008, EP058

4.6 DISCUSSÕES E RESULTADOS

Existe literatura extensiva sobre vulnerabilidades digitais, o processo de transformação digital e como essas vulnerabilidades afetam diversos mercados e campos de atuação. Alguns destes mercados tiveram mais artigos relacionados, devido a maior influência das vulnerabilidades digitais, como aconteceu com a indústria marítima. A diferença na quantidade de artigos pode se dar pelo quanto o setor é afetado pelas vulnerabilidades digitais, como também pelo risco gerado para outras esferas da sociedade, como o mercado de trabalho e a saúde da população.

A análise da literatura mostra um consenso a respeito do fato de que existem impactos advindos do processo de transformação digital e de suas potenciais vulnerabilidades para organizações, relações sociais, tecnologia, processos, mercado e meio ambiente. Os riscos são bem descritos e exemplificados por muitos artigos, também como as vulnerabilidades mais específicas em cada setor, como aeroportos, empresas de tecnologia da informação, governo, setor industrial, laboratórios forenses, empresas de transporte, entre outros. Essa quantidade de literatura específica mostra um alto nível de maturidade sobre o assunto. Porém, poucos estudos discutem os méritos do real impacto de uma vulnerabilidade específica.

Roberto D. Taufick [EP063] por exemplo, comenta sobre o vazamento de dados, argumenta que a avaliação da privacidade é circunstancial. Seu impacto no reconhecimento de marca e reputação das empresas como também o impacto da violação da privacidade em nível individual depende da percepção do quanto foi perdido na divulgação não autorizada de dados. As consequências de um vazamento de dados na reputação da empresa logo são esquecidas e a reputação volta ao normal. E que talvez seja mais vantagem lidar com essa curta consequência do que gastar milhões de dólares com medidas de segurança para evitar que isso aconteça.

Um outro ponto que chama atenção nos dados da RSL é a disparidade da quantidade de artigos que tratam do risco de ciberataques, em relação aos artigos que falam de outros riscos, como por exemplo, o risco da perda de dados devido a uma perda não-intencional da base de dados, ou o risco de vazamento de dados confidenciais por um erro de um funcionário. Quando se trata de riscos cujos efeitos são mais subjetivos e, consequentemente, mais dificilmente mensuráveis, esse número se reduz ainda mais. Nesse quesito, podemos citar riscos de danos psicológicos ou até mesmo de integridade física. Segundo [EP016], métodos tradicionais de avaliação de risco na área de IoT deveriam ser expandidos para incluir visões não-cibernéticas, que também são críticas para a operação de um negócio. Vale

salientar que, segundo Wangyal [EP016], “The current assessment of non-cyber aspects is inadequate.”.

O mais sério dos impactos encontrados é o impacto vindo das vulnerabilidades em sistemas críticos pela sua ligação à vida humana, causando uma perda irreparável. Sistemas críticos devem ser prontamente avaliados antes da sua implementação. Isso fica mais aparente nos setores onde a falha desses sistemas tem consequências catastróficas como portos, metroferroviários, aeroespaciais, tratamento de água, sistemas de saúde.

Muitos artigos sobre a Transformação Digital mostram que ela deve ser vista como um processo. Um método constante e consciente de organizações se adequarem a novas tecnologias e normas sociais. TD deve ser um tópico discutido nos altos níveis gerenciais. Gerentes devem conhecer as possíveis soluções tecnológicas num horizonte que tem a possibilidade de substituir processos e tecnologias correntes, mas também investigar as implicações das suas implementações e possíveis vulnerabilidades para a organização, seu pessoal e outras áreas.

5 **CONCLUSÃO**

O presente trabalho aplicou o método de Revisão Sistemática da Literatura de KITCHENHAM (2004) com o objetivo de responder a seguinte questão central de pesquisa:

QC: Quais os impactos das vulnerabilidades trazidas pela transformação digital nas organizações, sob as perspectivas das dimensões de Pessoas, Processos e Tecnologia?

As bases escolhidas para a pesquisa foram a IEEE e a Science Direct. A pesquisa nas bases retornou 3446 artigos, onde 3303 foram eliminados utilizando critérios de exclusão e 25 foram posteriormente eliminados na avaliação de qualidade. Em seguida, foi utilizado o critério de responsividade em relação às perguntas de pesquisa, o que resultou em um total de 69 artigos selecionados para a RSL.

Esses artigos foram então analisados em busca de respostas para as perguntas de pesquisa. De acordo com essa análise, descobrimos que as vulnerabilidades mais comuns listadas pelos artigos são ações cometidas pelas próprias pessoas dentro da organização, a falta de conhecimento especializado, a autenticação vulnerável, a criptografia frágil, e a colaboração com terceiros. Além dessas, outras vulnerabilidades mencionadas com menos frequência foram listadas na Tabela 1.

Foi descoberto também que essas vulnerabilidades podem ter impacto tanto nas pessoas de dentro, quanto nas de fora da organização. Para os funcionários, a adequação a novas políticas e diretrizes de segurança pode ser onerosa e ser percebida como um inconveniente para as tarefas diárias. Para os usuários ou clientes da organização, uma das maiores preocupações é com a privacidade e o vazamento de dados confidenciais. As mudanças necessárias na cultura organizacional também podem impactar tanto funcionários quanto a liderança da empresa. É visto que o impacto nas pessoas não se restringe somente ao mundo cibernético, mas pode inclusive se transformar em consequências físicas ou psicológicas, em alguns casos chegando até a ameaçar vidas.

Quando se fala de processos organizacionais, a necessidade de reconhecer todas as vulnerabilidades cibernéticas advindas da digitalização é fundamental para um administração digitalmente segura, mas pode ser um processo lento e oneroso para a organização. Além disso, alguns crimes cibernéticos funcionam pela interrupção da operação ou serviço.

Já na tecnologia, as principais preocupações se referem à adequação dos sistemas a novos padrões de segurança e a necessidade de constante atualização das técnicas de segurança para acompanhar a evolução dos crimes cibernéticos. Além disso, quando todas as

barreiras de proteção falham e um crime cibernético acontece, vemos impactos como diminuição da performance de sistemas ou a alteração de bases de dados.

Durante a discussão dos dados, notou-se a discrepância entre a quantidade de artigos que falam sobre riscos cibernéticos em relação aos outros muitos riscos que podem vir pela transformação digital de uma organização, mostrando o impacto de tecnologias baseadas em redes globais como a Internet no contexto de TD. Existem também poucos artigos que discutem o mérito dos impactos listados pela maior parte dos artigos, e se eles realmente justificam os custos gerados ao implementar medidas de segurança.

Mais uma vez, é importante ressaltar que o objetivo deste trabalho não é desencorajar a transformação digital, elencando os seus pontos negativos. Muito pelo contrário, a observação das vulnerabilidades advindas de uma transformação digital é essencial para possibilitar a criação de políticas de segurança e medidas de proteção efetivas, que venham a facilitar uma TD segura e eficiente para uma organização. Incluir tópicos e subtópicos de todos os resultados do TCC. É uma das partes mais importantes do trabalho e precisa ser bastante detalhada em todos os aspectos. Gráficos, estudos, tabelas, com suas devidas explicações. Incluir tópicos e subtópicos de todos os resultados do TCC. É uma das partes mais importantes do trabalho e precisa ser bastante detalhada em todos os aspectos. Gráficos, estudos, tabelas, com suas devidas explicações.

5.1 LIMITAÇÕES E AMEAÇAS

Esse trabalho se deparou com algumas limitações e ameaças. Tempo e saúde do autor foram as maiores ameaças para a conclusão desse artefato. A quantidade de bases de pesquisa é uma limitação do trabalho, duas outras seriam utilizadas para a entrega final, Scopus e ACM. Mas, devido à qualidade e seriedade do processo de seleção dos artigos, as bases foram removidas do escopo. Apenas uma pesquisa foi feita por base, usando o mesmo conjunto de palavras chave e, para não limitar a área de pesquisa, as palavras chave podem ter ficado muito genéricas, onerando a possibilidade de detalhar consequências de vulnerabilidades próprias de uma única área.

5.2 TRABALHOS FUTUROS

Como o tema da transformação digital tem sido pesquisado de forma extensiva por várias áreas, nós obtivemos um número alto de artigos que apareceram na coleta de dados. Por esse motivo, as bases Scopus e ACM, inicialmente previstas para fazerem parte da análise, tiveram que ser removidas. Em trabalhos futuros, as bases removidas do escopo poderiam ser utilizadas para enriquecer ainda mais os argumentos e análises a respeito do tema. A escolha de novas bases que trabalham mais aspectos sociais ajudariam a apontar outras vulnerabilidades organizacionais que não do ambiente técnico específico de TI.

Um mapeamento sistemático dos artigos sobre as vulnerabilidades provenientes do processo de transformação digital em diferentes áreas de atuação, usando as maiores bibliotecas virtuais, juntamente com critérios de qualidade mais objetivos, poderia ser de grande valor para o estado da arte sobre TD.

Neste trabalho, TD nas organizações foi tratada de forma geral, não foram feitas divisões e análises a respeito de áreas de atuação específicas. A possibilidade de trabalhos discursando sobre as vulnerabilidades e seus impactos em áreas específicas como, manufatura, transporte, portos, bancos e etc é interessante. Embora esse trabalho sirva como base para muitas empresas simultaneamente, uma revisão mais específica poderia abordar detalhes os quais fogem do escopo deste trabalho.

Sendo dados coletados apenas da revisão da literatura, os resultados dos achados na literatura poderiam ser comparados com pesquisas de campo sobre vulnerabilidades em pequenas empresas e outras corporações dispostas. As vulnerabilidades foram enumeradas, mas as possibilidades de ações para mitigação das mesmas não foram exploradas. As pesquisas de campo poderiam ser usadas também para conseguir dados sobre quais ações já foram feitas para reduzir os impactos de vulnerabilidades específicas e métodos para diminuir tanto incidências quanto impactos.

REFERÊNCIAS

GOOGLE. **Google Trends,** 2022. Digital Transformation. Disponível em: <https://trends.google.com/trends/explore?q=Digital%20Transformation&geo=SE>. Acesso em: 2 maio 2022.

JONES, M.D.; HUTCHESON, S.; CAMBA, J.D. Past, present, and future barriers to digital transformation in manufacturing**:** A review. **Journal of Manufacturing Systems**, vol. 60, pp. 936–948, 2021.

YAMASHIRO, C.S.; MANTOVANI, D. **Transformação digital: maturidade digital das empresas no brasil.** 2021. Disponível em: < http://www.aisel.aisnet.org>. Acesso em: 2 maio 2022.

SKRODELIS, H.K.; ROMANOVS, A. Cyber-physical risk security framework development in digital supply chains. *In*: **2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS).** pp. 1–5, IEEE, 2021.

CULOT, G. *et al*. Addressing industry 4.0 cybersecurity challenges. **IEEE Engineering Management Review**, vol. 47, no. 3, pp. 79–86, 2019.

ALAHMARI, A. A.; DUNCAN, R. A. Towards cybersecurity risk management investment: A proposed encouragement factors framework for SMES. *In*: **2021 IEEE International Conference on Computing (ICOCO)**, pp. 115–121, IEEE, 2021.

KITCHENHAM, B. **Procedures for Performing Systematic Reviews**, Technical Report TR/SE-0401. Department of Computer Science, Keele University and National ICT. Australia. 2004.

SAARIKKO, T.; WESTERGREN, U. H.; BLOMQUIST, T. Digital transformation: Five recommendations for the digitally conscious firm. **Business Horizons**, vol. 63, no. 6, pp. 825–839, 2020.

PANGARKAR, Y. S. A.; ARORA, V. Exploring phygital omnichannel luxury retailing for immersive customer experience: The role of rapport and social engagement. *In*: **Journal of Retailing and Consumer Services**, vol. 68, 2022

TIJAN, S. A. A. P. E.; JOVIC, M. Digital transformation in the maritime transport sector. *In*: **Technological Forecasting and Social Change**, vol. 170, 2021

ALDABBAS, M.; TEUFEL, S.; TEUFEL, B. The importance of security culture for crowd energy systems. *In*: **2017 Information Security for South Africa (ISSA)**, pp. 10–15, IEEE, 2017.

PRAMANIK, H. S.; KIRTANIA, M.; PANI, A. K. Essence of digital transformation - manifestations at large financial institutions from North America. **Future Generation Computer Systems,** vol. 95, pp. 323–343, 2019.

LIERE-NETHELER, K.; PACKMOHR, S.; VOGELSANG, K. **Drivers of digital transformation in manufacturing**. 2018. Disponível em: < http://www.aisel.aisnet.org>. Acesso em: 2 maio 2022.

MORAKANYANE, R. *et al.* Determining digital transformation success factors. *In*: **Proceedings of the 53rd Hawaii International Conference on System Sciences**, 2020.

ITU. **International telecommunications union statistics**. Disponivel em: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em: 11 de maio de 2022.

TAM, T.; RAO, A.; HALL, J. The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. **Computers & Security**, vol. 109, p. 102385, 2021.

LEE, I. Cybersecurity: Risk management framework and investment cost analysis. **Business Horizons**, vol. 64, no. 5, pp. 659–671, 2021.

HUMAYUN, M. *et al.* Cyber security threats and vulnerabilities: a systematic mapping study. **Arabian Journal for Science and Engineering**, vol. 45, no. 4, pp. 3171–3189, 2020.

SIMMONDS, M. Instilling a culture of data security throughout the organization. **Network Security**, vol. 2018, no. 6, pp. 9–12, 2018.

CASEY, E.; SOUVIGNET, T. R. Digital transformation risk management in forensic science laboratories. **Forensic Science International**, vol. 316, p. 110486, 2020.

HEAD, L. Risk management – why and how. **International Risk Management Institute**, Dallas, Texas, 2009.

COWAN, A. Coming off the tracks: the cyberthreats facing rail operators. *In*: **Network Security**, vol. 2021, pp. 12–14, 2021.

YUCEL, S. Estimating the benefits, drawbacks and risk of digital transformation strategy. *In*: **2018 International Conference on Computational Science and Computational Intelligence (CSCI)**, pp. 233–238, IEEE, 2018.

DIGMAYER, C; JAKOBS, E. Developing safety cultures for Industry 4.0. New challenges for professional communication. In: **2019 IEEE international professional communication conference (proComm)**. IEEE, 2019. p. 218-225.

ROMERO, D. *et al*. Five management pillars for digital transformation integrating the lean thinking philosophy. *In*: **2019 IEEE International conference on Engineering, technology and Innovation (ICE/ITMC)**. IEEE, 2019. p. 1-8.

APÊNDICE A — ESTUDOS INCLUÍDOS NA RSL

Tabela 7 - Lista de estudos incluídos na RSL

Código	Título	Autor	Fonte	Ano
EP01	IT Infrastructure Security Risk Assessment using the Center for Internet Security Critical Security Control Framework: A Case Study at Insurance Company	H. Winarno; F. Yasin; M. A. Prasetyo; F. Rohman; M. R. Shihab; B. Ranti	IEEE	2020
EP02	Growing Digital Vulnerability: A Case Study of Threats to Pakistans National Assets	F. Al Faisal; S. A. S. Kazmi; H. Abbas	IEEE	2021
EP03	Smart Secure: A Novel Risk based Maturity Model for Enterprise Risk Management during Global Pandemic	V. M. Deshpande; A. Desai	IEEE	2021
EP04	Cyber Insurance of Information Systems: Security and Privacy Cyber Insurance Contracts for ICT and Helathcare Organizations	G. Hatzivasilis; P. Chatziadam; N. Petroulakis; S. Ioannidis; M. Mangini; C. Kloukinas; A. Yautsiukhin; M. Antoniou; D. G. Katehakis; M. Panayiotou	IEEE	2019
EP05	Data Risks Identification in Healthcare Sensor Networks	K. Lopatina; V. A. Dokuchaev; V. V. Maklachkova	IEEE	2021
EP06	Estimating the Benefits, Drawbacks and Risk of Digital Transformation Strategy	S. Yucel	IEEE	2018
EP07	Risk Management for Digital Transformation in Architecture	Y. Masuda; S. Shirasaka; S. Yamamoto; T. Hardjono	IEEE	2017

	Board: A Case Study on Global Enterprise			
EP08	Identification and Mitigation Tool for Sql Injection Attacks (SQLIA)	W. H. Rankothge; M. Randeniya; V. Samaranayaka	IEEE	2020
EP09	Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage	D. Vaczi; E. Toth-Laufer; T. Szadeczky	IEEE	2020
EP10	IoTVT Model: A Model Mapping IoT Sensors to IoT Vulnerabilities and Threats	M. Nicho; S. Girija	IEEE	2021
EP11	On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats	A. Angelogianni; I. Politis; F. Mohammadi; C. Xenakis	IEEE	2020
EP12	Development of Vulnerable Web Application Based on OWASP API Security Risks	M. Idris; I. Syarif; I. Winarno	IEEE	2021
EP13	Five Management Pillars for Digital Transformation Integrating the Lean Thinking Philosophy	D. Romero; M. Flores; M. Herrera; H. Resendez	IEEE	2019
EP14	Risks Identification in the Exploitation of a Geographically Distributed Cloud Infrastructure for Storing Personal Data	V. V. Maklachkova; V. A. Dokuchaev; V. Y. Statev	IEEE	2020
EP15	Digital Transformation: New Drivers and New Risks	V. A. Dokuchaev	IEEE	2020
EP16	A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT)	S. Wangyal; T. Dechen; S. Tanimoto; H. Sato; A. Kanai	IEEE	2020

EP17	Cybersecurity Guideline for the Utility Business a Swiss Approach	S. Teufel; R. Burri; B. Teufel	IEEE	2018
EP18	A Novel Deep Learning RBM Based Algorithm for Securing Containers	S. Kamthania	IEEE	2019
EP19	Some Security Problems and Aspects of the Industrial Internet of Things	G. Tsochev	IEEE	2020
EP20	Cyber-physical Risk Security Framework Development in Digital Supply Chains	H. K. Skrodelis; A. Romanovs	IEEE	2021
EP21	Security vs. Flexibility: Striking a Balance in the Pandemic Era	V. Soni; D. Kukreja; D. K. Sharma	IEEE	2020
EP22	Big Data Privacy Breach Prevention Strategies	S. Varshney; D. Munjal; O. Bhattacharya; S. Saboo; N. Aggarwal	IEEE	2020
EP23	Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs	A. A. Alahmari; R. A. Duncan	IEEE	2021
EP24	Determining Bring Your Own Device (Byod) Security Policy Compliance Among Malaysian Teleworkers: Perceived Cybersecurity Governance as Moderator	C. Hai Goh; A. Ping Teoh	IEEE	2021
EP25	An Architecture-based Modeling Approach Using Data Flows for Zone Concepts in Industry 4.0	M. Kern; E. Taspolatoglu; F. Scheytt; T. Glock; B. Liu; V. P. Betancourt; J. Becker; E. Sax	IEEE	2020

EP26	A Cyber-Security Strategy for Internationally-dispersed Industrial Networks	R. L. de Moura; A. Gonzalez; V. N. L. Franqueira; A. L. Maia Neto	IEEE	2020
EP27	A secure cloud storage system for small and medium enterprises	J. Newport; B. von Solms	IEEE	2017
EP28	The Information System Security Governance Tasks in Small and Medium Enterprises	H. K. Skrodelis; J. Strebko; A. Romanovs	IEEE	2020
EP29	Security and Privacy in IoT based E-Business and Retail	K. Kaushik; S. Dahiya	IEEE	2018
EP30	SCADA Security in Various Industrial Sectors	B. Spoorthi; D. Harekal	IEEE	2018
EP31	Context-Aware Data Loss Prevention for Cloud Storage Services	Y. J. Ong; M. Qiao; R. Routray; R. Raphael	IEEE	2017
EP32	A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices	R. Layton; S. Elaluf-Calderwood	IEEE	2019
EP33	System Dynamics perspective for Adoption of Internet of Things: A Conceptual Framework	S. Tripathi	IEEE	2019
EP34	Towards a data-driven enterprise: Effects on information, governance, infrastructures and security	A. Polzonetti; M. Sagratella	IEEE	2017
EP35	Addressing Industry 4.0 Cybersecurity Challenges	G. Culot; F. Fattori; M. Podrecca; M. Sartor	IEEE	2019
EP36	Applying NIST SP 800-161 in	L. Al-Alawi; R. Al-	IEEE	2021

	Supply Chain Processes Empowered by Artificial Intelligence	Busaidi; S. Ali		
EP37	Blockchain at the Shop Floor for Maintenance	D. Welte; A. Sikora; D. Schönle; J. Stodt; C. Reich	IEEE	2020
EP38	Developing Safety Cultures for Industry 4.0. New Challenges for Professional Communication	C. Digmayer; E. -M. Jakobs	IEEE	2019
EP39	Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions	M. O. Kalinin; V. M. Krundyshev	IEEE	2021
EP40	Cybersecurity Challenges in Large Industrial IoT Systems	B. Leander; A. Čaušević; H. Hansson	IEEE	2019
EP41	Privacy Preservation of Sensitive Dara in Big Data Analytics - A Survey	A. S. DEVI; A. CHINNASAMY	IEEE	2021
EP42	SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape	S. U. A. Laghari; S. Manickam; A. K. Al-Ani; S. U. Rehman; S. Karuppayah	IEEE	2021
EP43	Digital transformation strategy making in pre-digital organizations: The case of a financial services provider	Simon Chanias, Michael D. Myers, Thomas Hess	SD	2019
EP44	Essence of digital transformation—Manifestations at large financial institutions from North America	Himadri Sikhar Pramanik, Manish Kirtania, Ashis K. Pani	SD	2019
EP45	Digital transformation readiness:	Marek Deja, Dorota Rak,	SD	2021

	perspectives on academia and library outcomes in information literacy	Brigitte Bell		
EP46	Organizational vulnerability of digital threats: A first validation of an assessment method	Roland W. Scholz, Reiner Czichos, Peter Parycek, Thomas J. Lampoltshammer	SD	2020
EP47	Ready for digital transformation? The effect of organisational readiness, innovation, airport size and ownership on digital change at airports	Nigel Halpern, Deodat Mwesiumo, Pere Suau-Sanchez, Thomas Budd, Svein Bråthen	SD	2021
EP48	Can traditional organizations be digitally transformed by themselves? The moderating role of absorptive capacity and strategic interdependence	Evangelia Siachou, Demetris Vrontis, Eleni Trichina	SD	2021
EP49	Current and future state of Portuguese organizations towards digital transformation	Natércia Durão, Maria João Ferreira, Carla Santos Pereira, Fernando Moreira	SD	2019
EP50	The impacts of digital transformation on the labor market: Substitution potentials of occupations in Germany	Katharina Dengler, Britta Matthes	SD	2018
EP51	Port cybersecurity and threat: A structural model for prevention and policy development	Chalermpong Senarak	SD	2021
EP52	Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior	Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar, Xiaohong Yuan	SD	2019

EP53	Analyzing socio-technical risks in implementation of Industry 4.0-use cases	Stefan Gabriel, Tobias Grauthoff, Robert Joppen, Arno Kühn, Roman Dumitrescu	SD	2021
EP54	ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things	Mohiuddin Ahmed, Surender Byreddy, Anush Nutakki, Leslie F. Sikos, Paul Haskell-Dowland	SD	2021
EP55	Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel	Chalermpong Senarak	SD	2021
EP56	Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue	Ignacio de la Peña Zarzuelo	SD	2021
EP57	Avoiding digitalization traps: Tools for top managers	Phillip C. Nell, Nicolai J. Foss, Peter G. Klein, Jan Schmitt	SD	2021
EP58	Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership	Morta Vitunskaite, Ying He, Thomas Brandstetter, Helge Janicke	SD	2019
EP59	Critical infrastructures cybersecurity and the maritime sector	Juan Ignacio Alcaide, Ruth Garcia Llave	SD	2021
EP60	Technological trajectories and scenarios in seaport digitalization	Tommi Inkinen, Reima Helminen, Janne Saarikoski	SD	2021
EP61	The challenges of cybersecurity in health care: the UK National	Saira Ghafur, Emilia Grass, Nick R Jennings,	SD	2019

	Health Service as a case study	Ara Darzi		
EP62	Estimating the impact of IT security incidents in digitized production environments	Olga Bürger, Björn Häckel, Philip Karnebogen, Jannick Töppel	SD	2019
EP63	The underdeterrence, underperformance response to privacy, data protection laws	Roberto D. Taufick	SD	2021
EP64	The perceived relationship between digitalization and ecological, economic, and social sustainability	Barbara Brenner, Barbara Hartl	SD	2021
EP65	Digitalization of agriculture: A way to solve the food problem or a trolley dilemma?	Evagelos D. Lioutas, Chrysanthi Charatsari, Marcello De Rosa	SD	2021
EP66	A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense	Amrita Dahiya, Brij B. Gupta	SD	2021
EP67	The strategy for implementation of the digitization in factories	Miroslav Fusko, Monika Buckova, Martin Krajcovic, Radovan Svitek	SD	2019
EP68	Expected impact of industry 4.0 technologies on sustainable development: A study in the context of Brazil's plastic industry	Elpidio Oscar Benitez Nara, Matheus Becker da Costa, Ismael Cristofer Baierle, Jones Luis Schaefer, Guilherme Brittes Benitez, Leonardo Moraes Aguiar Lima do Santos, Lisianne Brittes Benitez	SD	2021

EP69	Barriers to the adoption of industry 4.0 technologies in the manufacturing sector: An inter-country comparative perspective	Alok Raj, Gourav Dwivedi, Ankit Sharma, Ana Beatriz Lopes de Sousa Jabbour, Sonu Rajak	SD	2020