The Role of Cybersecurity in Information Systems in Organizations: a systematic literature review

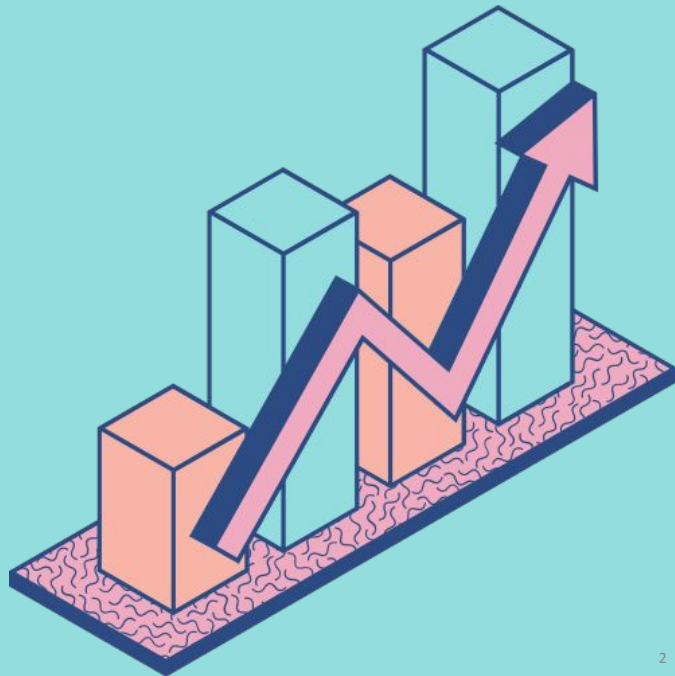
Pedro Sobral, 98491

Eduardo Santos, 93107

Pedro Bastos, 93150

Gonçalo Passos, 88864

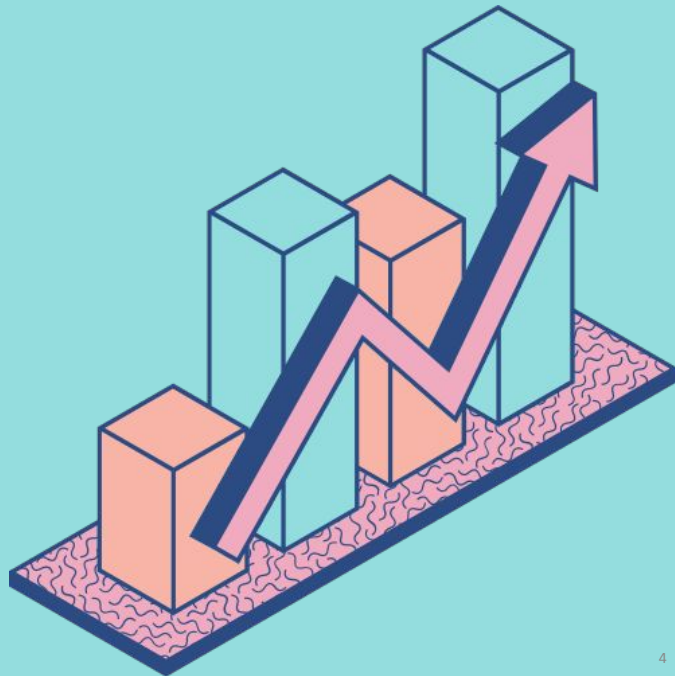
Introdução



Cibersegurança

- É uma das principais preocupações das empresas na era digital moderna;
- O potencial de ciberameaças tem vindo a aumentar substancialmente à medida que as tecnologias digitais continuam a desenvolver-se;
- A tarefa de proteger os sistemas de informação tornou-se mais difícil devido às novas vulnerabilidades e vetores de ataque;
- Os cibercriminosos estão a tornar-se mais competentes;
- Compreender a função da cibersegurança nos sistemas de informação é um aspeto crucial para as organizações.

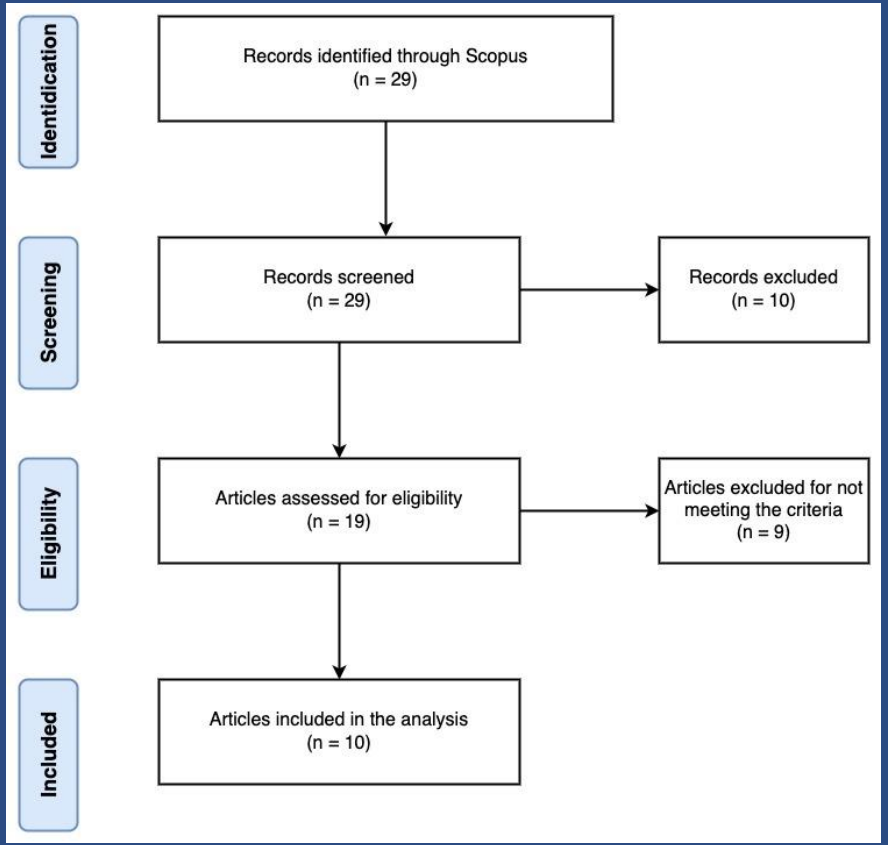
Metodologia



Seleção de Artigos

QUERY (Scopus DB, 2017-2023):

(“cybersecurity” AND
“role” AND
“Information Systems” AND
“Organizations”)

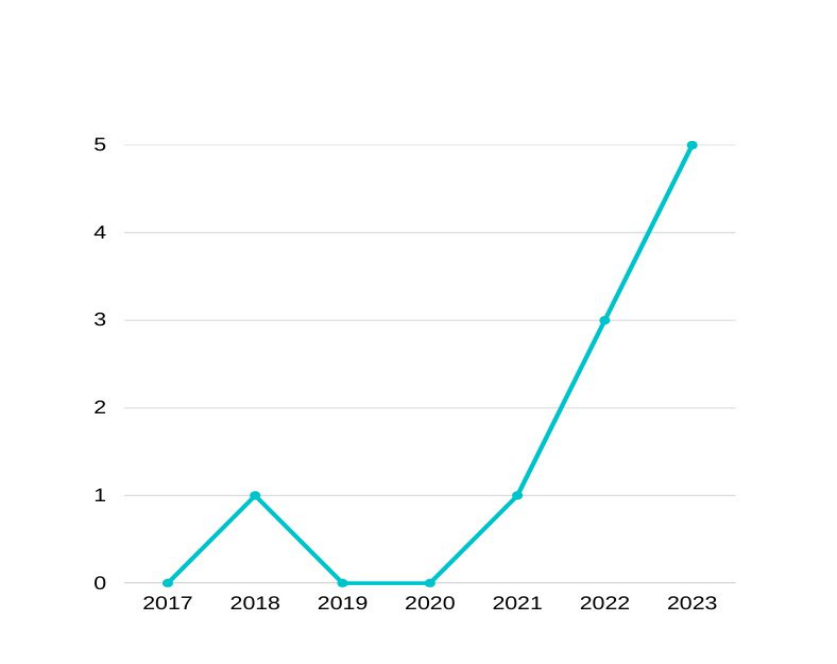


Análise dos dados

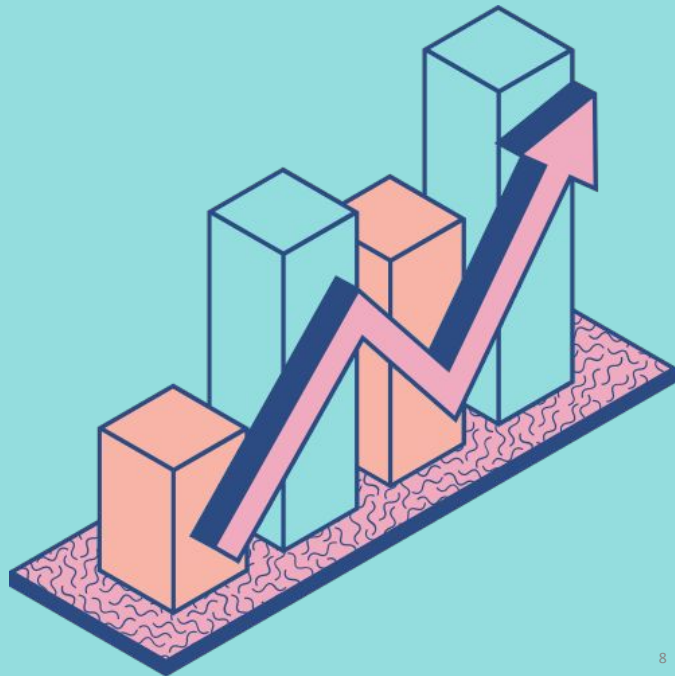
Tópicos	Número de Artigos
Cybersecurity Awareness in Organizations	2
Reasons for Increase in Cyber-attacks	3
Importance of the Highest Positions in the Prevention and Management of Security Breaches	3
The Role of External Auditors and IT Modernization in Reducing Cybersecurity Risks	2

Análise dos artigos

- Nos últimos anos, as organizações aumentaram disponibilidade e dinheiro colocado em cibersegurança;
- A nossa procura reflete o estudo crescente da área;



Consciencialização da Cibersegurança nas Organizações



Tipos de Ataques Cibernéticos

- Ataques de Phishing
- Ransomwares
- Malwares
- Ataques por injeção de SQL
- Ataques de Negação de Serviço (DoS ou DDoS)
- etc.

Consciencialização afetada por:

- Formação em cibersegurança;
- Formação académica;
- Experiência profissional;
- Área de estudos;
- Género;
- Idade;
- Formação;
- Local de residência.

CIA

Qualquer informação encontrada no ambiente cibernético, incluindo dispositivos em rede, infraestruturas, sistemas de telecomunicações, serviços e aplicações, deve ser protegida com base nos três principais objetivos da CIA:

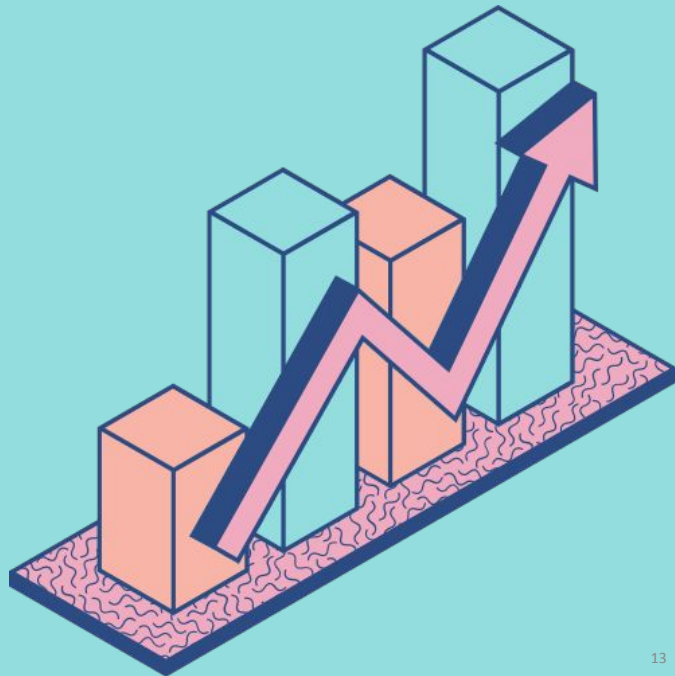
- Confidencialidade (C);
- Integridade (I);
- Disponibilidade (A).

CSA

- É essencial dar formação em CSA (Cyber Security Awareness) às pessoas que trabalham diretamente com os sistemas de informação.

- Esta instrução pode melhorar o nível de proteção tanto da organização como dos próprios indivíduos.

Importância dos cargos mais elevados na prevenção de falhas de segurança



Importância da gestão de topo na cibersegurança

- Top management teams (TMTs).
- A atenção das TMT à cibersegurança desempenha um papel mediador nas avaliações dos riscos para a segurança da informação (ISRA) na sequência de violações da cibersegurança.
- Os TMT são cruciais na definição da cibersegurança como uma prioridade máxima e na alocação de fundos para a análise do risco.

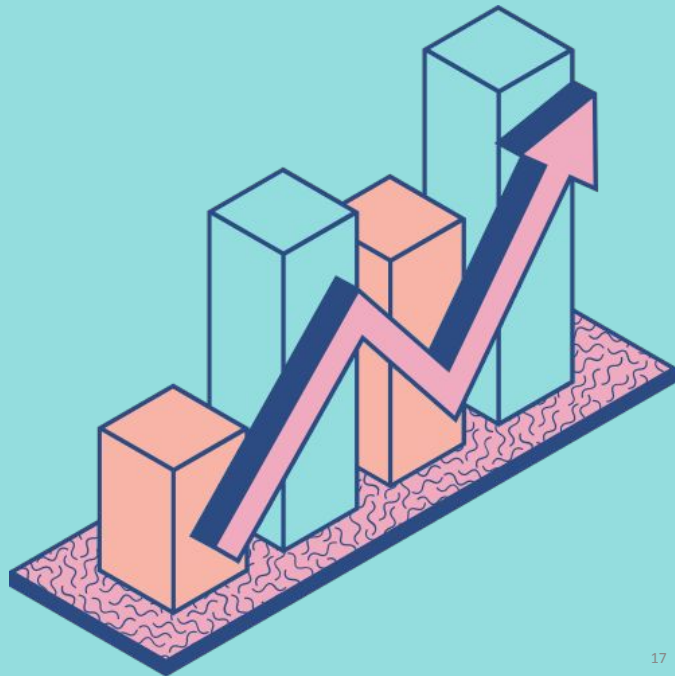
Liderança estratégica e Cyber-Resiliency

- Os ciberataques têm efeitos negativos na reputação, na perda de dados e na perda de conhecimentos nas empresas digitais.
- Há falta de conhecimentos empíricos sobre a forma como os líderes estratégicos influenciam e apoiam as estratégias de cibersegurança.
- Desenvolvimento de quadros de governação e compreensão do ecossistema e das interacções com parceiros e fornecedores.
- Os líderes estratégicos desempenham um papel fundamental na promoção de medidas de cibersegurança e na sua incorporação na cultura empresarial.

Programas de desenvolvimento de liderança para profissionais de cibersegurança e IT

- Os programas tradicionais de formação técnica ignoram frequentemente o desenvolvimento das qualidades de liderança dos profissionais de cibersegurança e de tecnologias da informação (IT).
- É importante criar programas formais de desenvolvimento da liderança especificamente concebidos para profissionais de cibersegurança e de IT.
- Estes programas devem melhorar competências como o pensamento estratégico, a comunicação, a gestão de equipas, a resolução de problemas e a tomada de decisões.
- Investir no desenvolvimento de líderes de cibersegurança e de IT melhora toda a postura de cibersegurança e estabelece uma cultura que valoriza os conhecimentos técnicos e a liderança efectiva.

Razões do aumento de ciberataques



Ciberataques nos Sistemas de Informação de Saúde

- Cada vez há mais dados e metadados neste setor em nambiente virtual.

- Proteger os dados de pacientes, e os exames médicos por todas as questões de privacidade que o setor implica é um desafio constante e cada vez mais difícil.

Para ter todo o tipo de dados bem protegidos e seguros, neste setor é importante:

- Assegurar que todos os sistemas de informação se encontram atualizados;
- Que sejam cumpridas as últimas regulamentações
- Que haja neste setor, pessoas bem instruídas capazes de oferecer o suporte necessário, isto desde o técnico de cibersegurança até ao profissional que opera com o sistema.

Ciberataques nos Sistemas de IIoT

- IIoT (Industrial Internet of Things) engloba setores como, transportes , energia, serviços, bastante importante na nossa sociedade
- Aumento crescente do número destes equipamentos ligados à rede
- Verificando-se um aumento também do número de ataques, tendo em alguns casos consequências severas.
- Posto isto, este setor enfrenta diversos desafios, tendo que arranjar soluções para estes problemas, pois um ataque em IIoT pode abrir uma panóplia de potenciais ataques nas restantes partes do sistema.

Ciberataques em trabalhadores remotos

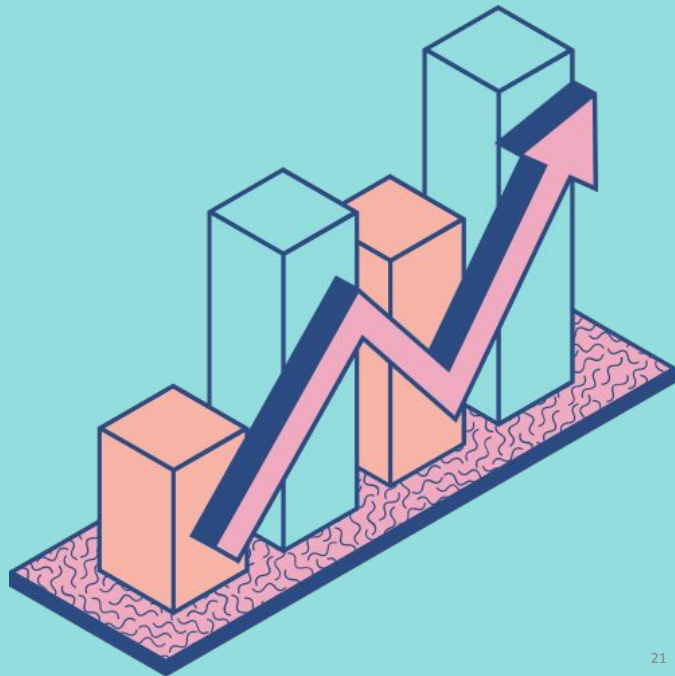
- Número de trabalhadores remotos tem aumentado nos últimos anos

- Logo mais pessoas estão expostas a ataques todos os dias

Algumas medidas para prevenir possíveis ataques são:

- Melhorar o conhecimento sobre cibersegurança dos trabalhadores
- Usar VPNs
- Ter palavras passes fortes e únicas
- Ter atenção á caixa de email
- Evitar redes públicas
- Manter os sistemas operativos e as aplicações atualizadas

O papel de auditores externos e da modernização do IT na redução de riscos de segurança



Sistemas Legacy vs Sistemas Cloud

Legacy

- “Security-by-antiquity”;
- Acessibilidade limitada reduz vulnerabilidade;
- Falta de documentação e ferramentas desatualizadas resulta em sistemas menos visíveis, limitando as capacidades dos atacantes;

Cloud

- Cloud tem mais capacidade e recursos para fornecer proteção efetiva;
- interfaces standard reduzem acessibilidade dos atacantes;
- Cloud atrai os melhores especialistas em segurança;
- migração para Cloud envolve constante modernização;

Auditores Externos

- Normalmente, auditores externos não possuem conhecimento em IT suficiente;

- Foram estudadas relações entre inovação digital e:
  - conhecimento em IT dos auditores externos;
  - motivação dos auditores na área de IT;
  - performance e falhas de segurança, dependendo do conhecimento dos auditores;

Redução de riscos de cibersegurança

- Modernização digital, tanto nos sistemas em si como no processo de auditoria, é concluída como beneficial;
- Estudos mostram que um grande quantidade de Sistemas Legacy provoca mais incidentes;
- Um pequeno aumento no budget em cloud resulta numa grande diminuição de riscos;
- Auditores externos mais educados em IT resulta na detecção de falhas;

Conclusão

- Promover a consciencialização dos utilizadores reduz o risco de ciberataques.
- A proteção dos dados requer cultura da segurança dentro das organizações.
- Riscos são menores quando são implementadas soluções modernas de segurança.