

ERNANE ROSA MARTINS
(ORGANIZADOR)

A CIÊNCIA DA COMPUTAÇÃO E O
DESENVOLVIMENTO DE CONTEÚDO
TECNOLÓGICO RELEVANTE
PARA A SOCIEDADE

ERNANE ROSA MARTINS
(ORGANIZADOR)

A CIÊNCIA DA COMPUTAÇÃO E O
DESENVOLVIMENTO DE CONTEÚDO
TECNOLÓGICO RELEVANTE
PARA A SOCIEDADE

2020 by Atena Editora

Copyright © Atena Editora

Copyright do Texto © 2020 Os autores

Copyright da Edição © 2020 Atena Editora

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira

Diagramação: Natália Sandrini de Azevedo

Edição de Arte: Lorena Prestes

Revisão: Os Autores



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição *Creative Commons*. Atribuição 4.0 Internacional (CC BY 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

Conselho Editorial

Ciências Humanas e Sociais Aplicadas

Profª Drª Adriana Demite Stephani – Universidade Federal do Tocantins
Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas
Prof. Dr. Alexandre Jose Schumacher – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso
Profª Drª Angeli Rose do Nascimento – Universidade Federal do Estado do Rio de Janeiro
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná
Prof. Dr. Antonio Gasparetto Júnior – Instituto Federal do Sudeste de Minas Gerais
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília
Prof. Dr. Carlos Antonio de Souza Moraes – Universidade Federal Fluminense
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa
Profª Drª Cristina Gaio – Universidade de Lisboa
Profª Drª Denise Rocha – Universidade Federal do Ceará
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia
Prof. Dr. Edvaldo Antunes de Farias – Universidade Estácio de Sá
Prof. Dr. Eloi Martins Senhora – Universidade Federal de Roraima
Prof. Dr. Fabiano Tadeu Grazioli – Universidade Regional Integrada do Alto Uruguai e das Missões
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná
Profª Drª Ivone Goulart Lopes – Istituto Internazionale delle Figlie de Maria Ausiliatrice
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense
Profª Drª Keyla Christina Almeida Portela – Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso
Profª Drª Lina Maria Gonçalves – Universidade Federal do Tocantins
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof. Dr. Marcelo Pereira da Silva – Universidade Federal do Maranhão
Profª Drª Miranilde Oliveira Neves – Instituto de Educação, Ciência e Tecnologia do Pará
Profª Drª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa
Profª Drª Rita de Cássia da Silva Oliveira – Universidade Estadual de Ponta Grossa
Profª Drª Sandra Regina Gardacho Pietrobon – Universidade Estadual do Centro-Oeste
Profª Drª Sheila Marta Carregosa Rocha – Universidade do Estado da Bahia
Prof. Dr. Rui Maia Diamantino – Universidade Salvador
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande
Prof. Dr. William Cleber Domingues Silva – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

Ciências Agrárias e Multidisciplinar

Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano
Prof. Dr. Antonio Pasqualetto – Pontifícia Universidade Católica de Goiás
Profª Drª Daiane Garabeli Trojan – Universidade Norte do Paraná

Profª Drª Diocléa Almeida Seabra Silva – Universidade Federal Rural da Amazônia
Prof. Dr. Écio Souza Diniz – Universidade Federal de Viçosa
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul
Prof. Dr. Fágner Cavalcante Patrocínio dos Santos – Universidade Federal do Ceará
Profª Drª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Júlio César Ribeiro – Universidade Federal Rural do Rio de Janeiro
Profª Drª Lina Raquel Santos Araújo – Universidade Estadual do Ceará
Prof. Dr. Pedro Manuel Villa – Universidade Federal de Viçosa
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará
Profª Drª Talita de Santos Matos – Universidade Federal Rural do Rio de Janeiro
Prof. Dr. Tiago da Silva Teófilo – Universidade Federal Rural do Semi-Árido
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

Ciências Biológicas e da Saúde

Prof. Dr. André Ribeiro da Silva – Universidade de Brasília
Profª Drª Anelise Levay Murari – Universidade Federal de Pelotas
Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás
Prof. Dr. Edson da Silva – Universidade Federal dos Vales do Jequitinhonha e Mucuri
Profª Drª Eleuza Rodrigues Machado – Faculdade Anhanguera de Brasília
Profª Drª Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina
Prof. Dr. Ferlando Lima Santos – Universidade Federal do Recôncavo da Bahia
Prof. Dr. Fernando José Guedes da Silva Júnior – Universidade Federal do Piauí
Profª Drª Gabriela Vieira do Amaral – Universidade de Vassouras
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria
Profª Drª Iara Lúcia Tescarollo – Universidade São Francisco
Prof. Dr. Igor Luiz Vieira de Lima Santos – Universidade Federal de Campina Grande
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará
Profª Drª Magnólia de Araújo Campos – Universidade Federal de Campina Grande
Profª Drª Mylena Andréa Oliveira Torres – Universidade Ceuma
Profª Drª Natiéli Piovesan – Instituto Federaci do Rio Grande do Norte
Prof. Dr. Paulo Inada – Universidade Estadual de Maringá
Profª Drª Renata Mendes de Freitas – Universidade Federal de Juiz de Fora
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

Ciências Exatas e da Terra e Engenharias

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto
Prof. Dr. Alexandre Leite dos Santos Silva – Universidade Federal do Piauí
Prof. Dr. Carlos Eduardo Sanches de Andrade – Universidade Federal de Goiás
Profª Drª Carmen Lúcia Voigt – Universidade Norte do Paraná
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Prof. Dr. Juliano Carlo Rufino de Freitas – Universidade Federal de Campina Grande
Profª Drª Luciana do Nascimento Mendes – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Prof. Dr. Marcelo Marques – Universidade Estadual de Maringá
Profª Drª Neiva Maria de Almeida – Universidade Federal da Paraíba
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

Conselho Técnico Científico

Prof. Me. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo
Prof. Me. Adalberto Zorzo – Centro Estadual de Educação Tecnológica Paula Souza
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba
Prof. Me. André Flávio Gonçalves Silva – Universidade Federal do Maranhão

Profª Drª Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico
 Profª Drª Andrezza Miguel da Silva – Universidade Estadual do Sudoeste da Bahia
 Prof. Dr. Antonio Hot Pereira de Faria – Polícia Militar de Minas Gerais
 Profª Ma. Bianca Camargo Martins – UniCesumar
 Profª Ma. Carolina Shimomura Nanya – Universidade Federal de São Carlos
 Prof. Me. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro
 Prof. Ma. Cláudia de Araújo Marques – Faculdade de Música do Espírito Santo
 Prof. Me. Daniel da Silva Miranda – Universidade Federal do Pará
 Profª Ma. Dayane de Melo Barros – Universidade Federal de Pernambuco
 Prof. Me. Douglas Santos Mezacas -Universidade Estadual de Goiás
 Prof. Dr. Edwaldo Costa – Marinha do Brasil
 Prof. Me. Eliel Constantino da Silva – Universidade Estadual Paulista Júlio de Mesquita
 Profª Ma. Fabiana Coelho Couto Rocha Corrêa – Centro Universitário Estácio Juiz de Fora
 Prof. Me. Felipe da Costa Negrão – Universidade Federal do Amazonas
 Profª Drª Germana Ponce de Leon Ramírez – Centro Universitário Adventista de São Paulo
 Prof. Me. Gevair Campos – Instituto Mineiro de Agropecuária
 Prof. Me. Guilherme Renato Gomes – Universidade Norte do Paraná
 Profª Ma. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia
 Prof. Me. Javier Antonio Albornoz – University of Miami and Miami Dade College
 Profª Ma. Jéssica Verger Nardeli – Universidade Estadual Paulista Júlio de Mesquita Filho
 Prof. Me. José Luiz Leonardo de Araujo Pimenta – Instituto Nacional de Investigación Agropecuaria Uruguay
 Prof. Me. José Messias Ribeiro Júnior – Instituto Federal de Educação Tecnológica de Pernambuco
 Profª Ma. Juliana Thaisa Rodrigues Pacheco – Universidade Estadual de Ponta Grossa
 Prof. Me. Leonardo Tullio – Universidade Estadual de Ponta Grossa
 Profª Ma. Lilian Coelho de Freitas – Instituto Federal do Pará
 Profª Ma. Liliani Aparecida Sereno Fontes de Medeiros – Consórcio CEDERJ
 Profª Drª Lívia do Carmo Silva – Universidade Federal de Goiás
 Prof. Me. Luis Henrique Almeida Castro – Universidade Federal da Grande Dourados
 Prof. Dr. Luan Vinicius Bernardelli – Universidade Estadual de Maringá
 Profª Ma. Marileila Marques Toledo – Universidade Federal dos Vales do Jequitinhonha e Mucuri
 Prof. Me. Rafael Henrique Silva – Hospital Universitário da Universidade Federal da Grande Dourados
 Profª Ma. Renata Luciane Polsaque Young Blood – UniSecal
 Profª Ma. Solange Aparecida de Souza Monteiro – Instituto Federal de São Paulo
 Prof. Me. Tallys Newton Fernandes de Matos – Faculdade Regional Jaguaribana
 Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

**Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)**

C569 A ciência da computação e o desenvolvimento de conteúdo tecnológico relevante para a sociedade [recurso eletrônico] / Organizador Ernane Rosa Martins. – Ponta Grossa, PR: Atena, 2020.

Formato: PDF

Requisitos de sistema: Adobe Acrobat Reader

Modo de acesso: World Wide Web

Inclui bibliografia

ISBN 978-65-86002-68-3

DOI 10.22533/at.ed.683202003

1. Computação – Pesquisa – Brasil. 2. Sociedade e tecnologia.
I. Martins, Ernane Rosa.

CDD 004

Elaborado por Maurício Amormino Júnior – CRB6/2422

Atena Editora

Ponta Grossa – Paraná - Brasil

www.atenaeditora.com.br

APRESENTAÇÃO

A Ciência da Computação estuda as técnicas, metodologias e instrumentos computacionais, visando automatizar os processos e desenvolver soluções com o uso de processamento de dados. Este livro, se propõe a permitir que seus leitores venham a conhecer melhor o panorama atual da Ciência da Computação no Brasil, assim como, os elementos básicos desta ciência, por meio do contato com alguns dos conceitos fundamentais desta área, apresentados nos resultados relevantes dos trabalhos presentes nesta obra, realizados por autores das mais diversas instituições.

A Ciência da Computação, proporciona inúmeros benefícios para a sociedade moderna, tais como: a criação de empregos, o desenvolvimento de novos equipamentos, o ganho de produtividade nas empresas e o acesso à informação. Os estudos desta área são aplicados em diversas outras áreas do conhecimento, proporcionando a resolução de diferentes problemas da sociedade, sendo assim, cada vez mais estes profissionais são valorizados e prestigiados no mercado de trabalho. As empresas enxergam atualmente a necessidade de profissionais cada vez mais qualificados nesta área, a fim de que possam promover ainda mais inovação, desenvolvimento e eficiência.

Dentro deste contexto, este livro aborda diversos assuntos importantes para os profissionais e estudantes desta área, tais como: a utilização das Tecnologias de Informação e Comunicação (TIC's), a acessibilidade na web, a simulação por eventos discretos, as metodologias ativas, as técnicas de Data Mining, os Objetos Digitais de Aprendizagem (ODA), o uso do *Facebook* como interface didático-pedagógica, a aprendizagem colaborativa, os Sistemas de Informação Social, e a avaliação de softwares educativos, como por exemplo, a ferramenta Alice.

Sendo assim, os trabalhos apresentados nesta obra, permitem aos leitores analisar e discutir os relevantes assuntos abordados, tendo grande importância por constituir-se numa coletânea de trabalhos, experimentos e vivências de seus autores. Espera-se que esta venha a ajudar tanto aos alunos dos cursos de Ciência da Computação quanto aos profissionais atuantes nesta importante área do conhecimento, a enfrentarem os mais diferentes desafios da atualidade. Por fim, agradeço a cada autor, pela excelente contribuição na construção deste livro, e desejo a todos os leitores, uma excelente leitura, repleta de boas, novas e significativas reflexões sobre os temas abordados, e que estas possam contribuir fortemente no aprendizado.

Ernane Rosa Martins

SUMÁRIO

CAPÍTULO 1	1
A UTILIZAÇÃO DAS <i>TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO (TIC'S)</i> NAS AULAS DA DISCIPLINA CÁLCULO	
Rávila Beatriz Costa Furtado Edilson Santos Melo Eldilene da Silva Barbosa Wagner Davy Lucas Barreto Gustavo Nogueira Dias	
DOI 10.22533/at.ed.6832020031	
CAPÍTULO 2	11
ACCESIBILIDAD WEB. UN APORTE DE RESPONSABILIDAD SOCIAL UNIVERSITARIA	
Sonia Itatí Mariño Pedro Luis Alfonzo María Viviana Godoy Guglielmone	
DOI 10.22533/at.ed.6832020032	
CAPÍTULO 3	18
ANÁLISE DE UMA IMPLEMENTAÇÃO OPEN SOURCE PARA GERENCIAMENTO E SEGURANÇA DE REDE	
Vitor Hugo Melo Araújo	
DOI 10.22533/at.ed.6832020033	
CAPÍTULO 4	31
METODOLOGIAS ATIVAS COM O USO DE MAQUETES INTEGRADAS AO ENSINO DA DISCIPLINA DE LOGÍSTICA	
Reinaldo Toso Júnior Luis Borges Gouveia	
DOI 10.22533/at.ed.6832020034	
CAPÍTULO 5	47
MINERÍA DE DATOS PARA LA DETERMINAR LOS PERFILES DE RENDIMIENTO ACADÉMICO DE LOS ALUMNOS EN LA UNNE	
Julio César Acosta David Luis La Red Martínez	
DOI 10.22533/at.ed.6832020035	
CAPÍTULO 6	60
OBJETO DIGITAL DE APRENDIZAGEM COMO FERRAMENTA PEDAGÓGICA PARA O ENSINO E A APRENDIZAGEM NO ENSINO FUNDAMENTAL	
Lenir Santos do Nascimento Moura Marilene Kreutz de Oliveira Ozanira Lima dos Afritos	
DOI 10.22533/at.ed.6832020036	
CAPÍTULO 7	77
TECNOLOGIA E EDUCAÇÃO ABERTA E DIGITAL: NOVOS ENFOQUES NA CONTEMPORANEIDADE	
Willian Lima Santos Rosana Maria Santos Torres Marcondes Izabel Silva Souza D'Ambrosio	

Manoel Messias Santos Alves
DOI 10.22533/at.ed.6832020037

CAPÍTULO 8 89

SOCIAL INFORMATION SYSTEMS: AN APPROACH TO COMPLEXITY

Jeferson Gonçalves de Oliveira
Cristiana Fernandes De Muyllder
Marta Macedo Kerr Pinheiro
Ana Maria Pereira Cardoso

DOI 10.22533/at.ed.6832020038

CAPÍTULO 9 107

UMA ANÁLISE DA FERRAMENTA ALICE NO ENSINO DA LÓGICA DE PROGRAMAÇÃO

Márcia Antônia Dias Catunda
Mayumi Passos Lopes

DOI 10.22533/at.ed.6832020039

SOBRE O ORGANIZADOR..... 116

ÍNDICE REMISSÍVO 117

ANÁLISE DE UMA IMPLEMENTAÇÃO OPEN SOURCE PARA GERENCIAMENTO E SEGURANÇA DE REDE

Data de aceite: 18/03/2020

Vitor Hugo Melo Araújo

Mestre em Tecnologia – Faculdade de Tecnologia
- UNICAMP
Limeira – São Paulo

RESUMO: Este artigo é resultado de uma dissertação de mestrado que teve como objetivo modelar a partir de um modelo computacional o OSSIM para que fosse possível avaliar e possibilitar melhorias no desempenho, em especial estudar e avaliar sua performance e pontos críticos. Para atingir tais objetivos, foi realizada uma revisão da literatura, envolvendo o tema, com uma breve contextualização sobre Segurança de Redes e Detecção de Intrusão, Fundamentação sobre o OSSIM, Simulação por Eventos Discretos e Teoria de filas, além de análise de trabalhos já existentes. A metodologia da pesquisa segue os passos apontados por Freitas Filho (2008), com formulação e análise do problema; planejamento do problema; formulação do modelo conceitual, coleta de macro informações e dados; tradução do modelo; verificação e validação; projeto experimental; experimentação; interpretação e análise estatísticas dos resultados. Foram

propostas duas formas de se efetuar a validação, a primeira utilizando um modelo analítico conhecido em que o modelo de simulação foi validado com relação ao modelo analítico com 95% de confiança e a segunda se baseando em dados colhidos pelas referências bibliográficas em que as informações geradas apresentaram similaridade e as informações geradas são confiáveis. Conclui-se que os atrasos em agentes baseados em IDS podem comprometer à segurança de rede dentro das organizações em função do grande número de ataques virtuais planejados por cibercriminosos pelo mundo.

PALAVRAS-CHAVE: Simulação por Eventos Discretos. OSSIM. Open Source. Desempenho.

ANALYSIS OF AN OPEN SOURCE IMPLEMENTATION FOR NETWORK SECURITY AND MANAGEMENT

ABSTRACT: This article is the result of a master's dissertation has aimed to model OSSIM through a computational model, enabling its evaluation and performance improvements, mainly the study and evaluation of its performance and critical points. To do that so, this dissertation reviewed the literature concerning the matter, including a brief contextualization on Network

Security and Intrusion Detection, Rationale on OSSIM, Discrete-Event Simulation and Queueing Theory, as well as the analysis of existing works. The research methodology follows the steps pointed out by Freitas Filho (2008), with problem formulation and analysis; problem planning; formulation of the conceptual model, collection of macro information and data; model translation; verification and validation; experimental design; experimentation; interpretation and statistical analysis of data collected. Were proposed two ways to perform the validation, the first using an analytical model known in the simulation model was validated with respect to the analytical model with 95% confidence interval and the second based on data collected by the references in the information generated showed similarity and the information generated are reliable. It has been concluded that delays in IDS-based agents may compromise network security within organizations due to the large number of virtual attacks planned by cybercriminals around the world.

KEYWORDS: Discrete-Event Simulation. OSSIM. Open Source. Performance.

1 | INTRODUÇÃO

As redes de computadores estão cada vez mais em evidência, principalmente com a utilização da Internet.

À medida em que as redes são cada vez mais utilizadas surgem as necessidades de técnicas e serviços de segurança e uma boa política é necessária para se administrar a rede e garantir a sua segurança, como antivírus, *firewall* e diversos outros métodos de prevenção de ataques.

Além da segurança vale destacar a importância do gerenciamento da rede, que faz um monitoramento e controle centralizado remoto (STALLINGS, 2005). O responsável pelo gerenciamento da rede precisa conhecer as ferramentas disponíveis para um planejamento mais eficaz envolvendo a segurança. Dentre estas ferramentas destaca-se o OSSIM – *Open Source Security Information Management* (Gerenciador de Informações de Segurança de Código Aberto).

O OSSIM tem como objetivo unificar o monitoramento e a segurança de redes em uma única ferramenta. Foi criado devido às necessidades dos profissionais de segurança em redes, fornecendo as capacidades essenciais de segurança em uma plataforma unificada. É mantido pela empresa *Alien Vault*, que promove o desenvolvimento contínuo do projeto OSSIM (ALIENVAULT, 2016).

O uso desta ferramenta única auxilia e dá maior suporte ao administrador de segurança, ao contrário do que se teria utilizando diversas ferramentas independentes.

Observou-se que o estudo do OSSIM pode ser complementado com técnicas de simulação por eventos discretos. Com o estudo da simulação da ferramenta

OSSIM, podemos realizar algumas modificações sobre o processamento a fim de avaliar o desempenho e, comparar o desempenho com outras ferramentas além de identificar possíveis problemas relacionados a requisitos não cumpridos.

Este artigo é um resumo da dissertação de mestrado defendida na Faculdade de Tecnologia da Unicamp por Araújo (2019).

A principal contribuição para a área da tecnologia da informação e comunicação (TIC) está, portanto, na criação de uma abordagem por meio de simulação gerada a partir de eventos discretos, podendo assim antecipar problemas futuros.

Sendo assim, o objetivo geral do trabalho é modelar por um modelo computacional o OSSIM para que possamos avaliar e possibilitar melhorias no desempenho deste.

2 | REFERENCIAL TEÓRICO

Nesta seção serão revisados os principais conceitos relacionados ao OSSIM e à simulação por eventos discretos.

2.1 Segurança de Redes e Detecção de Intrusão

A internet se faz presente hoje em toda e qualquer residência e estabelecimento e sua alta acessibilidade acaba gerando um uso imprudente por parte das pessoas, que em geral não conhecem os riscos associados à segurança de dados. Funcionários acabam por não seguir as normas dos seus locais de ofício e ameaças à segurança acabam emergindo.

Foi pensando nessa vulnerabilidade e em uma forma de auxiliar os administradores de redes que surgiram as diversas ferramentas e aplicações para controle da segurança. Para obtenção de um funcionamento estável é necessária uma gestão das redes de computadores, que consiste em uma boa gestão interna. Contudo, ainda é possível o aparecimento de falhas provocadas por agentes externos e diversos tipos de ataques danosos e/ou intrusos (TAVARES, 2015).

Intrusão pode ser considerada como qualquer tipo de atividade ou ação não autorizada, que ocorre dentro ou fora de uma rede de computadores, no qual as ações podem vir a afetar a disponibilidade, integridade, ou confiabilidade dos recursos da rede de forma direta ou indireta (TAVARES, 2015 p.16).

Tavares (2015) apresenta dois tipos de IDS: os HIDS (*Host Intrusion Detection System*) e os NIDS (*Network Intrusion Detection System*). Os HIDS monitoram um determinado host, que por sua vez atua de forma independente na rede, e disponibiliza suas próprias informações. Os NIDS agem no tráfego da rede, avaliando as atividades suspeitas.

2.2 Fundamentação Teórica sobre o OSSIM

Donado et al. (2011) e Polo (2008) conceituam o OSSIM como uma ferramenta *Open Source*, usada para o gerenciamento e segurança da rede, incorporando mais de 15 programas que têm a função de coletar informações para processamento posterior, permitindo a exibição a partir de um ponto central.

O OSSIM é um *framework* que possui diversas ferramentas populares de gestão de segurança, oferecendo grande capacidade e um alto desempenho no tratamento dos dados. Algumas ferramentas do OSSIM se destacam como – Snort, Nessus, Ntop, Nagios e Osirir. Santos et al. (2009) definem estas ferramentas do seguinte modo:

- Nessus: ferramenta de auditoria, muito utilizada para detectar e corrigir vulnerabilidade nos PCs da rede local;
- Snort: considerado um dos melhores *softwares* quando se trata de IDS – *Intrusion Detection System* (Sistema de Detecção de Intrusão);
- Ntop: faz um monitoramento passivo na rede, no qual coleta dados sobre os protocolos e *hosts* da rede;
- Nagios: sistema que consegue gerar relatórios de acesso e *status* das máquinas, detectando problemas que podem estar ocorrendo em uma máquina antes que elas afetem gravemente o sistema. Este sistema tem aplicação no processo de obtenção de informações de monitorização de serviços;
- Ossec: Pode tomar algumas medidas para determinados tipos de ataques, como o bloqueio temporário do IP que está sendo atacado e envio de uma notificação sobre o alerta por e-mail. Em Tavares (2015) verificamos que o OSSEC é um HIDS multiplataforma. Suas outras características são: escalável – implementa um forte componente de correlação – integra a análise de diversos logs – faz alerta em tempo real – faz resposta ativa. É fácil de ser executado e passível de aplicação na maioria dos sistemas, sendo um dos agentes mais importantes para o OSSIM.

Podemos afirmar que a principal finalidade do OSSIM é selecionar as principais ferramentas *open source* e agregar em uma única solução poderosa de SIEM. Sua análise das ameaças é feita por meio de correlação e informa em tempo real o estado de risco do ambiente. Seu *design* permite aos gestores de segurança em redes algo agradável e organizado.

A arquitetura do OSSIM é composta por quatro elementos: sensores, servidores, banco de dados e console. Os sensores, que podem ser ativos ou passivos, monitoram a atividade da rede. Já os servidores recebem as informações dos sensores, centralizam e fazem relatórios que explicam a informação recolhida. Em seguida, o banco de dados armazena essas informações e, por fim, o console exibe o gráfico dos resultados e as configurações do sistema (POLO, 2008). As figuras representam a arquitetura do OSSIM (Figura 1) e o console principal (Figura 2).

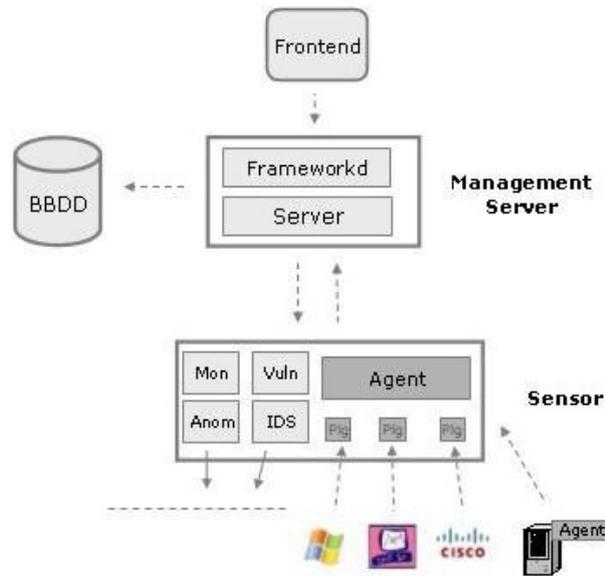


Figura 1 - Arquitetura de uma GPU.

Fonte: <https://www.alienvault.com/wiki/lib/exe/fetch.php>

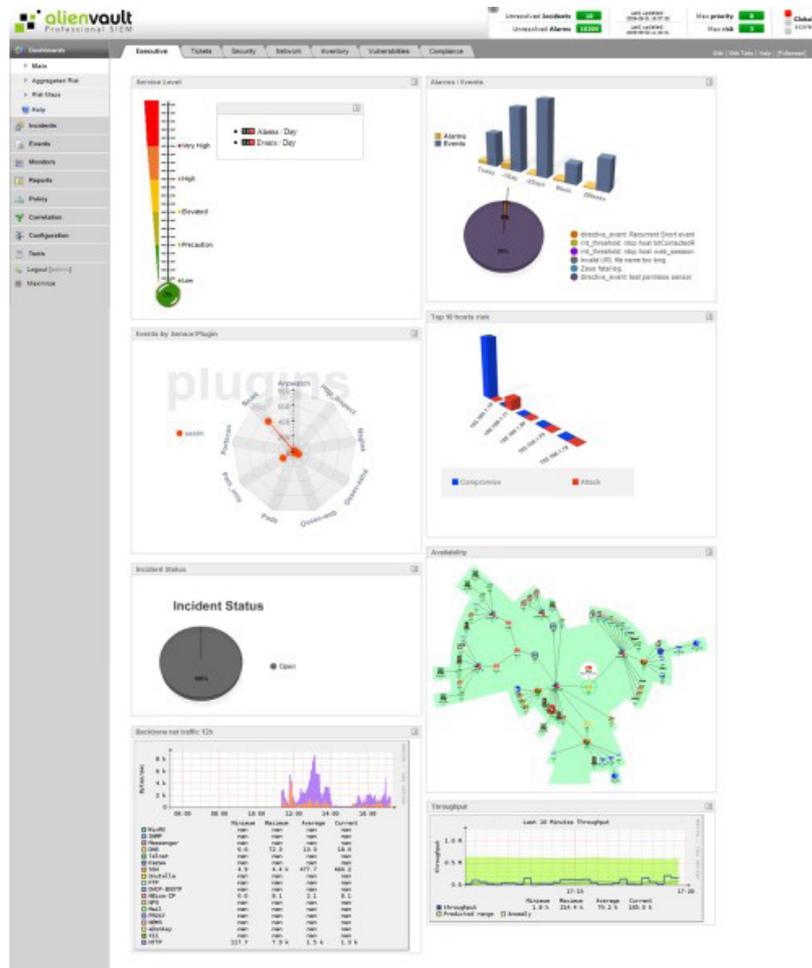


Figura 2 - Console Principal do OSSIM.

Fonte: <http://www.previsioni.com.br/jailsonjan/>

2.3 Simulação

Segundo Prado (2003, p.24), “Simulação é uma técnica de solução de um problema pela análise de um modelo que descreve o comportamento do sistema

usando um computador digital”, sendo este o conceito de simulação mais aceito atualmente.

Para o Sasaki (2007, p. 5) a simulação por eventos discretos “... é simplesmente a execução de um programa de computador que implementa um autômato de estados temporizados”. Ou seja, trata-se de uma técnica que utiliza um simulador e sua execução se dá pela entrada e saída dos dados.

Segundo Prado (2003), as pessoas preferem a simulação por três motivos: pela simplicidade de sua aplicação, pelo o estudo da viabilidade da implementação de um novo sistema para possíveis análises, e por não apresentar interferência com o sistema real.

A simulação é um modelo muito utilizado em pesquisa, desde eventos complexos até os mais simples, e neste trabalho ela é empregada com o objetivo de realizar um modelo computacional do OSSIM, para que se possa avaliar e possibilitar melhorias no desempenho do mesmo.

Dentre os softwares para simulação, destaca-se o Arena®, lançado em 1993 pela empresa *Systems Modeling*, sucessor de outros dois *softwares* de sucesso, SIMAN e CINEMA, ambos desenvolvidos pela mesma companhia.

De acordo com Prado (2003), o Arena® dispõe de um conjunto de blocos utilizados para representar uma aplicação real, funcionando como os comandos de uma linguagem de programação (Fortran, Cobol, VB, etc.) e, projetados sob a perspectiva da simulação. O Arena, em sua versão livre [estudante], foi utilizado na versão inicial deste projeto.

Para classificar uma simulação de sistemas discretos e contínuos, é preciso se basear em uma variação ao longo do tempo.

A característica dos modelos de sistema discretos é a utilização de variáveis discretas no tempo, que, conforme apontado por Ramírez (2006) podem ser determinísticos e estocásticos, sendo o conceito de tempo discreto os instantes de tempo em que o sistema muda. São considerados modelos discretos aqueles em que há incrementos na contagem de tempo da simulação, podendo os valores serem fixos.

Já os sistemas contínuos as variáveis se modificam ao longo do tempo e não em instantes ou intervalos de tempo. Ou seja, o avanço da contagem de tempo é contínuo, permitindo determinar os valores das variáveis a qualquer momento.

A simulação *Event-Driven*, técnica que pode ser utilizada em diversos sistemas e empregada em evento, se mostra eficiente em sistemas que não possuem relógios que sincronizam os modelos ou quando alguns estados dos modelos podem se alterar (NETO, 2001).

2.4 Teoria das Filas

A teoria das filas refere-se à modelagem analítica de sistemas e no que se resulta em esperas. Seu objetivo é avaliar as quantidades e determinar maneiras de minimizar os impactos negativos de espera. De forma exemplificada podemos citar as filas em caixas de supermercado.

Outros exemplos encontramos no trabalho de Oliveira et al. (2017). Para as autoras, apoiadas nos estudos de Lovelock e Wright (2002), o processo de formação de filas se dá quando há um elevado número de chegadas, que acaba excedendo a capacidade de atendimento do sistema, geralmente com problemas relacionados a administração da capacidade.

A teoria de filas é hoje estudada por muitos autores, mas em síntese se refere a processos em que os usuários recebem um serviço pelo qual esperam por um período de tempo, e nos quais a demanda é maior que a capacidade de atendimento. Sendo assim, a fila irá sempre existir quando o atendimento do servidor for menor que a chegada dos usuários (ARANTES, 2015).

Em resumo a teoria das filas é um ramo da probabilidade que estuda a formação de filas, através de análises matemáticas precisas e propriedades mensuráveis das filas, avaliando assim a eficiência da prestação do serviço.

Estudar a teoria das filas é uma forma de analisar conceitos que influenciam a operação de um sistema, como forma de atendimento, disciplina da fila, forma de chegada e estrutura do sistema de atendimento (OLIVEIRA et al., 2017). As equações se dão da seguinte maneira: as chegadas utilizam a distribuição de Poisson com média λ chegadas/tempo, sendo que o tempo utiliza uma distribuição exponencial de Poisson com média μ (OLIVEIRA et al., 2017).

Considerando as informações até aqui discutidas, é notável a importância em se reconhecer o tipo de sistema que será necessário, para que as fórmulas corretas sejam empregadas (FREITAS FILHO, 2008). Existem inúmeras variações de sistemas e modelos, sendo os mais utilizados o M/M/1 (modelo mais estudado),

O modelo de fila M/M/1 possui chegadas e atendimentos Markovianos (distribuição de Poisson ou Exponencial negativa), sendo distribuição exponencial a distribuição probabilística mais importante, que é representada por um parâmetro λ (ARANTES, 2015).

3 | METODOLOGIA

A metodologia deste trabalho segue os passos apontados por Freitas Filho (2008), com formulação e análise do problema; planejamento do problema; formulação do modelo conceitual, coleta de macro informações e dados; tradução

do modelo; verificação e validação; projeto experimental; experimentação; interpretação e análise estatísticas dos resultados.

3.1 Formulação e Análise do Problema

A dissertação propõe a realização da simulação na ferramenta OSSIM, analisando a taxa de ocupação dos recursos disponíveis, os gargalos do processo, o tempo de fila, o tempo de permanência no sistema, a quantidade de alertas gerados, além de permitir a análise de cenários alternativos de aplicação da ferramenta avaliando os pontos críticos do OSSIM.

3.2 Planejamento do Projeto

No decorrer do trabalho definimos a metodologia e iniciamos a proposta de simulação. Verificou-se que o único material necessário foi um computador, com processador Intel® Core (TM) i7 – 7500U 2.7GHz, memória de 16GB e Sistema Operacional Windows 10 64 bits, com o *software* Arena® Acadêmico (*Student*) instalado, com a previsão orçamentária inicial sem custo.

3.3 Formulação do Modelo Conceitual

De acordo com Freitas Filho (2008), é recomendado que o modelo inicie de forma simplificada, e vá crescendo até atingir a forma mais complexa do sistema a ser modelado, contemplando todas as suas características.

3.4 Coleta de Macroinformações e Dados

Para conduzir os futuros esforços de coleta de dados para alimentação de parâmetros do sistema modelado, utilizou-se o cenário de ataques proposto por Tavares (2015), a qual foi verificado o comportamento do OSSIM exposto a ataques.

Observou-se cerca de 300 mil eventos registrado na base de dados, após 24 horas de monitoramento. Tais valores foram utilizados provisoriamente, podendo ser obtidos por meio de medidas e/ou melhorados por meio de pesquisa futura.

3.5 Tradução do Modelo

Visando realizar o estudo de simulação da ferramenta OSSIM, utilizaremos o modelo apresentado na Figura 3 por meio do *software* Arena®, para permitir a avaliação de seu desempenho e tratamento dos eventos gerados por seus agentes.

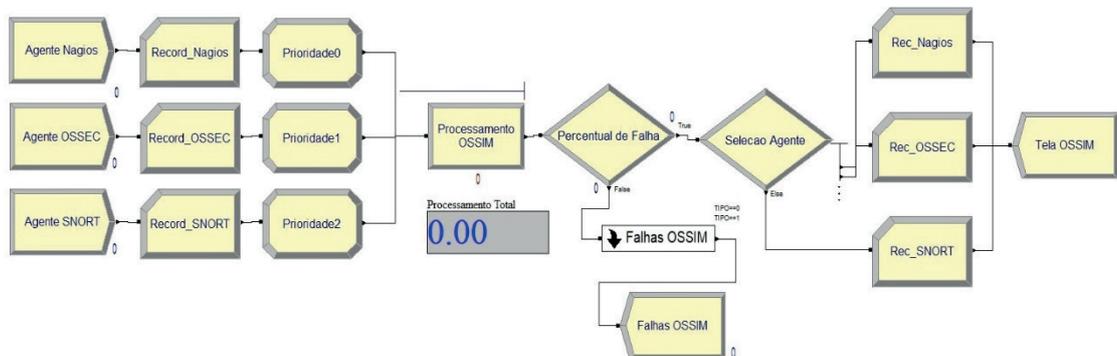


Figura 3 - Modelo Computacional OSSIM. Desenvolvido pelo autor.

Para a criação do modelo computacional OSSIM foi escolhido como fonte de geração dos eventos três ferramentas das cinco destacadas por Santos et al. (2009): Nagios (sua principal função é gerar relatórios de acesso e *status* das máquinas detectando possíveis problemas na mesma antes que eles afetem o sistema), OSSEC (responsável por verificar integridade, analisar e detectar *rootkits*) e o Snort (responsável pela captura de pacotes, análise de tráfego de rede – *Sniffer*).

3.6 Verificação e Validação

São propostas duas formas de se efetuar a validação. A primeira utiliza um modelo analítico conhecido e mostra que seus resultados são similares à simulação e a segunda se baseia em dados colhidos pelas referências bibliográficas.

A comparação com o modelo analítico é servirá como base para avaliar a correção do modelo conforme poder ser vistos os parâmetros da Tabela 1. As equações do modelo de prioridade do tipo HOL para os tempos médios de esperas na fila são as da Equação 1 (JAISWAL, 1961).

$$W_k = \frac{\frac{1}{2} \sum_{i=1}^k E[S_i^2]}{(1 - \rho_1 - \dots - \rho_{k-1})(1 - \rho_1 - \dots - \rho_k)} \quad (1)$$

PARÂMETRO	NAGIOS	OSSEC	SNORT
Entidades por Chegada	1	1	1
Tempo entre as Chegadas	6s	2s	2s
Prioridade	0	1	2
Duração	1s	0,1s	0,1s

Tabela 1 – Valor dos Parâmetros da Simulação para Efeito de Validação

Os valores de tempo médio de permanência no sistema são $R_k = W_k + E[S_k]$, $\rho_k = \lambda_k \cdot E[S_k]$, $E[S_k]$ é o tempo médio de serviço e $E[S_k^2]$ é seu segundo momento.

AGENTE	Matlab	Arena
NAGIOS	1,24	1,27 ±0,11
OSSEC	0,39	0,37 ±0,04
SNORT	0,41	0,35 ±0,04

Tabela 2 – Tempo no Sistema por Agente: Matlab e Arena

Portanto, os resultados da Tabela 2 mostram que, com 95% de confiança, o modelo de simulação está validado com relação ao modelo analítico.

A verificação e validação do modelo também se baseou no trabalho proposto por Tavares (2015) em que as informações geradas em nossa simulação apresentam similaridades com a do autor.

O modelo utilizado vai de acordo com os objetivos do estudo e as informações geradas são confiáveis, uma vez que todos os procedimentos foram seguidos fidedignamente e seguem as necessidades deste momento. Uma vez verificado e validado, o modelo de simulação poderá ser refinado com outros valores e distribuições que mais refletem a realidade.

Utilizando os valores de parâmetros da simulação conforme Tabela 1 para executar a simulação, conseguimos os dados para tempo de fila por agente e taxa de utilização dos recursos, mostrados nas Tabelas 3 e 4.

AGENTE	TEMPO MÉDIO	TEMPO MÍNIMO	TEMPO MÁXIMO
NAGIOS	1,5583s	1,0000s	12,4426s
OSSEC	0,4883s	0,1000s	9,2149s
SNORT	0,6028s	0,1000s	3,8218s

Tabela 3 – Tempo de Fila por Agente

RECURSO	TAXA DE OCUPAÇÃO
Processamento OSSIM	51,69%

Tabela 4 – Taxa de Utilização

Neste modelo foram gerados 14.379 eventos do Agente Nagios, 43.225 eventos OSSEC e 259.640 Snort. Foram processados 317.250 agentes sendo que 301.345 foram apresentados à Tela do OSSIM, 15.905 foram direcionados como falha, ou seja, falsos positivos que foram processados utilizando assim recursos desnecessários.

Observamos que apesar de uma taxa de ocupação próximo de 52% (Tabela

4) alguns agentes tiveram um tempo máximo muito alto (Tabela 3), e esses atrasos podem ser prejudiciais à segurança de rede.

4 | RESULTADOS

Partindo da análise do modelo da Seção 3.6 onde propomos duas formas de se efetuar a validação, sendo a primeira utilizando o modelo analítico conhecido mostrando que seus resultados são similares à simulação e a segunda se baseia em dados colhidos pelas referências bibliográficas.

Na validação com modelo analítico tivemos um percentual de 95% de confiança, ou seja, o modelo de simulação está validado com relação ao modelo analítico. Houve uma pequena variação (diferença inferior a 95%) para o Agente de menor prioridade (SNORT).

Na validação com o modelo real da literatura em que as informações geradas em nossa simulação apresentaram similaridade e, uma vez verificado e validado, o modelo de simulação poderá ser refinado com outros valores e distribuições que mais refletem a realidade.

A aplicação da simulação neste contexto contribuiu inicialmente para que tivéssemos uma visão geral da solução OSSIM, trata-se de uma simulação de extrema importância para o dimensionamento e/ou planejamento do sistema.

5 | CONCLUSÕES

Este trabalho teve como objetivo geral modelar por um modelo computacional o OSSIM, a fim de avaliar e possibilitar melhorias no desempenho deste. Sendo assim, o modelo de simulação foi validado com relação ao modelo analítico conhecido com 95% de confiança e por meio de comparação com o modelo real da literatura, onde foi possível reconhecer que os resultados da aplicação de simulação proposta nesta dissertação se mostram válidos e confiáveis, adequando-se aos estudos de segurança em redes de computadores.

A simulação por eventos discretos se mostrou eficiente e mais apurada. Analisamos a taxa de ocupação dos recursos disponíveis, os gargalos do processo, o tempo de fila, o tempo de permanência no sistema, a quantidade de alertas gerados.

Quando nos deparamos com os resultados da pesquisa notamos que o atraso em agentes baseados em IDS pode ser prejudicial à segurança de rede, visto que podem ocorrer ataques e sequestros de informações sigilosas.

Espera-se que esse artigo possa contribuir para um melhor entendimento no

que se refere à temática e, principalmente, ofereça subsídios para novos estudos na área de segurança de redes.

No entanto, algumas inquietações apareceram ao longo do trabalho como: comportamento do OSSIM para os sistemas embarcados, casos de IoT (Internet das Coisas), carros autônomos com OSSIM, e um maior detalhamento dos estudos de caso. Com os itens em questão, observa-se que ainda há a necessidade de maiores detalhamentos, que visem suprir a carência de referencial teórico sobre estes temas, em especial com exemplos concretos dos resultados obtidos.

Sendo assim, e considerando que o tema é relevante para a área da tecnologia e segurança em redes, propomos pôr fim a realização de novos estudos procurando suprir as carências ora citadas.

REFERÊNCIAS

ALIENVAULT. ***OSSIM is Trusted by Thousands of Security Professionals in 140 Countries... and Counting.*** 2016. Disponível em: <www.alienvault.com/products/ossim>. Acesso em: 15 fev. 2017.>

ARANTES, C. da S. C. **Teoria de filas e simulação: Um paralelo entre o modelo analítico e o modelo por simulação para modelos de fila m1m1 e m1m1c.** Pontífica Universidade Católica de Goiás, Goiás, 2015.

ARAÚJO, V. H. M. **Análise de uma Implementação Open Source para Gerenciamento e Segurança de Rede.** Universidade Estadual de Campinas, Faculdade de Tecnologia. Limeira, 2019.

DONADO, S. A. et al. Mr-spel. **Marco de referencia para la gestión de seguridad de la información del sistema de pagos en línea de universidades oficiales en colombia.** Generación Digital, nº 16, 2011.

FREITAS FILHO, P. J. d. **Introdução à Modelagem e Simulação de Sistemas com Aplicações em Arena.** 2ª edição. Florianópolis: Visual Books, 2008.

JAISWAL, N. K. **Preemptive resume priority queue.** Operations Research, v. 9, n. 5, p. 732–742, 1961.

NETO, E. L. A. **Ambiente de simulação de redes a eventos discretos.** Universidade Estadual de Campinas, Campinas, 2001.

OLIVEIRA, F. de Fátima de et al. **Análise de teoria das filas: Sistema de filas de um serviço de pronto atendimento.** Anais da engenharia de produção. Unidade Central de Educação. FAEM Faculdade, Chapecó, 2017.

POLO, D. M. **Análisis, diseño e implementación del esquema de seguridad perimetral para la red de datos de la uisek – ecuador.** Universidad Internacional Sek, Equador, 2008.

PRADO, D. S. do. **Usando o Arena em Simulação.** 3º vol. Belo Horizonte: INDG Tecnologia e Serviços Ltda., 2003.

RAMÍREZ, J. V. **Simulação por eventos discretos para a otimização de uma clínica de fisioterapia.** Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

SANTOS, D. et al. **Ferramentas de Gerência de Rede – Uma Abordagem sobre o OSSIM.** Universidade Salvador, Salvador, 2009.

SASAKI, N. K. **Simulação de sistemas de comunicação Óptica baseada em simulação a eventos discretos.** Universidade Estadual de Campinas, Campinas, 2007.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas.** 5ª edição. Rio de Janeiro: Campus, 2005.

TAVARES, L. A. D. N. **Análise de Eventos de Segurança: Baseado no OSSIM.** Universidade do Minho, Portugal, 2015.

ÍNDICE REMISSIVO

A

Accesibilidad Web 11, 13, 14, 15, 16, 17

Alice 107, 108, 109, 110, 111, 112, 113, 114, 115

Almacenes de datos 47

Aprendizagem 1, 2, 3, 4, 7, 8, 9, 10, 33, 35, 37, 39, 43, 44, 45, 60, 61, 62, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 106, 109, 112, 113, 114, 115

C

Cálculo 1, 2, 3, 4, 7, 8, 9, 10, 39, 48

Complexity 89, 90, 91, 95, 99, 100, 101, 102, 103, 104, 105, 106

Computação 107, 110, 115, 116

Comunicação 1, 2, 3, 4, 8, 9, 10, 20, 30, 45, 75, 77, 79, 80, 81, 83, 85

Cybernetic Theory 90, 92, 94

D

Data Mining 47, 48, 49, 56, 58

Desempenho 18, 20, 21, 23, 25, 28, 43, 113

E

Educação 3, 8, 29, 31, 32, 34, 36, 43, 44, 60, 65, 68, 75, 76, 77, 79, 80, 81, 82, 83, 85, 86, 87, 88, 104, 109, 115, 116

Ensino-aprendizagem 1, 77, 78, 81, 82, 84, 88, 112

Ensino da logística 31, 32, 41

Ensino tecnológico 31, 44

Estándares 11, 12, 13

Eventos 18, 19, 20, 23, 25, 26, 27, 28, 29, 30, 110

Eventos Discretos 18, 19, 20, 23, 28, 29, 30

G

General Theory of Systems 90

I

Informação 1, 2, 3, 4, 7, 8, 9, 10, 20, 21, 77, 79, 80, 87, 89, 90, 104, 116

Information Theory 90, 91, 95

Integração 2, 31, 38, 39, 41, 66

Interação 9, 10, 60, 63, 75, 78, 80, 83, 84, 85, 86, 87, 107, 112

L

Linguagem de programação 23, 109, 110

Lógica de programação 107, 108, 109, 111, 113, 114

M

Metodologia ativa 31, 32, 38, 41

Minería de datos 47, 49, 56, 58, 59

Modelos predictivos 47, 50

O

Objeto Digital de Aprendizagem 60

Open Source 18, 19, 21, 29

OSSIM 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30

P

Photomath 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Plataformas educativas 11, 56

Prática pedagógica 60, 66, 70, 74, 87

Programação 23, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116

Q

QRCODE 31, 32, 38, 39, 41, 42

R

Rendimiento académico 47, 48, 49, 50, 51, 52, 54, 57, 58

Responsabilidad social 11, 12, 13, 16

S

Simulação 18, 19, 20, 22, 23, 25, 26, 27, 28, 29, 30, 33, 34, 64, 74

Social Information Systems 89, 90, 91, 98, 100, 101

Software 1, 5, 6, 7, 10, 11, 12, 13, 14, 16, 17, 25, 39, 58, 107, 108, 109, 110, 111, 112, 113, 116

Software educativo 107

T

Tecnologias 1, 2, 3, 4, 7, 8, 9, 10, 35, 67, 77, 79, 80, 83, 84, 87, 104, 105, 116

U

Usabilidade 112

W

WCAG 2.0 11, 13, 14, 16, 17

 **Atena**
Editora

2 0 2 0