



VIII SINGEP

Simposio Internacional de Gestao de Projetos, Inovacao e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302

8TH INTERNATIONAL CONFERENCE



ANÁLISE DA GESTÃO DE RISCOS COM FOCO EM REQUISITOS DE SISTEMAS DE SEGURANÇA DE DADOS PARA HEALTHCARE

ANALYSIS OF RISK MANAGEMENT WITH FOCUS ON DATA SECURITY SYSTEM REQUIREMENTS FOR HEALTHCARE

FABIO MARTINS DIAS

UNINOVE – UNIVERSIDADE NOVE DE JULHO

MAURO LUIZ MARTENS

UNINOVE – UNIVERSIDADE NOVE DE JULHO

Nota de esclarecimento:

Comunicamos que devido à pandemia do Coronavírus (COVID 19), o VIII SINGEP e a 8ª Conferência Internacional do CIK (CYRUS Institute of Knowledge) foram realizados de forma remota, nos dias **01, 02 e 03 de outubro de 2020**.

Agradecimento à orgão de fomento:

Prezados colegas, participantes, equipe e demais envolvidos. É com imensa satisfação que venho a agradecer pela oportunidade de poder participar do VIII Singep. Espero estar contribuindo para o fomento da ciência e de nosso setor.



VIII SINGEP

Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302

8TH INTERNATIONAL CONFERENCE



ANÁLISE DA GESTÃO DE RISCOS COM FOCO EM REQUISITOS DE SISTEMAS DE SEGURANÇA DE DADOS PARA HEALTHCARE

Objetivo do estudo

Estudar a gestão de riscos com foco na identificação de requisitos de sistemas de segurança de dados para controle em healthcare. Nesse sentido, desenvolve-se um estudo de planos de gerenciamento de riscos evidenciando itens mínimos de segurança para dispositivos médicos e melhores práticas que devem ser empregadas.

Relevância/originalidade

Estatísticas mostram um quadro preocupante sobre os desafios a serem superados pela cibersegurança no setor de healthcare. Dados mostram que, somente nos EUA, o setor sofre quatro violações de dados por semana. Em perspectiva, um em cada três cidadãos americanos é vítima de violações de informações, sendo o setor que mais são encontradas brechas de segurança digital.

Metodologia/abordagem

Com uma pesquisa descritiva, baseia-se na revisão sistemática da literatura, por meio da coleta dos dados com a pesquisa bibliográfica e interpretação do estado da arte com análise de conteúdo. Utiliza-se palavras-chave assertivas, critérios de seleção das fontes, interpretação dos artigos e análise das bases de dados para representar um amplo espectro.

Principais resultados

Não há um modo completamente eficaz de impedir todas as violações de cibercriminosos, entretanto a cibersegurança deve fazer parte dos processos de gestão das organizações. Com esta visão uma série de requisitos de segurança de dados são identificados como um meio de melhorar a resiliência através de elementos mínimos de segurança cibernética.

Contribuições teóricas/metodológicas

Contribui com análises de mensuração da literatura, identificando as principais lacunas encontradas, identificando os principais autores nesse segmento.

Contribuições sociais/para a gestão

Contribui com um plano de gerenciamento de riscos e estratégias para combater riscos cibernéticos com requisitos mínimos para segurança de dispositivos médicos.

Palavras-chave: Cibersegurança, Sistemas ciber-físicos, Indústria 4.0, Gestão de saúde



VIII SINGEP

Simposio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302

8TH INTERNATIONAL CONFERENCE



ANALYSIS OF RISK MANAGEMENT WITH FOCUS ON DATA SECURITY SYSTEM REQUIREMENTS FOR HEALTHCARE

Study purpose

Study risk management with a focus on identifying data security system requirements for health control. In this sense, develop a study of risk management plans that allow minor items of safety for medical devices and best practices that should be employed.

Relevance / originality

Statistics show a worrying picture about the challenges to be overcome by cybersecurity in the healthcare sector. Data shows that in the US alone, the industry suffers four data breaches a week. In perspective, one in three American citizens is a victim of information breaches, the sector with the most digital security breaches found.

Methodology / approach

With a descriptive research, it is based on the systematic review of the literature, through the collection of the data with the bibliographic research and interpretation of the state of the art with content analysis. Assertive keywords, criteria for selecting sources, interpreting articles and analyzing databases are used to represent a wide spectrum.

Main results

There is no completely effective way to prevent all violations by cybercriminals, however cybersecurity must be part of organizations' management processes. With this vision, a series of data security requirements are identified as a means of improving resilience through minimal elements of cybersecurity.

Theoretical / methodological contributions

It contributes to the analysis of measurement of the literature, identifying the main gaps found, identifying the main authors in this segment.

Social / management contributions

Contributes to a risk management plan and strategies to combat cyber risks with minimum requirements for medical device security.

Keywords: Cybersecurity, Cyber-Physical System, Industry 4.0, Health management