



TECNOLOGIA E GESTÃO DA INOVAÇÃO

ERNANE ROSA MARTINS
(Organizador)

 **Atena**
Editora
Ano 2022



TECNOLOGIA E GESTÃO DA INOVAÇÃO

ERNANE ROSA MARTINS
(Organizador)

 **Atena**
Editora
Ano 2022

Editora chefe

Profª Drª Antonella Carvalho de Oliveira

Editora executiva

Natalia Oliveira

Assistente editorial

Flávia Roberta Barão

Bibliotecária

Janaina Ramos

Projeto gráfico

Bruno Oliveira

Camila Alves de Cremo

Daphynny Pamplona

Luiza Alves Batista

Natália Sandrini de Azevedo

Imagens da capa

iStock

Edição de arte

Luiza Alves Batista

2022 by Atena Editora

Copyright © Atena Editora

Copyright do texto © 2022 Os autores

Copyright da edição © 2022 Atena Editora

Direitos para esta edição cedidos à Atena Editora pelos autores.

Open access publication by Atena Editora



Todo o conteúdo deste livro está licenciado sob uma Licença de Atribuição *Creative Commons*. Atribuição-Não-Comercial-NãoDerivativos 4.0 Internacional (CC BY-NC-ND 4.0).

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores, inclusive não representam necessariamente a posição oficial da Atena Editora. 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.

Todos os manuscritos foram previamente submetidos à avaliação cega pelos pares, membros do Conselho Editorial desta Editora, tendo sido aprovados para a publicação com base em critérios de neutralidade e imparcialidade acadêmica.

A Atena Editora é comprometida em garantir a integridade editorial em todas as etapas do processo de publicação, evitando plágio, dados ou resultados fraudulentos e impedindo que interesses financeiros comprometam os padrões éticos da publicação. Situações suspeitas de má conduta científica serão investigadas sob o mais alto padrão de rigor acadêmico e ético.

Conselho Editorial**Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto

Profª Drª Alana Maria Cerqueira de Oliveira – Instituto Federal do Acre

Profª Drª Ana Grasielle Dionísio Corrêa – Universidade Presbiteriana Mackenzie

Profª Drª Ana Paula Florêncio Aires – Universidade de Trás-os-Montes e Alto Douro

Prof. Dr. Carlos Eduardo Sanches de Andrade – Universidade Federal de Goiás

Profª Drª Carmen Lúcia Voigt – Universidade Norte do Paraná



Prof. Dr. Cleiseano Emanuel da Silva Paniagua – Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Prof. Dr. Douglas Gonçalves da Silva – Universidade Estadual do Sudoeste da Bahia
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Profª Drª Érica de Melo Azevedo – Instituto Federal do Rio de Janeiro
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará
Profª Dra. Jéssica Verger Nardeli – Universidade Estadual Paulista Júlio de Mesquita Filho
Prof. Dr. Juliano Bitencourt Campos – Universidade do Extremo Sul Catarinense
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
Prof. Dr. Marco Aurélio Kistemann Junior – Universidade Federal de Juiz de Fora
Prof. Dr. Miguel Adriano Inácio – Instituto Nacional de Pesquisas Espaciais
Profª Drª Neiva Maria de Almeida – Universidade Federal da Paraíba
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Profª Drª Priscila Tessmer Scaglioni – Universidade Federal de Pelotas
Prof. Dr. Sidney Gonçalo de Lima – Universidade Federal do Piauí
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista



Diagramação: Camila Alves de Cremo
Correção: Mariane Aparecida Freitas
Indexação: Amanda Kelly da Costa Veiga
Revisão: Os autores
Organizador: Ernane Rosa Martins

Dados Internacionais de Catalogação na Publicação (CIP)

T255 Tecnologia e gestão da inovação / Organizador Ernane Rosa Martins. – Ponta Grossa - PR: Atena, 2022.

Formato: PDF

Requisitos de sistema: Adobe Acrobat Reader

Modo de acesso: World Wide Web

Inclui bibliografia

ISBN 978-65-258-0252-7

DOI: <https://doi.org/10.22533/at.ed.527223105>

1. Tecnologia. I. Martins, Ernane Rosa (Organizador). II. Título.

CDD 601

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora

Ponta Grossa – Paraná – Brasil

Telefone: +55 (42) 3323-5493

www.atenaeditora.com.br

contato@atenaeditora.com.br



DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.



DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access*, *desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce*, ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.



APRESENTAÇÃO

A nossa sociedade está em constante evolução em todas as áreas do conhecimento. Esta obra pretende apresentar o panorama atual relacionado a ciência, a tecnologia e a inovação, com foco nos fatores de progresso e de desenvolvimento. Apresentando análises extremamente relevantes sobre questões atuais, por meio de seus capítulos.

Estes capítulos abordam aspectos importantes, tais como: discussões sobre a importância dos minerais para uma gestão sustentável dos processos e do manejo correto dos resíduos; investigação das produções dos programas de Mestrado e Doutorado Profissional, entre 2015 e 2020, que fornecem subsídios na área de Mecatrônica no Brasil; identificação, caracterização e análise dos elementos/artefatos/registros a serem extraídos, com a utilização de ferramentas forenses gratuitas, que possam contribuir para estudos, perquirição, evidenciação de perícias, investigações técnicas e pesquisas na análise forense computacional; intervenção didática que utiliza uma simulação computacional como um meio de ensino prático no ensino remoto; avaliação do desenvolvimento e a produção de cebolas Serena F1 sob diferentes concentrações do fertilizante PUMMA; discussão da literatura dos materiais nanohíbridos, destacando as suas potencialidades e limitações em aplicações clínicas e ambientais; apresentação dos dados obtidos pelo projeto de extensão Letramento Literário, da Universidade Tecnológica Federal do Paraná (UTFPR), durante o ano de 2021; utilização da literatura de Cordel como um meio de ensino prático na aula de Eletricidade; proposta da “Mostra de ideias inovadoras da UTFPR – Campus Dois Vizinhos” com o objetivo de estimular a cultura do empreendedorismo e inovação na comunidade universitária, proporcionando ambiente para apresentação de ideias inovadoras, tendo em vista contribuir com o ecossistema regional de inovação no sudoeste do Paraná; bibliometria sobre a Inclusão Financeira Digital no Brasil; papel do tutor na Educação a distância, habilidades técnicas, pessoais e profissionais que um profissional de TI possa ter para auxiliar um Juiz, Delegado ou qualquer pessoa que necessite de uma perícia.

Nesse sentido, esta obra é uma coletânea, composta por excelentes trabalhos de extrema relevância, apresentando estudos sobre experimentos e vivências de seus autores, o que pode vir a proporcionar aos leitores uma oportunidade significativa de análises e discussões científicas. Assim, desejamos a cada autor, nossos mais sinceros agradecimentos pela enorme contribuição. E aos leitores, desejamos uma leitura proveitosa e repleta de boas reflexões.

Ernane Rosa Martins


SUMÁRIO

CAPÍTULO 1..... 1

A MINERAÇÃO E O USO DOS MINERAIS EM ELEMENTOS DO COTIDIANO: O SMARTPHONE

Rafaela Baldí Fernandes

Luis Henrique Caetano Moraes

 <https://doi.org/10.22533/at.ed.5272231051>

CAPÍTULO 2..... 11


A PRODUÇÃO CIENTÍFICA EM MECATRÔNICA

Rodolfo dos Santos de Souza Lovera

Jocilaine Carvalho de Araujo

Rose Aparecida de França

Roberto Kanaane


 <https://doi.org/10.22533/at.ed.5272231052>

CAPÍTULO 3..... 29

APLICAÇÃO DE FERRAMENTAS GRATUITAS NA INVESTIGAÇÃO FORENSE COMPUTACIONAL DOS SISTEMAS OPERACIONAIS: ANDROID E IOS

Clauderson Marchesan Biali

João Carlos Pinheiro Beck

 <https://doi.org/10.22533/at.ed.5272231053>

CAPÍTULO 4..... 40

APRENDENDO A LEI DE COULOMB COM O AUXÍLIO DAS SIMULAÇÕES: UM RELATO DE EXPERIÊNCIA

Elismárcio Mandú dos Santos

Daniel Cesar de Macedo Cavalcante

Alessio Tony Batista Celeste


 <https://doi.org/10.22533/at.ed.5272231054>

CAPÍTULO 5..... 44

AVALIAÇÃO DO DESEMPENHO DA CEBOLA SERENA F1 SOB DIFERENTES CONCENTRAÇÕES DE FERTILIZANTE PUMMA

Rangel Ferreira da Silva

Aline Rocha

 <https://doi.org/10.22533/at.ed.5272231055>

CAPÍTULO 6..... 55

DESENVOLVIMENTO DE NOVOS MATERIAIS NANOHÍBRIDOS: TENDÊNCIAS E DESAFIOS EM APLICAÇÕES AMBIENTAIS E CLÍNICAS

Jemmyson Romário de Jesus

Jéssica Passos de Carvalho

Edileuza Marcelo Vieira

Lucas Hestevan Malta Alfredo


Tatianny de Araujo Andrade
Rafael Matias Silva
Tiago Almeida Silva

 <https://doi.org/10.22533/at.ed.5272231056>

CAPÍTULO 7..... 67

DISEÑO Y VALIDACIÓN DE UN INSTRUMENTO PARA ANALIZAR APLICACIONES MÓVILES QUE FAVORECEN EL MLEARNING: APLICACIONES MÓVILES SUJETAS A ANÁLISIS


Vivian Aurelia Minnaard
Claudia Lilia Minnaard

 <https://doi.org/10.22533/at.ed.5272231057>

CAPÍTULO 8..... 75

LETRAMENTO LITERÁRIO: UM PROJETO DE EXTENSÃO INVESTIGANDO A LITERATURA DE LÍNGUA INGLESA NO PNBE E NO PNLD

Ilga Rosalina Fernandes Ribeiro
Marcia Regina Becker

 <https://doi.org/10.22533/at.ed.5272231058>

CAPÍTULO 9..... 91

LITERATURA DE CORDEL NO ENSINO DE ELETRICIDADE: UM RELATO DE EXPERIÊNCIA

Henrique Cândido Feitosa
Gabriel Bezerra de Oliveira
Alessio Tony Batista Celeste
Daniel Cesar de Macedo Cavalcante

 <https://doi.org/10.22533/at.ed.5272231059>

CAPÍTULO 10..... 98

MOSTRA DE IDEIAS INOVADORAS DA UTFPR – CAMPUS DOIS VIZINHOS

Tifany Karol da Silva
Almir Antonio Gnoatto
Alfredo de Gouvêa
Juliana Mara Nespolo

 <https://doi.org/10.22533/at.ed.52722310510>

CAPÍTULO 11..... 106

O PAPEL DO TUTOR NA EDUCAÇÃO A DISTÂNCIA

Edileide Barbosa de Lima
Rosimeire Martins Régis dos Santos

 <https://doi.org/10.22533/at.ed.52722310511>

CAPÍTULO 12..... 119

PANORAMA DA INCLUSÃO FINANCEIRA DIGITAL: UMA ANÁLISE BIBLIOMÉTRICA

Ralbert de Almeida Menezes

Mário Jorge Campos dos Santos


Clara Angélica dos Santos

 <https://doi.org/10.22533/at.ed.52722310512>

CAPÍTULO 13..... 133

PERFIL PROFISSIONAL PARA UM PERITO FORENSE COMPUTACIONAL NO BRASIL

Euclides Peres Farias Junior

 <https://doi.org/10.22533/at.ed.52722310513>

SOBRE O ORGANIZADOR..... 155

ÍNDICE REMISSIVO..... 156

PERFIL PROFISSIONAL PARA UM PERITO FORENSE COMPUTACIONAL NO BRASIL

Data de aceite: 02/05/2022

Data de submissão: 24/02/2022

Euclides Peres Farias Junior

IPOG – Instituto de Pós-Graduação e Graduação, Universidade Tecnológica Federal do Paraná (UTFPR), Grupo de Estudos em Redes e Segurança Computacional (GENETSEC)
<http://lattes.cnpq.br/2993749906763460>

RESUMO: A Perícia Forense Computacional é sem dúvidas nenhuma, uma das mais brilhantes carreiras da atualidade. Saber quais habilidades, problemáticas e responsabilidades que este profissional deve encarar na atuação de um Laudo Pericial, é de suma importância. O objetivo deste estudo se dá na pesquisa como um norteador das habilidades técnicas, pessoais e profissionais que um profissional de TI possa ter para auxiliar um Juiz, Delegado ou qualquer pessoa que necessite de uma perícia. Além de levantar informações para mostrar a ciência do tamanho e da responsabilidade que um Perito Forense Computacional no Brasil deve ter. Foram abordadas as leis que envolvem a área de Perícia autorizam o profissional liberal a se candidatar a perito forense computacional. Por fim, é apresentado um levantamento bibliográfico e indicadores através dos dados do Estado do Paraná nos últimos três anos até 2019, com o propósito de situar qual é a realidade brasileira de demandas nesta área. Concluiu-se que não basta ser apenas um entusiasta para ser

um Auxiliar técnico ou um Perito *Ad hoc*, deve ter habilidades profissionais, pessoais e em determinados momentos até espirituais para enfrentar uma cena de crime. Porém, mostra quão promissora e desafiadora é a profissão de Perícia Forense Computacional.

PALAVRAS-CHAVE: Perito Forense Computacional, Computação Forense, Crime Virtual.

ABSTRACT: Computer Forensics is undoubtedly one of the brightest careers today. Knowing which skills, problems and responsibilities this professional must assume in the performance of an Expert Report is of paramount importance. The objective of this study is given in the research as a guide of the technical, personal and professional skills that an IT professional can have to assist a Judge, Delegate or anyone who needs an expertise. In addition to collecting information to show the science of the size and responsibility that a Computer Forensic Expert in Brazil must have. Laws involving the area of Expertise that authorize the liberal professional to apply to be a computer forensic expert were addressed. Finally, a bibliographic survey and indicators are presented through data from the State of Paraná in the last three years until 2019, with the purpose of situating the Brazilian reality of demands in this area. It was concluded that it is not enough to be just an enthusiast to be a technical assistant or an ad hoc confrontation, you must have professional, personal and determined skills until the crime scene. However, it shows how promising and challenging the profession of Computer Forensics is.

KEYWORDS: Computer Forensics Expert, computer forensics, Cybercrime.

1 | INTRODUÇÃO

A Internet nos últimos anos vem oportunizando conectividade e integração global no mundo todo, com isto pode se dizer que novos tempos tecnológicos estão cada vez mais sólidos, vários benefícios têm abrangido a humanidade como entretenimento, notícias, trabalhos virtuais em fim, uma série de novos *modus operandis* que a sociedade teve que se adaptar e ainda estão em franca expansão e adaptação. Porém, acompanhado dos benefícios também vieram os problemas considerados crimes, que de acordo com o dicionário online da língua portuguesa Priberam (2021) a palavra “Crime”, trata-se de “Qualquer violação muito grave de ordem moral, religiosa ou civil, punida pelas leis; todo o delito previsto e punido pela lei penal; Delito, fato repreensível, infração de um dever”. Por se tratar de crimes de forma virtual, de acordo com o dicionário da língua portuguesa Dicio (2021) a palavra “Virtual”, trata-se de “Não real; simulado eletronicamente: imagens virtuais”. Estas definições são de suma importância para classificarmos então a que tipo de crimes que estamos tratando neste trabalho, ou seja, por não ter uma definição única, mas sim a junção das duas definições “Crimes Virtuais”, são então aqueles cometidos de forma eletronicamente de forma local ou pela rede mundial de computadores, a Internet. Desta forma, segundo Eleutério e Machado (2011) a Perícia Forense ou Análise Digital Forense trata-se da modalidade de perícia criada para combater crimes digitais por meio de análises e métodos que buscam a coleta através de evidências comprovadas. Entretanto, (FREITAS, 2006) já havia definido que a forense computacional pertence ao ramo da criminalística, desta forma, compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam elas por componentes físicos, ou, por dados que foram processados eletronicamente e armazenados em qualquer tipo de mídias computacional. Através destas conectividades e recursos tecnológicos totalmente interconectados, aliado ao advento massivo de dispositivos móveis que de acordo com um estudo apresentado pela empresa de consultoria Gartner, aponta que deverá ter em 2022 6,2 bilhões de dispositivos conectados, o que garante um aumento de 125 milhões de dispositivos a mais em uso no ano de 2022 do que foi em 2020 no Brasil (OLHAR DIGITAL, 2021).

Atualmente estamos passando por um período de muitos crimes cometidos de forma virtual, superando assim, os crimes considerados não virtuais, cujos mais comuns são, furtos de contas eletrônicas, e sequestros de equipamentos através de criptografias, difamação, crimes de informações falsas, denominados *fake news*, ataques massivos para negação de serviços dentre outros crimes virtuais que, também estão em franca expansão. Entretanto, não é só de crimes virtuais que um perito forense computacional deve trabalhar, pois, diversos crimes estão sendo solucionados em função do auxílio da forense computacional, que são aplicados em dispositivos eletrônicos, equipamentos com

conectividades e ou mesmo na aplicação de técnicas de Inteligência Artificial (IA) para auxiliar na comprovação de um crime, como por exemplo, IA aplicada para detectar fraudes em assinaturas, detecção de fraudes de sistemas financeiros, identificação de autoria de crimes ou mesmo identificação de criminosos já registrados em bancos de dados da polícia civil.

Desta forma, o propósito deste trabalho, é discutir qual o perfil profissional de um Perito Forense Computacional no Brasil, uma vez que atender as demandas de perícia tem sido um desafio de grandes proporções, uma vez que em muitos estados da nação trata-se de uma atividade exclusiva dos órgãos públicos Federais e Estaduais, provocando assim um deficit de profissionais, acumulando centenas de milhares de ações ainda sem solução, ou mesmo, sem a perícia propriamente dita efetuada. Então qual seria a formação profissional que um perito forense de obter, quais são os principais desafios desta profissional pode enfrentar, qual o grau de expertise e experiência que deve ser exigido para que um profissional se apresente como perito forense. As instituições de ensino têm propostos boas formações? No papel de um Juiz, qual seria o profissional adequado para uma perícia forense computacional? E no papel das empresas privadas, ou pessoa física, qual seria o perito forense a ser contratado para sua contratação? Perguntas estas que são feitas e estão ecoando em todos os corredores das academias, empresas e demais instituições que visam atender este mercado pujante de oportunidades de trabalho. Desta forma, este trabalho tem por finalidade uma pesquisa puramente bibliográfica a fim de elucidar as questões pertinentes ao perfil do profissional para a Perícia Forense Computacional.

2 | CRIMES VIRTUAIS E CRIMES ATENDIDOS PELA COMPUTAÇÃO

Os crimes virtuais são os mais diversos possíveis, onde pode-se dizer que é mais provável hoje em dia, uma pessoa sofrer algum tipo de crime virtual do que um crime convencional não virtual. Porém, na perícia forense computacional, não só de crimes virtuais compõe o hol de atividades deste profissional, o qual apontam diversos casos que há a necessidade de atuação do profissional de Informática, aplicar seus conhecimentos para comprovar um possível crime ou delito que fora cometido de fora não virtual, mas que através dos recursos tecnológicos, é possível comprovar e evidenciar a intenção do crime cometido a posteriori.

Um dos casos emblemáticos da atualidade que certamente requer uma investigação profunda, se dá em função de ataques de ransomware, uma vez que trata-se de uma das ameaças que apresentam maior índice de perigo para as organizações, entretanto, é comum as empresas negligenciar este tipo de ataque, pois o que parece estar fora do alcance dos gestores das empresas é que neste tipo de ataque que já causou prejuízos para grandes corporações como mostra o relatório sobre os principais ataques de ransomware

publicado pela empresa Kaspersky (2021) como o ataque ocorrido em junho de 2020 na gigante automotiva Honda, que sofreu o ataque de ransomware da *Snake* (conhecida como *Ekans*) o qual atingiu seus escritórios nos EUA, Europa e Japão. Ao ser descoberto, a Honda pôs a produção em espera em certos locais para lidar com a interrupção em sua rede de computadores. Para este ataque, os hacker utilizaram ransomware em troca de dar a chave de criptografia, prática comum deste tipo de ataque, porém a Honda informou que os atacantes não tinham apresentado qualquer evidência de perda de informações pessoalmente identificáveis.

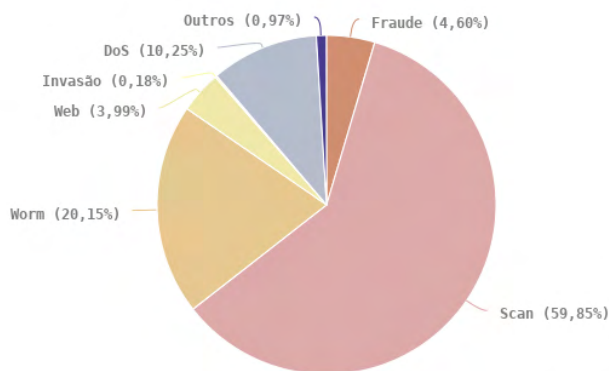
Outro caso emblemático se deu no ataque à empresa de Câmbio *Travelex*, o qual forçou a empresa desligar todos os sistemas de informática e a confiar na caneta e no papel, como resultado do prejuízo, a empresa teve que derrubar seus sites em 30 países. Este ataque se deu por um bando de ransomware chamado de *Sodinokibi*, conhecido como Revil, exigindo assim da empresa *Travelex* a quantia de 6 milhões de dólares, uma vez que os invasores alegaram ter invadido a empresa por mais de seis meses antes e assim, possibilitando o download de 5Gb de dados sensíveis de clientes, incluindo número de cartão de crédito. Ataques de ransomware à Universidade de Utah em agosto de 2020, onde foi divulgado que a Universidade pagou um resgate de US\$457.000 Dólares a criminosos cibernéticos para evitar que eles liberassem arquivos confidenciais roubados durante o ataque. Este ataque criptografou servidores da unidade de Ciências Sociais e Comportamentais da Universidade, como nos dados roubados continham informações de estudantes e funcionários, a Universidade decidiu pagar o resgate para evitar a divulgação dos mesmos, assim como a instituição orientou seus alunos e funcionários a monitorar seus dados financeiros como proteção.

No Brasil, ataque de ransomware no Superior Tribunal de Justiça em novembro de 2020, a infraestrutura cibernético do STJ sofreu um ataque de ransomware massivo, o que fez com que o site da instituição ficasse offline. Neste ataque, os criminosos afirmaram que toda a base de dados do Tribunal tinha sido criptografado e que qualquer tentativa de restauro seria em vão. Além disso, os hacker deixaram uma nota de resgate pedindo ao Tribunal que os contatassem através de um endereço *ProtonMail*. Os hackers também tentaram atacar vários outros sites relacionados ao governo brasileiro. De acordo com a (VAULTREE, 2021), além de muitas outras empresas, a *JBS Foods* também teve suas bases de dados atacadas por *ransomware*, que obrigou a interromper suas operações nos EUA e afetou também suas fábricas de processamento na Austrália e no Reino Unido, este ataque gerou temores de escassez de alimentos e interrupções na cadeia de abastecimento de alimentos nos EUA, além de destacar a profunda dependência das empresas em seus sistemas, com relatos de trabalhadores tendo que realizar tarefas de açougue manualmente – algo que não era feito a muitos anos no frigorífico com o porte da *JBS Foods*. Mas o mais emblemático ataque de *ransomware* desta natureza se deu na empresa de soluções de *TI Kaseya*, que anunciou a invasão em seus dados. Como

trata-se de uma empresa que fornece software de tecnologia de informação para outras empresas, o ataque gerou um efeito dominó, afetando cerca de 1.500 organizações em diversos países. Este ataque teve a reivindicação de autoria do grupo cibercriminoso *Revil*, exigindo um resgate de US\$ 70 milhões em *Bitcoins*. Porém a empresa resolveu colaborar com o FBI (Agência de Infraestrutura de Segurança Cibernética dos EUA), ocasionando assim, vinte dias depois do ataque, a recuperação dos dados através de uma chave de criptografia universal para recuperar o acesso a seus arquivos. Este ataque mostrou então que são indistintos seus alvos, mostrando que as empresas estão susceptíveis a ataques desta natureza.

Aliados a este tipo de ataques, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br), apresenta o gráfico anual de janeiro a dezembro de 2020 na figura 1, o qual é utilizado como fonte de informação para a segurança da informação.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020
Tipos de ataque



© CERT.br – by Highcharts.com

Figura 1 – Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2020.

Fonte: CERT.br (2021).

É importante ressaltar que estes incidentes também podem gerar ações judiciais que ocasionem a necessidade do serviço do profissional intitulado Perito Forense Computacional, embora a maioria dos casos são tratados como problemas voltados para a Segurança Computacional, o que normalmente são solucionados dentro das próprias organizações, sem o registro de crimes nos órgãos competentes que certamente enquadraria dentro dos preceitos da Lei regulamentada na esfera nacional e internacional, de acordo com o porte da empresa, como foi possível observar nas informações relatadas por empresas mundiais

que sofreram ataques.

3 | FUNDAMENTOS DO DIREITO DIGITAL E SUAS LEIS

Embora exista a necessidade iminente de se tratar problemas e incidentes relacionados à segurança computacional, é de vital importância o esclarecimento à cerca do que é lícito e do que é ilícito, ou seja, do que pode-se fazer com relação aos conhecimentos adquiridos com a segurança cibernética do que não é permitido, desta forma, (VECCIA, 2019) afirma que com o advento do crescimento do uso da tecnologia, houve então uma quebra de paradigma no momento em que muitas coisas estavam sendo utilizadas de forma tecnológica, o qual propôs uma nova modalidade intitulada computacional. Porém, essa modalidade não trouxe só benefícios, mas também proporcionou a criação de uma nova modalidade de atividade ilícita, cujo qual recebe diversos nomes, como crimes cibernéticos, crimes eletrônicos, crimes virtuais, *cybercrimes*, crimes digitais dentre outros. Assim, diante disso, conceituar e tipificar este tipo de delito não é uma tarefa trivial, uma vez que a tecnologia proporciona diversas formas de assumir um crime e está em constante evolução (VECCIA, 2019).

Algumas definições mais aceitas respeito da definição de *cybercrimes*, tais como a de Reith, carr e Gunsch (2002): “Crimes cibernéticos não são, necessariamente, novos crimes, pois podem ser crimes clássicos que exploram o poder proporcionado pelo computador e a acessibilidade de informações, principalmente através da Internet”. Através desta definição, abre-se então a oportunidade da discussão sobre crimes virtuais de forma remota, o qual MADALENA (2016) afirma que para a correta aplicação do direito na Internet, é de vital importância uma análise da relação jurídica que intimamente dialoga com este fenômeno, uma vez que este fato, figura então a assertiva de grande importância para o jurista, que certamente caberá a ele a capacidade de identificar quando está regulando uma relação jurídica interferida pela Internet ou quando regulará relações jurídicas próprias da Internet.

Através destas definições é mister que o assunto de ciberespaço deve ser aprofundado e conhecido, pois alguns autores como Huebner et al. (2003), enumeraram e classificaram os crimes cibernéticos por áreas, tais como:

- Crimes centrados no computador: trata-se de uma atividade criminosa capaz de atingir sistemas computacionais, redes de computadores, mídias de armazenamento de dados ou outros dispositivos computacionais;
- Crimes auxiliados por computador: é aquele cujos sistemas computacionais são utilizados como ferramentas para auxiliar as atividades criminosas já existentes antes mesmo do computador, por exemplo uma ameaça de morte via redes sociais ou e-mail;
- Crimes por computadores incidentais: atividades criminosas onde a utilização de um computador é eventual.

Porém a classificação mais aceita é a que divide os crimes cibernéticos em próprios, que são de uso exclusivo em ambientes considerado cibernético, e impróprio, considerado aberto. Desta forma, crimes próprios ou exclusivamente cibernético, exige a dependência da utilização de um computador. Pois a execução depende inevitavelmente deste recurso como meio e objeto da prática delituosa, o qual transforma assim o ambiente computacional no objeto jurídico a ser tutelado. É importante ressaltar que no Brasil a Lei 12.737/2012 conhecida como “Lei Carolina Dieckmann” tem alguns pontos de tratamento de crimes cibernéticos, uma vez que nesta categoria de crime, são enquadradas a criação e disseminação de vírus e código maliciosos, negação de serviços, invasão de banco de dados e demais ações consideradas criminosas na área de segurança computacional. Já crimes cibernéticos considerados impróprios ou aberto, são aqueles cujo ambiente computacional é utilizado como meio para a conduta criminosa ou ilícita, o qual são enquadrados nesta categoria crimes contra a honra, ameaça, falsificação, estelionato, furtos dentre outros, embora estes crimes não necessitam da tecnologia para serem tipificados e podem ser praticadas por qualquer pessoa.

Como qualquer crime de qualquer natureza, a comprovação da autoria não é uma tarefa fácil, no crime cibernético não é diferente, pois também é considerado de grande complexidade, uma vez que demanda prova pericial, frene às características de volatilidade, virtualidade e anonimato do ambiente computacional. Desta forma, entender à diversidade de paradigmas tecnológicos e perfis de criminosos uma vez que se apropria de todos os recursos computacionais disponíveis como robótica, inteligência artificial e lógica, apresentando-se então como um árduo trabalho para identificação do sujeito ativo de um delito cibernético, além do conhecimento cognitivo e autodidata do indivíduo que praticou o crime a ser desvendado, ações estas que qualificam assim um sujeito ativo no cibercrime. Já o sujeito passivo nos crimes cibernéticos são as próprias vítimas, o ofendido, o titular do bem jurídico tutelado pela norma penal, ou seja, pode ser uma pessoa física ou jurídica, público ou privado. Desta forma, o Estado é então o titular do chamado *jus puniendi* (direito de punir) e o sujeito passivo constante, quanto o particular é o sujeito passivo variável (VECCIA, 2019).

Baseado na *jus puniendi* é importante frisar que é papel do Estado como o titular e soberano para legislar, governar e aplicar a lei e a pena no exercício de uma jurisprudência. Desta forma, entende-se que a vontade concreta da lei deverá ser exercida pelo poder judiciário estadual e federal desde que esteja dentro de suas jurisdições. Embora a Constituição Federal, em seu artigo 21, inciso XI, prevê que os serviços de telecomunicações devem ser de competência da União, os crimes cibernéticos possuem competência do poder judiciário estadual sendo excepcional a competência do poder judiciário federal, uma vez que esta competência é dada em função da territorialidade e do local onde o crime foi praticado, mas podem ser também tratados nas esferas federais, uma vez que podem ser praticados de diversos locais da nação o fora do país. Em decorrência

disso (VECCIA,2019) define que:

Uma das grandes dificuldades para a definição da competência e a aplicação da lei penal no espaço se encontra no fato de que o ambiente computacional, quando parte da rede mundial de computadores, não é delimitado por um território. Extrapolando-se as barreiras de soberania, jurisdição estatal, tempo e espaço.

As legislações então, são de suma importância além da execução de uma perícia forense computacional, pois é através da lei que se é permitido ou não a execução deste trabalho. A Lei nº 12.737/2012¹ fala sobre a tipificação criminal de delitos informáticos, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal – CP) bem como concede outras providências. Nesta alteração, foram acrescentados no (CP) os artigos 154-A e 154-B, e os artigos 266 e 298 foram refeitos com uma nova redação. Já a Lei nº 12.965/2014² mais conhecida como Marco Civil da Internet (MCI) trata de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Pois surgiu como a realização de um projeto de lei amplamente debatido na sociedade civil brasileira, que teve ampla participação da pluralidade dos seus integrantes. Através destas leis e jurisprudência, (MADALENA,2016) afirma que esta lei é considerada indispensável à manutenção e organização da vida social na Internet, o que apresentou-se como um exemplo para o mundo, ainda que alguns setores deste sistema tenham que se debater e criticar, carecendo em especial, na correta interpretação para sua pretensa efetividade. Desta forma, este é o fato gerador que o desenvolvimento do direito, a doutrina e a jurisprudência vêm desenvolvendo e cumprindo o seu papel dogmático captando valores intrínsecos na norma.

4 | REDES DE COMPUTADORES E A SEGURANÇA DA INFORMAÇÃO

As redes de computadores oferecem acessos às mais diversas informações possíveis entre usuários e sistemas de comunicação. De acordo com (KUROSE, 2013), uma rede de computadores tem o papel de interconectar diversos dispositivos computacionais ao redor do mundo. Por este motivo, existe a necessidade de organizar, monitorar e gerenciar todos os elementos que a compõem. Uma vez que, ao prover conectividade entre pessoas ou organizações os objetivos de uma rede é compartilhar arquivos, recursos computacionais, conexões remotas, transferência de dados e a disponibilidade de serviços de comunicação através de e-mails, redes sociais dentre outros serviços. Uma das definições clássicas mais aceita sobre gerência de rede é que o gerenciamento de rede deve oferecer a integração e a coordenação de elementos de hardware, software e recursos humanos, a fim de monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, bem como contar com elementos que possam satisfazer as exigências operacionais, de desempenho

1 BRASIL. Lei nº12.737, de 30 de novembro de 2012. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acessado em 04 de dez. 2021.

2 BRASIL. Lei nº12.965, de 23 de abril de 2014. Disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acessado em 04 de dez. 2021.

e de qualidade de serviço baseado em tempo real a um custo razoável (SAYDAM, 1996). Em última instância, a gerência de redes tem o papel importante no sentido de estabelecer o equilíbrio entre as necessidades do usuário, com as características do serviço que se propõe atuar, de forma a aproveitar da melhor forma possível, aspectos tanto técnicos como econômicos nos recursos de uma rede. Partindo deste princípio, o papel de um gerente de rede se dá na responsabilidade da condução das atividades relacionadas à Gerência das Redes, cujo Sistema de gestão de rede é composto por um conjunto de ferramentas, processos e métodos com o propósito de dar auxílio ao administrador em todas as tarefas que uma rede demandar (KUROSE, 2013).

Diante destas afirmações, pode-se dizer que há uma iminente dependência das organizações quanto ao uso da tecnologia da informação, em especial na era atual onde tudo está conectado em diversos modelos de redes, com as mais diversas aplicações possíveis tanto em hardwares como em softwares. Portanto, o administrador de rede deve ter à mão as ferramentas de gerenciamento adequadas de forma atender suas necessidades, são elas: detecção de falha em uma placa de interface em um hospedeiro ou roteador, monitoramento de hospedeiros, monitoração de tráfego para auxiliar outros recursos de redes, detecção de mudanças rápidas em tabelas de roteamento, monitoramento de SLA - Acordo de Nível de Serviços (do inglês *Service Level Agreements*) e por fim a detecção de invasão (KUROSE, 2013).

Em apoio às necessidades do administrador de rede, o gerenciamento de rede foi padronizado pela ISO (acrônimo em inglês de *International Organization for Standardization*), através da norma ISO/IEC 7498-4. Esta norma então definiu cinco áreas funcionais de redes: gerenciamento de falhas, gerenciamento de configuração, gerenciamento de contabilidade, gerenciamento de desempenho e, por fim, gerenciamento de segurança. Estas áreas são normalmente reconhecidas como FCAPS (acrônimo em inglês *Fault, Configuration, Accounting, Performance and Security*), o que levou a grande aceitação por parte dos fabricantes de software e hardware de rede, pois propôs a padronização tanto das tecnologias empregadas, quanto também exigiu padrão aos fabricantes proprietários. Os detalhes das cinco áreas do gerenciamento de redes padronizadas pela ISO e didaticamente registradas por (KUROSE, 2013) são:

1. Gerenciamento de desempenho: a meta estabelecida para o gerenciamento de desempenho é quantificar, medir, informar, analisar e controlar o desempenho dos diferentes componentes de uma rede. Os dispositivos individuais intermediários, inclusive o trajeto pela rede, são essenciais. Protocolos como o SNMP (do inglês *Simple Network Management Protocol*) - Protocolo Simples de Gerenciamento de Rede, amparado pela RFC 3410, possui um papel fundamental no gerenciamento de redes;
2. Gerenciamento de Falhas: se dá através de registros, detecção e reação às condições de falhas existentes na rede. Segundo (KUROSE, 2013), existe uma

indefinição entre o gerenciamento de falha e o gerenciamento de desempenho. Desta forma, pode-se considerar que o gerenciamento de falha como o tratamento imediato de falhas transitórias da rede, o que pode-se considerar uma ação proativa. Já o gerenciamento de desempenho, usa uma abordagem de longo prazo em relação ao desempenho da rede no que se refere a demandas variáveis de tráfego e falhas na rede, o que permite dizer que é uma ação reativa;

3. Gerenciamento de configuração: este gerenciamento permite que um administrador de rede tenha condições de saber quais são os dispositivos que fazem ou não parte da rede que está sendo administrada, bem como quais são as configurações adequadas de hardware e software. Este tipo de gerenciamento é amparado pela RFC 3139 que oferece então, uma visão geral sobre o gerenciamento de requisitos de configuração para redes com o protocolo IP;

4. Gerenciamento de contabilização: tem a função de permitir que o administrador da rede tenha a condição de especificar, registrar e controlar os acessos de um usuário e dispositivos utilizados por uma rede. Este gerenciamento pode abordar aspectos de controle através de cotas de utilização, cobrança por utilização e alocação de acesso privilegiado a um determinado recurso que por sua vez, faz parte do gerenciamento da contabilização;

5. Gerenciamento de segurança: controla o acesso aos recursos da rede, porém é importante ter uma política bem definida. Os componentes de suma importância no gerenciamento de redes atualmente vai desde as centrais de distribuição de chaves, autoridades certificadoras, o uso de *firewalls*, Sistema de Detecção de Intrusão - IDS (do inglês *Intrusion Detection System*) e um Sistema de Prevenção de Intrusão - IPS (do inglês *Intrusion Prevention System*).

As abordagens feitas sobre o gerenciamento de rede, são de fundamental importância para o entendimento de premissas essenciais para a segurança, em especial, porque geralmente são usadas medições ativas ou passivas para detectar possíveis problemas de monitoramento ou problemas de segurança nas redes (PERDICES,2018). A segurança precisa ser totalmente integrada na arquitetura da rede, uma vez que existem demandas significativas para transformar a Internet de um simples paradigma de entrega de pacotes, para se transformar em um paradigma diversificado construído em torno dos dados, conteúdo e em especial dos usuários, ao invés das máquinas (PAN, 2011).

A segurança de rede é uma das áreas de estudos constante na busca por soluções a diversidade de ataques ou roubo cibernético. Entretanto, para tratar aspectos de segurança, são necessárias etapas que antecedem a segurança, tal como o gerenciamento da rede com o objetivo de obter controle e medidas técnicas na busca da privacidade, integridade e a disponibilidade dos dados. Desta forma, a segurança de rede de computadores deve incluir dois aspectos importantes em suas funções: a segurança física e a segurança lógica. Onde a segurança física significa que os equipamentos e as instalações relacionadas estão protegidas contra ataques, perdas e demais incidentes. A segurança lógica deve incluir a

integridade das informações, sigilo e disponibilidade (LI, 2012).

5 | O PROFISSIONAL DA TECNOLOGIA DA INFORMAÇÃO

No Brasil existem diversos cursos de formação para promoção profissional na área da Computação, quer seja cursos técnicos, cursos superiores, pós-graduação, mestrado e doutorado. Entretanto a profissão do Informático não é regulamentada dentro do Ministério do Trabalho e tão pouco por um órgão que regulamente esta profissão. Entretanto, estamos vivendo a era da escassez do Profissional de Tecnologia da Informação. Uma vez que vivemos a era do mundo compartilhado e globalizado, o mundo dos ambientes remotos, o mundo da educação à distância (EAD) e dos *home offices*. Desta forma, é importante saber o que um profissional da área de Tecnologia da Informação (TI) atua, por se tratar de um mercado muito amplo em franco crescimento. A TI então é o facilitador dos processos, e o principal meio para prover a possibilidade do aumento da produtividade, a redução de custos e em especial, para a gestão e governança aplicados em uma empresa que deseja ser competitiva e promissora para o futuro.

Através destas definições, pode-se dizer que o profissional de TI é o responsável por gerenciar as informações em uma organização, de forma a criar e compartilhar em redes de computadores, ser capaz de fazer gerenciamento de dados, construção de programas, gerenciar sistemas operacionais, construir códigos de Inteligência Artificial e também fazer análise de sistemas aplicados ao mercado. Desta forma, de acordo com (MAISDADOSDIGITAIS, 2021) é fundamental sabermos quais são as habilidades que o profissional de TI deve ter além do conhecimento técnico, são eles:

- Habilidades constantes com rapidez, estar atento às tendências dos negócios, comportamentos, mudanças do mercado, e em especial acompanhar a atualização e mudanças do ciclo de vida de tecnologia, que hoje está cada vez mais curta;
- Ter a plena compreensão da empresa/indústria que trabalha, bem como deve estar envolvido no negócio e no segmento da empresa;
- Ter a capacidade de obter uma visão ampla de negócio, uma vez que sua tomada de decisão deve ser assertiva, bem como útil ao desenvolvimento de estratégias que garantam o direcionamento de ações com foco em atingir por completo os objetivos e expectativas da empresa;
- Este profissional deve ser capaz de enxergar o todo a partir das partes que são de vital importância para o desenvolvimento de sistemas e soluções, bem como deve ter o pensamento analítico, permitindo assim que este profissional tenha condição de prever e de avaliar riscos iminentes;
- Gestão de TI deve estar totalmente engajada com equipes. Uma vez que a gestão de projetos é a área que assume e lidera os demais setores da TI;

- Outro idioma como o Inglês é de vital importância para profissional de TI, pois o mundo globalizado e as informações tecnológicas são predominantemente em Inglês, então esta é um requisito obrigatório.

Já o portal do (G1., 2021), afirma que:

A área de Tecnologia da Informação oferece diversas possibilidades. Além de programadores e desenvolvedores, cientistas de dados e analistas de cibersegurança são algumas das profissões de destaque nesse setor. Os programadores, por exemplo, desenvolvem e aperfeiçoam sites, aplicativos, programas de computador, sistemas operacionais, sistemas de empresas e redes sociais. É uma profissão transversal, que permite a atuação em diferentes setores, como serviço, comércio e indústria. Um dos motivos para a expansão dessas profissões é que elas são consideradas sustentáveis. Isso porque a digitalização das atividades econômicas pode reduzir entre 10% e 20% a emissão total de gases de efeito estufa.

O (GUIADECARREIRA, 2021), afirma que o profissional da carreira em Ciência da Computação deve:

O profissional formado em Ciência da Computação atua basicamente na elaboração de programas de informática. Um bacharel em Ciência da Computação cria desde ferramentas simples, como um aplicativo financeiro para lançar despesas pessoais, até programas complexos de gerenciamento de produção ou de processamento de informações. Um cientista da computação, como é chamado o profissional formado em Ciência da Computação, pode ser contratado para trabalhar em uma equipe de desenvolvedores, criando software de acordo com a necessidade dos clientes. Também pode atuar no departamento de Pesquisa e Desenvolvimento (P&D) de uma empresa.

Ainda explorando o profissional na carreira de Redes de Computadores, o (GUIADECARREIRA, 2021) afirma que este profissional deve ter o seguinte perfil:

Organização, pensamento lógico e capacidade de resolver problemas são características fundamentais para este profissional. Trabalhar em equipe também é importante para o tecnólogo em Redes de Computadores. Diferentemente do técnico, que tem nível médio e atua de forma mais pontual, o tecnólogo é preparado para cuidar da gestão dessas redes, detectar e resolver problemas, propor novas soluções e gerenciar equipes. Para isso, de saber se comunicar bem, distribuir tarefas e delegar atividades. O tecnólogo em Redes de Computadores é responsável por elaborar, implantar, manter e gerenciar projetos físicos e lógicos de computadores, incluindo a conectividade entre sistemas diferentes, garantindo que programas, sistemas e equipamentos possam se comunicar dentro de uma mesma rede. Garantir a segurança de acesso também faz parte de suas responsabilidades.

Frente a estas definições é importante observar o que é necessário para que o profissional da computação queira atuar como “Perito Forense Computacional”, que de acordo com o (PROFISSIONAISTI, 2021) deve ter as seguintes habilidades:

Basicamente o Perito Forense Computacional é o profissional encarregado de recuperar informações de computadores e outros dispositivos eletrônicos a fim de obter evidências de um crime. Normalmente esses profissionais

trabalham diretamente com forças policiais ou empresas privadas coletando, analisando e documentando informações, onde os equipamentos analisados podem estar danificados ou comprometidos de alguma forma. Se você já assistiu alguma série do tipo CSI, já deve ter visto um perito com um HD queimado ou mesmo uma placa danificada tentando recuperar informações... Este é um profissional PERITO.

Já o portal eletrônico da Associação Nacional dos Peritos em Computação Forense (APECOF, 2021) admite em sua associação, profissionais de nível superior em computação ou direito, que nunca tenha sido condenado por qualquer crime e que tenha um curso de formação em computação forense homologado pelos membros. Então, as agências em sua concepção deve traçar o perfil do profissional de TI que tenha condições conduzir uma perícia criminal, levando em consideração que o tema da Computação Forense Criminal tem seus requisitos, mecanismos e instruções. Em função das técnicas e especializações para recuperação de dados, análise de logs, gerenciamento de redes e sistemas operacionais, surge então a Perícia Forense Computacional, o qual já está bem consolidada no âmbito jurídico, cuja finalidade é auxiliar na solução de casos onde são cometidos crimes através do uso de dispositivos computacionais, entende-se por dispositivos computacionais todos os equipamentos que tiverem processamento eletrônico, conectividade capaz de processar, armazenar e prover compartilhamento de informações quer seja textual, áudio ou vídeo, bem como ações remotas através da rede mundial de computadores a Internet. Desta forma, é importante citar o artigo 159, o Código de Processo Penal Brasileiro (CPP) exige que “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior”. Através desta afirmação, a Análise Forense Computacional deverá ser realizada por profissionais devidamente habilitados, informação esta complementada por ELEUTÉRIO e MACHADO (2011) que diz que a Análise Forense Computacional “destina a determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crimes, por meio de métodos-técnicos-científicos, conferindo-lhes validade probatória em juízo”. Ainda reforçando o tema, para o CPP de acordo com o artigo 158 “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado”, artigo esse que justifica a importância de um profissional devidamente capacitado, a fim de que tenha condições de fazer avaliações das informações em meio digital, o que lhe confere o título de Perito Forense Computacional. Outra definição aceita, foi dada por QUEIROZ e VARGAS (2010) afirmaram que para ser um perito considerado bom profissional, é imprescindível que tenha boa conduta, é necessário um bom conhecimento nos princípios básicos do direito, sigilo, privacidade, e conhecimento aprofundado nas tecnologias e ferramentas computacionais, bem como ter uma boa noção sobre psicologia do criminoso, e preferencialmente o *feeling* de analisar comportamentos criminosos e motivos para realizar tal ataque ou crime através do uso da computação.

A profissão então de Perícia Forense Computacional como recomendação, deve seguir algumas legislações como requisitos básicos, tais como a Lei LGPD (Lei Geral de Proteção dos Dados), Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 12.965/2014 do Marco Civil da Internet, como embasamento jurídico inicial. Como domínio técnico, é recomendado ao candidato obter conhecimentos sólidos em sistemas como:

- Sistemas Operacionais (Unix, Linux, Windows, MAC OS, Android e IOS);
- Sólidos conhecimentos de Hardware computacional, aparelhos *smarts*;
- Sólidos conhecimentos em imagens digitais;
- Sólidos conhecimentos em Redes de Computadores;
- Sólidos conhecimentos e Segurança computacional (criptografia, esteganografia, assinatura digital).

Desta forma, este profissional deve preferencialmente possuir uma boa experiência em sistemas computacionais, com certificações mínimas recomendadas como Pós-Graduação em Computação Forense. Este profissional deve ser extremamente organizado, ter habilidade de atenção aos detalhes e estar em constante atualização de todas as ferramentas usuais no mercado, como afirma José Milagre do (JUSBRASIL, 2021):

Além do perito digital ter uma formação aprofundada em tecnologia, deve demonstrar experiências em *frameworks*, *compliance* e melhores práticas previstas na tecnologia da informação como SOX, COBIT, ITIL, PCI, ISO 27001, bem como da legislação básica brasileira, Código Civil, Código Penal, Consolidação das Leis do Trabalho, e principalmente, normas processuais e procedimentais que regulamentam a produção da prova pericial no Brasil.

6 | OPORTUNIDADES E DEFICIÊNCIA DOS ÓRGÃOS PÚBLICOS NAS REALIZAÇÕES DE LAUDOS

A área da forense computacional em todo o Brasil está inevitavelmente congestionada pela falta de profissionais que representam o Estado, em especial pela demanda galopante que diariamente aumenta e em especial, pela demora nos processos jurídicos com suas burocracias e Leis que naturalmente os impedem de dar vazão rápida no pedido de laudos. Porém, é mister que a falta de profissionais concursados para atender a demanda em todo o território nacional esteja cada vez mais tornando este setor num dos grandes deficit profissionais. Ao analisar o material disponível por (CAOP, 2021), o qual divulgou um texto a pedido da 2ª Reunião de Trabalho do Grupo de Pesquisa em Atuação Criminal, resultado explorado nos últimos três anos antes de 2019, para mostrar a situação primeiro voltado aos problemas de cunho estadual e regional no Estado do Paraná. Faz-se saber que neste documento descrito pela (CAOP, 2021), o texto versa sobre as Cautelas em Relação à Busca e Apreensão que diz o seguinte:

Enquanto medida cautelar, a busca e apreensão – voltada ao apossamento

dos elementos instrutórios descritos no art. 240, § 1º, do CPP – somente poderá ser decretada quando presentes os requisitos do *periculum in mora* e do *fumus boni juris*. Particularmente em relação ao último, as fundadas razões correspondem:

(a) A um juízo de probabilidade sobre o possível encontro de objetos que possam constituir prova de infração penal, que estejam no local ou com a pessoa a ser revista;

(b) A um juízo de probabilidade de que os objetos ou pessoas procuradas efetivamente tenham relação com a investigação de um fato criminoso; e

(c) A presença de indícios da existência do crime que se investiga. Precisamente por isto, previamente a definir-se pela adoção desta medida, é de todo recomendável que esta aferição seja realizada pela Promotoria criminal.

A partir desta informação, o próximo assunto versa sobre as Cautelas em Relação à Perícia Digital e Computacional, o qual apresenta o que é, o que faz e qual o seu potencial dentro da Seção de Computação Forense do Instituto de Criminalística do Estado do Paraná. Com isto, o (CAOP, 2021) descreve que para se adotar uma perícia computacional forense é essencial compreender a finalidade e a potencialidade do setor responsável pela elaboração da perícia. Desta forma, destaca ainda a importância da computação forense em seu crescimento diário dentro do cenário atual que vivemos, de forma que aumentam também os registros dos chamados crimes virtuais, o qual também é acompanhado pelo aumento da complexidade do seu uso. Motivo este que leva o (CAOP,2021) a descrever que a interpretação de (PINHEIRO,2013) como:

A importância da computação forense cresce a cada dia, na medida em que aumentam os registros dos chamados crimes virtuais, bem como sua complexidade. Inserida na ciência criminalística, a computação forense consiste no uso de métodos científicos para a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais.

Partindo destes princípios, pode-se dizer que a coleta de evidências corresponde a uma atividade que exige muita cautela, em função especial de que em caso de ser realizado de forma errada, pode levar a perda do material a ser periciado e, principalmente, torna ilícita a prova produzida, inviabilizando assim o trabalho conduzido (CAOP,2021). Para isto, a Seção de Computação Forense do Estado do Paraná, conta com laboratórios em Curitiba e Londrina, embora tenham que atender todo o estado (realidade até 2019), possuíam centralizadas suas ações na cidade de Curitiba e assim, os principais exames realizados nestas seções são (CAOP,2021):

- Exame pericial em equipamentos computacionais, portáteis e de telefonia móvel (*Notebook, Tablet, Smartphone, e etc.*);
- Exame pericial em mídia de armazenamento computacional (disco rígido, cartão de memória, CD, DVD, etc.);

- Exame em local de informática (tal como sala de computador/Data Center);
- Exame em local de Internet (local de crime na internet);
- Busca e apreensão de vestígios cibernéticos e tratamento de dados criptografados.

Além dos exames comuns, a Seção abrange todas as áreas das Ciências Forenses, o qual trabalha em conjunto preparando o vestígio para análise em outras seções do Instituto de Criminalística tal como as Seções de Audiovisuais, Engenharia, Documentoscopia e Crimes Contra Pessoa. Porém, é de competência da Polícia Científica do Estado do Paraná, de acordo com os termos do inciso V, do artigo 33 do Decreto 5.887/2005, “*o desenvolvimento de campanhas educativas de esclarecimento e orientação à população*”, o qual é feito através do Projeto de Ciências Forenses na Escola, contemplando a divulgação de materiais sobre o uso responsável de computadores em apoio a SaferNet Brasil. Baseado nestas afirmações, o trabalho do (CAOP, 2021) relata ainda que:

A Polícia Científica figura há anos como o órgão de segurança pública do Estado do Paraná que possui os maiores índices de déficit em seus quadros de pessoal. Tal circunstância impacta diretamente na capacidade de realização de sua atividade-fim de maneira tempestiva, com reflexos diretos no desenvolvimento regular da persecução penal daquelas infrações penais que dependem da atividade pericial para elucidação. Os reflexos deste problema se estendem, inclusive, à população carcerária de presos provisórios do Estado, que hoje, dentro de uma perspectiva nacional, já é considerada uma daquelas que mais tempo permanece aguardando julgamento definitivo.

Desta forma, é importante ressaltar que estes dados são de 2019 pelo fato de não haver este estudo em 2021 o 2020 foram feitos levantamentos como mostra as Figuras 1 e 2, o qual mostra o quantitativo de material a ser periciado. Como é possível observar, na Figura 1, a quantidade maior de material a ser periciado está centrado em aparelhos celulares, o qual aponta um total de 14.840 equipamentos, em segundo lugar os Hds (discos rígidos de computadores) que foram apreendidos para perícia, segundo de *Notebooks* e demais equipamentos. Baseado nestes dados, a Figura 2 apresenta então a quantidade relativa de equipamentos periciados durante este período, o que chama a atenção então para a comprovação do tamanho do deficit produzido dentro desta órgão de Segurança Pública no Estado do Paraná e que certamente pode-se ter como exemplo para outros estados da nação.

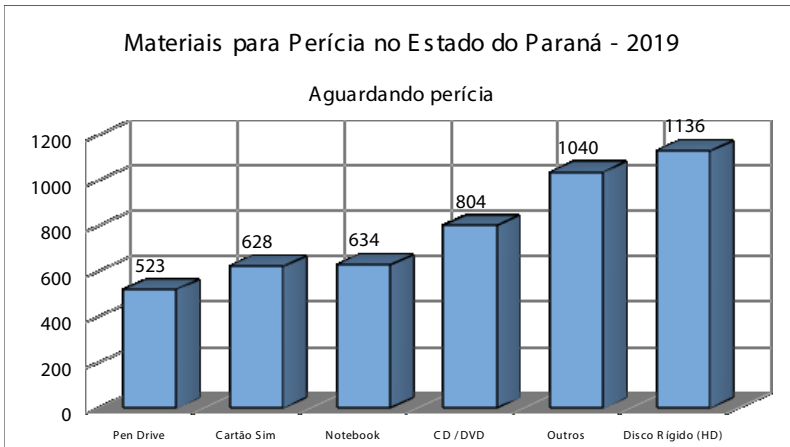


Figura 2 – Materiais para Perícia no Estado do Paraná 2019.

Fonte: Adaptado de (CAOP, 2021).

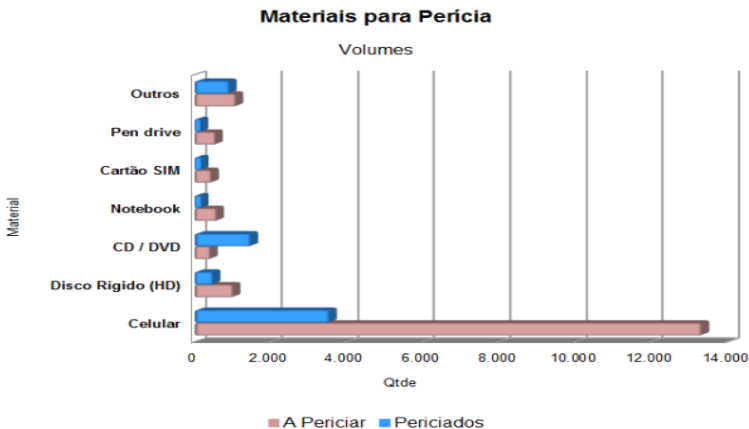


Figura 3 – Materiais para Perícia no Estado do Paraná 2019, comparativo dos materiais periciados.

Fonte: (CAOP, 2021).

Diante dos expostos nas Figuras 2 e 3, foram então levantados especificamente quanto à capacidade operacional da Seção de Computação Forense do Instituto de Criminalística em suprir a demanda durante o período, o que constatou-se conforme mostra a Figura 4 a situação de precariedade no atendimento para suprir o quantitativo de equipamentos a serem periciados naquele período (2019).

Projeção para zerar pendências

Peritos Ativos (média)	Produtividade Média (horas/mês)			
6,34	172			

Material	Complexidade (horas perícia)	Estoque (unidades)	nº de horas (perícia x und)	nº de anos (zerar estoque)
Celular	6	14.840	89.040	7,42
Disco Rígido (HD)	30	1.136	34.080	2,84
CD / DVD	1	804	804	0,07
Notebook	30	634	19.020	1,59
Cartão SIM	1	628	628	0,05
Pen drive	3	523	1.569	0,13
Outros	3	351	1.053	0,09
Cartão de Memória	3	238	714	0,06
Tablet	6	154	924	0,08
Disquete	2	95	190	0,02
Câmera Digital	3	60	180	0,02
CPU	30	30	900	0,08
Cartão Magnético	1	29	29	0,00
All-In-One	30	21	630	0,05
MP3/MP4/MP5	3	17	51	0,00
Netbook	30	13	390	0,03
		19.605	150.501	12,55

Figura 4 – Projeção para zerar pendências na Perícia no Estado do Paraná 2019.

Fonte: (CAOP, 2021).

Diante deste cenário, em função de verificar-se esta alta demanda, foi buscada a alternativa de exames periciais através da criação de filiais de atendimento que o Estado do Paraná adotou. O que foi mais assustador e relevante para as tomadas de decisão, foi justamente a perícia em aparelhos celulares, o qual apresenta um total de 7,42 anos para zerar o estoque, o que naturalmente mostra que não há condições de redução, em função em especial do uso atual destes equipamentos eletrônicos.

Como forma de oportunidade profissional, em consulta com o mercado de trabalho pela busca de profissionais da área, tanto para empresas que desejam criar o departamento de segurança, como para empresas que já atuam em perícias e auditorias, podemos destacar que de acordo com (MILAGRE,2021) a carreira de Perito Forense Digital até o ano de 2021, paga uma faixa de salário de R\$8.000,00 até R\$35.000,00. Já o site Educa Mais Brasil (EDUCAMAISBRASIL, 2021), apresenta um gráfico composto do nível das empresas com grau de progressão e porte das empresas, bem como mostra também o salário médio baseado no seu porte, que neste caso aponta as empresas de Pequena, Média e Grande. Entretanto, é importante destacar que existe uma diferença distinta dentro da área de perícia, onde um Perito Criminal é um funcionário público que trabalha na Polícia, mas não é um policial mas sim um auxiliar da justiça que escreve um laudo. Um Perito Digital, tem como premissa possuir um curso superior, ser concursado como funcionário público Estadual ou Federal e deve ser nomeado pelo chefe do Poder Executivo, e assim, deverá tomar posse em exercício, porém não necessariamente precisa ser um perito Oficial, bem como em algumas situações, não necessita ter formação específica, embora seja

recomendado.

O Perito Digital deve executar perícias solicitadas pelas polícias, pelo Poder Judiciário, pelo Ministério Público e por Comissões Parlamentares de Inquéritos (CPI) (VECCIA, 2019). Já o Perito *Ad Hoc* é aquele profissional nomeado normalmente por um Juiz ou por um Delegado, o qual pode atuar na área criminal na ausência de um perito oficial, ou mesmo em qualquer outra área tal como cível, trabalhista, familiar dentre outras áreas, uma vez que a Tecnologia da Informação (TI) está totalmente inseridas nestas áreas.

O Assistente Técnico por sua vez, é aquele profissional que é contratado pelas partes, quer seja de acusação ou de defesa, para que possa fazer o acompanhamento, análise e o trabalho do perito oficial ou o perito nomeado (*ad hoc*). Desta forma, o Assistente Técnico existe tanto no Código de Processo Penal como no Código de Processo Civil (PINHEIRO, 2013). Entretanto, todos estes profissionais deve ter a responsabilidade do peso do cargo que exerce, pois ele pode incriminar, ou libertar um indivíduo com seu trabalho, bem como também deve estar preparado para atuar em cenas de crimes violentos com atuações presenciais pós-crime, o que naturalmente impactam qualquer pessoa que não esteja acostumado com situações desta natureza, daí a importância de se avaliar sua experiência, sua capacidade cognitiva, seu estado mental e espiritual para atuar nesta profissão.

7 | CONCLUSÃO

Este trabalho teve como objetivo fazer um levantamento de qual é o perfil do profissional para que um Juiz tenha condições de requisitá-lo. As habilidades jurídicas neste contexto é um diferencial de extrema relevância, uma vez que em se tratando de crimes, toda nação tem a obrigação de constituir leis que os embase para tomada de decisão em um processo penal diante do juri. Entretanto, não só de leis este profissional deve estar alinhado, pois naturalmente existe o fator envolvimento com a cena de um crime, envolvimento com a cadeia de custódia, ou mesmo o envolvimento com as tarefas, processos e protocolos que são de suma importância para validar um laudo técnico. Além de todas estas premissas, este profissional deve ter sólidos conhecimentos técnicos para atuar na área forense digital ou computacional. Pois, como pode ser constatado neste trabalho, o perito forense computacional ou digital, deve conhecer de sistemas operacionais para todas as plataformas de ambientes, quer seja de equipamentos pessoais, equipamentos de médio e grande porte empresariais, o que o leva a um nível razoável de experiência, uma vez que não é trivial ter sólidos conhecimentos por exemplo em ambientes Microsoft, em especial no Sistema Operacional Windows (servidor e usuário) ou em equipamentos embarcados, sólidos conhecimento em Sistemas Operacionais Unix, Linux (servidor e usuário) ou em equipamentos embarcados, sólidos conhecimentos de Sistemas Operacionais para aparelhos celulares (*smartphones* ou não), de todos os fabricantes possíveis, onde os mais usuais são *Iphone* IOS e Android. Desta forma, não obstante, este profissional

deve ter então, naturalmente alguns anos de experiência no mercado de trabalho, pois se não tiver estas experiências, não serão tão convincentes seus laudos, além de seus investimentos em capacitações com certificações em sistemas, redes de computadores, hardwares, além é claro de certificações na áreas específicas voltadas para a Segurança Computacional e da Informação. Desta forma, está evidente que é uma profissão que está em franca expansão, e que requer algumas políticas públicas que possam regulamentar o Perito Forense Digital/Computacional particular, poder atuar para auxiliar nas ações dos processos que estão cada vez mais se acumulando dentro dos tribunais, em especial pelos dados apresentados que foram alarmantes, isto que foi somente em um estado, o que reflete naturalmente em todos os estados da nação. Portanto, uma regulamentação mais forte e mais atuante, deve ser levada em consideração para dar apoio aos profissionais que queiram seguir esta brilhante carreira.

REFERÊNCIAS

[CRIME]. In: **PRIBERAM, Dicionário Online de Português.**, 2021. Disponível em: [<https://dicionario.priberam.org/crime>]. Acesso em: 22/11/2021.

[VIRTUAL]. In: **DICIO, Dicionário Online de Português.**, 2021. Disponível em: [<https://www.dicio.com.br/virtual/>]. Acesso em: 22/11/2021.

ABNT, **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520:** citações: elaboração. Rio de Janeiro, 2002.

ABNT, **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724:** formatação de trabalhos acadêmicos. Rio de Janeiro, 2002.

APECOF. **Associação Nacional dos Peritos em Computação Forense.** Disponível em: <https://apecof.org.br/v2/> Acessado em: 08 DEZ. 2021.

CAOP, **Centro de Apoio Operacional das Promotorias: Perícias Criminais – Cautelas na Produção da Prova Pericial.** Disponível em: https://criminal.mppr.mp.br/arquivos/File/Pericias_criminais_-_orientacoes_na_producao_probatoria_-_final.pdf Acessado em: 09 de dez. 2021.

CERT.br. **Tecnoblog: Incidentes reportados ao CERT.br** referente aos meses de Janeiro a Dezembro de 2020. Disponível em: <https://cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html> Acessado em: 22 de nov. 2021.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** 1. Ed. São Paulo: Novatec, 2011.

FREITAS, Andrey Rodrigues. **Perícia Forense Aplicada à Informática.** Rio de Janeiro: Editora Brasport, 2006.

G1. **Profissional de TI: entenda o que faz e veja os cursos que o Senai oferece na área.** Disponível em: <https://g1.globo.com/especial-publicitario/o-futuro-do-trabalho/noticia/2021/12/06/profissional-de-ti-entenda-o-que-faz-e-veja-os-cursos-que-o-senai-oferece-na-area.ghtml>. Acessado em: 07 de dez. 2021.

GUIADACARREIRA. **Ciência da Computação: curso, carreira e mercado.** Disponível em: <https://www.guiadacarreira.com.br/guia-das-profissoes/ciencia-da-computacao/>. Acessado em: 07 de dez. 2021.

JUSBRASIL. **A profissão do futuro: Como ser um perito digital ou perito em informática e iniciar na carreira (2021).** Disponível em: <https://josemilagre.jusbrasil.com.br/artigos/483116816/a-profissao-do-futuro-como-ser-um-perito-digital-ou-perito-em-informatica-e-iniciar-na-carreira-2021>

KASPERSKY. Tecnoblog: **Principais ataques de Ransomware de 2020.** Disponível em: <https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020>. Acessado em: 22 de nov. de 2021.

KUROSE, James F. **Redes de Computadores e a Internet: uma abordagem top-down.** 6ª Ed. São Paulo: Pearson Education do Brasil, 2013.

LI, Fuguo. Study on security and prevention strategies of computer network. In: **2012 International Conference on Computer Science and Information Processing (CSIP).** IEEE, 2012. p. 645-647.

MADALENA, Juliano. **Regulação das fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital.** *Revista dos Tribunais*, v. 974, p. 81-110, 2016.

MAISDADOSDIGITAIS. Blog. **Mais Dados Digitais: o que o profissional de TI faz? Entenda de uma vez por todas.** Disponível em: <https://www.maisdados.com.br/o-que-o-profissional-de-ti-faz-entenda-de-uma-vez-por-todas/>. Acesso em: 06 de dez. 2021.

OLHAR DIGITAL. **Tecnoblog: Número de dispositivos inteligentes deve superar o de humanos em breve.** Página inicial. Disponível em: <https://olhardigital.com.br/2021/04/05/ciencia-e-espaco/dispositivos-inteligentes-deve-superar-numero-de-humanos>. Acesso em: 22 de nov. de 2021.

PAN, Jianli; PAUL, Subharthi; JAIN, Raj. **A survey of the research on future internet architectures.** *IEEE Communications Magazine*, v. 49, n. 7, p. 26-36, 2011.

PERDICES, Daniel et al. **Network performance monitoring with flexible models of multi-point passive measurements.** In: 2018 14th International Conference on Network and Service Management (CNSM). IEEE, 2018. p. 1-9.

PINHEIRO, Patrícia Peck. **Direito Digital.** 5 ed. São Paulo: Saraiva, 2013. p. 322

PROFISSIONAISTI. **Carreira em TI: O que faz um Perito Forense Computacional.** Disponível em: <https://www.profissionaisti.com.br/carreira-em-ti-o-que-faz-um-perito-forense-computacional/>. Acessado em 07 de dez. 2021.

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e perícia forense computacional.** Brasport, 2010.

REITH, M.; CARR, C.; GUNSCH, G. **An examination of digital forensic models.** *International Journal fo Digital Evidence*, 1 (3):1-12,2002.

SAYDAM, Tuncay; MAGEDANZ, Thomas. **From networks and network management into service and service management.** Journal of Network and Systems Management, v. 4, n. 4, p. 345-348, 1996.

VAULTREE. **Tecnoblog: Ciberataque: conheça os três maiores ataques de ransomware de 2021 até agora.** Disponível em: <https://www.vaultree.com/pt-br/post/ciberataque-conheca-os-tres-maiores-ataques-de-ransomware-de-2021-ate-agora/> Acessado em: 22 de nov. 2021.

VECCIA, Evandro Dalla. **Perícia digital: da investigação à análise forense.** Campinas, SP: Editora Millenium, 2019.

SOBRE O ORGANIZADOR

ERNANE ROSA MARTINS - Pós-Doutorado em E-learning pela Universidade Fernando Pessoa (UFP). Doutor em Ciência da Informação com ênfase em Sistemas, Tecnologias e Gestão da Informação, na Universidade Fernando Pessoa (UFP), em Porto/Portugal, reconhecido como equivalente ao curso de Doutorado em Ciência da Informação, da UnB. Mestre em Engenharia de Produção e Sistemas pela UCG, possui Pós-Graduação em Tecnologia em Gestão da Informação, Graduação em Ciência da Computação e Graduação em Sistemas de Informação. Professor de Informática no Instituto Federal de Educação, Ciência e Tecnologia de Goiás – IFG (Câmpus Luziânia) ministrando disciplinas nas áreas de Engenharia de Software, Desenvolvimento de Sistemas, Linguagens de Programação, Banco de Dados e Gestão em Tecnologia da Informação. Pesquisador do Núcleo de Inovação, Tecnologia e Educação (NITE), certificado pelo IFG no CNPq. ORCID: <https://orcid.org/0000-0002-1543-1108>. Página pessoal: <https://ernanemartins.wordpress.com/>

ÍNDICE REMISSIVO

A

Android 9, 29, 30, 31, 33, 34, 35, 36, 39, 146, 151

Aplicações 15, 26, 55, 56, 57, 59, 60, 61, 63, 64, 86, 107, 141

C

Capacitação 18, 78, 98, 101, 102, 103, 108

Competências 11, 12, 13, 15, 18, 19, 20, 24, 27, 41, 108, 110, 117, 118

Computação 12, 17, 20, 24, 28, 39, 54, 129, 133, 135, 143, 144, 145, 146, 147, 149, 152, 153, 155

Computacional 14, 16, 29, 30, 31, 40, 41, 133, 134, 135, 137, 138, 139, 140, 144, 145, 146, 147, 151, 152, 153

Comunidade 78, 92, 93, 98, 101, 103, 104, 109, 114, 120

Conhecimento 12, 13, 16, 17, 19, 20, 24, 26, 27, 41, 42, 76, 77, 85, 87, 92, 93, 94, 95, 96, 100, 101, 106, 107, 109, 110, 111, 112, 113, 114, 115, 117, 121, 123, 124, 139, 143, 145, 151

COVID-19 119, 120, 131

Crime 133, 134, 135, 138, 139, 144, 145, 147, 148, 151, 152

Cultura 12, 22, 45, 46, 52, 54, 77, 78, 80, 82, 93, 96, 98, 100, 101, 103, 104, 116

D

Desenvolvimento 1, 3, 5, 8, 11, 13, 15, 16, 19, 22, 44, 46, 47, 48, 52, 54, 55, 61, 64, 76, 77, 79, 81, 89, 90, 92, 94, 96, 97, 98, 99, 100, 101, 103, 104, 105, 108, 109, 110, 115, 117, 120, 121, 131, 140, 143, 144, 148, 155

Digital 12, 13, 18, 22, 29, 47, 54, 82, 83, 88, 89, 119, 120, 121, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 134, 138, 145, 146, 147, 150, 151, 152, 153, 154

E

Educação 11, 19, 22, 24, 27, 28, 41, 42, 43, 44, 79, 80, 81, 82, 89, 90, 92, 94, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 115, 116, 117, 118, 120, 143, 155

Empreendedorismo 98, 100, 101, 103, 104, 105

Ensino 11, 19, 20, 21, 22, 24, 40, 41, 42, 43, 77, 78, 79, 80, 81, 82, 84, 88, 89, 91, 92, 93, 94, 95, 96, 97, 98, 100, 101, 102, 103, 104, 106, 107, 108, 109, 110, 113, 114, 115, 116, 117, 118, 135

Extensão 30, 38, 75, 77, 79, 83, 88, 99, 101

F

Forense 29, 30, 31, 38, 39, 133, 134, 135, 137, 140, 144, 145, 146, 147, 149, 150, 151,

152, 153, 154

H

Hardware 4, 140, 141, 142, 146

I

Ideias 52, 98, 101, 102, 103, 107, 112

Inclusão 81, 108, 119, 120, 121, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132

Indústria 4.0 11, 12, 13, 18, 24, 27, 28

Informação 12, 14, 78, 96, 101, 106, 108, 132, 137, 140, 141, 143, 144, 145, 146, 147, 151, 152, 155

Inovação 18, 27, 60, 98, 99, 100, 101, 103, 104, 105, 121, 155

Instrumento 67, 68, 69, 70, 72, 73, 74, 97

Internet 1, 2, 3, 4, 12, 15, 16, 17, 29, 38, 42, 73, 86, 95, 96, 106, 109, 116, 122, 134, 138, 140, 142, 145, 146, 148, 153

L

Leitura 48, 75, 76, 77, 78, 81, 84, 85, 86, 87, 88, 89, 90

Letramento 75, 77, 87, 88

Literário 75, 76, 77, 79, 80, 82, 87, 88

Literatura de Cordel 84, 91, 92, 93, 96, 97

M

Materiais 6, 8, 19, 20, 26, 46, 55, 56, 57, 58, 59, 60, 61, 62, 64, 65, 78, 85, 101, 110, 111, 114, 116, 145, 148, 149

M-learning 67, 68, 69, 70

N

Nanohíbridos 55, 56, 57, 59, 61, 62, 64

P

Políticas 9, 74, 75, 77, 99, 105, 107, 115, 119, 120, 121, 132, 152

Problemas 1, 8, 9, 18, 46, 75, 95, 96, 100, 101, 104, 120, 134, 137, 138, 142, 144, 146

Produção 8, 11, 13, 14, 15, 16, 17, 18, 19, 20, 24, 26, 44, 45, 46, 47, 49, 50, 53, 54, 55, 57, 58, 59, 96, 100, 101, 103, 109, 110, 132, 136, 144, 146, 152, 155

Projeto 19, 27, 41, 54, 75, 77, 78, 81, 83, 84, 88, 89, 92, 94, 96, 100, 115, 116, 140, 148

Prototipagem 98, 101, 102, 104, 105

Q

Química verde 55, 58, 64

R

Remoto 40, 41, 42, 43, 91, 95, 96

S

Segurança 19, 30, 56, 61, 113, 133, 137, 138, 139, 140, 141, 142, 144, 146, 148, 150, 152

Serviços 119, 120, 121, 123, 134, 139, 140, 141

Simulação computacional 40, 41

Sistemas 12, 13, 14, 15, 16, 17, 18, 20, 24, 26, 27, 29, 30, 39, 61, 62, 109, 135, 136, 138, 140, 143, 144, 145, 146, 151, 152, 155

Smartphones 1, 2, 4, 5, 8, 9, 10, 29, 30, 31, 38, 39, 122, 151

Software 4, 19, 20, 24, 31, 48, 54, 73, 74, 119, 120, 124, 137, 140, 141, 142, 144, 155

T

Tecnologias inovadoras 11, 13, 15, 17, 18, 23

V

Virtual 42, 68, 84, 111, 113, 114, 115, 133, 134, 135, 152


W


Workshops 98, 99, 101, 102, 103




TECNOLOGIA E GESTÃO DA INOVAÇÃO

www.atenaeditora.com.br 

contato@atenaeditora.com.br 

[@atenaeditora](https://www.instagram.com/atenaeditora) 


www.facebook.com/atenaeditora.com.br 


 **Atena**
Editora


Ano 2022

TECNOLOGIA E GESTÃO DA INOVAÇÃO



www.atenaeditora.com.br 

contato@atenaeditora.com.br 

[@atenaeditora](https://www.instagram.com/atenaeditora) 

www.facebook.com/atenaeditora.com.br 

Atena
Editora

Ano 2022