INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

ESTUDO SOBRE O ATUAL CENÁRIO DOS CIBERCRIMES DENUNCIADOS NA CIDADE DE LUANDA

Matias Francisco Sanches Tavares

Dissertação de Mestrado em Ciências Policiais

Especialização em Criminologia e Investigação Criminal

Orientação Científica:

Prof. Doutor Sérgio Ricardo Costa Chagas Felgueiras

Lisboa, Outubro de 2024

Epígrafe

“Todo o nosso progresso tecnológico, que tanto se louva, o próprio cerne da nossa civilização, é como um machado na mão de um criminoso”.
(Albert Einstein)

Dedicatória

O meu eterno agradecimento vai para a minha avó (Madalena Chimambo), *in memoriam*, que apesar de não ter tido a oportunidade de frequentar uma escola não mediu esforço e vinculou, desde a mais tenra idade, em mim a vontade de não abdicar e acreditar que com paciência e dedicação não existe o impossível e fazendo de mim o homem que hoje sou.

Agradecimentos

Em primeiro lugar agradeço a Deus por conceder-me força e coragem de estar longe de casa em busca do conhecimento.

Agradeço em especial à minha mãe, aos meus irmãos, minha avó Judith (*in memoriam*), tia Paula "Kabua" (*in memoriam*), aos tios Valente e Mendes, aos professores Sérgio Ricardo Felgueiras (por ter acreditado na minha orientação), Nuno Poiares, Mário Ferreira Monte, João Fernando Mendes, a direção do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), a Nelma Albertina Sambo (que tem sido o meu suporte emocional), Angelina Domingos (graças à sua insistência pelo ISCPSI, foi possível este diploma), Adelina Figueiredo, as famílias Mavungo, Domingos e Eduardo, aos meus amigos: Rosa Tchivandja, Fernando Neto, Isabel de Faria, José Chicuata, Policarpo Pedro, Thuany Fernandes, Anita Salohuma, Marta da Costa, Luís da Costa, Raquel Valentim, Simão Kativa (que tem sido um pai), Ernestina Sitaque, Tomás Tchimanha, Madeca, Rossana Jessy, Pequeno, João Vumbi, Djamila Suphia, Gilson Katimba, aos meus amigos da rua da Vaidade (Cabinda), a empresa Google (pelos conteúdos públicos fornecidos) e a todos aqueles que direta ou indiretamente têm contribuído para o êxito da minha trajetória académica e que face a exiguidade do espaço não foram citados, mas nunca serão esquecidos.

Muitos não quiseram acreditar e nem dar força e por isso não foram esquecidos os demais professores que compõem o corpo académico do ISCPSI, administrativos, pessoal de base e os colegas do XV curso de Criminologia e Investigação Criminal, pois são consequentes. Louvados sejam estes e de todos aqueles que se mantiveram firmes, acreditaram e continuam a acreditar num futuro próspero.

O meu especial obrigado vai para a Eunice Tchivandja, por continuamente apoiar-me durante a difícil estadia na cidade de Lisboa, e ao professor Nuno Picas dos Santos, pelo grande didata que é, e com a sua sapiência tem contribuído bastante na continua edificação da qualidade de ensino do ISCPSI e permitiu a minha fácil integração num meio que não conhecia.

Obrigado a todos…

ÍNDICE

Lista de Figuras

Lista de gráficos

Lista de tabelas

Lista de Siglas e Abreviaturas

Art.º	Artigo
CI	Comunidade Internacional
CIA	Central Intelligence Agency
CPD	Centro de Processamento de Dados
CPLP	Comunidade dos Países de Língua Portuguesa
CTTU	Correios, Telégrafos e Telefones do Ultramar
DCCI	Direção de Combate aos Crimes Informáticos
DNPCSD	Direção Nacional das Políticas de Cibersegurança e Serviços Digitais
DOS	Disk Operating System
DW	Deutsche Welle
ENATEL	Empresa Nacional de Telecomunicações
ENCTA	Empresa Nacional de Correios e Telégrafos de Angola
EPTEL	Empresa Pública de Telecomunicações
ES	Engenharia Social
IA	Inteligência Artificial
IISSCC	International Information System Security Certification Consortium
INE	Instituto Nacional de Estatística
IP	Internet Protocol
IRC	Internet Relay Chat
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
P2P	Peer-to-Peer
PGR	Procuradoria-Geral da República
PIN	Personal Identification Number
RAID	Redundant Array of Inexpensive Disk
SI	Sistemas Informáticos
SIC	Serviço de Investigação Criminal
SO	Sistema Operativo
TCP	Transmission Control Protocol
TIC	Tecnologias de Informação e de comunicação
UNODC	Escritório das Nações Unidas sobre Drogas e Crime

USDHS U.S. Department of Homeland Security

VOA Voz da América

VOIP Voice Over Internet Protocol

Resumo

O presente trabalho visa o estudo sobre o atual cenário dos cibercrimes denunciados na cidade de Luanda. Nesta investigação, levanta-se o seguinte problema: como se manifesta o cibercrime denunciado na cidade de Luanda? De modo a ser respondida a problemática da investigação, foi traçado como objetivo geral a descrição de como se manifestam os cibercrimes denunciados na cidade de Luanda. Como objetivos específicos, foram traçados os seguintes: descrever os principais cibercrimes denunciados na cidade de Luanda, descrever os principais alvos dos cibercrimes denunciados na cidade de Luanda, descrever as medidas implementadas pelo governo de Angola para o combate dos cibercrimes denunciados na cidade de Luanda e propor recomendações para a prevenção contra os cibercrimes na cidade de Luanda. A pesquisa foi realizada com recurso a fontes bibliográficas sobre a temática que possibilitaram entender as teorias do crime e levar-nos a abordagem do cibercrime e das suas formas de manifestação. Não existem estudos oficiais sobre os cibercrimes denunciados na cidade de Luanda, e com vista a gerar mais informações para futuras pesquisas conclusivas optou-se pela realização de uma pesquisa exploratória com uma abordagem quantitativa, sem, no entanto, trabalhar-se com hipótese que visariam a confirmação ou não dos resultados da pesquisa. Foram aplicados dois (2) questionários: um (1) destinado aos especialistas de instituições públicas e privadas e outro ao público-geral, de modo a compreender como ambos os grupos abordam e lidam com crimes desta natureza bem como a maneira como estes crimes se manifestam nas instituições e na sociedade em geral. Os resultados indicam que nas instituições os cibercrimes se manifestam predominantemente por meio de *phishing* e *ransomware*, enquanto, entre a população geral, prevalecem o *skimming* e o *phishing*. Em conclusão, entende-se que a falta de norma específica para o combate de crimes desta natureza, a fraca cooperação com países e instituições com maior experiência, a fraca infraestrutura tecnológica capaz de acompanhar a demanda, a falta de formação e treino dos recursos humanos, a falta elaboração de protocolos de resposta contra ataques cibernéticos, a falta de confiança da população nas atividades levadas acabo pelo governo, a falta de instrução e de abordagem regular deste fenómeno constituem elementos que tornam a cidade de Luanda alvo apetecível para o cometimento dos cibercrimes.

Palavras-chave: Cibercrime; Cibersegurança; Ciberespaço; *Phishing*; Cidade de Luanda.

Abstract

This work aims to study the current scenario of cybercrimes reported in the city of Luanda. In this investigation, the following research problem arises: how does cybercrime reported in the city of Luanda manifest itself? To answer the research problem, the general objective was to describe how cybercrimes reported in the city of Luanda manifest themselves. As specific objectives, the following were outlined: describe the main cybercrimes reported in the city of Luanda, describe the main targets of cybercrimes reported in the city of Luanda, describe the measures implemented by the government of Angola to combat cybercrimes reported in the city of Luanda and propose recommendations for the prevention of cybercrime in the city of Luanda. The research was conducted using bibliographical sources on the subject and made it possible to understand the theories of crime and lead us to an approach to cybercrime and its forms of manifestation. There are no official studies on cybercrimes reported in the city of Luanda, and with a view to generating more information for future conclusive research, it was decided to carry out exploratory research with a quantitative approach, without, however, working with hypotheses that would aim to confirmation or not of the search result. two (2) questionnaires were applied: one (1) aimed at specialists from public and private institutions, and the other for the general public, to understand how both groups approach and deal with crimes of this nature, as well as the way in which these crimes manifest themselves in institutions and society in general. The results indicate that, in institutions, cybercrimes manifest themselves predominantly through phishing and ransomware, while, among the general population, skimming and phishing. In conclusion, it is understood that the lack of specific standards for combating crimes of this nature, the weak cooperation with countries and institutions with greater experience, the weak technological infrastructure capable of keeping up with demand, the lack of education and training of human resources , the lack of elaboration of response protocols against cyber-attacks, the population's lack of trust in the activities carried out by the government, the lack of education and regular approach to this phenomenon constitute elements that make the city of Luanda an attractive target for the commission of cybercrimes .

Keywords: Cybercrime; Cybersecurity; Cyberspace; Phishing; City of Luanda.

INTRODUÇÃO

Antiga colónia portuguesa descoberta por Diogo Cão, em 1482, Angola é um Estado que faz parte da África Austral e Central. Faz fronteira ao norte com a República do Congo e a República Democrática do Congo, ao sul com a República da Namíbia, a este com a República da Zâmbia e ao oeste com o Oceano Atlântico. Possui uma extensão geográfica de 1.246.700 km^2 (Tavares, 2016). A capital do país é a cidade de Luanda, que segundo a Lei 29/11 de 1 de setembro, n.º 168, I Série, no capítulo I, Art.º 4.º, ponto 2, define que a província de Luanda, com sede na cidade de Luanda entendido como município de Luanda), integra os seguintes municípios: Luanda, Cacuaco, Belas, Viana, Cazenga, Icolo e Bengo e Quiçama.

Após a independência, a 11 de novembro de 1975, o país mergulhou numa guerra civil que culminou em maio de 1991, com os acordos de Alvor, mas que infelizmente em setembro de 1992 ressurgiu a guerra até ao alcance da paz, a 4 de abril de 2002. Entre estes dois (2) períodos da guerra civil, no final da década de 1990, alguns setores públicos da cidade de Luanda começaram a ter acesso aos serviços de internet, via satélite, o que demostra que o país começava a ter interesse pela digitalização dos serviços, mesmo de forma limitada. Contudo, com o alcance da paz o Estado libertou alguns setores sob a sua esfera, principalmente os serviços de telefonia móvel, permitindo assim o surgimento de empresas privadas para revolucionarem o setor. Inicialmente os serviços eram fornecidos na cidade de Luanda e posteriormente nas cidades de Cabinda, Benguela e Lubango, e mais tarde nas demais localidades. Com a passagem dos serviços analógicos para o digital, as empresas passaram a fornecer os serviços de internet o que permitiu o crescimento do uso dos dispositivos eletrónicos, o alargamento do número de usuários e de forma natural foram também aparecendo casos de cibercrimes.

O século XX, também chamada a era da digitalização, tem propiciado o surgimento e o desenvolvimento de tecnologias que têm permitido o uso massivo das mesmas e fruto disso tendem a mudar a forma de interação entre as pessoas de diferentes latitudes, tornando-as cada vez mais dependentes das tecnologias, particularmente dos serviços de internet que no entender de Nascimento (2016) apesar dos benefícios e o crescimento que estes serviços trazem para a sociedade tem sido um elemento causador da transferência de algumas atividades rotineiras para o ciberespaço e, consequentemente, o aparecimento de condutas ilícitas, denominadas cibercrimes,

levadas acabo por pessoas com determinados conhecimentos na matéria e que os usam com intuito de alvejarem instituições e pessoas singulares por intermédio de dispositivos eletrónicos. Em Angola, particularmente na cidade de Luanda, o uso dos serviços de internet cresce a cada dia que passa, e algumas vezes sem devida observância das medidas de segurança com vista a salvaguardar de informações privilegiadas, propiciando assim um ambiente para a prática dos cibercrimes que hoje representam uma ameaça à escala global e afeta governos, empresas e pessoas singulares.

No que respeita à investigação em causa é necessário compreender as diferenças existentes nos conceitos de cibercrime, ciberespaço e cibersegurança. Ribeiro (2015) define o cibercrime como sendo atos criminosos perpetuados com recurso a dispositivos eletrónicos contra uma pessoa ou a um Sistema Informático (SI) de modo a causar danos e o bloqueio de serviços podendo ser praticado em qualquer lugar do mundo. Esta definição é completada por Santos (2015) ao incluir as infrações tradicionais, tais como: a fraude, a falsificação, o roubo de identidade, a distribuição de material pedo-pornográfico, incitamento ao ódio racial, ataque contra os sistemas informáticos, recusa de serviço e software malicioso.

A ação que visa o cometimento do cibercrime pode ser feita de dois modos: os de baixa tecnologia e os de alta tecnologia. Os de baixa tecnologia, normalmente não exigem conhecimentos profundos de informática pois o alvo é a vítima ao passo que os de alta tecnologia normalmente exigem profundos conhecimentos de programação, pois o objetivo é a danificação do SI. (Robalo, 2021)

O ciberespaço é entendido como um espaço virtual na internet que anulou fronteiras físicas e aproximou virtualmente as pessoas, formando uma nova dimensão espacial que permite um contato imediato a todos aqueles que estejam conectados a rede, independentemente da sua localização geográfica. (Nascimento, 2016)

A cibersegurança é definida por Pereira (2022) como sendo o conjunto de medidas e ações de prevenção, controlo, deteção, reação, análise e correção que visam a manutenção do estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e SI no ciberespaço, e das pessoas que nele interagem.

O histórico do cibercrime na cidade de Luanda é preocupante na medida que tem evoluído consideravelmente e os cibercriminosos tendem a adotar diferentes técnicas de formas a atingirem os alvos através do *phishing*, *ransomware*, crimes financeiros,

clonagem de cartões/*skimming* e transferências ilícitas (via *internet banking*). Crimes desta natureza provocam danos económicos, afetam a fidúcia nas transações *online*, invadem a intimidade das pessoas e comprometem a infraestrutura tecnológica.

Esta investigação insere-se na área temática do cibercrime, tendo como objeto de estudo a compreensão dos cibercrimes denunciados na cidade de Luanda. A pergunta de partida é: como se manifesta o cibercrime denunciado na cidade de Luanda? O objetivo geral consiste em descrever como se manifestam os cibercrimes denunciados na cidade de Luanda.

Os objetivos específicos foram organizados da seguinte forma: descrever os principais cibercrimes denunciados em Luanda; identificar os principais alvos desses crimes; descrever as medidas implementadas pelo governo de Angola para combatê-los; e propor recomendações para a sua prevenção na cidade. Em função dos objetivos traçados para esta investigação, e considerando as limitações bibliográficas e as dificuldades na obtenção de informações, foi realizado um estudo de natureza exploratória, com enfoque quantitativo e caráter descritivo, visando obter mais informações sobre os cibercrimes denunciados na cidade de Luanda e, assim, fomentar a realização de pesquisas futuras de caráter conclusivo. Os resultados foram apresentados e interpretados pela análise das amostras estatísticas (por gráficos e tabelas) e que garantem a total fidelidade e veracidade da pesquisa, com o auxílio de duas (2) ferramentas eletrónicas: SPSS e *Microsoft Office Excel*.

A dissertação insere-se na área temática do cibercrime e foi estruturado por capítulos da seguinte maneira:

No capítulo 1, que trata do marco teórico sobre o crime e o cibercrime, foi realizada uma análise de algumas teorias do crime fundamentais para a compreensão do fenómeno em estudo, dado que este se carateriza por uma conduta criminosa. Esta análise conduziu-nos à teorização dos cibercrimes e das suas diversas formas de manifestação.

No capítulo 2, dedicado à contextualização do conceito de cibersegurança, foi apresentada uma resenha sobre o conceito de cibersegurança e a importância crucial de sua manutenção, abordando o triângulo da cibersegurança (disponibilidade, integridade e confidencialidade), bem como as principais práticas adotadas para a sua preservação em empresas e por indivíduos.

No capítulo 3, que trata das TIC e do cibercrime em Angola, foi analisado o crescimento das infraestruturas tecnológicas e a normatividade relacionada com o

cibercrime, além da incidência dos cibercrimes e dos danos económicos causados na cidade de Luanda. Foram também discutidos os setores mais visados, as medidas implementadas para o combate ao cibercrime, a cooperação internacional em matéria de cibersegurança, e realizada uma avaliação sobre a importância do estudo dos cibercrimes denunciados em Luanda.

No capítulo 4, marco metodológico, fez-se a abordagem dos procedimentos seguidos durante a investigação e que contempla a pergunta de investigação, os objetivos, a definição do universo e da amostra, a definição do tipo e o método da pesquisa, a justificativa, os procedimentos, a definição das técnicas de recolha de dados, os instrumentos e técnicas de processamento.

No capítulo 5, apresentação e discussão dos resultados, foi dedicado para a análise dos questionários por inquérito dirigidos separadamente aos especialistas de instituições públicas e privadas da cidade de Luanda e outro dirigido à população geral.

Na conclusão, foi realizada uma análise geral do objetivo principal e dos objetivos específicos propostos, a fim de verificar se foram alcançados em função das questões levantadas ao longo do trabalho. Em seguida, foram apresentadas algumas recomendações, com o intuito de contribuir para a melhoria da situação atual do cibercrime na cidade de Luanda e servir de suporte para futuras investigações.

A exploração deste tema permite compreender como as instituições e a população de uma metrópole em crescimento lidam com essa ameaça. Além disso, o estudo contribui com informações que servirão de base para futuras investigações, bem como para a formulação de políticas públicas e apoio dos profissionais de segurança cibernética, permitindo-lhes antecipar melhor as possíveis ameaças e preparar medidas de prevenção e respostas mais eficazes

1. MARCO TEÓRICO SOBRE O CRIME E O CIBERCRIME

A teoria do crime é um campo multidisciplinar que abrange áreas como a criminologia, o direito penal, a sociologia, a psicologia, entre outra, e que procura perceber os elementos constituintes do crime e as razões que levam as pessoas a cometerem atos ilícitos. No entanto a busca pelo conhecimento da sua origem faz com que o pesquisador tenha uma base sólida, maior segurança e entendimento para tratar os conceitos, as teorias, as caraterísticas e os elementos do crime. Existem várias teorias do crime (provocando por vezes alguma divergência doutrinal) que se concentram em diferentes aspetos, tais como: económicos, biológicos, sociais e psicológicos do comportamento criminoso (Coelho, 2023).

Para que uma conduta seja considerada crime é necessário compreender as teorias do crime e os seus elementos típicos que apesar de poderem variar de acordo a cada ordenamento jurídico, geralmente possuem elementos característicos, tais como a culpabilidade, a tipicidade e a ilicitude.

As bases para a atual teoria geral do crime começaram com a ser influenciadas a partir do pensamento jurídico de André Tiraqueau, no século XVI, que refletiam relativamente ao entendimento das normas sociais e legais, através da abordagem de temas como a honra, a família e as obrigações sociais, entendendo-se assim que já se analisava o crime como um facto ilícito e punível praticado com dolo ou negligência. As suas análises permitem que sejam compreendidos como determinadas condutas eram reguladas e consideradas criminosas pela sociedade e pela lei (Brito, 2019).

Durante a Idade Média, a teoria do crime foi influenciada por crenças religiosas sobre a justiça e o pecado, sendo a justiça vista como a punição pelo cometimento do pecado. No entanto, com o surgimento do Iluminismo, no século XVIII, a teoria do crime começou a basear-se mais em ideias científicas, o que veio posteriormente a permitir o desenvolvimento da teoria geral do crime, baseada em critérios objetivos (a intenção do autor e a gravidade do dano causado). Com o desenvolvimento da Criminologia e da Psicologia Criminal, a partir do século XIX, a teoria do crime passou a considerar fatores como as condições psicológicas do autor, as causas sociais, o ambiente social e económico, e mais recentemente as tecnologias forenses (impressão digital e a análise de DNA), que permitem uma melhor investigação dos crimes (Mocinho, 2023).

Apesar da existência de divergências na interpretação das teorias do crime, far-se-á uma análise sobre opiniões de diferentes autores, atendendo que a investigação em

causa tem como foco o estudo sobre o atual cenário dos cibercrimes denunciados na cidade de Luanda. Para tal, é imprescindível começar por definir e tipificar o que se entende por crime (do ponto de vista geral).

No entender de Bezerra (2017) o conceito de crime pode diferenciar em função dos aspetos de maior realce, sendo os principais: material (procura entender o que é relevante para ser considerado um conduta criminoso e a sua relevância para o direito penal), formal (analisa as consequências jurídicas da infração, com o realce ao tipo de sanção) e analítico (tem em consideração os elementos estruturais da infração).

Para Mocinho (2023) existem diversas teorias que procuram explicar o conceito de crime e cada uma delas com as suas particularidades e existindo ideias transversais como a de que o crime é um fato socialmente danoso ou a de que a responsabilidade criminal deve ser sempre atribuída ao seu autor e não a outras pessoas.

Apesar dos crimes acompanharem a existência humana, com a transição do século XX para o século XXI surgiu um novo tipo de crime com a peculiaridade de frequentemente ser praticado em ambiente virtual, com recurso a internet ou os Sistemas Informáticos (SI), e que no entender de Machado (2017) podem atentar contra as pessoas e ao património (material e imaterial), e que com o crescimento e o desenvolvimento da Inteligência Artificial (IA) tende a aumentar.

Para que um campo de investigação seja considerado científico, deverá ter um conhecimento autónomo e ampliável, com base a pesquisas de especialistas e desenvolvimento de teorias aplicáveis a área do conhecimento. As teorias tradicionais de análise do crime oferecem contributo valioso para se buscar e explicar as razões que estão por trás do cometimento dos crimes que hoje são maioritariamente praticados no mundo digital. É difícil a explicação dos cibercrimes com base a uma única teoria do crime, pois é um fenómeno transversal e com diferentes caraterísticas no modo de atuação dos seus praticantes, daí que para a sua melhor compreensão diversas teorias se interlaçam. Neste trabalho, são abordadas as seguintes teorias do crime: a teoria da anomia, a teoria da associação diferencial, a teoria da subcultura, a teoria da oportunidade e a teoria do anonimato. A escolha dessas teorias do crime teve como base a forma como se manifesta o cibercrime denunciado na cidade de Luanda, pois entende-se serem as que mais se aproximam e melhor explicam a realidade em estudo.

A evolução científica da criminologia e da sociologia permitiu que no século XX surgisse a teoria da anomia, desenvolvida pelo sociólogo francês Émile Durkheim,

com a sua obra o Suicídio, onde procurou explicar a anomia com base nas taxas variáveis de suicídios em diferentes sociedades e períodos, pela ausência de normas sociais claras e pela falta de integração das normas sociais existentes (Rego, 2019).

A respeito, Baratta (2002) entende que o crime é um fenómeno normal da sociedade e não necessariamente nocivo e estando presente em todas as sociedades desde o nascimento ao convívio social entre os homens.

No entender de Calhau (2006, p. 60) “a anomia é uma situação social onde falta coesão e ordem, especialmente no tocante a normas e valores”, o que vai de encontro ao defendido por Barreiras (2021) ao referir que nessa teoria o sujeito se considera feliz quando as suas faltas forem compatíveis com os meios para satisfazê-las.

A falta de lei específica e consistente para o combate dos cibercrimes em Angola, particularmente na cidade de Luanda, cria um vácuo que ao ser aproveitado pelos cibercriminosos contribui na criação de um ambiente permissivo que afeta a contínua vontade da apresentação de denúncias diante das autoridades, pelas pessoas coletivas e singulares, pois acreditam pouco na capacidade punitiva das autoridades.

A segunda teoria do crime a ser estudada neste trabalho, a teoria da associação diferencial, surge na década de 1930 com um paradigma mais sociológico e tendo como expoente Edwin Sutherland. Essa teoria é basilar para a compreensão dos crimes associativos e o fenómeno do crime organizado, partindo do princípio que o crime não pode ser definido simplesmente como a inadaptação de pessoas de classes menos favorecidas e defende que os processos de comunicação no seio do grupo são determinantes para a prática do delito (Shecaira, 2004).

Essa visão, também é defendida por Ferro (2008) ao afirmar que o comportamento criminoso é aprendido em interação com outras pessoas e que este não é herdado, deixando a entender que a teoria se concentra na interação social e na influência do ambiente social na aprendizagem do comportamento criminoso.

Em suma, a escolha da teoria da associação diferencial para a realidade em análise, visa fundamentalmente para a compreensão de como os fenómenos sociais podem afetar no cometimento dos cibercrimes denunciados na cidade de Luanda, na medida que a falta de oportunidade de emprego, o difícil acesso a educação, as desigualdades socioeconómicas, entre outras, podem direcionar pessoas a procurarem por opções que possam suprir os seus desejos, e que podem incluir a prática dos cibercrimes.

A terceira teoria associada ao estudo é a teoria da subcultura delinquente, desenvolvida por Albert Cohen. Esta teoria faz parte das várias teorias pertencentes

a escola sociológica de Chicago que muito contribuiu para a revolução da criminologia e trazendo a multiplicidade de interpretações sobre a delinquência, em especial, a juvenil, para tentar explicar a criminalidade, o criminoso, a vítima e o meio. Esta teoria, carateriza o crime como a consequência da identificação dos jovens para a aquisição de *status* com base a uma realidade venerável com a qual se identifica. (Liberati, 2007)

A tarefa de definir o conceito de subcultura não é fácil e implica a existência de modelos normativos opostos aos que governam a cultura predominante, que, por vezes, surge em razão de uma posição coletiva de conflito e frustração no interior de uma certa cultura. Neste sentido, o crime é entendido como o reflexo da interiorização e do acatamento de um definido código cultural que torna a delinquência categórica e envolve a apreensão de ações a partir de uma filosofia de crenças e valores. (Dias & Andrade, 2013)

Com base nestes ideais, ao serem desconsideradas as normas e os fatores sociais convencionais, a subcultura delinquente promove um sentimento que gera conformismo, consenso e homogeneização entre os seus praticantes. Portanto, deve-se levar em consideração o significado dos dados, atos e objetos característicos dessa comunidade. (Queiroz & Lavor, 2020)

Com o crescimento e a evolução contínua da tecnologia, a subcultura delinquente ganha cada vez mais preponderância no mundo do cibercrime, pois influencia consideravelmente as motivações e as ações praticadas pelos cibercriminosos, funcionando como uma escola de ensino do cometimento do crime com a partilha de estratégias e ferramentas, por parte dos mais experientes e entendidos na matéria para os mais novos, exercendo deste modo um forte poder de atração sobre os jovens e adolescentes que facilmente podem ser seduzidos com promessas de obtenção da fama, dinheiro e poder, através de praticas que desafiam as autoridades competentes e procuram promover as suas próprias normas de convivência. Como resultado disso, o sucesso dos ataques cibernéticos e as habilidades dos seus praticantes são alvos de reconhecimento interno da subcultura delinquente e levam a sua ascensão dentro de um grupo.

A quarta teoria do crime que apoia este estudo é a teoria da oportunidade que ao contrário das outras não é atribuída a um único criador, pois resulta da evolução combinada de teorias com as suas cambiantes e abordagens e a contribuição gradual de autores como Marcus Felson, Lawrence Cohen, Ronald Clarke, Derek Cornish, Robert Brzezinski, Paul Brantingham, entre outros. Segundo estes, para a ocorrência

de um ato criminoso devem coincidir três (3) elementos: um infrator motivado, a ausência de guardião e um alvo vulnerável. (Felson & Clarke, 1998)

Na sua génese a teoria era aplicada no estudo da criminologia tradicional, mas na atualidade tem-se apresentado revelante para a análise do cibercrime uma vez que obsequia uma perspetiva útil ao enfatizar a importância da redução das oportunidades que permitam a ocorrência dos crimes para o fortalecimento da segurança dos SI, consciencialização dos usuários sobre os riscos e contribuir na implementação das medidas de prevenção da incidência de crimes desta natureza. (Bedendo, 2008)

Com a evolução social, a teoria geral do crime hoje é vista como uma abordagem pluralista de enfoques e perspetivas, na medida que procura enfatizar a intenção do autor e o dano por si causado bem como os fatores ambientais e sociais que sofrem influências pelas mudanças políticas. Para esta pesquisa, tomamos como referência as ideias de Bezerra (2017), pois são abragentes e fazem uma abordagem aos elementos material, formal e analítico, os três (3) elementos básicos a ter-se em conta para a tipificação de um ato como crime.

Apesar da rápida evolução tecnológica mundial trazer consigo múltiplos benefícios também podem criar sentimentos desajustados no seio das pessoas, das instituições e nas normas de convivência social e incentivarem a busca de oportunidades ilícitas com aprendizagem de algoritmos e técnicas de invasão. Para tal, os cibercriminosos tendem a ser criteriosos e calculistas nas decisões que tomam e os métodos a aplicar para cada tipo de ataque, de modo a maximizarem os lucros e a minimizarem os riscos de serem descobertos.

A quinta teoria do crime utilizada para o apoia do estudo em causa é a teoria do anonimato, que face aos importantes avanços tecnológicos, particularmente dos serviços de internet, funciona como elemento essencial que incentiva o cometimento dos cibercrimes por possibilitar que os seus praticantes mantenham o anonimato e deste modo conseguirem ampliar o seu campo de atuação, causando impactos negativos na vida das suas vítimas e aos SI. (Lima, 2021)

A discussão sobre o conceito de anonimato traz consigo a interpretação de que ela é aproveitada e utilizada para encobrir os delitos cometidos no mundo virtual, cujo alcance não é fácil de ser controlado e previsto, desafiando a efetividade das políticas públicas criminais por conta das complicações de serem identificados os agentes criminosos por trás dos ciberataques. (Gleicher, 2008)

No entender de Melo (2017) o anonimato pode ser praticado por qualquer utilizador dos serviços de internet ou grupo de pessoas com o intuito de poderem emitir opinião, disseminar informações ou para o cometimento de crimes virtuais, sem correrem o risco de serem descobertas e sofrerem represálias. Essa ideia é completada nos estudos de Suxberger e Pacheco (2019) ao defenderem que o anonimato deve ser percebido como uma das características que mais incentivam a ocorrência dos crimes cibernéticos.

Com base as teorias do crime utilizadas nesta pesquisa e de acordo aos desafios enfrentados pelas autoridades de Angola no combate a este fenómeno global, é fundamental que o governo, investigadores, particularmente na cidade de Luanda, instituições privadas e a população percebam e levam-nas em consideração e adaptá-las ao contexto local a fim de ser garantida uma resposta eficaz ao cibercrime.

1.1 Visão geral sobre o conceito do Crime

Com o crescimento tecnológico o conceito de crime tende a evoluir com a sociedade e na opinião de Machado (2008), desde os tempos mais remotos o crime tem sido objeto de reflexão e especulação, apesar de que só a partir do século XIX passou a ser analisado com abordagens científica.

A análise do conceito de crime é um processo complexo que envolve a consideração de múltiplos elementos e perspetivas que por vezes vão para além do que é tido como plasmado. Algumas definições sobre o crime são enunciadas nesta investigação e convergem no aspeto material, analítico e legal. Assim, é necessário que se adote uma abordagem que não olha apenas para as normas legais, mas, também, que tenha em consideração questões de fórum social, cultural e político que são fundamentais na definição, aplicabilidade e a promoção de políticas criminais que contribuem para a segurança e a justiça. (Caiúve, 2020)

No entender de Fernandes e Fernandes (2002, p. 17) “o crime é uma realidade variável, portanto, relativo no tempo, no contexto e no espaço dos aspetos socioculturais”.

Anthony Giddens (2008) diz-nos que

> o crime refere apenas à conduta inconformista que viola uma lei e que para o seu entendimento existem duas (2) áreas relacionadas, mas distintas, que estão envolvidas no estudo do crime e do desvio: a criminologia (trata das

> condutas comportamentais sancionadas pela lei) e a sociologia do desvio (interessa-se pela pesquisa criminológica e também a conduta fora do âmbito do direito penal). (pp. 205-206)

Todavia, Mocinho (2023), defende que a definição formal do crime está relacionada com a ideia de que um ato só pode ser considerado criminoso caso exista uma lei penal que o defina como tal. Apesar disso, o autor defende que tecnicamente o conceito de crime pode ser analisado tendo em apreciação três (3) aspetos: material, legal e analítico.

Rostirolla et al. (2021) define o crime com base ao critério legal, como qualquer conduta que colida contra a norma penal, considerando todo ato humano proibido pela lei penal. No critério material os autores entendem tratar-se de toda a ação ou omissão que fere um bem jurídico penalmente tutelado. Por fim, sob o ponto de vista do critério analítico analisam os elementos principais do crime de forma homogénea. Qualquer conduta que colida contra a norma penal, considerando todo ato humano proibido pela lei penal. No critério material os autores entendem tratar-se de toda a ação ou omissão que fere um bem jurídico penalmente tutelado. Por fim, sob o ponto de vista do critério analítico analisam os elementos principais do crime de forma homogénea.

No entender de Mocinho (2023)

> o conceito legal de crime está focado na análise da norma penal e na sua aplicação prática. O conceito material está relacionado à ideia de que um ato só pode ser considerado criminoso se tiver causado um dano ou prejuízo a algum bem jurídico protegido pelo ordenamento jurídico. O conceito analítico concentra-se em três elementos fundamentais: a conduta, a tipicidade e a ilicitude. De acordo com essa abordagem, para que uma conduta seja considerada crime […]. (pp. 4-5)

O código penal angolano, defende no art.º 12.º, nos n.ºs 1.º[1], 2.º[2] e 3.º[3] que para um indivíduo ser condenado por um crime, é necessário que tenha agido de forma voluntária, conscientemente e com a intenção de cometer o crime.

Para esta pesquisa, adota-se a definição de Mocinho (2023), pois, além de abordar os critérios comuns, ela também analisa o crime com base na existência prévia de uma lei que o tipifica. Assim, compreende-se que, para que um ato seja considerado crime, é fundamental que a conduta do agente seja avaliada quanto à sua tipicidade, culpabilidade e punibilidade, e, acima de tudo, esteja em consonância com as normas, críticas e o funcionalismo da teoria geral do crime, incluindo suas diferentes correntes teóricas.

1.2 Noções sobre o cibercrime

Tentar reduzir esta nova realidade criminal a um único conceito é tarefa árdua, pois a nova era digital trouxe avanços tecnológicos significativos, mas também uma nova realidade para a prática criminosa: o cibercrime. Essa nova realidade refere-se a atividades ilícitas normalmente realizadas no espaço virtual, que vão desde o roubo de dados pessoais até ataques complexos contra as infraestruturas críticas e representando um enorme desafio para a segurança global.

A evolução tecnológica facilita e melhora a qualidade de vida, mas também traz prejuízos. O processo da globalização e a evolução das TIC muito têm contribuído para a diminuição da distância na comunicação entre as pessoas e instituições através da utilização de e-mails, redes sociais e diversas ferramentas tecnológicas que têm dinamizado o uso dos serviços da internet e a comunicação mundial (Machado, 2017).

Nesta perspetiva, Conceição (2023) defende que a rápida evolução tecnológica cria um ambiente desafiador, obrigando a perseverantes atualizações nas medidas de segurança e a necessidade de respostas coordenadas de modo a serem enfrentadas as ameaças cibernéticas que no entender de Santos et al. (2008) diz respeito a vantagem ilícita obtida através do uso das novas tecnologias, no ciberespaço, podendo manifestar-se relativamente aos seus conteúdos, violação de dados

[1] Age com dolo, sob a forma de intenção, quem, representando um facto que preenche um tipo de crime, actuar com intenção de o praticar.

[2] Age com dolo, sob a forma de dolo necessário, quem representar a realização de um facto que preenche um tipo de crime como consequência necessária da sua conduta.

[3] Age com dolo, sob a forma de dolo eventual, quem representar a realização de um facto que preenche um tipo de crime como consequência possível da sua conduta e, apesar disso, actuar conformando-se com aquela realização.

pessoais e confidenciais, burla de telecomunicações, falsidade informática, acesso ilegítimo a SI e a sabotagem.

No entendimento de Almeida (2014) nos cibercrimes o objeto da ação é um computador ou qualquer outro equipamento derivado da tecnologia que serve como meio para o seu cometimento. O autor justifica que nos cibercrimes a não existência da utilização de um destes equipamentos não preenche os elementos típicos deste crime e considerando os dispositivos eletrónicos o elemento-chave neste tipo de criminalidade.

Maia et al. (2016) entendem que inicialmente o conceito de cibercrime era reduzido aos crimes exclusivamente cometidos com recurso a dispositivos informáticos como o computador, redes de computadores ou outros meios de acesso, traduzindo-se deste modo aos ataques contra a disponibilidade, integridade e confidencialidade dos SI e dos recursos de *hardware*. Face à transnacionalidade destes crimes e a sua evolução, Santos (2015) argumenta que ele inclui as infrações tradicionais (fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (distribuição de material pedo-pornográfico e incitamento ao ódio racial) e crimes exclusivamente ligados a computadores e sistemas informáticos (ataques contra os sistemas informáticos, recusa de serviço e proliferação de software malicioso).

Machado (2017) entende que

> os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a intercetação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e discriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros. (p. 15)

No entender da Associação Portuguesa de Apoio à Vítima (APAV, 2021) a crescente utilização da Internet e das TIC deu lugar ao surgimento de novos crimes de natureza informática que transcendem aos ataques contra a disponibilidade, integridade e confidencialidade dos sistemas informáticos, surgindo deste modo conceitos como o crime eletrónico, e-crime, crime digital e o cibercrime.

Para Zalana (2016) o cibercrime é o resultado da interconexão intrínseca à sociedade digital, onde informações valiosas e sistemas críticos são disponibilizados *online* e, estando assim suscetíveis a ataques, englobando diversas formas de atividades

maliciosas, que no entender de Cambundo (2021) podem ser o *phishing*, *ransomware*, ataques a SI e fraudes *online*, e que normalmente são praticados por *crackers*[4] individuais, grupos criminosos organizados ou entidades estatais com objetivos variados, tais como ganhos financeiros ilícitos, espionagem cibernética e motivações ideológicas.

Não existe consenso quanto à expressão utilizada para denominar este tipo de criminalidade pois, a expressão cibercrime por vezes é tratada por crime informático ou crime tecnológico (Santos, 2015). A respeito, a Agência Especializada da Organização das Nações Unidas sobre Drogas e Crime (UNODC, 2024) defende que apesar de não existir uma definição clara sobre o cibercrime, considera mais adequado incluir neste conceito não tanto um tipo de atos, mas um conjunto de atos ou condutas que podem ser organizados em categorias com base no objeto do crime ou no *modus operandi*.

O ordenamento jurídico angolano ainda não possui uma lei contra os cibercrimes e a mais próxima definição que se encontra está na Lei nº 7/17, lei de proteção das redes e sistemas informáticos, de 16 de fevereiro, no Art.º 4.º, alínea g), definindo crimes informáticos como “aqueles cometidos com recurso aos sistemas eletrónicos e as novas tecnologias de informação e de comunicação”.

Caiúve (2020, p. 93) considera que o cibercrime é “o ato de usar um computador para obter ou alterar dados eletrónicos ou para possibilitar a utilização ilegal de um computador ou sistema, conseguindo uma transferência não consentida de ativos patrimoniais de outrem”.

Na visão de Pereira (2022, p. 17) “o cibercrime ocorre no ciberespaço o qual as ações são praticadas com recurso à internet, onde se incluem os crimes informáticos, ou seja, aqueles praticados contra os sistemas informáticos, os dados e as informações alojados nos sistemas de informação”.

Com a crescente utilização dos meios tecnológicos e a conetividade a internet trouxe benefícios no acesso aos serviços públicos, maiores transações comerciais e maior tráfego de comunicações entre as pessoas. Contudo, também aumenta a incidência no cometimento dos cibercrimes na cidade de Luanda que variam desde o roubo de

4 Termo usado para designar alguém com conhecimentos avançados de informática, mas com intenções maliciosas que podem incluir a invasão de sistemas de segurança, roubo de informações, causar danos, obter ganhos ilícitos ou simplesmente a prática da pirataria informática.

identidade, ataques a infraestruturas tecnológicas, fraudes financeiras e clonagem de cartões, representando deste modo uma ameaça a segurança cibernética.

A escolha da definição de cibercrime, com base aos autores referenciados, é fundamental pois ajusta na abordagem e na análise dos resultados da temática em estudo. Assim, para a pesquisa em causa a definição de cibercrime adotada é a de Pereira (2022) pois preenche os elementos típicos dos cibercrimes, nomeadamente: o espaço, o recurso a internet e os dispositivos eletrónicos. Para além disso, a definição reflete a realidade e os desafios vivenciados diariamente na cidade de Luanda desde o ponto de vista económico, social, tecnológico e político.

Sendo a cidade de Luanda o maior centro económico, político, social, tecnológico, jurídico e académico de Angola, entender e instruir-se sobre o emergente fenómeno do cibercrime é crucial para proteger não só a cidade, mas também ser uma barreira contra os cibercrimes para todo o país.

1.3 Conceito de Ciberespaço

Num mundo cada vez mais globalizado e dependente da tecnologia surgem constantes desafios ligados com a nova ordem geopolítica baseada nos conceitos de Estado-Nação o que tem permitido a abolição das fronteiras territoriais, a integração dos mercados, a ampliação do potencial nas comunicações e a velocidade no circuito das informações, o que tem levado que as relações sociais deixassem de se prender ao contexto local e aumentassem com as conexões globais. (Bergmann, 2014)

Em 2010, Santos diz-nos que o uso massivo da internet e o consequente aumento do número de dispositivos eletrónicos transformou a dinâmica funcional do mundo e tem criado oportunidades de trabalho e ao mesmo tempo ameaças que afetam a segurança, a privacidade coletiva e singular, e as infraestruturas tecnológicas, mas, no entanto, é fundamental procurar-se entender o ciberespaço, seu conceito e as suas características.

É recorrente a confusão concetual entre a telemática e o ciberespaço, sendo a telemática referir-se as comunicações a distância, via informática, ao passo que o ciberespaço se refere ao ambiente virtual que utiliza os dispositivos de comunicação para o estabelecimento de relações virtuais, criando deste modo um novo paradigma (Gontijo et al., 2016). O ciberespaço ajuda no crescimento e desenvolvimento de qualquer país nas mais variadas esferas da sociedade e facilita o provimento de serviços de uma forma mais célere e tornando-a num novo espaço para o

desenvolvimento de tarefas que anteriormente só eram possível fisicamente. (Zalana, 2016)

O termo ciberespaço surgiu a partir do livro de ficção científica, Neuromancer, escrito em 1984, por William Gibson, no qual o autor retrata de uma realidade que se constitui por um conjunto de tecnologias enraizadas de tal forma na vida em sociedade que lhe modifica as estruturas e princípios, transformando o próprio homem como objeto de uma realidade virtual que o conduz e determina (Gontijo, Mendes, Viggiano, & Paixão, 2016).

Lévy (2010) diz-nos que

> ciberespaço é um espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização tendo a vocação de colocar em sinergia todos estes dispositivos, tornando-o deste modo no principal canal de comunicação e suporte da humanidade. (pp. 92-93)

Aparício (2017) defende que

> o ciberespaço, tal como é hoje percecionado, representa uma evolução, melhoria e em alguns casos substituição, no que diz respeito ao processo comunicacional em geral e a transmissão de informação, em particular, desde cartas, livros, ou qualquer outro tipo de documentação que, outrora, era armazenada em caixas de arquivo colocadas, muitas vezes, em depósitos de armazenagem, de difícil acesso e consulta é hoje guardada noutro tipo de caixas, de natureza virtual (e já não física), dotadas de enormes capacidades de armazenamento e grande facilidade de acesso. (p. 33)

A respeito, Cleyson (2021) entede que o ciberespaço é o espaço, não físico, composto por redes de computador, principalmente a internet, onde as pessoas podem manter a comunicação de diferentes maneiras: através de mensagens eletrónicas, grupos de discussão e videoconferência.

Para a caracterização do ciberespaço deve-se ter em conta quatro (4) elementos com os quais se pode estabelecer o paralelismo para o mundo físico sobre a ideia de espaço: local (saber onde está algo em relação a nós), distância (o quão longe está algo), tamanho (questões associadas a dimensões) e a rota (associado a questões de navegação). (Bryant, 2016)

O espaço deixou de cingir-se somente ao território geográfico ou as instituições do Estado, passando a aglomerar também um espaço invisível, o ciberespaço, no qual se manifestam a diversidade da divergência humana e se alteram as qualidades do ser, bem como os modos de fazer sociedade. (Velloso, 2018)

Criar um território significa apropriar-se dele (material e simbolicamente) das suas variadas dimensões, procurando o Estado e as suas instituições mantê-lo como forma de poder e controle (Lemos, 2019). A projeção do tempo para a rede geograficamente localizada no ciberespaço renuncia às características tradicionais do território de um Estado, que derivam pela crescente interdependência resultante da globalização e velocidade comunicacional dos fluxos de informação que cruzam todas as fronteiras terrestres em tempo real sem a possibilidade de filtrar todo o volume informativo no ciberespaço, constituindo-se num facto perturbador. (Fernandes et al., 2012)

O ordenamento jurídico angolano, define o ciberespaço na Lei nº 7/17, lei de proteção das redes e sistemas informáticos, de 16 de fevereiro, no Artigo (Art.º) 4.º, alínea f, como “o conjunto dos sistemas tecnológicos e infraestruturas de redes telemáticas, bem como do conjunto de informações e serviços de *internet*”.

A rapidez com que o ciberespaço evolui exige um desafio constante sobre a perceção e a compreensão de suas implicações sociais, éticas e políticas. No entender de Machado (2015) o ciberespaço é um conceito que transcende as fronteiras físicas, permitindo a comunicação e a transferência de informações em escala global, tendo se tornado um palco de revolução de informações onde somos confrontados com questões complexas que vão desde a cibersegurança, a privacidade online, a influência das redes sociais e a dinâmica da economia digital. Morais (2022) defende que na era da revolução tecnológica o ciberespaço tornou-se sinónimo de poder e não apenas um ambiente tecnológico, o que representa uma imersão nas complexidades do ciberespaço através da exploração das suas origens e ramificações na sociedade contemporânea, e na medida que se desvendam os segredos que tecem essa teia digital surgem novos desafios e a infinidade de se alcançar o fim deste espaço.

Para esta pesquisa, o conceito operacional de ciberespaço escolhido é o de Morais (2022) pois analisa o ciberespaço como uma revolução tecnológica no espaço virtual onde frequentemente são cometidos crimes transnacionais que muitas das vezes dificultam a aplicação da lei e a cooperação internacional.

Ao analisar o ciberespaço como uma área criminal transnacional, é essencial ser adotada uma abordagem colaborativa entre Estados, empresas públicas e privadas, órgãos de justiça, organizações internacionais e outros atores. O ciberespaço representa um ambiente propício à inovação e ao desenvolvimento tecnológico, e a sua proteção tornou-se um símbolo de poder. Por isso, o estudo deste tema é crucial para entender o cenário atual dos cibercrimes denunciados na cidade de Luanda, além de permitir o aproveitamento do avanço tecnológico, adaptando-o às necessidades locais e impulsionando a diversificação da economia, a atração de investimentos, o empreendedorismo digital, bem como a melhoria no acesso a recursos educacionais e aos serviços de saúde.

1.4 Tipos de Cibercrimes

A revolução digital do século XXI transformou a maneira como interagimos, nos mais variados campos do convívio social, dando origem a uma face obscura para o cometimento de crimes tecnológicos, chamados cibercrime, em função duma maior interligação dos nós das redes informáticas com recurso a técnicas complexas e sofisticadas. Face a existência de múltiplas condutas com caraterísticas de cibercrimes, existe a necessidade de os classificar em função à sua tipologia.

Os ataques de cibercrimes têm diversos objetivos, visando diferentes alvos e usando diferentes técnicas. Qualquer serviço, computador ou rede que esteja conectado à *internet*, pode ser alvo de um ataque cibernético, assim como qualquer computador com acesso a internet pode participar de um ataque cibernético (Martins, 2015).

Segundo Almeida (2015) nos cibercrimes os atacantes costumam usar técnicas com vista a serem encontradas vulnerabilidades que possam ser exploradas e assim concretizarem os seus intentos. Os motivos que podem levar ao cometimento desses ataques são variados e contemplam a simples diversão ou a realização intencional de ações criminosas de modo a demonstrar o seu poder, prestígio, motivações financeiras, motivações ideológicas e motivações comerciais.

Os cibercrimes podem constituir uma ameaça a qualquer sistema computacional em função das vulnerabilidades encontradas e podendo estas serem ataques do tipo

passivo ou ativo. Os objetivos dos ataques passivos visam a monitorização da transmissão de dados para obter-se informações sem que exista a danificação dos seus recursos. Ao contrário destes, os ataques ativos alteram e criam um fluxo de dados falsos com recurso ao disfarce, repetição, modificação de mensagens e negação de serviços e que por norma são difíceis de serem impedidos por conta da grande variedade de vulnerabilidades de *hardware* e de *software* (Lento, 2016).

No entender de Fonseca (2021), estes não podem ser vistos apenas como crimes que ocorrem na internet, mas também aos crimes que poderão permanecer sem a existência dela.

Por se tratar de um crime multifacético e de difícil definição, o cibercrime apresenta diversas formas de manifestação que desafiam as estruturas tradicionais de segurança e exigem abordagens inovadoras, adaptadas à realidade atual. Entre os tipos mais comuns, destacam-se a exploração de vulnerabilidades, ataques de engenharia social (ES), *malware*, *phishing*, fraude de identidade, clonagem de cartões/*skimming*, transferências ilícitas, *ransomware* e ciberespionagem. Neste ponto, serão abordados com atenção algumas manifestações dos cibercrimes bem como as suas particularidades. Para além disso, procuramos explorar as motivações por trás de cada tipo de ataque bem como as decisões tomadas para a sua contraposição com vista à proteção da sociedade e que por vezes podem colidir com questões de privacidade e liberdades individuais.

1.4.1 Exploração de vulnerabilidades

A propagação e o desenvolvimento tecnológico presenciados no século XXI têm proporcionado ameaças sem fronteiras, com cibercriminosos que continuamente buscam encontrar vulnerabilidades para explorar os sistemas de defesa cibernética de diversos países, organizações e indivíduos (Martins, 2015). Segundo Isoni e Vidotti (2015), o perfil do atacante pode ser descrito por dois padrões: atacantes internos (originários da própria organização, empresa ou instituição) e atacantes externos (geralmente provenientes da Internet). Estes últimos realizam ataques baseados em padrões previamente definidos e sequenciais, com o objetivo de rastrear a rede ou o computador-alvo e identificar vulnerabilidades específicas, criando assim uma base de dados contendo endereços IP que podem ser atacados a qualquer momento.

Segundo Tanenbaum (2015), a exploração destas vulnerabilidades tem como objetivo obter benefícios, chamar a atenção ou até mesmo prejudicar alguém ou uma

organização. Para isso, os atacantes invadem sistemas de informação (SI) em busca de informações, efetuam alterações, roubam senhas, apagam arquivos, entre outras ações. Estes crimes são, na sua maioria, perpetrados por *hackers*[5], *crackers*, *script kiddies*[6] e estudantes[7].

A vulnerabilidade é um campo de conhecimento obrigatório em segurança da informação, por se tratar do elemento muito explorado em ataques cibernéticos, pois trata-se de um ponto fraco que resulta em um incidente de segurança (Nakamura, 2016). Essa ideia é completada nos estudos de Costa (2017) ao determinar que as mesmas são um ponto fraco existente num sistema ou numa organização e que pode permitir a concretização de um ataque físico ou virtual, sendo que as mais sonantes vulnerabilidades tendem a acontecer em plataformas *web*.

Para Kim e Solomon (2018) as vulnerabilidades são fraquezas que permitem que as ameaças sejam percebidas e que podem danificar ou comprometer um sistema com a criação de um potencial risco suscetível de provocar um evento negativo. Contudo, os autores entendem que a solução para a proteção dos ativos contra esses riscos passa pela eliminação das vulnerabilidades, o mais rapidamente possível, devendo-se, no entanto, ponderar-se cuidadosamente se o custo de proteger alguns ativos não são maiores que os valores dos próprios ativos.

No entender de Piekarski (2018) as vulnerabilidades existem em todas as vertentes desde a humano, *hardware*, protocolos, sistemas operativos (SO), aplicações, redes e falhas inerentes ao próprio processo de fabricação tecnológico que ao serem exploradas provocam danos singulares ou coletivas. No tocante às vulnerabilidades tecnológicas virtuais, Nakamura (2016) entende que por regra o ataque é feito com recurso aos *exploits* (*softwares* que utilizam dados ou códigos próprios que exploram as fraquezas de ativos), podendo estes serem dos mais variados tipos, desde *exploits* para serviços e aplicações remotas, aplicações *web*, escalada de privilégios, negação de serviço e *shellcode*.

A vulnerabilidade pode ocorrer em três (3) fases distintas, nomeadamente: a partir do momento em que se esteja a desenhar o sistema, antes de iniciar-se o processo da

5 Com conhecimentos de programação, SI, falhas de segurança, desenvolvem técnicas e programas de invasão, compartilham conhecimentos e não corrompem dados intencionalmente.
6 Com poucas habilidades e que por sorte encontram um SI sem proteção e fazem a intrusão através de falhas conhecidas.
7 Autor de ataques com o objetivo de divertir-se e vasculhar mensagens de correio eletrónico de outrem.

sua implementação; quando se introduz um algoritmo menos adequado durante o processo de programação de um determinado sistema. Por isso, é denominada de vulnerabilidade de implementação, pela utilização incorreta de um sistema com a introdução de palavras-passe fracas ou pela configuração de comunicações sem o suporte de canais seguros, deixando deste modo a possibilidade de existência do risco face a este tipo de ameaças. (Ferreira, 2022)

As ameaças podem ser feitas a partir do ambiente interno ou a partir do ambiente externo de uma organização, podendo elas serem intencionais ou acidentais e praticadas por uma ou mais pessoas ou por uma organização, devendo, no entanto, serem identificadas e classificadas para uma melhor abordagem. Identificá-las e encontrar as devidas respostas não é um processo que seja fácil, pois, por vezes pode ser muito caro ou demorado eliminar a ameaça (Jorge, 2021). Na impossibilidade de eliminação das ameaças, Almeida (2019) entende que devem ser protegidas as informações contra as vulnerabilidades, permitindo que na persistência da ameaça não se consiga fazer a sua exploração.

Em 2022, Madi e Castro descrevem que para cada vulnerabilidade encontrada a sua exploração requer o uso de métodos, técnicas e ferramentas próprios usadas pelos cibercriminosos. Como se demonstra por Franzese (2023) se a vulnerabilidade for física e que possibilita o fácil acesso ao Centro de Processamento de Dados (CPD), o cibercriminoso pode a cessar fisicamente ao servidor e roubá-lo por inteiro. A fim de prevenir e evitar estas vulnerabilidades, Melo (2023) entende que um ataque só acontece porque as vulnerabilidades são exploradas pelos atacantes, existindo para tal a necessidade da eliminação de todos os pontos fracos do ambiente envolvente, nos mais variados níveis.

Embora a expansão da infraestrutura tecnológica na cidade de Luanda seja um fenómeno positivo para o crescimento e desenvolvimento da sociedade, também traz problemas relacionados à vulnerabilidade. A vulnerabilidade refere-se à identificação, análise e mitigação de possíveis pontos fracos dos sistemas de informação (SI), das infraestruturas físicas e dos erros humanos que, quando explorados por agentes maliciosos, podem comprometer o funcionamento de uma organização. Estudar, entender e abordar questões relacionadas com a vulnerabilidade, diante da rápida ascensão tecnológica na cidade de Luanda, não deve ser visto como uma medida reativa, mas sim proativa, capaz de auxiliar na proteção das infraestruturas tecnológicas contra os cibercrimes, que, por sua natureza, geram consequências

devastadoras para diversos setores da sociedade. Para além disso, estudar as vulnerabilidades orienta as estruturas governamentais da cidade de Luanda, a adoção de regulamentos e normas que visam a proteção de informações, a garantia da privacidade dos usuários e o fortalecimento da resiliência cibernética e, assim, estar mais bem provida com capacidades de resposta e recuperação, pois planos bem elaborados minimizam o impacto dos ataques e garantem a continuidade dos serviços essenciais.

Com base nas definições de vulnerabilidade utilizadas nesta pesquisa, adota-se a definição de Costa (2017), pois o autor não se limita a analisar a vulnerabilidade exclusivamente no mundo virtual, mas também a relaciona ao ambiente físico, reconhecendo que, muitas vezes, os ataques ocorrem por meio de sabotagens em instalações físicas devido a falhas conhecidas. Além disso, o autor destaca que a vulnerabilidade também pode resultar de negligência humana.

1.4.2 Ataques de Engenharia Social

A prática que visa obter informações confidenciais por meio da manipulação da vítima, comumente denominada Engenharia Social (ES), é antiga, mas foi trazida para a era digital com a proliferação da tecnologia, tornando a informação uma moeda valiosa. A ES progrediu rapidamente, acompanhando o avanço das tecnologias e das ameaças à sua segurança. Do ponto de vista da segurança da informação e cibernética, a ES atingiu o seu auge na segunda metade do século XX (Vilaça & Araújo, 2016). Esta evolução é também defendida por Moreira (2019) ao afirmar que a ES, dentro da Segurança da Informação, ganhou força no início da década de 1990, na forma de atuação do então famoso hacker, Kevin Mitnick[8].

A lendária história do cavalo de Tróia, que mais tarde inspirou a criação do vírus informático homônimo, é considerada das mais antigas ocorrências documentadas de Engenharia Social (ES). Diferente de outras ameaças à segurança das Tecnologias de Informação e Comunicação (TIC), a ES busca explorar fragilidades humanas (Tavares, 2017). Apesar da divergência existente, quando ao período do surgimento da ES, no entender de Gonçalves, Ogawa, e Lima (2022), elas são simples linhas de código e *firewalls* que se infiltram nos elementos de qualquer sistema, aproveitando as vulnerabilidades humanas de modo a contornar as mais avançadas barreiras

8 Programador e *hacker* norte-americano, trabalhou como gerente de uma empresa de segurança tendo sido descoberto mundialmente a partir da década de 1990.

tecnológicas em busca do acesso não autorizado com vista à obtenção de informações confidenciais de sistemas corporativos e dados sensíveis.

Alves (2010) refere que

> Os ataques de ES podem ser divididos em dois grupos: Os ataques diretos, caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, fax e pessoalmente. Este exige do engenheiro social, um planeamento antecipado e bem detalhado, além de um segundo na eventualidade do primeiro não der certo, para além de muita criatividade e articulação para que o plano seja bem-sucedido. Quanto aos ataques indiretos, são caraterizados pela utilização de *software* para proceder a invasão, como o cavalo de Troia ou através de *sites* e *e-mails* falsos com vista a obtenção de informações desejadas. (p. 15)

Mitnick e Simon (2003) afirmam que, apesar dos altos investimentos em tecnologia de segurança, das melhores ações de formação e da contratação das principais empresas de segurança, ainda persistem as vulnerabilidades humanas, que facilitam as invasões. No entender dos autores durante o processo da criação das políticas para a manutenção da segurança tecnológica o ser humano é tido como o elemento mais fraco, uma vez que a inocência, a malícia (*inside threat*) e a ignorância humana pode contribuir para a ruína da segurança de todo o sistema.

Em 2012, Fontes afirma que, diante da crescente evolução tecnológica, busca-se cada vez mais melhorar a segurança da informação, tanto em relação a pessoas, quanto a *software* e *hardware*, por meio de técnicas sofisticadas de criptografia, com o uso de algoritmos matemáticos complexos. Desta forma, quando um invasor decide realizar um ataque, ele encontra barreiras suficientemente fortes, que o levam a utilizar meios mais simples, como a engenharia social. Nesse sentido, Machado (2014, p. 119) observa que “quando alguém deseja invadir ou a cessar informações de uma organização, é muito mais fácil recorrer à engenharia social”. A cooperação dos usuários é essencial para a eficácia da segurança, pois tem um impacto sobre a confidencialidade, a integridade e a disponibilidade da informação, e por conta disso os usuários devem manter a confidencialidade da senha (evitando o registo da mesma

em papéis), utilizar senhas de qualidade e não compartilhar senhas para que não seja comprometida a segurança da informação. (Lyra, 2015)

Na busca incessante de informações, na maior parte sigilosas, surgem e erguem-se os *cracks* e os engenheiros sociais que se valem das suas técnicas de persuasão para obterem acesso a informações valiosas, pois por norma essas pessoas possuem grande capacidade de ludibriarem as outras devido a sua facilidade comunicativa e ao seu poder persuasivo. (Velloso, 2018)

Diferentemente dos sistemas de uma empresa, no entender de Meier (2018) o comportamento humano não é homogeneamente controlável, pois cada um possui a sua maneira de ser e agir face as abordagens dos cibercriminosos. Assim, cada pessoa possui características singulares que podem ser exploradas para a sua manipulação. Contudo, para a construção de um ataque são combinadas táticas que permitem o acesso à informação não disponível a todos mediante a exploração das vulnerabilidades relacionadas com as suas características comportamentais. (Silva, 2019)

Gonçalves (2019) diz-nos que

> qualquer pessoa dentro de uma organização pode ser alva de ES, independentemente da sua posição na hierarquia da organização, isto porque as pessoas acabam por ser facilmente identificadas através dos média, em websites e até em redes sociais. Deste modo, muitos dos e-mails de colaboradores e diretores são descobertos através de uma simples pesquisa no google. (p. 13)

A ES é um processo utilizado por cibercriminosos para manipular pessoas a realizarem, involuntariamente, ações que as tornam vulneráveis. Esses criminosos exploram a falta de conscientização e o conhecimento das vítimas, provocando danos à confidencialidade, integridade e disponibilidade de seus recursos ou ativos, sejam eles pessoais ou organizacionais (Gonçalves, 2019). A ES é muito utilizada em matéria de segurança da informação, na medida que os invasores tendem a explorar as fraquezas humanas e contornarem as medidas de segurança tecnologicamente implementadas, através de ligações telefónicas, e-mails, mensagens de texto, redes sociais ou pessoalmente, com o objetivo de instigarem as pessoas a divulgarem

senhas, informações confidenciais ou a realizarem ações prejudiciais à segurança. (Cleyson, 2021)

No entender de Ariza, Azambuja, Nobre, e Granville (2022, p. 3) “a ES refere-se à exploração do comportamento humano no tocante ao uso dos sistemas de informações para a obtenção de dados e informações relevantes de potenciais alvos”. Outro aspecto destacado pelo autor é que os criminosos de Engenharia Social (ES) tiram proveito de uma relação de confiança existente com a vítima, manipulando-a ou influenciando-a psicologicamente para obter uma posição vantajosa. O objetivo é acessar informações confidenciais, realizar ações específicas e obter acesso a sistemas e recursos protegidos. Gonçalves et al. (2022, p. 10) dizem-nos que “ES é uma arte utilizada por pessoas mal-intencionadas para realizar ataques a segurança da informação, como roubos e sequestro, com objetivo de causar danos a terceiros e obter alguma vantagem sobre empresas ou usuários de TIC”.

Várias são as definições que podem ser utilizadas para se definir a ES, mas, para esta pesquisa opta-se pela definição utilizada por Gonçalves (2019) pois congrega os elementos primordiais que contribuem para o cometimento da ES, como a existência de um ato, o cibercriminoso, que por regra nutre a confiança da pessoa manipulada e que possui as informações desejadas que quando obtidas podem provocar sérios danos aos recursos lógicos e físicos de uma determinada organização.

É de suma importância o estudo da ES para a análise que se faz sobre o cenário atual dos cibercrimes na cidade de Luanda, pois pela crescente conectividade, digitalização dos serviços e o crescimento da população, tornam-se alvos atrativos para crimes desta natureza, uma vez que existe pouca literacia cibernética no seio das organizações e a população o que pode facilitar a exploração das fraquezas humanas.

1.4.3 *Malware*

A história do *malware* está inteiramente ligada com à evolução da computação e da propagação do mundo digital. O termo é um neologismo que tem à sua origem a partir das palavras *malicious* (malicioso) e *software*, tratando-se de um programa de computador malicioso concebido para causar prejuízos em sistemas digitais, como a exploração de vulnerabilidades, realização de atividades indesejadas em redes e dispositivos digitais (Afonso, 2015).

Segundo Nakamura (2016), o termo *malware* engloba uma ampla variedade de ameaças que podem incluir vírus, *worms*, *trojans*, *spyware*, *adware*, *bots*, *backdoors*,

sendo que a cada método distinto possui à sua forma de infiltração e impactos prejudiciais.

No entender de Tavares (2016) existem diferentes tipos de *malware*, e cada possuindo distintas características que causam impactos e danos, e a sua compreensão é crucial para a proteção de dados e SI. Essa ideia é complementada por Santos (2017) ao referir que para fazer-se análise e abordagem sobre o *malware*, há que levar-se em consideração as diferentes variantes que a mesma apresenta e que nem sempre é consensual a sua definição, pois algumas são multidisciplinares, como o caso de um *keylogger* que é projetado para recolher informações de autenticação, mas que também pode atuar como um *worm* que se propaga e ao mesmo tempo envia emails de *spam*. Contudo, Batistela (2018) reforça que a propagação do vírus é feita de máquina em máquina, deixando novas infeções, à medida que o usuário os enviar para outros, com ficheiros executáveis infetados, dispositivos de armazenamento, redes de computadores, e-mails ou outros meios de transmissão de dados e gerando um ambiente cíclico, reiniciado a cada envio, e procurando infetar o maior número de máquinas.

Embora o termo vírus informático tenha sido utilizado de forma genérica, na sua génese, atualmente existem distinções em função as suas características e os seus objetivos específicos: vírus de Arquivo, vírus de *boot*, vírus de e-mail, vírus residentes, vírus metamórficos, entre outros (Batista, 2018). No entanto, Reis (2018) entende que os *worms* foram criados apenas para se multiplicar e perturbar a largura de banda, mas sem alterar funcionalidades dos sistemas, contrariamente do que hoje acontece ao fazerem o transporte de *payload*[9] que espalham *ransomwares* que infetam os sistemas por onde passam.

Em termos de segurança informática, Costa (2017) entende que os *worms* referem-se a um tipo de *malware* que possui a capacidade de propagação autónoma e consegue enviar cópias completas de si para outros computadores podendo os hospedeiros moverem-se por conta própria, procurando explorar vulnerabilidades nos sistemas e aplicativos através de redes de computadores, e-mails ou outros meios de comunicação com vista a causar danos e a extração de informações valiosas como a lista de contactos de e-mails e enviar cópias de si para os computadores alvos.

[9] Código desenhado para realizar ações maliciosas

Apesar da existência de programas de antivírus, sistemas de deteção e prevenção de intrusões e *firewalls*, as ameaças oriundas de *malware* ainda são persistentes tanto que muitos SI estão infetados por diferentes tipos de *malware* cada vez mais inteligentes e criteriosos para a recolha de informações através da utilização de algoritmos de inteligência artificial capazes de o camuflar, como se fosse um *software* licenciado. (Kim, 2018)

O crescente aumento do uso de aplicações para acesso aos serviços bancários ou compras *online*, em alguns casos como o único meio de acesso, tem sido acompanhado pela evolução de ataques por *malware*, projetado para o roubo de credenciais de acesso, como o *trojan* bancário Anubis que inclui táticas de *ransomware* e que podem levar o utilizador a perca de toda a informação no seu dispositivo móvel (Silva, 2020). Para tal, Madi e Castro (2022), entendem que em função as capacidades de se auto copiarem e moverem-se entre computadores, os *worms* podem consumir muitos recursos da máquina hospedeira e banda de rede, defendendo a aplicação de medidas de segurança são essenciais para prevenir infeções por *worms* e que devem incluir as atualizações regulares de *software*, *firewalls* e *softwares antimalware*.

Paulino, Schoucair, Junior e Maia (2022) consideram que

> o malware é um software malicioso, como um programa informático, que se instala ocultamente em um sistema de dados, sem o conhecimento ou consentimento do seu proprietário, permitindo o monitoramento e a captura remota de informações e dados recebidos, armazenados e transmitidos pelo dispositivo eletrónico infetado, para extração de dados e obtenção de informações de forma oculta, além de possibilitar a ativação de algumas funcionalidades do equipamento, como microfone, câmera e o acesso à sua geolocalização. (p. 65)

Os programas maliciosos assumem diversas formas e são uma verdadeira ameaça ao mundo digital. A compreensão da origem do *malware* é crucial para contextualizar a sua evolução e a necessidade constante de inovação em segurança cibernética, pois a sua evolução representa um desafio para a manutenção da cibersegurança,

uma vez que os desenvolvedores de *malware* buscam constantemente novas formas de contornar as defesas de segurança (Cleyson, 2021).

O *spyware* é uma terminologia informática usada para descrever o conjunto de programas espiões que monitoram os SI e com capacidades de mudarem o *adware*[10] gerador dos *pop-ups* que recolhem informações, atividades e hábitos dos usuários na internet e que sem o consentimento do utilizador transmitem-nos a uma entidade externa (Mitshashi, 2011). Contudo, Tavares (2017) reforça que estes programas podem ser instalados no computador como trojans, quando o usuário visita sites com códigos maliciosos exploradores de vulnerabilidades no navegador da Web, ou como softwares livres, sem a aprovação do utilizador, sendo o tipo mais comum de informação recolhidas os endereços dos sites visitados, os sites de motores de busca usados, a versão do SO ou os *softwares* usados no computador infetado.

Por norma, este tipo de *software* inclui programas como o sniffer (intercetam senhas), *keyloggers* (registam as teclas pressionadas pelo usuário), *cookies* (que registam as visualizações habituais do utilizador na internet) e os *bugs* web (incorporados em páginas de *web* ou de e-mail e recolhem informações sobre a data/hora de acesso, endereço de *Internet Protocol* (IP) e navegador do SI. (Batista, 2018)

Quanto ao *Adware*, trata-se de uma variante de malware projetado especificamente para apresentar propagandas, muitas vezes de maneira intrusiva e indesejada, e que por regra não prejudicam o computador quando incorporados em programas e serviços, como patrocínios ou ganhos financeiros, por individualidades coletivas ou singulares que se dedicam ao desenvolvimento de programas livres. Quando o seu uso é feito de forma maliciosa abre janelas publicitárias no navegador e que ao serem clicadas direcionam o usuário a sites maliciosos sem que este saiba que esteja a ser alvo de monitoramento. (Mitshashi, 2011)

O *adware* não tem como principal objetivo causar danos ao sistema ou roubar informações confidenciais, mas sim gerar receitas para os criadores por intermédio de exibição de anúncios. (Velloso, 2018)

Os *Bots* (*robots*) são programas automatizados capazes de se propagarem, encontrar e explorar vulnerabilidades ou falhas de segurança na configuração de *software* para instalar pequenos programas designados de *daemons* que funcionam sem o conhecimento do utilizador do sistema (Mauser e Diógenes, 2014). Contudo, os *Bots*

10 Programa de computador que execute e exibe automaticamente uma grande quantidade de anúncios sem a permissão do usuário

podem ser controlados remotamente por intermédio de comandos fornecidos por *hackers* de formas a manipular os sistemas infetados, sem o conhecimento do usuário (Nakamura, 2016). Na opinião de Batista (2018) o atacante ao comunicar-se com o *Bots* instrui-o a desferir ataques a outros sistemas, recolher dados e enviar *spam*.

Por regra, a comunicação entre o invasor e o computador pode ocorrer pela via de canais de *Internet Relay Chat* (IRC), servidores *Web* ou redes de arquitetura *Peer-to-Peer* (P2P) e que ao ser estabelecida a comunicação o invasor envia instruções para que ações maliciosas sejam executadas, como o furto de dados e a infeção do computador, e enviar spam[11]. (Quintão, 2022)

Quanto aos *backdoors*, Nakamura (2016) refere-os como sendo a entrada não autorizada ou secreta sobre um SI, as suas funcionalidades e aos seus programas e que por norma é geralmente criado de forma intencional pelos desenvolvedores, administradores de sistemas ou programadores com o intuito de permitir o acesso ao sistema sem a necessidade de estar sujeito a quaisquer procedimentos de segurança. Apesar dos *Backdoors* serem normalmente utilizados por programadores, para testes, este recurso pode ser explorado por um agente malicioso e garantir o acesso remoto não autorizado a uma máquina e que pode ser inserido como parte de ataques cibernéticos. (Santos, 2017)

Diferentemente das formas já mencionadas, o *trojan* (cavalo de Troia) teve sua inspiração na mitologia grega, em que, durante a Guerra de Troia, tropas inimigas foram infiltradas por meio de uma enorme estátua de cavalo de madeira. No mundo da computação, esse conceito deu origem ao famoso *backdoor Back Office*, criado pelo grupo de *hackers Cult of the Dead Cow*. Trata-se de um *malware* malicioso, propagado a partir da década de 1990, que consiste em um programa aparentemente inofensivo, mas com uma função oculta de *backdoor*, que contorna os mecanismos de autenticação e engana os usuários quanto à sua verdadeira natureza, levando-os a instalá-lo em sistemas operativos (SO) por meio do *download* de protetores de tela, cartões virtuais, álbuns de fotos, jogos, *software*, anexos de e-mails ou websites (Batista, 2018). Uma vez instalado, o cavalo de Troia executa ações prejudiciais, que vão desde o roubo de credenciais, números de cartões de crédito/débito, destruição de dados, danificação do sistema, entres outros, de forma anónima. (Melo R. C., 2023)

11 Mensagens não solicitadas, geralmente enviadas em grandes quantidades, através de meios eletrónicos, como e-mails, mensagens de texto ou mensagens em redes sociais.

Na era da tecnologia digital, em que os cibercrimes são frequentes, cidades como Luanda, onde muitos serviços dependem da conexão digital, experimentam diversos benefícios, mas também expõem sua população e infraestruturas a uma variedade de ameaças cibernéticas. Entre essas ameaças, destaca-se o uso de *malware*, um meio empregado por cibercriminosos para obter informações cruciais, causando danos significativos. Por isso, é essencial compreender o funcionamento dos ataques cibernéticos via *malware*, uma vez que, à medida que aumenta o número de usuários de dispositivos eletrónicos, também crescem os riscos e a eficácia dos ataques com recurso a *malware*, resultando em perdas significativas, muitas podendo levar anos para serem recuperadas. O estudo do *malware* é fundamental para fornecer as informações necessárias para a detenção, precaução, alívio e respostas adequadas contra os ataques do género que acontecem na cidade de Luanda e, assim oferecer aos cidadãos uma maior segurança e um ambiente digital de confiança.

1.4.4 *Ransomware*

A palavra *ransomware* é um neologismo criado a partir da fusão das palavras *ransom* (resgate) e *malware*. Apesar de ser um antigo problema a segurança tecnológica, a sua abordagem surge na década de 1980, com o vírus de *Disk Operating System* (DOS), chamado Casino, que todos os dias 15 de abril, fazia *backup* da *Random Access Memory* (RAM) e o *File Allocation Table* (FAT) e, posteriormente apagava todo o conteúdo do disco duro. Apesar disso, na altura, os usuários não pagavam pela extorsão, mas tinha de participar do jogo, estilo caça-nível, que o casino exibia na tela e pontuar, de formas a recuperar os seus dados. (Alecrim, 2016)

No entender de Oliveira (2016) existem duas (2) formas de atuação do *ransomware* em circulação: a *locker ransomware* (projetado para impedir o acesso à interface do dispositivo) e a *crypto ransomware* (projetado para encontrar e criptografar dados importantes armazenados no computador, tornando-os inacessíveis até o envio da chave de descriptografia).

Em 1989 teve a primeira aparição de um *ransomware* que exigia resgate em dinheiro, conhecido como *PC Cyborg*, que era distribuído por disquete que reescrevia apenas o arquivo de sistema autoexec.bat, ocultava pastas e criptografava os nomes de arquivos na unidade C, ludibriando os usuários sobre a caducidade das suas licenças de *software*, e exigindo uma quantia monetária ($189), para desbloquear os seus arquivos. Apesar disso, esse tipo de *ransomware* enfrentava alguns insucessos pois

o processamento de dados e a criptografia eram feitos de forma simétrica[12] e não assimétrica[13]. (Liska e Gallo, 2017)

Os primeiros ataques de *ransomware* modernos (*Krotten*, *Cryzip* e *MayArchive*) surgiram entre 2005 e 2006, na Rússia, através da utilização da criptografia RSA[14] que bloqueiam dados e sistemas informáticos e exigindo resgate. Por esta altura o *ransomware* já era capaz de compactar arquivos e os sobrescrevia com arquivos compactados com senhas (Brito, 2016). Para além disso, Mello (2021) acrescenta que os mesmos eram enviados como arquivos de texto a informar a vítima que os seus arquivos poderiam ser recuperados mediante o pagamento de uma quantia monetária. O autor argumenta que, embora o *ransomware* tenha sido inicialmente comum na Rússia, a rentabilidade de seus ataques aumentou a sua popularidade e levou à sua proliferação pela Europa, Ásia, América, África e Oceania. Em 2013 um novo tipo de *ransomware* surgiu com arquivos encriptados do SI da vítima, forçando-a ao pagamento do seu resgate. Como consequência das novas características do ransomware, este passou a ser chamado de *cryptolocker*, tendo posteriormente dado origem os *crypto-ransomwares*, também conhecidos como *cryptodefense* ou *cryptorbit*, que passaram a encriptar transações e dados bancários, arquivos *web*, *Office*, vídeos, imagens, scripts, textos e outros arquivos do tipo não binário, com a possibilidade de apagar-se os *backups* existentes. (Morais, 2021)

Definir e classificar o *ransomware* não é fácil, mas na sua maioria agem com base a três princípios essenciais: busca pelo alvo (o *malware* procura arquivos que indiciam conter dados importantes da vítima), a extorsão (nessa fase a vítima perde acesso aos seus dados) e a exibição de mensagem de resgate (mostram a vítima que só voltará a ter o acesso aos seus dados mediante um pagamento). (Oliveira, 2019)

Para Liska e Gallo (2017) *ransomware* é um código malicioso que ao ser executado no computador da vítima faz com que os dados armazenados não sejam acessíveis e em seguida o cibercriminoso exige da vítima o pagamento de resgate de maneiras a reavê-los e voltar a ter acesso ilimitado ao sistema.

Araújo (2019) diz-nos que

[12] Composta por uma chave, usada tanto para criptografar quanto para descriptografar
[13] Composta por duas chaves distintas, sendo uma usada para criptografar e outra para descriptografar
[14] É amplamente utilizado para transmissão segura de dados onde a chave de encriptação é pública e a chave de decriptação é secreta.

> *ransomware* é um tipo de vírus que faz parte de uma classe específica de malware que é utilizada nas chamadas extorsões digitais, pois obriga suas vítimas a pagarem determinado valor em troca do completo controlo de seus dados. Essencialmente, existem duas classes: a Locker (que impede a vítima controlar e aceder o equipamento infetado, praticamente inutilizando-o) e a Crypto (bloqueia o acesso aos dados armazenados no equipamento infetado, utilizando criptografia). (p. 94)

Em 2022, Silva, Souza, e Melo, dizem-nos que o *ransomware* é um tipo de *malware* cuja finalidade é o bloqueio de dados de sistemas, procurando infiltrar-se em redes corporativas, através de e-mails de *phishing*, que ao serem manipulados fazem invasão e o sequestro dos dados, extorquindo as vítimas para recuperarem o acesso ao sistema ou aos arquivos, através do pagamento de resgate, maioritariamente por transferência em moeda eletrónica (*Bitcoins*), por trata-se de um meio de pagamento de difícil rastreio, pois dificilmente se consegue saber para qual conta a transferência se reflete.

Barker, Fisher, Scarfone e Souppaya (2022) entendem que

> *ransomware* é um tipo de *malware* que criptografa os dados de uma organização e exige o pagamento como condição para restaurar o acesso a esses dados. O ransomware também pode ser usado para roubar informações de uma organização e exigir pagamento adicional em troca da não divulgação das informações às autoridades, concorrentes ou ao público. Os ataques de *ransomware* visam os dados ou a infraestrutura crítica da organização, interrompendo ou impedindo as operações e colocando um dilema para a gestão: pagar o resgate e esperar que os invasores mantenham a sua palavra sobre restaurar o acesso e não divulgar os dados, ou não pagar o resgate e tentar restaurar as operações […]. (p. 1)

Para Morais (2021) os ataques de *ransomware* diferem dos outros eventos de segurança cibernética por obterem acesso clandestino as informações e causarem

um impacto imediato nas operações, deixando-as com pouco tempo para amenizarem esse impacto e restaurarem os sistemas. Por isso, Barker et al. (2022) recomendam que as instituições devem treinar os seus funcionários, os técnicos especializados e os gestores sobre a importância da prevenção, antes que ocorram os ataques, seguindo os protocolos internamente elaborados para a redução do sucesso dos ataques de *ransomware* e, assim, ajudar na detenção precoce destes ataques e se conseguir recuperar destes ataques.

Em cenário urbano, como o de Luanda, onde a infraestrutura digital é essencial para o funcionamento diário, a ameaça de *ransomware* representa um risco significativo. A identificação e o estudo desses vetores de infeção são essenciais para a elaboração e desenvolvimento de medidas preventivas destinadas à mitigação de futuras ameaças, bem como para o aprimoramento dos mecanismos de defesa. Este estudo não pode ser subestimado, pois fornece dados que auxiliam na prevenção e na criação de sistemas de defesa robustos, com o objetivo de proteger contra este fenómeno, que cresce gradualmente na cidade de Luanda. Além disso, apoia processos de investigação criminal, científica e inovação no campo da cibersegurança, promovendo o desenvolvimento contínuo nas diversas esferas da sociedade luandense.

1.4.5 *Phishing*

O termo *phishing* provém do neologismo inglês fishing (pesca) e *phreaks* (termo que identificava os primeiros *hackers*) no qual os cibercriminosos enviam links em sites de modos a atraírem vítimas vulneráveis, que podem ser singulares ou coletivas, a revelarem informações confidenciais. (Silva, 2014)

Tavares (2017) diz-nos que

> *Phishing* é derivado da palavra pesca em inglês, e é intencionalmente mal escrita para mostrar a facilidade de confundirmos palavras similares, fazendo uma comparação com a facilidade de confundir um domínio ligeiramente errado. Neste caso, a vítima é o peixe que morde a isca através de e-mails não autênticos, mensagens em redes sociais ou plataformas de mensagens instantâneas e sites falsificados, imitando o verdadeiro, mas geralmente possuindo um nome de domínio ligeiramente diferente. (p. 38)

Os primeiros relatos de ataques informáticos por meio *phishing* remontam da década de 1990, perpetuados por um grupo de *hackers* que buscavam pela obtenção, não convencional, de informações confidenciais, através da criação de falsas contas de utilizador e cartões de crédito, que posteriormente passaram a enviar mensagens aos utilizadores, solicitando atualizações de contas. Como consequência desse ato, conseguiram obter *passwords* e outras informações confidenciais (Neves, 2022).

A Fraude por e-mail, também conhecida como *phishing*, é uma forma de fraude *online* em que os cibercriminosos enviam e-mails falsificados com o objetivo de obterem informações pessoais, financeiras ou confidenciais das vítimas. Por regra, essas mensagens parecem autorizadas e enviadas por empresas, solicitando as vítimas informações (senhas, números de cartão de crédito, dados pessoais, *links* falsificados que redirecionam para sites falsos ou alegar urgência e ameaças) e convencê-las a agirem o mais rápido possível, sem, no entanto, verificarem a autenticidade da mensagem. (Silva et al., 2022)

Para Félix (2022) com a utilização de técnicas de ES, “é possível adquirir informação sensível de forma fraudulenta, como nomes de utilizador e palavras-passe, tentando enganar os utilizadores de websites populares, enviando-lhes por e-mail, ou outros meios, versões falsas de sites a fim de fornecerem as suas credenciais,” (p. 27).

No entender de Ariza et al. (2022) existem duas (2) categorias usadas para a classificação dos ataques de ES: os baseados nos computadores/tecnologias e os de manipulação direta dos indivíduos, sendo enquadrado o *phishing* na primeira categoria pois, apesar do indivíduo ser o meio para se atingir o fim os ataques são feitos com recurso aos meios tecnológicos.

Em 2020, Rodrigues diz-nos que “*phishing* é um tipo de ataque caracterizado pelo uso de ES, como forma de cometer cibercrimes. O propósito destes ataques é conseguir manipular as vítimas, levando-as a fornecer dados pessoais, acessos privilegiados ou informação confidencial aos hackers.” (p. 5)

Na perceção de Dias (2021) o *phishing* é tido como uma tentativa fraudulenta realizada de forma sólida a diversas vítimas para aceder às suas informações pessoais ou financeiras, através de chamadas telefónicas, mensagens de texto ou e-mails, e que por alegada necessidade de verificação de dados, o atacante solicita à vítima às suas credenciais tais como: o utilizador, *password*, número de cartão ou códigos de acesso, entre outros.

Para Sousa (2023) “o phishing é um tipo de ataque de Engenharia Social que tem como principal objetivo enganar a vítima, através de uma mensagem maliciosa, para que esta partilhe informação sensível.” (p. 6)

Com a evolução das formas de prevenção, Goncalves (2023) é de entendimento que os criminosos que usam ataques baseados com o *phishing* também vão sofisticando os seus métodos com o surgimento de novas variações de *phishing*, como o *business* e-mail compromise[15], *spear phishing*[16], *USB phishing*[17], *smishing*[18], *whaling*[19], *Wi-Fi phishing*[20], *NFC phishing*[21] e *QRCode phishing*[22].

Apesar da evolução e a sofisticação das variantes de ataques por *phishing*, no entender de Diniz, Porto e Santos (2014) o e-mail tornou-se na forma mais simples de comunicação e à sua adoção é independe da capacidade de investimento tecnológico. Para os autores, o mais importante no uso do e-mail é o grau de comprometimento da instituição em relação ao meio de comunicação escolhido pelos usuários de modos a se estabelecer a comunicação. Assim sendo, Rodrigues (2020) entende que o ataque por email continua a ser o canal com maior apetência, motivado pelo fato de existir uma maior fluidez na distribuição de mensagens pelo e-mail, entre empresas e os clientes e vice-versa.

Apesar do conhecimento dos danos causados pelos ataques com recurso ao *phishing*, muitos usuários continuam a ser vítimas destes ataques causado por alguma ignorância, desconhecimento das políticas de segurança e sobre as reais consequências danosas. Para além disso, há que se ter em conta das reais capacidades de persuasão dos cibercriminosos, contras às suas vítimas, com vista a obtenção de informação sensíveis, jogando um papel fundamental neste tipo de ataques. (Dias, 2021)

Para o processo de concetualização de *phishing* existem múltiplas definições. Para esta pesquisa, adota-se como definição postulada por Sousa (2023) pois procura ser mais abrangente ao relacionar o *phishing* como uma tática de ataque que busca de

15 Visa atacar empresas para obtenção de dinheiro ou informações confidenciais.
16 Realizado através do envio de e-mails fraudulentos, direcionados a indivíduos ou organizações.
17 Consiste em deixar cartas perdidas em locais estratégicos e observar o comportamento das pessoas, se enviam as cartas aos destinatários.
18 Serviços de mensagem de texto (SMS) parecendo ser de uma entidade legitima para as vítimas.
19 Visa atingir alvos de alto nível possuidoras de grande riqueza e influência social.
20 Ocorre em hotspots públicos, levando as vítimas a revelarem informações.
21 Permite a troca de dados entre dispositivos com um simples toque entre os mesmos.
22 Códigos de barras tridimensionais, em preto e branco, que armazenam informações que para os aceder é necessário um leitor ótico que descodifique o código que ao fazê-lo é redirecionado para uma aplicação sem a autorização.

alguma forma atrair as suas vítimas, por ES, através de falsos e-mails, com meios dos meios de comunicação que conseguem penetrar nos SI e recolherem os dados com vista a alcançarem o fim pretendido.

O *phishing* é uma porta de entrada para ataques cibernéticos que atingem diversos setores, são recorrentes e cada vez mais sofisticados na cidade de Luanda onde os cibercriminosos tendem a explorar as vulnerabilidades e procurando enganar as suas vítimas para obterem informações sensíveis. Estes ataques oferecem variadas consequências a sociedade Luandense, pois quer as pessoas singulares como as coletivas têm sofrido danos a reputação e perdas financeiras que causam elevados custos para a sua recuperação, pois por vezes chegam a ser devastadores.

O estudo detalhado das táticas de *phishing* na cidade de Luanda expõe as complexidades e os desafios que as autoridades enfrentam no campo da cibersegurança, bem como as possíveis respostas a esses ataques. Além disso, contribui para o avanço de programas educativos e para a consciencialização da população e das organizações, pois quanto mais souberem sobre as táticas de phishing, menos vulneráveis estarão a esse tipo de ataque.

1.4.6 Fraude de Identidade

A fraude de identidade na internet é um tipo de cibercrime em que criminosos buscam obter acesso não autorizado às informações pessoais de outra pessoa, visando obter benefícios financeiros ou outras vantagens indevidas. Este crime pode assumir diversas formas, como o roubo e a falsificação de identidade. (Brito et al., 2015)

Em 2018, Meier diz-nos que a fraude de identidade é um crime típico em cibersegurança no qual uma pessoa usa informações pessoais de outra pessoa, sem o seu consentimento, com o objetivo de cometer atividades ilegais. Este tipo de crime pode provocar problemas financeiros e pessoais graves à vítima, podendo redundar na perda de fundos, impacto na reputação de crédito e acumulação de dívidas.

Na perspetiva de Guedes e Gomes (2021) os efeitos da fraude de identidade na internet podem ser devastadores para as vítimas e as empresas com prejuízos financeiros, danos a reputação, passarem por um longo período de recuperação de identidade, enfrentarem questões legais, perda de clientes e parceiros comerciais.

É necessário atuar na prevenção e antecipação da fraude de identidade por meio da adoção de medidas de proteção adequadas, como: a proteção de informações pessoais, a criação de senhas fortes, a autenticação em dois fatores, o cuidado com

e-mails e mensagens suspeitas, a verificação de fontes de informação e o monitoramento regular de atividades financeiras e contas *online* (Ribeiro, 2023). Além dessas medidas de segurança, Sousa (2023) destaca a necessidade adicional de implementar medidas como *firewall*, sistemas de detenção de intrusos e criptografia de dados, essenciais para a manutenção da segurança. Tais medidas são especialmente recomendadas para organizações que lidam com informações sensíveis de clientes, uma vez que a fraude de identidade na internet é um crime grave, capaz de causar sérios danos financeiros e emocionais às vítimas.

A fraude de identidade na cidade de Luanda tem sido uma das formas mais comuns e recorrentes de cibercrime. A sua análise é um componente crítico da estratégia de combate ao cibercrime, pois envolve uma abordagem multifacetada (monitoramento, tecnologia, táticas educacionais e respostas a incidentes) e oferece uma maior compreensão do fenómeno, além de orientar a formulação de políticas públicas proativas capazes de mitigar os riscos e garantir a segurança nas transações *online*. Para tanto, o sucesso no combate a este crime depende da união de esforços entre o governo, os parceiros sociais, a população e entidades internacionais.

1.4.7 Clonagem de cartões / *Skimming*

A proliferação dos serviços de internet, que facilitam significativamente as trocas comerciais e o consequente aumento do consumismo, influenciado pelo avanço tecnológico e pela globalização, fatores presentes no cotidiano dos moradores de Luanda. Com esse desenvolvimento, as transações comerciais, antes realizadas com moeda em espécie e cheques, passaram a ocorrer de forma virtual, com a introdução de cartões de crédito/débito e transferências eletrônicas.

Independentemente da localização geográfica do comprador, a introdução da utilização do cartão/débito veio diminuir a distância entre o vendedor e o comprador e permitir a realização e pagamento de produtos e serviços no momento. Para além disso, permitiu que muitos serviços bancários que anteriormente eram realizados exclusivamente nos balcões passassem a ser realizados com o uso dos cartões e aplicativos por pessoas de todas as classes sociais (Bauman & May, 2010). Contudo, o novo paradigma mundial também transporta problemas e desafios, com especial destaque aos crimes virtuais que tendem a ser frequentes e sofisticados. A clonagem de cartões/skimming é um desses crimes que a cada dia vai ganhando destaque na sociedade por conta dos danos por si causados, principalmente ao cidadão comum,

onde os criminosos se aproveitam das técnicas da ES e das vulnerabilidades para obterem dados confidenciais e clonarem cartões. (Fassbinder, 2016)

Com o surgimento da pandemia da Covid-19 levou com que pessoas de quase todo o mundo ficassem em confinamento levou a que muitos serviços anteriormente oferecidos de forma presencial fossem transferidos para o mundo digital, migrando lojas físicas para lojas virtuais e redes sociais. O setor bancário não ficou isento a nova realidade, apesar de muitos bancos já fornecerem os mais variados serviços com recurso ao *mobile banking* e o *internet banking*, tendo a busca por estes serviços aumentado e proporcionalmente o *skimming*. (Gonçalves, 2021)

No entender de Júnior (2012), à medida que a tecnologia evolui, as formas utilizadas pelos cibercriminosos para cometer o *skimming* também se diversificam. De forma geral, o *skimming* é definido como o ato em que um indivíduo utiliza o cartão de crédito ou débito de outra pessoa sem o conhecimento do proprietário ou da entidade emissora, sendo que, na maioria das vezes, o cibercriminoso não possui qualquer ligação com o titular e não tem a intenção de contatar o proprietário ou reembolsar os gastos realizados.

Um dos principais problemas relacionados com cartões de crédito ou débito é o furto, roubo ou perda, o que pode gerar sérios problemas para o titular. Com o surgimento da tecnologia contactless, em muitos casos, não é necessário utilizar serviços que exijam o código PIN (Personal Identification Number), facilitando a cópia dos dados do cartão para práticas fraudulentas. O *skimming*, por vezes, ocorre imediatamente após o roubo ou perda do cartão, antes que as vítimas relatem o desaparecimento. (Silva, 2020).

1.4.8 Ciberespionagem

A espionagem remota desde o tempo dos fenícios, persas, hebreus e egípcios sendo visível em alguns rabiscos egípcios que citam algumas técnicas de espionagem. Sun Tzu já abordava sobre a espionagem no seu livro, a arte da guerra*,* apontando sobre a importância de se conhecer o inimigo e defendendo a ideia a qual o general criterioso e o governo esclarecido deviam utilizar as mais dotadas inteligências do exército para a espionagem (Silva, 2014).

A dependência tecnológica da sociedade no século XXI é algo novo bem como o uso do ciberespaço como um novo meio de competição geopolítica, transformando-se assim numa nova forma de estadismo que surge com *hackers* governamentais que

trabalham na espionagem com vista a antecipação aos ataques, os contra-ataques e agilizarem as retaliações. (Bergmann, 2014)

Em 2014, Silva diz-nos que a ciberespionagem é uma atividade com objetivo apenas de obter a informação de que se precisa, sem ser detetado, não se confundido com a figura tradicional de espionagem onde a recolha de informações ou subtração de documentação confidencial e secreta (procurando não ser descoberto, sob pena de elevadas consequências), não se aplicando ao ciberespião que se movimenta no ciberespaço e que apesar dos seus movimentos poderem ser detetáveis, dificilmente pode-se conseguir determinar exatamente o elemento responsável.

Para Velloso (2018) a ciberespionagem resume-se no roubo dos segredos de Estado armazenados em formato digital, em computadores e redes de TIC ou o uso de redes de computadores para obter acesso ilícito a informações confidenciais tipicamente na posse de um governo ou uma organização.

A *internet* tornou-se a mais importante forma de processamento de informações no mundo (desde financeiros, governos digitais, segurança, defesa e relações sociais), tendo por isso a capacidade de influenciar e transformar a sociedade bem como o ambiente em que ela está conectada. Com o crescente avanço da tecnologia e a ampliação dos investimentos na área de cibersegurança as ameaças no mundo digital também vão aumentando, sendo favoráveis as ações anónimas da ciberespionagem e deixando expostos os atores do ciberespaço (Magalhães, 2020). A ciberespionagem por vezes é confundido com o ciberataque, mas diferem no sentido de que a ciberespionagem é comummente levada acabo pelos governos, indivíduos ou organizações (com o objetivo de obterem vantagens estratégicas) ao passo que o ciberataque é uma ação levada acabo por cibercriminosos para o alcance de fins financeiros, vingança ideológicos ou políticos. De acordo com as características que apresentam, a diferença reside no impacto dos danos que são infligidos e que podem passar pela utilização de hackers ao serviço dos Estados de modos a provocarem resultados hostis a ordem internacional. (Guedes & Gomes, 2021)

Identificar um único ápice da ciberespionagem é bastante complexo visto que é um fenómeno em constante evolução e ocorre em vários contextos. No entanto, alguns eventos são notáveis e que marcam significativamente a história da ciberespionagem,

como por exemplo o incidente envolvendo o Stuxnet[23] que causou danos físicos a infraestruturas (Magalhães, 2020). Para além deste caso, Melo (2023) relata do caso do antigo analista de SI da *Central Intelligence Agency* (CIA), Edward Joseph Snowden, em 2013, quando revelou informações que despertaram a Comunidade Internacional (CI) para um maior investimento ao ciberespaço e a necessidade da cooperação internacional com vista a manutenção da segurança cibernética por meio de tratados, acordos e políticas de informação. Continuando, o autor realça sobre o reacendimento dessa tática a partir de 2019, por conta de Pandemia da Covid 19, e em 2022 com o surgimento da guerra entre a Rússia e a Ucrânia.

Guedes e Gomes (2021) argumentam que, embora a disseminação de informações nas plataformas digitais tenha se tornado um importante meio de propaganda, dando voz a muitos que antes não a tinham e diminuindo barreiras de espaço e tempo, a ciberespionagem não se limita apenas ao roubo de informações. Os autores citam, por exemplo, as *fake news*, que podem influenciar a opinião pública ao disseminar notícias falsas ou informações descontextualizadas.

Para o ponto em questão, adota-se a definição de Guedes e Gomes (2021), pois os autores analisam a ciberespionagem não apenas como um ato maioritariamente praticado por entidades governamentais com o objetivo de obter informações que as coloquem em uma posição vantajosa, mas também como uma potencial arma para a propagação de informações falsas, que podem levar a opinião pública a formar uma percepção distorcida da realidade.

Com o crescente uso da internet a escala mundial a ciberespionagem tornou-se numa ameaça global para a cibersegurança. Os Estados são frequentemente alvos de ataques do género, perpetuados por outros Estados, tendo em vista ao alcance de proveitos que podem incluir segredos financeiros, comunicações estratégicas, comerciais, pessoais, diplomáticos, militares e entre outros.

Numa cidade como Luanda, onde são projetadas políticas públicas que orientam as ações do governo, empresas de setores estratégicos (petróleo, diamantes, energia, gás, finanças e telecomunicações) estão sujeitas a ataques cibernéticos, que podem causar danos significativos e comprometer as ações governamentais. Neste contexto, a proteção contra a ciberespionagem é essencial para garantir e salvaguardar

23 Um worm de computador, descoberto em 2010, projetado especificamente para atacar o SO SCADA, desenvolvido pela Siemens e usado para controlar as instalações de enriquecimento de urânio no Irão.

informações sensíveis, de modo a amparar o governo, aumentar a competitividade das empresas e promover a estabilidade e segurança nacional.

2. A CONTEXTUALIZAÇÃO SOBRE O CONCEITO DA CIBERSEGURANÇA

Na sua génese, as redes de computadores eram utilizadas por investigadores universitários e por empregados de algumas empresas que partilhavam impressoras. Contudo, atualmente existem milhares de utilizadores que realizam atividades rotineiras como compras online, operações bancárias ou apresentação de declarações de impostos, tornando a segurança das redes um problema com enormes proporções. (Teles, 2015)

Machado (2015) diz-nos que que

> A necessidade de edificar mecanismos de proteção e defesa, destinados a garantir a livre circulação da *internet* e do ciberespaço, tem encaminhado os Estados para o aprofundamento de uma cultura de cibersegurança e à tomada de consciência coletiva, relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético. Assim, a nível internacional e nacional têm vindo a surgir normativos de cooperação, iniciativas legais e entidades que definem normas e princípios destinados a garantir uma internet sustentável e um comportamento aceitável. (p. 17)

Em 2019, Moreira diz-nos que a cibercriminalidade está presente na internet superficial e na *darkweb* (internet profunda). Na internet superficial, é onde está presente a maioria dos utilizadores, encontrando-se plataformas e serviços públicos/privados. Na *darkweb*, apesar de ter uma ligação com a internet superficial, trabalha-se com várias camadas de encriptação de modos a manterem-se ocultas as identidades e os caminhos de navegação, o que dificulta a descoberta das atividades ilícitas aí praticadas.

As últimas décadas têm sido marcadas com profundas mudanças na sociedade, sobretudo com a expansão das TIC, que tornou a humanidade numa aldeia globalizada e conferiu maiores poderes as pessoas em causar danos. Com isso, aumentam-se as preocupações na segurança dos sistemas interconectados e

exigindo mecanismos para a normatização, proteção e mitigação das vulnerabilidades causadas pelos danos do impacto desses ataques. (Teixeira, 2021)

Apesar de não existir um padrão universalmente consensual para a definição do termo cibersegurança, a sua origem é fruto do prefixo ciber (derivada da palavra cybernetics e utilizado pela primeira vez em 1991, para se referir a *internet*,) e a palavra segurança, em 1903, aquando do envio do código Morse por John (Aparício, 2017). Neste contexto, a cibersegurança tornou-se num elemento essencial para o normal funcionamento da economia global, procurando garantir a integridade das comunicações e a privacidade dos dados, sendo por isso necessário à sua garantia contra ameaças cibernéticas (pirataria informática, cibercrimes, disponibilidade, confidencialidade, cibercampanhas maliciosas e integridade) que de algum modo podem comprometer a segurança e a privacidade dos dados. (Pereira, 2022)

Couto (2018) diz-nos que

> a cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. (p. 23)

O conceito de cibersegurança é explicado por Oliveira (2021) como sendo uma proteção e defesa dos sistemas contra possíveis ataques maliciosos e redes de computadores com a implementação de normas de modos a se conseguir evitar possíveis danos de hardware ou de software. Contudo, o autor entende que apesar dos cuidados a serem observados para a proteção do ciberespaço, a cibersegurança deve também velar pela proteção do funciona no ciberespaço e em qualquer um dos seus ativos que possam ter uma relação direta ou indireta com o ele.

Para Faria (2022) “a cibersegurança ou segurança cibernética, é a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso, e a prática de garantir a confidencialidade, integridade e disponibilidade da informação no ciberespaço”. (p. 6)

Apesar da existência em Angola de diploma que aborda sobre os crimes informáticos, até ao momento não existe um diploma especializada para o tratamento, definição, prevenção e combate aos cibercrimes, sendo os casos dessa natureza quase sempre

remetidos para o código penal, aprovado em 2020, mas que dificilmente os consegue tratar na sua plenitude, dada a sua limitação sobre a matéria. O mais próximo que existe está na lei n.º 7/17, art.º 4.º, alínea h, de 16 de fevereiro, que define a cibersegurança como “a segurança relacionada ao ciberespaço.”

2.1 Triângulo da Cibersegurança

A cibersegurança tornou-se num dos temas emergentes e vitais na nova era digital e que face a rápida expansibilidade da tecnologia e a progressiva interconexão de dispositivos e sistemas, proporcionaram a revolução da maneira como vivemos, trabalhamos e nos comunicamos. (Canongia & Júnior, 2010)

A perseverante evolução dessas ameaças proporciona a cibersegurança uma constante batalha para a proteção dos sistemas, redes e dados em relação aos ataques e intrusões. Enfrentar esses desafios vão para além da simples implementação de tecnologias de segurança e agregam elementos como a conscientização dos usuários, processos de segurança bem definidos, políticas robustas e uma cultura organizacional que valorize a segurança da informação. Neste sentido, o triângulo de cibersegurança surge como elemento fundamental para a conceitualização de aspetos relacionados com a segurança da informação: confidencialidade, integridade e disponibilidade. (Fernandes et al., 2012)

Na era digital a informação se tornou moeda valiosa e a interconexão omnipresente, emergindo a confidencialidade como uma garantia que somente pessoas autorizadas terão acesso a informações sensíveis e assim salvaguardar os segredos empresariais e a sua privacidade face aos interesses de outros. (Teles, 2015)

As informações confidenciais devem ser tratadas de formas a abranger a parte verbal, escrita ou qualquer outra, podendo incluir especificações técnicas, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, informações sobre clientes, informações técnicas, financeiras, comerciais ou quaisquer outras que possam ser reveladas pela utilização do SI. (Bryant, 2016)

Gouveia (2017) diz-nos que

> A confidencialidade da informação é a qualidade ou estado de prevenir exposição ou acesso não autorizado à informação, por parte de indivíduos ou sistemas. A confidencialidade da informação deve assegurar que apenas

> aqueles que possuem direitos e privilégios de acesso a um particular conjunto de informação é que são capazes de o fazer […]. (p. 6)

A proliferação dos dispositivos com acesso à *internet* e a massiva concorrência ao armazenamento de dados em nuvem, tornam desafiante a manutenção da confidencialidade dos dados, com relação as constantes ameaças cibernéticas, e a integridade das informações confidenciais. Para além disso, o autor entende ser fundamental a manutenção da confidencialidade para o cumprimento dos padrões regulamentados para a proteção dos dados. (Gonçalves, 2019)

Diante desse cenário, a confidencialidade emerge como um pilar essencial da cibersegurança, desempenhando um papel crucial na proteção da privacidade, da propriedade intelectual e da segurança nacional, num mundo cada vez mais digitalizado e interconectado.

Relativamente a integridade dos dados, são necessárias estratégias e tecnologias que vão desde o controle de acesso rigoroso, implementação de assinaturas digitais, uso de tecnologias de detenção de intrusões, implementação de backups regulares e redundância de SI. No entanto, apesar das múltiplas medidas de integridade de dados existentes, à sua proteção continua a ser um desafio constante, sendo para tal necessário que organizações e indivíduos se mantenham constantemente vigilantes e atualizados sobre as novas tendências de cibersegurança. (Nakamura, 2016)

No entender de Liska e Gallo (2017) a integridade dos dados tornou- se um desafio complexo face a rápida evolução das ameaças cibernéticas que exigem medidas robustas de proteção dos SI e dos dados. A integridade dos dados é fundamental em comunicações críticas, transações financeiras ou registos médicos pois, a não observância pode comprometer a sua integridade e podendo levar a consequências graves como danos a reputação, impactos financeiros significativos e perda de confiança. Assim sendo, para Gouveia (2017) “a integridade da informação é a qualidade ou estado da informação em que esta constitui um todo e se encontra completa e não corrompida,” (p. 6)

Em suma, a integridade emerge como um pilar vital da cibersegurança, garantindo a confiança, a precisão e a confiabilidade das informações num mundo onde a segurança dos dados é uma preocupação crescente.

A disponibilidade, diz respeito a garantia da operacionalidade e acessibilidade dos serviços e dados, legitimamente solicitados, sem interrupções ou degradações

significativas de desempenho. É essencial a garantia da disponibilidade dos sistemas para o garante dos serviços essenciais, como: comunicações empresariais, sistemas bancários e sistemas de comunicação governamentais. (Zalana, 2016)

Para a manutenção da disponibilidade dos SI e serviços devem ser implementadas medidas e estratégias de segurança que podem incluir a implementação de *Redundant Array of Inexpensive Disk* (RAID), redundância via *hardware* ou *software*, sistemas de monitoramento e alerta precoce que possam identificar anomalias e a implementação de planos de recuperação de desastres de modos a reaver as suas funcionalidades, em caso de falhas. (Tavares, 2016)

Gouveia (2017) entende que apesar da disponibilidade da informação significar que a mesma esteja acessível ao SI e aos utilizadores com credenciais autorizadas, à sua garantia não se subscreve apenas numa questão meramente técnica, mas também pela consciencialização dos usuários sobre as práticas seguras do seu uso e sobre o impacto negativo que podem ser provocados pelos ciberataques a disponibilização dos serviços.

Interrupções e ataques cibernéticos que comprometem a disponibilidade podem causar consequências devastadoras que incluem danos à reputação, perda de receitas e riscos a segurança nacional. Para tal, é fundamental a manutenção da proteção contra ataques cibernéticos para se manter a disponibilidade dos serviços, através de mecanismos de defesa como os filtros de tráfego ou *firewall*. (Jorge, 2021)

Como muitas outras metrópoles em rápido crescimento a cidade de Luanda enfrenta variados desafios ligados a cibersegurança, sendo para tal necessária a manutenção do triângulo da cibersegurança para se proteger as mais variadas infraestruturas contra os ciberataques.

A manutenção desse triângulo não pode ser encarada apenas como uma medida técnica, mas também como uma necessidade hábil para a proteção da cidade contra as crescentes ameaças cibernéticas, pois a confidencialidade permite a proteção das informações sensíveis contra acessos não autorizados, a precisão dos dados é assegurada pela integridade que garante que os dados não tenham sido alvo de alguma alteração e a disponibilidade que garante a acessibilidade dos serviços essenciais, sempre que for necessário, sendo que a manutenção de um equilíbrio cuidadoso entre esses componentes é elementar para uma cibersegurança eficaz e resiliente.

A chave para o sucesso do triângulo da cibersegurança está na colaboração, investimento tecnológico e na educação, com vista a criação de uma cultura cibernética capaz de penetrar em todas os sectores da sociedade. Deste modo, a cidade de Luanda, pode-se defender contra os cibercrimes e também fomentar um ambiente digital seguro capaz de fornecer suporte ao seu desenvolvimento económico e social contínuo.

2.2 Práticas e Estratégias de Cibersegurança

No século XXI, as TIC têm assumido um papel cada vez mais central em todos os setores da sociedade e que face as vulnerabilidades exploradas pelos cibercriminosos, nos sistemas físicos e lógicos de armazenamento de dados, de modos a encontrarem dados sensíveis que possam ser uma mais-valia para os seus intentos, tornando o ciberespaço num novo campo de batalha. (Zalana, 2016)

De modos a prevenirem-se dos malefícios provocados pelos ciberataques e a salvaguarda dos dados e informações, têm sido implementadas estratégias e práticas de cibersegurança nos SI e em redes de computadores, tais como: controlo de acesso, *firewall*, proteção contra vírus, criptografia, isolamento e segmentação de rede, políticas de gestão de dispositivos e sistema de redundância

2.2.1 Controlo de Acesso

A eficácia de uma política de controlo de acesso está muito associada com a gestão dos modelos de segurança e não apenas com o simples uso de tecnologia de ponta. Ela varia de uma organização para outra e, é fundamental fazer-se antes uma análise ao perfil da organização para que seja definido o tipo de política de controlo de aceso adequado (lógico ou físico), pois quanto maior for o número de usuários maiores serão as precauções e consequentemente o investimento para a proteção do sistema de segurança. (Amorim, 2005)

Para a existência de uma organização é necessário que sejam salvaguardadas as informações e, como tal, a necessidade do garante da segurança das instalações que sejam adequadas com acessos condicionados. Para além da segurança física, deve ser levado em consideração a segurança lógica dos SI. (Carneiro, 2009)

Para Alves (2010) o objetivo da segurança lógica consiste na determinação de procedimentos que visam o controlo do acesso as informações e dados, e que em

função aos possíveis riscos ligados aos SI devem ser antecipados com a implementação de controlos de acesso.

White (2012) diz-nos que:

> O controlo de acesso é todo e qualquer implementação de procedimentos que visam a proteção dos equipamentos informáticos, restrição de acesso de pessoas numa empresa (prédio ou sala) utilizando meios mecânicos como passes de acesso, leitores biométricos, câmaras de vídeo segurança, fechaduras e chaves de maneiras a se evitarem males maiores. (p. 48)

O roubo de identidade tem afetado muitas pessoas e organizações em todo o mundo, sendo também uma das fraudes mais praticados no âmbito da cibersegurança. Relativamente ao controlo de acesso lógico, por norma é feito por intermédio de solicitação de login e senha, que devem coincidir com o registo da base de dados, para se auferir se realmente a pessoa que esteja a entrar no sistema está devidamente autorizada. (Oliveira, 2012)

A identificação é um ato no qual um usuário declara diante de um SI a sua identificação ao passo que a senha é a validação dessa declaração de identidade. Após a identificação e autenticação do usuário o SI deverá conceder ou não o acesso da rede ou do estabelecimento. Muitos especialistas em sistemas de segurança consideram que medidas de autenticação simples não garantem a inviolabilidade do SI, sendo para tal necessário o seu reforço com outros mecanismos. (Moreno, 2012)

A tecnologia de identificação e verificação por impressões digitais é outro modelo de controlo lógico de acesso para que seja restringido o acesso aos locais controlados ou áreas reservadas. Para tal, é necessário que seja previamente coletada e gravada a impressão digital num computador central que permitirá ou não o acesso do solicitante a área pretendida. No entanto, face ao avanço das tecnologias esse modelo de segurança vai perdendo fiabilidade pois em algumas ocasiões pode se contrafeita a impressão digital. (Silva, 2012)

Para além dos métodos de autenticação abordados, Almeida (2015) propõe a utilização da tecnologia biométrica, baseada na retina, que consiste na análise da camada dos vasos sanguíneos, situados no fundo da cavidade dos olhos, através da utilização de uma luz de baixa intensidade de modos a encontrar padrões singulares da retina que é considerada de muita precisão e impossível de ser adulterada, devido

a forte relação com os sinais vitais humano, pois é uma das poucas partes do corpo humano que não muda com o tempo.

Apesar de ser um método que leva pouco tempo para se auferir a autenticação, no entender de Nakamura (2016) tem sido bastante rejeitado pelos seus usuários por requerer dos mesmos a fixação dos olhos para um ponto luminoso, o que provoca um ligeiro desconforto a vista. Para além disso, exige que os usuários utilizadores de óculos os removam sempre que for aplicado o procedimento.

Em 2016, Brito diz-nos que outro mecanismo de segurança bastante utilizado é a tecnologia de reconhecimento de voz, considerada não intrusiva, que consiste num sistema de autenticação de voz, posteriormente transformada em texto. Por mais simples que pareça o seu funcionamento nem todo o ambiente é favorável a esse sistema pois a poluição sonora pode atrapalhar a precisão no seu reconhecimento, sendo, no entanto, recomendável que as cordas vocais não sofram anomalias (gripe ou estado emocional alterado).

Numa organização poderão existir funcionários que por inerência das suas funções têm acesso a diferentes seções e acesso a informações de outros departamentos. Por questões de segurança, os administradores dos SI devem implementar medidas que visam limitar o acesso dos funcionários ao sistema, tais como: o acesso aos ficheiros, aplicações, privilégios de instalar e desinstalar aplicações e as horas que devem ter acesso ao sistema. É evidente que as limitações de acesso devem ser diferentes, em função das responsabilidades de cada funcionário, e devem ser limitadas aos demais departamentos. (Reis, 2018)

O controle de acesso físico e lógico é elementar para a defesa contra os cibercrimes, em particular na cidade de Luanda. É importante que os gestores e administradores de SI na cidade de Luanda, procurem sempre pela implementação de políticas de proteção com limitações de acesso de modos a garantir que durante o período em que não são registadas atividades laborais (incluindo finais de semana e feriados) estes não consigam entrar nos sistema, pois os cibercriminosos tendem a realizar os seus ataques nos períodos com menor vigilância e assim impedir que os funcionários e invasores externos possam conseguir sucessos na suas atividades, que podem basear-se em transferência de fundos, roubo de senhas de cartões de créditos, roubo de projetos em curso e invasão a infraestrutura tecnológica que podem comprometer o normal funcionamento da organização.

Medidas robustas de controle de acesso, como a combinação de tecnologias e políticas, ajudam a mitigar riscos e garantir que apenas pessoas com autorização consigam aceder as áreas restritas e aos SI, proporcionando deste modo um ambiente estéril a invasão cibernética.

2.2.2 *Firewall*

Afirmar que um determinado sistema é completamente inume aos ataques é algo que pode levar os especialistas de TIC e ao mais comum usuário a caírem em comodismo e que posteriormente pode causar a perda parcial ou total das informações. Vários são os mecanismos utilizados para a segurança dos SI, mas nenhum deles garante segurança total. Para se tornar um SI mais seguro é necessário proteger-se o SI de qualquer tráfego inútil e potencialmente prejudicial ao seu funcionamento. Neste contexto, surge o *firewall* como um mecanismo para essa proteção.

Do ponto de vista da segurança, o *firewall* impede que qualquer elemento externo tente conectar-se a um dispositivo de uma rede privada. As grandes empresas tendem a ser os alvos apetecíveis dos ciberataques, quer por elementos internos ou externos. Deste modo, é fundamental que sejam instalados esses sistemas de defesa para proporcionarem maior segurança. (Júnior, 2008)

Relativamente a arquitetura do *firewall* numa rede, Moreno (2012) entende que deve ser implementado entre a rede interna e a rede não protegida com o objetivo de manter fora os intrusos, códigos maliciosos e informações indesejadas de modos a proteger os dados essenciais incorporados na rede. Para além disso, White (2012), acrescenta que para a manutenção de uma maior segurança o firewall deve ser configurado com regras relacionadas com o tráfego da rede para detetar tentativas de acesso, a partir de uma estação de trabalho, e acionar um alarme que possa despertar o administrador da rede a impedir ceno táfia invasão.

A expressão *firewall* é muitas das vezes comparada a uma parede de fogo que evita o seu alastramento ao interior de uma habitação. No SI ele desempenha as mesmas funções, mas no sentido de não permitir a propagação de dados nocivos a rede de computadores, podendo este ser um programa ou dispositivo de hardware com capacidades de filtrar informações que entram, principalmente por via da internet, no SI. (Santos, 2016)

O *firewall* é uma combinação entre a parte física e lógica do SI com a função de inspecionar o tráfego de entrada/saída em uma rede e decidir qual tráfego pode entrar

ou sair, controlar o fluxo de dados entre a rede interna e o mundo externo, permitir a definição de regras para o acesso externo ou interno, estabelecer a gestão do fluxo de tráfego dos recursos disponíveis (através da filtragem de pacotes), analisar dados disponíveis no cabeçalho dos pacotes (como o endereço IP) com base as regras implementadas. (Manfio, 2016)

No entender de Branco (2020), firewall pode ser um dispositivo ou servidor *proxy*[24] (*firewall* de *hardware*) ou *firewall* de programa (*firewall* de *software*) ou filtrador de pacote que é muito utilizado em redes *Local Area Network* (LAN) e implementado para detetar e proteger os SI e redes de computadores contra quaisquer ameaças, quer sejam elas internas ou externas, possuindo as duas vias de implementação a mesma finalidade de segurança.

O servidor *proxy* é utilizado pelos outros computadores para a cessarem páginas de internet que quando solicitadas são libertadas pelo servidor proxy e enviadas para o computador que fez a solicitação. e vice-versa, evitando assim que o computador remoto que hospeda a página de internet não entra em contacto direto com a parte da rede interna, da instituição. Por regra, com a utilização do servidor *proxy*, o endereço IP que fica registado é o do próprio *proxy* e não o do cliente porque geralmente os computadores da rede interna não são configurados a possuírem endereços válidos de internet. (Júnior, 2008)

Face as regras definidas para o seu funcionamento, o filtrador de pacote pode determinar que endereços IP podem ou não transmitir e receber dados de sites específicos da Internet, podendo serviços como o *e-mail* serem permitidos e outros como software de mensagens instantâneas serem bloqueados. O problema deste tipo de *firewall* está na aplicação das suas regras, pois o endereço IP remoto, o endereço IP do destinatário e a porta *Transmission Control Protocol* (TCP) usada podem incitar a diminuição do desempenho da rede ou então não serem suficientemente eficazes. Se a configuração for bem feita, autoriza apenas que computadores conhecidos troquem informações e tenham acesso aos recursos disponibilizados. (Miranda, 2008)

Apesar do servidor *proxy* oferecer alto nível de segurança, é mais lento que o filtrador de pacote porque o servidor *proxy* tem de ser criado para cada transação que solicita dados dentro da rede corporativa. (Santos, 2016)

[24] Computador com conexões superiores as dos clientes e com poder de armazenamento elevado.

Um dos princípios mais importantes a ser observado no processo de implementação de *firewall* é a defesa de profundidade (virtualização de interfaces de máquinas), devido a existência de vários serviços na mesma máquina, o que impõe a existência de combinados mecanismos de defesa e que falha de um não possa comprometer a defesa de todo o sistema. (Filho, 2017)

Sendo das primeiras linhas de defesa contra os ciberataques, são fundamentais o seu estudo e a compreensão do funcionamento do *firewall* para a definição da melhor estratégia de cibersegurança a ser adotada, especialmente na cidade como Luanda, pois fornece diretrizes concernentes a criação de barreiras com vista a impedirem acessos não autorizados das ameaças internas e externas, o bloqueio dos ataques conhecidos, a proteção de aplicações e serviços para a manutenção da segurança. Para tal, e de modos a ser maximizada a configuração do *firewall* devem ser feitas escolhas das soluções acertadas e o investimento em treinamentos contínuos dos recursos humanos, uma vez serem o elemento central em qualquer sociedade e assim tornar a cidade de Luanda uma parede contra os ciberataques direcionados ao país.

2.2.3 Proteção Contra Vírus

O crescente uso das TIC, principalmente os serviços de *internet*, contribui consideravelmente para o desenvolvimento da humanidade, mas também auxilia no aparecimento de pessoas predispostas a cometerem atos ilícitos com o auxílio de computadores com intuito de enviarem arquivos e programas maliciosos (vírus) que visam a impedir o normal funcionamento dos SI, causar perda de dados e aumentar as vulnerabilidades dos sistemas. Os vírus informáticos são resultantes de pesquisas feitas por peritos de informática, principalmente da área de SO que são o principal alvo desses ataques. (Colmenares, 2002)

O termo vírus deriva do latim vírus, que significa veneno ou toxina, que inicialmente era utilizado apenas nas ciências biológicas para designar agentes infeciosos e mais tarde aplicado no mundo da informática para designar programas maliciosos criados por hackers e crackers, com a mesma lógica de funcionamento do conceito original, necessitando para tal um hospedeiro para que possa replicar e infetar outros SI. Historicamente, o primeiro vírus de computador foi desenvolvido por Bob Thomas, em

1971, denominado Creeper, que se propagava pela *ARPANET*[25] mas sem causar danos ao SI, cujo objetivo era explorar as capacidades de replicação do vírus e mover entre os diferentes sistemas conectados. (Gonçalves, 2002)

De acordo com Roberto Mitshashi (2011):

> vírus são programas especificamente desenvolvidos para trazerem algum mal ao Sistema Informático tendo como propriedade a facilidade de se alastrar para outros computadores e redes, causando assim uma infeção massiva que vai desde a lentidão no processamento até a destruição completa do seu sistema de arquivos. (p. 23)

No entender de Batistela (2018) vírus informático é *malware* que tem como principal característica a capacidade de se alojar, replicar e propagar de um hospedeiro para outro e que no momento da sua execução provoca danos e agindo na maior parte das vezes sem o conhecimento e consentimento do usuário.

Existem vários tipos de vírus sendo os mais conhecidos o *worm*, o *spyware* e o *trojan*. Os *worms* são autónomos e duplicam rapidamente nos sistemas infetados e nas redes acessíveis, procurando explorar as facilidades para executar processos remotamente. Por sua vez, os *spywares* têm a capacidade de espionar as atividades que se desdobram no computador onde estão alojados, entrando despercebidamente, com a finalidade de copiar os dados e informações. Por último, os trojan, são arquivos que aparentam ser inofensivos, ocultando códigos maliciosos, e informam estar a executar uma determinada atividade, mas que na realidade executam outro tipo de atividade que pode danificar completamente o computador, sendo para tal necessário a existência de um programa antivírus atualizado para travá-lo. (Azevedo, 2013)

O antivírus utiliza o padrão que os desenvolvedores e pesquisadores conseguem catalogar e disponibilizar aos usuários, com o intuito de procurar vírus conhecidos que se encontram no computador ou na rede. Apesar disso, nem todos os vírus são eliminados pois todos os dias surgem novas variantes o que obriga a atualizações constantes do programa (manual ou automática), pois os vírus mais recentes são os

25 Advanced Research Projects Agency Network, foi uma rede de computadores desenvolvida pela agência do Departamento de Defesa dos Estados Unidos, ARPA.

mais perigosos e fáceis de passarem pelos sistemas de proteção desatualizados. (Moreno, 2012)

No entender de Filho (2017) o uso e a permanente atualização dos programas de *antivírus* em computadores e servidores é extremamente importante de formas a serem verificados os conteúdos que entram e saem dos SI e assim, sempre que for encontrada alguma infeção seja prontamente movida, reparada, limpa ou excluída.

Apesar de protegerem os SI, no entender de Gonçalves (2023) os *antivírus* possuem vantagens e desvantagens. Como vantagem é apontado o facto de o *antivírus* estar permanente na memória, não sendo necessário à sua ativação sempre que um programa é aberto ou quando se faz *download*[26] de ficheiros e aplicativos. Quanto as desvantagens, destacam-se a utilização constante de recursos da memória e do processamento, que provocam a constante execução e criação de falsos alarmes que depois de constantes interrupções podem levar o usuário a desabilitá-lo e deixar o SI desprotegido.

Os vírus causam perdas avultadas nas instituições governamentais, organizações privadas e a pessoas singulares, podendo provocar a perda parcial ou total dos dados e o cumprimento do normal funcionamento destas instituições. A proteção contra os vírus informáticos é fundamental na era da cibercriminalidade, particularmente em metrópoles como Luanda, de modos a garantir uma maior segurança, integridade e disponibilidade dos SI. Por norma ela deve envolver a combinação de tecnologias e investimentos para proporcionar uma segurança robusta que consigam enfrentar as ameaças do mundo digital.

O trabalho de *software antivírus* pode ser reduzido com o uso do *firewall* pois permite reduzir a carga do seu trabalho com o bloqueio das ameaças antes destas chegarem no SI. Apesar de terem papéis distintos, mas complementares, os dois (2) são elementos importantes que permitem a segurança nos SI através do modelo de segurança em camadas.

2.2.4 Criptografia

Terminologicamente, a criptografia surgiu a partir da fusão das palavras de origem *grega kryptós* (escondido) e *gráphein* (escrita), com o objetivo de permitir a codificação de mensagens as quais apenas o emissor e o recetor consigam obter e ler

[26] Baixar um arquivo da *internet* para um dispositivo: imagens, vídeos, músicas e documentos.

corretamente a comunicação, evitando que pessoas não autorizadas saibam do conteúdo das mesmas. (Mendes, 2007)

Para Oliveira (2012) a criptografia é uma técnica que tem sido utilizada há milhares de anos, principalmente na proteção de informações militares. No antigo exército romano, os planos de guerra eram criptografados, antes de serem enviados aos campos de batalha, e, assim, caso os inimigos intercetassem as mensagens não conseguiriam fazer a sua descodificação.

Historicamente a primeira criptografia que se tem registo data do ano 1900 a.C., no antigo Egito, por intermédio do arquiteto Khnumhotep II, no reinado do Faraó Amenemhet II, onde o arquiteto substituía alguns trechos e palavras de documentos importantes por símbolos de modos a dificultar que outras pessoas pudessem chegar aos tesouros referenciados nesses documentos. Mais tarde, a técnica foi modernizada e utilizada em países como a China e a Índia. (Almeida & Napp, 2017)

No entender de Oliveira (2012) a evolução da criptografia sempre foi acompanhada com a criptoanálise[27]. Geralmente, a criptografia é dividida por dois (2) elementos: algoritmo e chave. O algoritmo de criptografia é o conjunto de regras e cálculos matemáticas aplicadas aos dados de modo a transformá-los de uma forma legível para uma forma ilegível para que sejam difíceis de serem revertidas sem a chave correspondente que é um valor específico usado para controlar o processo de criptografia e descriptografia.

Com o avanço da tecnologia têm surgido novos métodos e técnicas criptográficas mais sofisticados que têm ajudado na prevenção dos ciberataques. Neste sentido são apresentadas dois (2) sistemas criptográficos: a criptografia simétrica e a criptografia assimétrica. (Stallings, 2015)

A criptografia simétrica consiste na existência de uma única chave que dá acesso à mensagem oculta trocada entre duas (2) partes, chave essa que deverá permanecer sempre em segredo. Tipicamente, a chave é representada por uma senha usada pelo remetente no momento da codificação da mensagem e pelo destinatário no momento da descodificação da mensagem. Com a utilização deste sistema, mesmo que um terceiro intercepta a mensagem e conheça o algoritmo utilizado na criptografia, não conseguirá decifrar a mensagem, pois ela está protegida pela chave, o que possibilita

[27] Área de estudo que visa entender os métodos criptográficos e descriptografar informações.

que as partes interessadas mantenham uma comunicação segura e se preocupam apenas com a segurança da chave. (Oliveira, 2012)

Apesar de ser uma técnica bastante utlizada para na segurança de SI, no entender de Silva (2019) uma das suas desvantagens reside na partilha da chave secreta entre o emissor e o recetor que pode ser um problema em sistemas onde o número de usuários ou dispositivos aumenta constantemente, pois em cada par de troca exige sempre uma chave diferente e a gestão contínua das mesmas.

A criptografia assimétrica é um modelo de criptografia criado pelo matemático inglês Clifford Cocks, na década de 1970. A lógica neste sistema consiste na utilização de duas (2) chaves diferentes (assimétricas) na comunicação, sendo uma privada e outra pública para cifrar e decifrar informações. Essas chaves estão matematicamente relacionadas de forma que o que é cifrado com uma chave só pode ser decifrado com a outra chave do par e vice-versa (Magalhães, 2020). Acerca das chaves, no entender de Branco (2020) a chave pública pode estar livre para qualquer pessoa que queira comunicar- se com a outra de modo seguro, mas a chave privada deverá ficar em posse de cada titular, pois é por intermédio desta que o recetor poderá descodificar a mensagem criptografada para ele.

A criptografia é uma ferramenta fundamental utilizada para o combate do cibercrime, pois oferece um sedimento de proteção aos dados sensíveis. Ao serem adotadas práticas robustas, baseadas em criptografia, as instituições e pessoas singulares na cidade de Luanda poderão reduzir o risco de ciberataques. No entanto, para que sejam atingidos esses benefícios é essencial que sejam encarados desafios concernentes com a conscientização dos usuários, a capacitação técnica e gestão das chaves.

2.2.5 Redundância

A informação é o bem mais valioso e importante de qualquer organização e deve ser mantida à sua segurança contra possíveis incidentes e ataques cibernéticos. Apesar dos discos duros dos computadores serem dispositivos resistentes, há que se ter alternativa a possíveis falhas que possam surgir, decorrentes da sua natural utilização. A danificação parcial ou total de um sistema de armazenamento de dados e informações pode significar a perda de dados que por vezes levaram anos a serem construídos. (Júnior & Pereira, 2014)

A utilização de sistemas de *backup* surgiu como alternativa para a proteção e manutenção dos dados as possíveis falhas. Contudo, face ao crescimento do processamento de dados, a partir da década de 1970, os sistemas de *backup* passaram a não corresponder com as necessidades da disponibilidade de dados, em casos de falhas nos discos duros. A partir desta altura, a indústria informática voltou-se para o desenvolvimento de sistemas de discos que fossem tolerantes a falhas. No Início, os fabricantes criaram sistemas simples que permitiam o espelhamento de discos para que toda a Informação lida ou armazenada fosse feita simultaneamente em dois (2) discos (Lobato, 2015). A solução encontrada respondia com as necessidades da época, porém a mesma era muito cara e trabalhosa, já que necessitava sempre do dobro da capacidade dos discos. (Testoni, 2016)

Motivados a desenvolver um sistema que fosse tolerante a falhas, com um menor custo e bom desempenho, os pesquisadores David Patterson, Garth Gibson e Randy Katz, da Universidade de Berkeley, escreveram em 1988 um documento denominado *a Case for Redundant Array of Inexpensive Disk* (RAID). Neste documento definiram cinco (5) níveis de RAID. Cada nível possuía uma forma diferente de interligação dos discos, distribuição de dados e a proteção do arranjo de discos. Basicamente, a ideia deste projeto é agrupar vários discos duros e formar uma única unidade lógica com funcionalidades de armazenar os dados de forma redundante e garantir a segurança em caso de avaria de algum disco que forma a paridade. (Tavares, 2016)

Júnior e Oliveira (2016) dizem-nos que

> O sistema Raid é uma tecnologia simples que melhora o desempenho das soluções de armazenamento externo através da divisão e duplicação das tarefas de um disco duro em matrizes ou vetores (*arrays*) para que sejam executadas operações de entrada e saída em paralelo e assim melhorar o desempenho ou criar redundância de dados, em caso de uma avaria na unidade ou ataques cibernéticos. (p. 46)

Apesar das vantagens inerentes a utilização do Sistema RAID para a proteção de dados, a redundância em uma matriz de discos traz consigo dois problemas: o primeiro versa sobre a escolha do método de cálculo da redundância, pois a maioria

das matrizes de discos usam paridade e poucos usam códigos de *Hamming*[28] ou de *Reed Solomon*[29]. O segundo problema é a escolha do melhor método para a distribuição da redundância pelos discos. (Testoni, 2016)

Apesar da existência de padrões para a distribuição da redundância, no entender de Tavares (2016) eles podem ser classificados em dois (2) esquemas: aqueles que concentram a informação redundante em um pequeno número de discos e aqueles que distribuem a informação redundante de maneira uniforme ao longo dos discos. Segundo ainda o autor, esquemas que distribuem uniformemente a informação redundante pelos discos são os preferidos pois evitam pontos de concentração e problemas de balanceamento de carga.

O processo de implementação do sistema RAID pode ser feito de duas (2) formas: por via *hardware* e por via *software*. A implementação via hardware exige um Servidor ou computador com placa controladora RAID dedicada, tirando deste modo a carga no processador. Para que a implementação via *hardware* funcione é necessário que o dispositivo esteja preparado para trabalhar com discos de sistema *hot swapping*[30] de modos a que estes estejam transparentes ao SO e serem vistos como único volume de armazenamento. (Testoni, 2016)

Sobre a implementação via *software*, no entender de Júnior e Oliveira (2016) é feita criando uma combinação de partições e discos no ambiente do SO ou por aplicativos desenhados e dedicados, através de *drivers* de *software*, não sendo por isso necessária a presença de uma placa controladora, pois o processamento dependente das capacidades do processador do computador.

Os RAID, foram pensados para ser otimizada a performance dos processadores, em virtude da lentidão dos discos, e assim facilitar os *backups* dos discos. De um modo geral, a utilização de um sistema RAID tem como objetivo a substituição de um disco de grande capacidade por múltiplos discos de capacidades menores e distribuir os dados de forma a proporcionar o acesso simultâneo aos mesmos, melhorando dessa forma o rendimento das operações de escrita, armazenamento e defesa. (Filho, 2017)

Com o aumento dos ciberataques o sistema RAID tem sido uma alternativa amplamente adotado e utilizado, motivado pelas vantagens que apresenta,

28 Código de bloco linear utilizado no processamento de sinal e que permite a transferência e armazenamento de dados de forma segura e eficiente.
29 Códigos cíclicos de correção de erros não binários.
30 Sistema que permite a substituição de discos duros enquanto o Servidor esteja em funcionamento.

designadamente a tolerância a falha, melhor rendimento (velocidade), processadores mais rápidos, melhor fiabilidade, exigências de capacidades aumentadas e a diminuição de preços na aquisição dos seus equipamentos.

A redundância dos discos fornece uma camada adicional de segurança e se tem revelado como uma importante prática para a proteção de dados e informações contra falhas de *hardware* acidentais ou resultantes de ataques cibernéticos, permitindo deste modo a resiliência, a recuperação de dados, a dificuldade adicional para alteração ou destruição de dados, a continuidade dos serviços e a disponibilidade. No entanto, é de suma importância ter em consideração que o Sistema *RAID* não se traduz numa solução completa de proteção contra todos os tipos de ataques cibernéticos, sendo crucial a implementação de outras medidas de segurança que visam garantir uma proteção abrangente. (Tavares, 2016)

2.2.6 Política de Gestão de Dispositivos

Com o crescimento e a proliferação da nanotecnologia tem permitido uma maior mobilidade da informação digital, passando ser prioritária a gestão dos dispositivos móveis no seio das instituições governamentais, privadas e pessoas singulares, pois estes guardam e manipulam informações sensíveis em redes corporativas e que facilitam a realização de tarefas em qualquer lugar. Deste modo, a adoção de políticas de gestão de dispositivos tem sido uma ferramenta essencial para a regularização do uso e acesso dos dispositivos na organização, permitindo assim a proteção dos dados sensíveis contra ameaças cibernéticas. (Costa, 2014)

Políticas de gestão de dispositivos são práticas, procedimentos e normas previamente estabelecidas pelas organizações para a garantia do controlo e uso dos dispositivos conectados a uma rede institucional, sendo basilar para o garante do desempenho, conformidade e segurança da rede. (Luna, 2018)

Para Cunha (2020) as políticas de gestão de dispositivos são o conjunto de normas e procedimentos implementos dentro de uma organização com vista a monitorização de dispositivos usados pelos funcionários ou que se encontram conectados à rede da empresa para o garante da conformidade regulatória, segurança dos dados e a eficiência operacional.

Entre as diferentes políticas de gestão de dispositivos que podem ser adotadas por uma organização, neste trabalho serão estudadas o registo e identificação dos

dispositivos, padrões de configuração e segurança, autenticação e controle de acesso, monitoramento e gestão remota e treinamento e conscientização.

As informações de identificação do *hardware* e *software* dos dispositivos deve incluir especificações técnicas como o espaço de armazenamento, processador, SO e a versão do software instalada. Cada dispositivo deve ser associado a um proprietário, dentro da organização, que por regra deve ser um usuário individual ou um determinado departamento de modos a facilitar a comunicação e a responsabilização sobre o uso. (Costa, 2014)

O registo e a identificação dos dispositivos são um componente crucial que envolvem a conceção e a manutenção detalhada dos dispositivos conectados a rede da organização. Para tal, é necessário que sejam observados critérios que incluem os endereços *IP*, endereços *MAC*, detalhes de *hardware* e *software*, número de série e quaisquer outras informações relevantes de identificação única. (Andrade, 2015)

Com relação aos padrões de configuração e segurança, o seu correta formato e definição garante que os dispositivos estejam formatados de forma segura e de acordo com as políticas de segurança estabelecidas pela empresa que devem incluir o uso de senhas fortes, atualizações de *software*, controle de rede, criptografia de dados, autenticação de dois (2) fatores e revisões periódicas para a garantia de uma melhor proteção. (Lovatto, 2015)

Em 2019, Fernández entende que durante o processo de configuração da autenticação e controle de acesso podem ser executadas políticas com vista a desativação temporária ou permanente de contas de usuários, após um número específico de tentativas de login malsucedidas, ou o bloqueio de tela em dispositivos móveis e computadores para se protegerem contra os acessos não autorizados (sempre que o dispositivo estiver inativo) por meio de força bruta ou ataques cibernéticos.

Quanto ao monitoramento e gestão remoto da rede é tida como uma política que permite que os administradores de redes de TI consigam acompanhar o seu desempenho, identificar problemas, aplicarem atualizações e fazerem as correções necessárias mesmo quando estão fora do local de trabalho, que para uma maior segurança é importante que esteja configurada com sistemas capazes de ativarem alertas e notificações automatizadas de possíveis tentativas de acesso não autorizado, falhas de *hardware*, falhas de *software* e violações das políticas de segurança. (Klauberg, 2016)

Apesar da existência de variadas políticas de gestão de dispositivos é necessário trabalhar-se continuamente na formação e conscientização dos elementos envolvidos através de esclarecimentos sobre as responsabilidades a serem observadas no uso dos dispositivos, as obrigações a serem seguidas com vista a proteção das informações sensíveis (relatos de incidentes de segurança e a manutenção da atualização dos dispositivos) e como deverão agir em caso de ciberataques. As formações devem ser abrangentes, de tal forma a congregar funcionários mais antigos e novos. (Gonçalves, 2015)

Para além das medidas abordadas, é necessário serem implementadas ferramentas de auditoria que registam e monitoram as atividades de autenticação e acesso dos usuários de formas a permitir a deteção de comportamentos suspeitos ou tentativas de acesso não autorizado, o que facilita nos processos de investigação de incidentes de cibersegurança. Para tal, é essencial que sejam feitas revisões periódicas aos protocolos, padrões de configuração e segurança para que estejam garantidos o seu alinhamento com as melhores práticas e as ameaças recentes. (Tavares, 2016)

3. AS TIC E O CIBERCRIME EM ANGOLA

No princípcio da década de 1990 surge a internet em Angola, que a princípio era limitada a instituições governamentais, diamantíferas, tecnológicas e petrolíferas, através de conexões discadas. Com a expansão das infraestruturas de telecomunicações, permitiu maior acesso a estes serviços e consequentemente o surgimento massivo dos cibercrimes. (Menezes, 2016)

A República de Angola emergiu de três décadas de guerra civil, e, em 2002, iniciou uma nova era de reconstrução e desenvolvimento. A partir desse momento, as TIC passaram a desempenhar um papel central e indispensável na modernização e no impulso de diversos setores, promovendo o crescimento e o desenvolvimento tecnológico do país (Tavares, 2016).

3.1 A normatividade do cibercrime e a infraestrutura tecnológica em Angola

A existência das leis e a sua coabitação com os recursos oferecidos pelas TIC são imprescindíveis para o desenvolvimento sustentável de qualquer sociedade e setor. A respeito desse fenómeno, o executivo angolano, através do despacho presidencial n.º 71/11, de 12 de setembro, reconhece que:

> de uma forma inequívoca o sector das Tecnologias de Informação e Comunicação constitui um importante elemento indutor do desenvolvimento social e da prosperidade económica do país e um fator essencial na luta contra a pobreza e a exclusão social das classes desfavorecidas, bem como um catalisador da modernidade para o povo angolano, sobre o qual assenta a edificação da sociedade de Informação e do conhecimento.

Historicamente o começo das comunicações em Angola data desde 1798, no tempo do governador geral da colónia, António de Melo, com a emissão, pelo reino de Portugal, do alvará para o estabelecimento dos Correios e a publicação do seu regulamento, tendo mais tarde, em 1885, encomendados os primeiros cinquenta (50) telefones para uso público. (Pertence, 2021)

Segundo o Instituto Angolano das Comunicações (INACOM, 2020) em 1999 criou-se o INACOM com o objetivo de proporcionar a liberalização da concorrência do mercado das telecomunicações e a sua regularização, sob a supervisão do Ministério das Telecomunicações e Tecnologias de Informação. Fruto disso, foi possível a implementação dos serviços de telefonia móvel pública e privada (Angola Telecom e Unitel), inicialmente nas províncias de Luanda, Benguela e Cabinda.

Com o alcance da paz, em 2002, o governo começou a trabalhar em regulamentos para o fortalecimento e restruturação do setor das telecomunicações e das TIC, suportada com base ao planeamento elaborado pela estrutura governamental e que se consubstancia em três (3) estágios, figura 1, aprovado pelo Despacho Presidencial n.º 71/11, de 12 de setembro, publicado no Diário da República a 4 de agosto de 2011.

O primeiro estágio (reforma), de 2001 a 2010, é dedicado a reabilitação das infraestruturas tecnológicas danificas durante o conflito armado, consubstanciando-se no Livro Branco das Telecomunicações, aprovado em 2001, que define as metas a serem alcançadas durante a reabilitação e a abertura gradual do setor ao investimento privado. No segundo estágio (desenvolvimento), de 2011 a 2015, é dedicado ao fortalecimento da estrutura do mercado e o desenvolvimento de novos conteúdos e serviços das TIC com a sua distribuição de forma inclusiva. No terceiro estágio (consolidação), de 2016 a 2020, tem como foco a liderança regional e africana no domínio das TIC, através da criação de um setor forte e coeso que possa gerar emprego e contribuição socioeconómica para o País.

Figura 1: Estágios de desenvolvimento das TIC em Angola

Fonte: Despacho Presidencial n.º 71/11, de 12 de setembro.

Segundo o INACOM (2020), diante da crescente demanda por serviços de TIC, regista-se um aumento no uso de redes privadas, que têm contribuído significativamente para o progresso tecnológico e das telecomunicações no país. Como resultado, estão licenciadas doze (12) empresas provedoras de serviços de internet e quatro (4) operadoras de telecomunicações móveis, que desempenham um papel crucial no avanço tecnológico e na diversificação da economia.

Com os avançados registados, quer em infraestruturas como em projetos de lei, em 2017 acontece o maior avanço tecnológico registado em Angola com o lançamento do seu primeiro satélite geoestacionário de telecomunicações (Angosat 1), com centros de controlo em Sochi e em Luanda, mas precocemente apresentou problemas de telemetria e desvio da órbita definida, não tendo por isso alcançado os objetivos traçados. Apesar dos constrangimentos e a não concretização dos objetivos, este projeto permitiu que o país passasse a fazer parte do leque das nações exploradoras do espaço sideral e começou-se a projeção e a construção do Angosat 2 que em 2022 conseguiu entrar com sucesso na órbita geoestacionária definida e aos poucos vai melhorando o fornecimento do sinal da *Internet*, quer em zonas urbanas como em zonas recônditas. (Miala, 2022)

Muito se tem feito para o melhoramento das TIC em Angola, em particular na cidade de Luanda que é o principal centro de restruturação e criação de políticas públicas, criando deste modo mecanismos para a existência de um mercado competitivo e com maior qualidade na prestação dos serviços. Apesar do alcance de alguns marcos, muitos objetivos traçados ainda estão por ser atingidos, alguns relevantes e definidos no Livro Branco de Tecnologias de Informação e de Comunicação, como a criação de uma base infraestrutural de excelência que suporta a implementação de todos os

serviços da sociedade de informação assentes nas TIC, a modernização da administração pública, contínua criação de normas que se adaptam a nova realidade, a criação de um Centro de Dados (para promoção do crescimento digital assente em ambientes de armazenamento confiável), maior alcance das TIC no sistema de ensino, maior rigor na fiscalização do uso das TIC, maior cooperação com parceiros nacionais e estrangeiros. (Escrivão, 2021)

Devido à forte dependência mundial das TIC e para que os objetivos do governo angolano sejam alcançados, é imprescindível um maior investimento no setor da cibersegurança. O uso da *internet* frequentemente expõe as infraestruturas tecnológicas a vulnerabilidades e ameaças de cibercrimes, resultantes da necessidade de fornecer serviços essenciais à sociedade. (Miala, 2022)

No que se refere ao cibercrime, não há uma data documentada e tornada pública sobre o seu surgimento na sociedade angolana, especialmente na cidade de Luanda. No entanto, segundo Pertence (2021), é provável que tenha ocorrido a partir de 2002, quando a conectividade digital, por meio da *internet* e das TIC, começou a se expandir, tornando-se mais acessível e difundida no país, e de forma gradual a presença destes crimes passaram a ser notórios.

Relativamente ao cibercrime e a cibersegurança, Angola atravessa uma fase de crescimento para o fortalecimento das suas normas e infraestruturas com vista ao combate deste fenómeno. Portanto, entende-se que não seja de todo atípico o surgimento de indefinições sobre a estrutura que realmente possa coordenar toda a política, divergências essas que se ligam as já existentes, entre as leis e tratados de diferentes países, e a falta de imposição de responsabilidades aos provedores de acesso à *internet*. (Menezes, 2016)

A digitalização e a globalização são dois (2) fatores com impacto relevante para o aumento dos cibercrimes na cidade de Luanda, resultante do maior número de acesso aos serviços de internet, com o recurso aos mais variados dispositivos eletrónicos, os cibercriminosos realizam atividades ilícitas que vão desde o roubo de identidade, *phishing*, *ransomware* e outros tipos de cibercrimes. (Pedro, 2022)

Para o combate ao cibercrime têm sido criados e aprovados diplomas para a sua regulamentação e proporcionar melhor ambiente de cibersegurança. Entre estes diplomas destacam-se o despacho presidencial n.º 71/11 de 12 de setembro (que aprova o livro branco das tecnologias de informação e de comunicação), a Lei n.º 23/11 de 20 de junho (sobre as comunicações eletrónicas e dos serviços da sociedade

da informação), o decreto presidencial n.º 202/11 de 22 de julho (sobre o regulamento das tecnologias e dos serviços da sociedade da informação), a Lei n.º 7/17 de 16 de fevereiro (sobre a proteção das redes e sistemas informáticos), a Lei n.º 22/11 de 17 de junho (sobre a proteção de dados pessoais), a resolução n.º 33/19 de 09 de julho (adesão a convenção da União Africana sobre a cibersegurança e proteção de dados pessoais) e a Lei n.º 38/20, de 11 de novembro (que aprova o código penal angolano). Apesar da aprovação, em 2017, da Lei sobre a proteção das redes e sistemas informáticos, ela não trata especificamente o cibercrime, mas é um marco importante para o surgimento de normas que visam o tratamento especializado de matérias ligadas à cibersegurança e ao cibercrime que tendem a aumentar, sobretudo os cometidos com recurso às redes sociais. (Caiúve, 2020)

A ameaça cibernética, é considerada como sendo um risco face aos interesses de qualquer país, por isso, impõe-se a criação de estruturas capazes de coordenar e implementar medidas rigorosas de prevenção e combate ao cibercrime. Enquanto se aguarda pela criação de uma Agência Nacional de Cibersegurança (responsável em coordenar o monitoramento e responder às ameaças de cibercrimes em tempo real), foi criado, através do Decreto Presidencial n.º 179/17, de 09 de agosto, no Art.º 41.º, a Direção de Combate aos Crimes Informáticos (DCCI), sob tutela do Serviço de Investigação Criminal (SIC), com competências de:

- Auxiliar as autoridades jurídicas e judiciárias na administração da justiça, no âmbito da prevenção e repressão dos crimes informáticos, sem prejuízo da sua autonomia tática, técnica e operacional;
- Investigar e efetuar a instrução preparatória dos processos-crime da sua competência, bem como executar as diligências processuais delegadas pelo Ministério Público;
- Controlar o potencial delituoso no limite das suas competências;
- Determinar e catalogar redes ou grupos de criminosos informáticos e proceder ao rastreamento do modus operandi utilizado para o cometimento dos crimes;
- Promover a adoção de medidas, métodos e técnicas eficazes na prevenção dos crimes informáticos;
- Organizar, planificar, propor ações de divulgação pública, através de palestras, colóquios, seminários, relatórios ou edições periódicas por intermédio da informação disponível para a prevenção dos crimes informáticos;

Para além da criação da DCCI existe também a Direção Nacional das Políticas de Cibersegurança e Serviços Digitais (DNPCSD), afeto ao Ministério das Telecomunicações, Tecnologias de Informação e Comunicação Social, que trabalha para a manutenção da cibersegurança e a Procuradoria-Geral da República (PGR) que tem um papel central para o combate do cibercrime, pois cabe a si a coordenação das investigações contra os indivíduos e grupos envolvidos em atividades criminosas que acontecem tanto no ciberespaço como no mundo real.

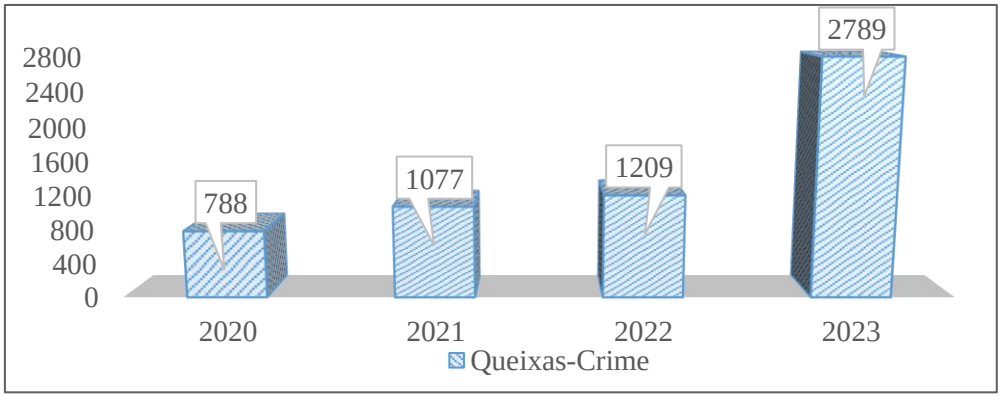
O atual cenário dos cibercrimes em Angola, em especial na cidade de Luanda que é considerada o maior centro tecnológico do país, tem promovido alguns debates com vista a sua melhor compreensão, com realce para a Conferência Nacional sobre Cibercrime, realizada entre os dias 21 e 22 de novembro de 2023, com a participação de especialistas de diferentes instituições.

3.2 A incidência do cibercrime e os danos causados na cidade de Luanda

A cidade de Luanda tem registado aumento significativo de casos de cibercrimes que afetam empresas públicas, privadas e pessoas singulares que no entender do Comissário Aristófanes dos Santos[31], entrevistado pela Voz da América (VOA) a 14 de dezembro de 2014, apesar do fenómeno ser novo na realidade angolana a tendência dos cibercrimes é crescente a cada ano. Contudo, considera serem relativamente baixos se comparados aos casos que ocorrem em alguns países da América (Brasil e os EUA) ou da Europa (França, Rússia e Inglaterra).

Os dados apresentados pela DCCI, referentes ao período compreendido entre os meses de janeiro a novembro, entre os anos 2020 a 2023, revelam existir uma subida exponencial dos cibercrimes denunciados na cidade de Luanda. (gráfico 1)

Gráfico 1: Índice de Crimes Informáticos Denunciados



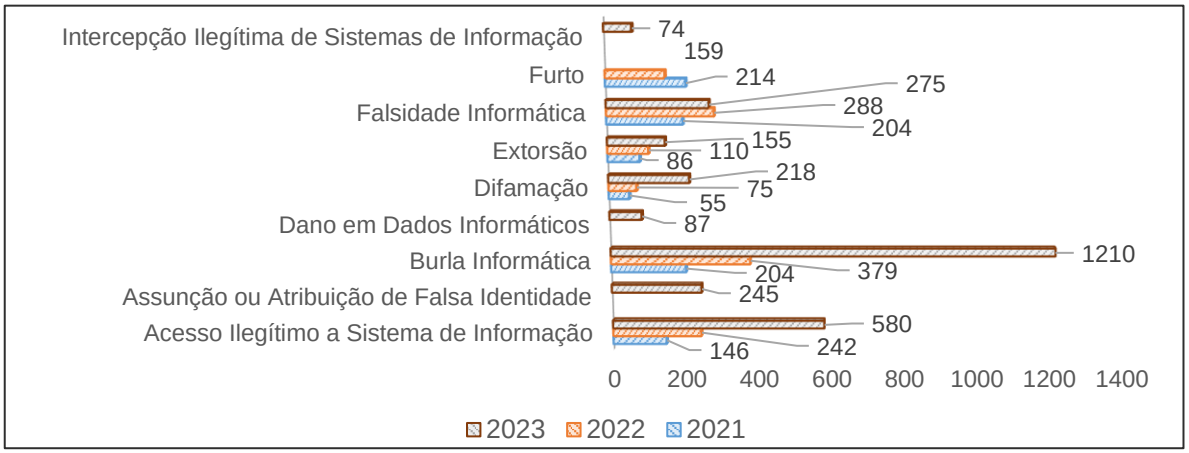
Fonte: Relatório da DCCI

[31] Delegado e Comandante Provincial do Ministério do Interior na Província de Benguela.

Em 2020, foram registadas 788 queixas-crime; em 2021, esse número subiu para 1.077, representando um aumento de 289 denúncias, ou 36,68% em relação ao ano anterior. Em 2022, houve 1.209 casos registados, um aumento de 132 casos em relação ao ano anterior, correspondendo a um crescimento de 12,26%. Já em 2023, foram registadas 2.789 denúncias de cibercrimes, um aumento de 1.580 novos casos, correspondendo a uma taxa de crescimento de 130,69% em relação ao ano anterior. Por fim, comparando o número de denúncias de 2020 com as de 2023, observa-se uma diferença de 2.001 casos, o que corresponde a um aumento de 253,93% nos casos denunciados de cibercrime na cidade de Luanda.

Para melhor entendimento dessa incidência criminal, o gráfico 2 espelha com maior precisão a manifestação dos cibercrimes denunciados entre os anos 2021 a 2022, entre os meses de janeiro a novembro. Infelizmente, pela não disponibilidade de dados não foi possível fazer-se a abordagem sobre a manifestação dos cibercrimes denunciados no ano de 2020.

Gráfico 2: Incidência Criminal entre 2021 e 2023



Fonte: Relatório da DCCI

Com base nos dados disponíveis, a burla informática é o crime que mais tem crescido e, consequentemente, causado danos às instituições públicas, privadas e as pessoas singulares. A cidade de Luanda, sendo o maior centro do país, tem sido o principal palco para o cometimento desses ataques e que tem provocado perdas financeiras e custos indiretos sobre os negócios, elevando, desta forma, a desconfiança por parte dos investidores quando a fidúcia da segurança da economia local.

Os registos apontam que entre os meses de janeiro à novembro dos anos 2021 a 2022, os cibercrimes denunciados causaram perdas financeiras avaliadas em 1.137.169.783,03 (um bilião e cento e trinta e sete milhões e cento e sessenta e nove

mil e setecentos e oitenta e três kwanzas e três cêntimos), ao passo que entre janeiro e novembro de 2023 registaram-se prejuízos avaliados em mil milhões de kwanzas. Os números indicam um crescimento do cibercrime e dos danos por ele causados, que, caso não sejam rapidamente contidos, poderão comprometer a estabilidade económica, afetar a produtividade industrial, aumentar as despesas governamentais, prejudicar a reputação, elevar os custos de recuperação e reparação, além de impactar os serviços públicos e privados. No entanto, é importante ressaltar que a cidade de Luanda ainda enfrenta desafios significativos em termos de infraestruturas tecnológicas, capacidade de elaboração e aplicação da lei e conscientização sobre a segurança cibernética, mas que pode beneficiar e colmatar algumas dessas debilidades caso seja ratificada a Convenção de Budapeste e a colaboração com organizações internacionais para o fortalecimento contra os cibercrimes e promover a segurança cibernética.

3.3 Os Setores mais visados dos cibercrimes na cidade de Luanda

Com o aumento dos casos dos cibercrimes denunciados nos mais variados setores da sociedade na cidade de Luanda, que em parte deve-se ao aumento da digitalização que não tem sido acompanhado com atualizações constantes de segurança e das infraestruturas tecnológicas, a questão da cibersegurança tornou-se um desafio a ser ultrapassado pelas autoridades. Entre os setores que têm sofrido ciberataques estão o Banco Nacional de Angola (BNA), os bancos privados, as empresas petrolíferas, as instituições do Estado e as microempresas. Estes ataques provocam constrangimentos significativos à segurança pública, à economia, aos clientes e à confiança do sistema financeiro. (Dias, 2019)

Como consequência das vulnerabilidades encontradas pelos cibercriminosos a maior empresa petrolífera de Angola, Sonangol, tem sido alvo de ciberataques, com realce ao ocorrido a 5 de junho de 2019 que provocou a paralisação das suas operações por dois (2) dias e o comprometimento de 7.000 computadores e dos dados neles guardados, numa altura que se realizava na cidade de Luanda a conferência internacional Angola Oil & Gas. (Mbinza, 2023)

A par do que por vezes acontece com as empresas públicas mencionadas, as demais empresas públicas também estão passíveis de sofrerem ciberataques, facilitadas pelo fraco investimento na cibersegurança e tecnologias desatualizadas, tornando-as vulneráveis e apetecíveis a ataques do género. Para além disso, regista-se o aumento

dos cibercrimes nas redes sociais e em outras plataformas digitais, sendo, no entanto, difícil à sua de investigação devido à fraca infraestrutura tecnológica existente, poucos recursos humanos com aptidão profissional e a inexistência de legislação específica que puna severamente os cibercriminosos e os crimes por si praticados, constituindo assim uma ameaça à segurança nacional. (Matondo, 2024)

Na opinião do especialista em ataques cibernéticos, Alberto Afonso, entrevistado pelo DW, a 18 de outubro de 2021, de acordo aos dados divulgados pela empresa *Data Group*, especialista em cibercriminalidade, Angola está entre os cinco (5) países africanos que mais ciberataques sofrem. Segundo ainda o especialista, por causa da pandemia do Covid-19 e o consequente confinamento das pessoas, registou-se aumento do uso das TIC por parte das empresas, ampliando igualmente as vulnerabilidades e os riscos dos ciberataques, provocados em parte pela negligência das instituições em não implementarem protocolos de prevenção, formações contínuas e aquisição de tecnologias que possam protegê-los contra os ciberataques e, preferindo, a utilização de sistemas desatualizados.

3.4 Medidas implementadas para o combate ao cibercrime

A revolução tecnológica transformou o mundo numa aldeia global permitindo que distâncias deixassem de constituir problemas, principalmente com o uso da internet, permitindo maior proximidade entre pessoas e organizações. A inclusão científica, tecnológica e estratégica para o desenvolvimento do país é crucial para o combate à pobreza e na edificação de uma sociedade de formas a tornar o país numa referência continental. (Fernandes, 2015)

Com a ténue modernização das infraestruturas tecnológicas e a maior abertura na utilização dos serviços de internet as instituições públicas, privadas e as pessoas singulares na cidade de Luanda têm sido afetadas pelos cibercrimes. Em réplica a estes ataques e de modo a enfrentar a crescente ameaça cibernética, o governo angolano tem agilizado políticas públicas para a prevenção e combate a este fenómeno e que incluem a criação de diplomas, infraestruturas tecnológicas, formação de quadros e colaboração com parceiros internacionais. (Menezes, 2016)

Segundo o Secretário de Estado para as Telecomunicações e Tecnologias de Informação e Comunicação Social, Mário Oliveira, entrevistado pelo *Deutsche Welle* (DW), a 18 de outubro de 2021, 90% dos ciberataques que se tem registado podem ser evitáveis se as instituições apostarem por mais investimento em medidas fortes

de cibersegurança. Para além disso, o governante sustenta que a não existência de um centro nacional para o combate ao cibercrime tem sido um grande problema, mas que o seu ministério tem trabalhado na criação de condições para a edificação e a operacionalização desse centro para que seja um firewall de bloqueio e resposta em tempo real a essas ameaças.

Segundo o relatório da DCCI, entre os anos 2020 à 2023 foram realizadas diversas ações com vista ao combate do cibercrime e que resultou na deteção e bloqueio de *links* de *phishing* com nomes de organizações, deteção e encerramento de perfis, recuperação de contas *hackeadas* de *Facebook* e *Instagram*, *IP* de organizações angolanas infetados, detenção e encerramento de campanhas de *phishing* no *Facebook* e *Instagram*, identificação de venda de dados de angolanos na *darkweb*, bloqueio de falsos perfis de entidades do governo, *links* patrocinados de *phishing* do Fundo de Fomento Habitacional, desmantelamento de uma rede que operava serviços ilegais de distribuição de TV pirata, desmantelamento de rede criminosa que se dedicava a clonagem de cartões Multicaixa, detenção de cidadãos que invadiam contas de *Facebook* de mulheres com intuito de obterem fotos e vídeos íntimos das vítimas que, posteriormente, eram alvas de chantagens e extorsão e a detenção de grupos organizados que utilizavam *links* patrocinados de *phishing* EMIS: *SIM SWAP* (solicitação de 2º via fraudulenta) e acesso fraudulento ao BAI Direto.

3.5 Cooperação internacional em matéria de cibercrime

Pela sua natureza os cibercrimes são de cariz transnacionais, pois o cibercriminoso pode a partir de qualquer parte do mundo perpetuar ataques a pessoas que se encontram em diferentes localidades com vista ao alcance das metas preconizadas, sendo, por isso, essencial a cooperação internacional entre os Estados e as demais organizações. Para tal, várias têm sido as formas de cooperação levado acabo pelos principais autores da comunidade internacional com realce para o estabelecimento de acordos, tratados e outros instrumentos jurídicos com vista a recolha e partilha de informações, em tempo útil, sobre os cibercrimes. (Zalana, 2016)

No que se refere à cooperação internacional em relação aos cibercrimes, Angola tem mantido contato com alguns parceiros, tanto no âmbito regional africano quanto na Comunidade dos Países de Língua Portuguesa (CPLP). Segundo o relatório final do primeiro encontro de cooperação sobre cibercrimes entre os Ministérios Públicos dos países da CPLP, realizado em Lisboa, no dia 7 de fevereiro de 2018, com a

participação de representantes de Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal, Timor-Leste e Macau (como observador), e do segundo encontro com o mesmo propósito, realizado na cidade da Praia, entre 11 e 12 de abril de 2019, com a participação de representantes de Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal, São Tomé e Príncipe, Timor-Leste e Guiné Equatorial, os objetivos focaram-se na troca de informações sobre o quadro jurídico no âmbito da cibercriminalidade. O intuito era reforçar a eficácia na colheita, preservação e utilização da prova digital em processos penais. No entanto, foi enfatizada a necessidade de que os países continuem a trabalhar na melhoria dos diplomas legais para enfrentar os cibercrimes, permitindo uma maior harmonia entre os diferentes ordenamentos jurídicos da CPLP. A terceira reunião presencial, agendada para 2020, não ocorreu devido à pandemia de Covid-19 e, por razões sanitárias, foi adiada para 2021, sendo realizada por videoconferência, em 2 de julho de 2021, com a participação de representantes de Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal, São Tomé e Príncipe e Timor-Leste. Segundo o relatório final desta reunião, além das recomendações anteriores, foram atualizadas as ações desenvolvidas e reforçadas as medidas de segurança devido ao aumento do uso de infraestruturas tecnológicas, provocado pela limitação da mobilidade humana durante o confinamento causado pela pandemia. O tema central da reunião foi justamente a evolução do cibercrime durante a pandemia.

No âmbito regional, desde 23 de maio de 2019, Angola é membro da Convenção de Malabo sobre Cibersegurança e Proteção de Dados Pessoais, um tratado adotado pela União Africana em 27 de junho de 2014. O preâmbulo da convenção, em sua alínea h, estabelece como objetivo a coordenação da segurança cibernética entre os Estados-Membros, criando um instrumento para combater violações de privacidade em todo o processo de colheita, tratamento, transferência, armazenamento e uso de dados pessoais, sempre com base no respeito às liberdades fundamentais, aos direitos das pessoas e às prerrogativas dos Estados-Membros, levando em consideração as melhores práticas reconhecidas internacionalmente. Com base nos princípios da convenção de Malabo, Angola tem participado em reuniões com vista ao fortalecimento da cooperação em matéria de combate aos cibercrimes, no continente africano. Segundo o relatório da DCCI, Angola participou na operação Africa *Cyber Surge I*, ocorrido entre os dias 18 julho a 5 de agosto de 2022, em Kigali / República do Ruanda, e através de relatórios de atividades cibernéticas fornecidos pela *Interpol*

com apoio de parceiros privados como a *Kasperky*, *Cisco*, *Group IB*, *Palo Alto Networks*, *Trend Micro* foram comunicados mais de 900 endereços *IPs* com atividade criminosas em Angola (atividades de *phishing*, ataques a *websites* governamentais, infraestruturas do governo vulneráveis e domínios maliciosos (*malware*). Fruto dessas informações e com base a cooperação com os provedores de serviços de *internet*, a nível local, foram interrompidas as atividades criminosas com envolvência desses endereços *IPs* maliciosos.

De modo a dar continuidade ao estabelecimento de parcerias para o combate de cibercrimes, o relatório da DCCI afirma que Angola participou da operação Africa Cyber Surge II, ocorrida entre os dias 19 a 30 de julho de 2023, em Dar-Es-Salam / República da Tanzânia, que notificou a existência de novas atividades cibernéticas relatadas pela Interpol em parceria com a *Kasperky*, *Cisco*, *Group IB, Palo Alto Networks*, *Trend Micro* onde foram mencionados a existência de mais de 2 mil endereços IPs com atividades criminosas em Angola e também mais de 22 mil terminais telefónicos nacionais vítimas de ciberataques em escala com recurso a atividades de *phishing*, C2 comando e controlo, *stealer-as-a-service* (roubo de informação como negócio), roubo de informações pessoais para venda na *darkweb*, urls maliciosos e *links* maliciosos.

Apesar dos esforços realizados pelo governo local em parceria com atores internacionais, ainda não existe uma convenção universalmente aceite pelos Estados. A Convenção de Budapeste é a que reúne maior consenso, mas, infelizmente, até ao momento, não foi ratificada pelo governo angolano. Por essa razão, a discussão sobre sua possível adesão tem sido recorrente, especialmente no seio da CPLP, com explicações sobre as vantagens dessa adesão. Na opinião do superintendente-chefe do SIC, Edgar Cuico, em entrevista à DW, 18 de outubro de 2021, Angola deveria aderir à convenção, por ser o acordo com maior consenso sobre cibercriminalidade, permitindo a colheita adequada de provas digitais e a responsabilização dos criminosos. Cuico argumenta que, mesmo com uma legislação interna que regule essa matéria, o alcance das investigações permanecerá limitada ao ordenamento interno, caso o país não adote um acordo internacional.

Segundo Pedro (2022) para combater o cibercrime transnacional é essencial a manutenção da cooperação internacional entre os países e que envolve a troca de informações, a coordenação de investigações e a implementação de estratégias conjuntas para prevenir e responder aos crimes desta natureza. Organizações como

a *Interpol*, além de tratados e acordos internacionais, trabalham para facilitar a cooperação entre os países na luta contra o cibercrime transnacional. Angola, por intermédio do Gabinete Nacional da Interpol, tem estado a beneficiar de um conjunto de iniciativas promovidas por esta Direção, com vista ao combate e repressão do cibercrime em África.

3.6 A importância do estudo dos cibercrimes denunciados na cidade de Luanda

O cibercrime é um fenómeno de natureza transnacional e com caraterísticas de anonimato digital e que torna complexa a sua prevenção e combate. Para tal é fundamental a manutenção da cooperação internacional para a troca de dados e informações e se fazer face as ameaças cibernéticas que não estão sujeitas a fronteiras geográficas específicas e, deste modo, conseguir chegar aos seus prevaricadores e à consequente detenção e desativação das organizações que se dedicam a estes tipos de crimes. (*Organisation for Economic Co-operation and Development* [OECD], 2012)

O estudo sobre o atual cenário dos cibercrimes denunciados na cidade de Luanda é de suma importância pois trata-se de um fenómeno multifacético e recente, sendo para tal necessária à sua compreensão e do impacto que pode causar nos mais variados setores da sociedade local e sobretudo a economia mundial. A cidade de Luanda não está imune a esta tendência global que tem provocado perdas financeiras que ascendem aos 600 biliões de dólares (o que representa cerca de 0,8% do PIB mundial) afetando empresas públicas, privadas, pessoas singulares, custos indiretos inerentes a implementação de medidas de segurança cibernéticas robustas e a recuperação dos ciberataques. (Lewis, 2018)

O constante aprimoramento das técnicas usadas pelos cibercriminosos para explorarem as vulnerabilidades de segurança (com ataques de *phishing*, *ransomware*, ES, entre outras), exige que sejam constantemente atualizados e sofisticados os mecanismos de defesa na cidade de Luanda. Para tal, é fundamental a criação e desenvolvimento de políticas públicas e leis específicas para o combate ao cibercrime e que deverão ser robustas e capazes de punirem severamente os cibercriminosos. (*U.S. Department of Homeland Security* [USDHS], 2021)

A segurança cibernética é de suma importância, pois para além do impacto económico que os cibercrimes causam, também representam uma ameaça para a segurança nacional, as Infraestruturas tecnológicas, as empresas petrolíferas, diamantíferas e

de energia e águas que tende a ser os alvos dos cibercriminosos devido à importância que representam e que face a uma possível paralisação provocariam sérios danos à sociedade e a economia nacional. (*Cybersecurity Ventures*, 2023)

A inclusão de tópicos de cibersegurança nos currículos escolares e a implementação de campanhas de consciencialização cibernética são estratégias úteis para preparar a sociedade contra os ciberataques. Instruir e informar a população luandense sobre os riscos do cibercrime, bem como promover a adoção das melhores práticas de segurança, visando a criação de uma cultura digital que inclua todas as esferas da sociedade, podem contribuir significativamente para a redução das vulnerabilidades e, consequentemente, da incidência dos ciberataques. (*Accenture Security*, 2019)

Investir na capacitação profissional é investir na segurança e na resiliência digital da cidade de Luanda. A formação de especialistas em cibersegurança é essencial para se enfrentar os ciberataques e que deve abranger especialistas bem treinados em TIC, polícias, magistrados, especialistas financeiros e demais setores da sociedade para se trabalhar melhor na prevenção, investigação e combate. (*National Institute of Standards and Technology* [NIST], 2020)

O cibercrime exibe um desafio na era digital, especialmente em sociedades com rápido crescimento digital, como a cidade de Luanda, onde o atual cenário dos cibercrimes denunciados não é dos mais favoráveis sendo para tal necessário a realização de estudos multidisciplinares, abordagens proativas e colaborativas na luta contra o cibercrime e permitir o melhor entendimento, prevenção e respostas as ciberameaças para a salvaguarda da segurança e a prosperidade dos seus habitantes. (International Information System Security Certification Consortium [IISSCC], 2020).

Para uma melhor compreensão deste fenómeno na cidade de Luanda, relativamente aos casos denunciados, urge a necessidade de fazer-se a interpretação dos dados recolhidos a partir da aplicação de dois (2) questionários por inquérito: o primeiro, aplicado a especialistas de instituições públicas e privadas (instituições financeiras, especialistas em TIC, polícias, magistrados e instituições de ensino) e o segundo, aplicado ao público geral.

4. MARCO METODOLÓGICO

O marco metodológico é tido como a espinha lombar de qualquer investigação científica, pois constitui o plano detalhado no qual são descritos os passos seguidos

durante a realização da investigação científica com vista a recolha, análise e interpretação dos dados para se responder à pergunta que norteia a investigação. Para tal, é fundamental que esta etapa seja baseada no rigor científico e transparência que devem pautar a conduta do investigador.

4.1 Pergunta de investigação e objetivos

O acesso aos mais variados serviços de *internet* na cidade de Luanda está em rápido crescimento, justificado pela expansão dos serviços de telecomunicações, especialmente da telefonia móvel. No entanto, quando esses serviços são utilizados sem a devida observância das medidas de segurança podem propiciar um ambiente favorável ao cometimento dos cibercrimes, que hoje representam uma ameaça global. Devido à sua natureza, esses crimes tendem a afetar empresas, governos e indivíduos, causando danos económicos, sociais, à confiança, à privacidade e à infraestrutura tecnológica.

Numa investigação é fundamental enunciar uma pergunta de partida que segundo Alvarenga (2012) deve ser levantada de forma interrogatória, pois desta maneira indica diretamente o que estudar e suscita a busca da resposta. Nesta enunciação, deve-se formular o problema no espaço, quer dizer, o contexto físico em que se produzirá o estudo, de forma a se evitar a incoerência e ambiguidade dos fatos.

Aragão (2017) entende que formular o problema

> consiste em dizer, de maneira explícita, clara, compreensível e operacional, qual a dificuldade com a qual nos defrontamos e que pretendemos resolver, limitando o seu campo e apresentando suas características. Desta forma, o objetivo da formulação do problema é torná-lo individualizado, específico e inconfundível. (p. 28)

Para a investigação em causa, levanta-se o seguinte problema de investigação: Como se manifesta o cibercrime denunciado na cidade de Luanda?

Em qualquer pesquisa científica é necessário que sejam definidos os objetivos que a orientam, pois revelam grande importância na escrita de qualquer investigação e projeto científico. Portanto, é por meio deles que se busca responder à pergunta da pesquisa. Nesse sentido, Minayo (2010) afirma que a formulação dos objetivos permite responder ao que é desejado com a pesquisa, ou seja, que intentos o

pesquisador delonga alcançar com a investigação. Deste modo, os objetivos devem ser iniciados com o verbo no infinitivo, o qual deve conter as variáveis com relação direta ao problema da investigação, sendo esta resultado do objetivo geral e que por sua vez desdobra-se nos objetivos específicos que devem ser de fácil entendimento e compreensão.

4.1.1 Objetivo geral

Cervo & Bervian (2002, p. 83) afirmam que no objetivo geral, "[...] procura-se determinar com clareza e objetividade, o propósito do estudante com a realização da pesquisa".

Segundo Alvarenga (2012) "os objetivos gerais, normalmente respondem ao problema genérico, quer dizer, a pergunta substantiva da investigação e referem-se aos resultados esperados da investigação, que para o seu alcance, apoiam-se aos objetivos específicos" (p.19).

Para esta pesquisa, o objetivo geral consiste em descrever como se manifestam os cibercrimes denunciados na cidade de Luanda.

4.1.2 Objetivos específicos

Os objetivos específicos funcionam como degraus de uma escada que levam ao cimo detalhando as etapas concretas e necessárias para o alcance dos propósitos preconizados, devendo eles serem pequenas metas, realistas, estimuladores e detalhadas do objetivo geral. Para este trabalho, temos como objetivos específicos os seguintes:

- **Descrever os principais cibercrimes denunciados na cidade de Luanda**: com este objetivo pretende-se descrever os tipos de cibercrimes denunciados na cidade de Luanda e deste modo permitir que as vítimas facilmente os identificam e sempre que foram alvos de ataque desta natureza possam tomar medidas conducentes na prevenção dos seus danos e relatá-los as autoridades competentes;
- **Descrever os principais alvos dos cibercrimes denunciados na cidade de Luanda**: tenciona-se com este objetivo contribuir nos conhecimentos que as pessoas possuem sobre os alvos preferenciais dos cibercriminosos na cidade de Luanda e assim permitir que as mesmas fiquem mais atentas sobre as

ameaças que enfrentam e ajudarem na promoção, prevenção e na educação sobre a segurança cibernética**;**

- **Descrever as medidas implementadas pelo governo de Angola para o combate aos cibercrimes denunciados na cidade de Luanda**: com esse objetivo tenciona-se saber quais a medidas existentes e implementadas pelo governo de modos a entender-se a eficácia das mesmas para o combate ao cibercrime na cidade de Luanda e as melhorias;
- **Propor recomendações para a prevenção contra os cibercrimes na cidade de Luanda**: no final da pesquisa serão propostas algumas medidas que poderão contribuir na melhoria do entendimento do cibercrime pelos especialistas e a população geral, a sua mitigação e os mecanismos de prevenção.

4.2 Universo e Amostra

Segundo Marconi e Lakatos (2003) a definição do universo ou população é entendida como sendo “o conjunto de seres animados ou inanimados que apresentam pelo menos uma caraterística comum, através do qual o investigador recolherá dados pertinentes para a sua investigação.” (p. 223)

Para Alvarenga (2012) o conceito de população ou universo deve ser entendido como o grupo que fará parte do estudo a ser realizado e que devem apresentar caraterísticas a serem analisadas e formada por pessoas, coisas, animais ou outras comunidades em estudo.

Os conceitos acima mencionados fazem entender que a definição da população constitui o passo que antecede ao processo da definição exata dos elementos com os quais se trabalhará, comummente chamados de amostra. Neste sentido, no entender de Gil (2008, p. 90) a amostra é “um subconjunto do universo ou da população, por meio do qual se estabelecem ou se estimam as caraterísticas desse universo ou população”.

Para Pocinho (2009, p. 11), a amostra resume-se em “um subconjunto retirado da população, que se supõe ser representativo de todas as características da mesma, sobre o qual será feito o estudo, com o objectivo de serem tiradas conclusões validas sobre a população”.

Alvarenga (2012, p. 65): defende que “a amostra é o processo de selecionar uma parte representativa da população para ser estudada”. Normalmente, este processo de

seleção sucede nas pesquisas onde a população é bastante numerosa e por razões de tempo e custos reduz-se a mesma a um subconjunto representativo, cujos resultados da pesquisa deverão ser generalizados à população.

Para a pesquisa em causa e com base aos últimos dados atualizados e publicados pelo Instituto Nacional de Estatística (INE), sobre o recenseamento geral da população e habitação, realizados em 2014, a cidade de Luanda tem uma população de 2.107.648 (dois milhões, cento e sete mil, seiscentos e quarenta e oito habitantes). Para a obtenção da amostra, utiliza-se o método de amostragem simples do tipo não probabilístico, composta pela amostra de especialistas e amostra de sujeitos voluntários, que resultou na participação de 385 (divididos por 115 especialistas de instituições públicas e privadas e 270 indivíduos pertencentes ao público-geral).

4.3 Tipo e Método da Pesquisa

Em função aos objetivos traçados para esta investigação far-se-á um estudo do tipo exploratório, que segundo Zikmund (2000) e Oliveira (2011) geralmente são úteis para diagnosticar situações, explorar alternativas ou descobrir novas ideias e geralmente conduzidos na fase inicial de uma pesquisa em que se procura esclarecer e definir a natureza de um problema de modos a gerar mais informações que possam ser adquiridas para a realização de futuras pesquisas conclusivas, sendo geralmente caracterizadas pela ausência de hipóteses.

Na perspetiva de Severino (2013) a pesquisa exploratória “busca apenas levantar informações sobre um determinado objeto, delimitando assim um campo de trabalho, mapeando as condições de manifestação desse objeto. Na verdade, ela é uma preparação para a pesquisa explicativa”. (p. 107)

Após a realização dos passos anteriores, deve-se definir o enfoque da investigação a ser realizada, que alguns autores classificam como níveis ou alcance da investigação. Esta etapa é fundamental, pois é nela que se estabelecem as estratégias a serem utilizadas ao longo de todo o processo de pesquisa. O estudo em questão terá uma abordagem quantitativa, visando desenvolver uma pesquisa que proporcione a compreensão e o conhecimento sobre os cibercrimes denunciados na cidade de Luanda. Embora seja um campo da informática em que se tem trabalhado há mais de duas décadas, há pouca bibliografia voltada para a realidade angolana, especialmente para a cidade de Luanda. Esse fato pode ser visto como um incentivo para que mais

pesquisadores aceitem o desafio e trabalhem nesta área, enriquecendo-a tanto do ponto de vista teórico quanto prático.

4.4 Justificativa

O histórico dos cibercrimes em Angola, particularmente na cidade de Luanda, tem evoluído na medida que a tecnologia vai crescendo e aumentando o uso e acesso aos dispositivos eletrónicos e aos mais variados serviços de internet, particularmente depois do fim da guerra civil, em 2002, que no entender de Novaes (2011) o crescente uso da internet e a transferência de algumas atividades rotineiras para o ciberespaço são entendidas como a ocorrência de comportamento danoso relacionado com o uso de dispositivos eletrónicos.

Na perspetiva de Guedes e Gomes (2021), o uso massivo dos dispositivos eletrónicos pode promover meios para a consumação de um crime virtual, como a obtenção de informação sigilosa e confidencial de sistema empresarial ou pessoal. Contudo, Campos (2018, p. 14), defende que “apesar dos benefícios do uso massivo dos dispositivos eletrónicos e da internet, apareceram oportunidades de fórum criminal: por um lado as ofensas tradicionais passaram a poder ser praticadas pelos meios informáticos por outro lado a internet fez nascer crimes que não seriam possíveis sem à sua existência”.

Este trabalho insere-se na área temática do cibercrime cujo objeto de estudo da investigação recai sobre o estudo dos cibercrimes denunciados na cidade de Luanda, que por conta do aumento de conectividades com dispositivos móveis e fixos têm proporcionado oportunidades aos cibercriminosos para o cometimento de delitos, maioritariamente com o recurso a ambientes envolvendo serviços *online*. Entre os cibercrimes mais conhecidos na cidade de Luanda estão os ataques de *phishing*, os crimes financeiros, os ataques de *ransomware*, a clonagem de cartões (*skimming*) e as transferências ilícitas.

O Estado tem realizado esforços para a criação e implementação de leis voltadas para o combate e segurança cibernética. Porém, até a altura ainda não existe uma lei específica para o tratamento de crimes deste fórum, sendo normalmente remetido a sua apreciação ao código penal e código processual penal ou em regulamentos que tratam de crimes informáticos, o que muitas das vezes são incapazes de os resolver.

A temática em estudo é revelante, atual e justifica-se o seu estudo na medida que são observados cada vez mais casos de cibercrimes na cidade de Luanda e pretende-se

com esta pesquisa contribuir para o levantamento de dados existentes sobre a temática e, deste modo, contribuir para a melhoria da prevenção, proteção, combate e a elevação da educação cibernética dos cidadãos sobre os crimes desta natureza.

4.5 Procedimentos

Para a conclusão da presente dissertação foi necessário a aprovação do projeto de investigação, por parte do ISCPSI, onde estão contidos os caminhos para a realização final da pesquisa. Aprovado o projeto elaborou-se a revisão da literatura do trabalho e posteriormente um questionário por inquérito dirigido aos especialistas ligados as mais variadas instituições públicas e privadas na cidade de Luanda e outro dirigido à população-geral, em anexo, que foram aplicados *online* e cara a cara. Para tal, foi necessário informar-se os participantes que os questionários eram exclusivamente para a recolha de dados destinados a realização da dissertação de mestrado em criminologia e investigação criminal e que à sua participação era anónima e confidencial, sendo que somente o pesquisador e o orientador teriam acesso os dados catalogados e que não incluem informações pessoais.

Por fim, foi assegurado aos participantes que sua participação na pesquisa era voluntária e não remunerada. Além disso, foi-lhes informado o direito de desistirem do questionário a qualquer momento, sem a necessidade de justificativa. Após lerem o termo de consentimento eletrónico, os participantes foram solicitados a fornecer sua aceitação na plataforma, para que pudessem responder aos questionários.

4.6 Técnicas de recolha de dados, instrumentos e técnicas de processamento

Para entender melhor o fenómeno do cibercrime na cidade de Luanda, foi necessário estudar os conceitos das teorias gerais do crime, dos cibercrimes e da cibersegurança. Dessa forma, realizou-se a colheita de obras, relatórios e publicações oficiais sobre a temática, complementada pela aplicação de questionários de inquérito, que foram registados automaticamente nos formulários eletrónicos criados na plataforma Google Forms. A recetividade aos questionários foi razoável, considerando que nem todos estão sempre disponíveis para participar de estudos académicos, e alguns foram substituídos.

Considerando as limitações bibliográficas e as características desta pesquisa, ela consiste numa investigação com enfoque quantitativo de caráter descritivo que, segundo Alvarenga (2012, p. 40), “está direcionada a determinar como são ou como

se manifestam as variáveis em uma determinada situação. Procura descrever os fenômenos em estudo, que podem ou não ser profundos".

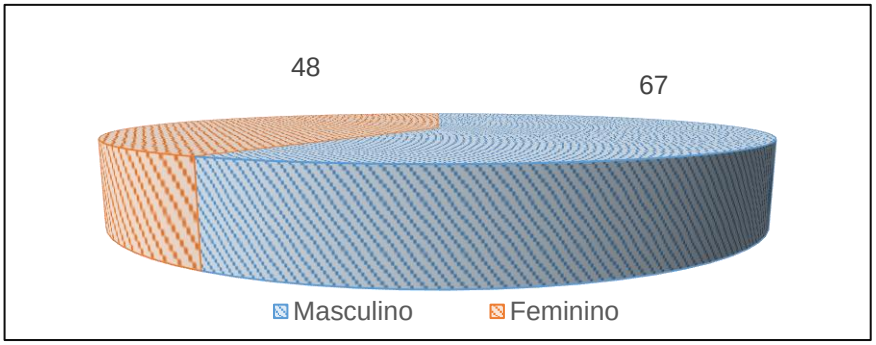
Os resultados foram apresentados e interpretados por meio da análise de amostras estatísticas (gráficos e tabelas), garantindo a total fidelidade e veracidade da pesquisa, com o auxílio de duas ferramentas eletrónicas: SPSS e Microsoft Office Excel.

5. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo serão apresentados os dados recolhidos da aplicação de dois (2) questionários por inquérito (um aplicado aos especialistas ligados a instituições públicas e privadas e outro aplicado a população geral) e em seguida à interpretação dos dados, bem como à sua relação com a revisão da literatura, de modo a responder à pergunta de investigação.

As análises dos dados obtidos dos dois (2) questionários serão feitas em separado. Num primeiro momento será realizada a análise e discussão dos resultados obtidos por meio do questionário dirigido aos especialistas de instituições públicas e privadas. Em seguida, serão analisados os resultados do questionário aplicado à população em geral. No que concerne ao questionário dirigido aos especialistas de instituições públicas e privadas, ele foi respondido por 115 indivíduos, sendo 67 (58,3%) do sexo masculino e 48 (41,7%) do sexo feminino, conforme ilustrado no Gráfico 3.

Gráfico 3: Sexo (especialistas)



Em função ao público-alvo, composto pelos especialistas (Tabela 1), as instituições financeiras tiveram a assiduidade de 19 (16,5%) pessoas, os especialistas em TIC tiveram a participação de 29 (25,2%) elementos, os polícias têm a frequência de 23 (20,0%) efetivos, os magistrados estão representados por 18 (15,7%) entidades e as instituições de ensino responderam 23 (22,6%) elementos.

Tabela 1: Público-Alvo (especialistas)

		Frequência	percentagem	percentagem válida	Percentagem acumulativa
Válido	Instituições Financeiras	19	16,5	16,5	16,5
	Especialistas em TIC	29	25,2	25,2	41,7
	Polícias	23	20,0	20,0	61,7
	Magistrados	18	15,7	15,7	77,4
	Instituições de Ensino	26	22,6	22,6	100,0
	Total	**115**	**100,0**	**100,0**	

As idades dos inqueridos foram organizadas por intervalos (Tabela 2). O primeiro intervalo compreende a faixa etária entres os 18 – 27 anos de idade e teve a participação de 18 (15,7%) inqueridos, o segundo intervalo compreende a faixa dos 28 – 37 anos de idade e teve a aceitação de 39 (33,9%) indivíduos, o terceiro intervalo compreende entre os 38 – 47 anos de idade e contou com participação de 45 (39,1%) personalidades e o quarto intervalo compreende a faixa composta por indivíduos com a idade igual ou superior aos 48 anos de idade e teve a frequência de 13 (11,3%) pessoas.

Para a amostragem dos especialistas, e considerando o caráter técnico de algumas questões, bem como a idade mínima de 18 anos de idade, estabelecida pela Lei Geral do Trabalho em Angola para o exercício de atividades laborais remuneradas, foi definida como a idade mínima. Para além disso, foram considerados elegíveis todos os especialistas vinculados nas instituições que compõem o estudo, desde que cumprissem os demais requisitos estabelecidos por cada instituição para o desempenho das respetivas funções.

Tabela 2: Idade (especialistas)

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	18 - 27	18	15,7	15,7	15,7
	28 - 37	39	33,9	33,9	49,6
	38 - 47	45	39,1	39,1	88,7
	Maior ou igual a 48	13	11,3	11,3	100,0
	Total	**115**	**100,0**	**100,0**	

Quanto ao quesito grau académico (Tabela 3), os inquiridos foram organizados em quatro (4) grupos, nomeadamente: Médio (12º Ano), Licenciatura, Mestrado e Doutorado. O grupo correspondente ao Médio (12º Ano) teve a aderência de 15 (13,0%) indivíduos, a classe dos Licenciados teve a participação de 65 (56,5%) pessoas, o grupo correspondente a Mestres teve a frequência de (27,8%)

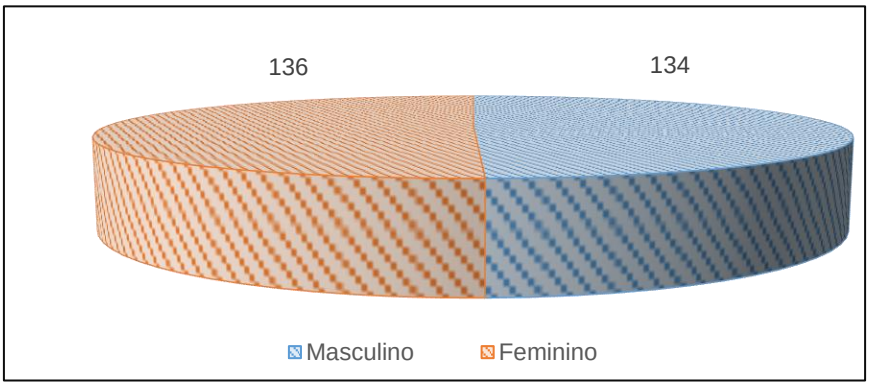
intervenientes e a classe correspondente aos Doutorados teve a frequência de 3 (2,6%) indivíduos.

Tabela 3: Grau Académico (especialistas)

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Médio (12° Ano)	15	13,0	17,0	13,0
	Licenciatura	65	56,5	52,6	69,6
	Mestrado	32	27,8	16,7	97,4
	Doutorado	3	2,6	5,9	100,0
	Total	**115**	**100,0**	**100,0**	

Quanto ao questionário referente ao público-geral, foi aplicado a 270 participantes (Gráfico 4), sendo 134 (49,6%) do sexo masculino e 136 (50,4%) do sexo feminino, correspondendo a 100% do público-alvo.

Gráfico 4: Sexo (público-geral)



Em relação às faixas etárias do público geral, foram organizadas em intervalos. O primeiro intervalo compreende indivíduos entre 8 e 17 anos de idade, com a participação de 6 voluntários (2,2%). O segundo intervalo abrange idades entre 18 e 27 anos de idade, contou com a participação de 75 indivíduos (27,8%). O terceiro intervalo contempla indivíduos com idade compreendida entre os 28 e 37 anos, com 101 participantes (37,4%). O quarto intervalo inclui indivíduos entre os 38 e 47 anos, com 71 participantes (26,3%). O quinto intervalo contempla indivíduos com 48 anos de idade ou mais, que teve a participação de 17 pessoas (6,3%), conforme apresentado na Tabela 4.

A idade mínima deste grupo em análise, fixou-se nos 8 anos de idade, uma vez que, com os avanços da tecnologia, crianças têm tido contato com o mundo digital cada vez mais cedo, especialmente com os serviços de *internet*, e fruto disso, muitas vezes acabam fornecendo informações pessoais de forma fidedigna, sem terem a

consciência dos riscos envolvidos, o que ressalta a importância da educação cibernética desde a infância.

Tabela 4: Idade (público-geral)

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	8 a 17	6	2,2	2,2	2,2
	18 a 27	75	27,8	27,8	30,0
	28 a 37	101	37,4	37,4	67,4
	38 a 47	71	26,3	26,3	93,7
	Maior ou igual a 48	17	6,3	6,3	100,0
	Total	**270**	**100,0**	**100,0**	

No questionário aplicado ao público-geral, também é analisado o quesito grau de escolaridade dos inqueridos, tendo para tal sido organizados em cinco (5) grupos, nomeadamente: Básico (9º Ano), Médio (12º Ano), Licenciatura, Mestrado e Doutorado. O agregado composto por elementos que possuem o ensino Básico (9º Ano) teve uma participação de 21 (7,8%) indivíduos, os indivíduos com o grau de ensino Médio (12º Ano) participaram por 46 (17,0%) ocasiões, os indivíduos com o grau de Licenciado responderam por 142 (52,6%) ocasiões, os inqueridos com o grau académico de Mestre tiveram a participação de 45 (16,7%) elementos e por último a classe dos que possuem o nível académico de Doutorado, tiveram a frequência de 16 (5,9%) elementos (Tabela 5).

Tabela 5: Grau Académico (público-geral)

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Básico (9° Ano)	21	7,8	7,8	7,8
	Médio (12° Ano)	46	17,0	17,0	24,8
	Licenciatura	142	52,6	52,6	77,4
	Mestrado	45	16,7	16,7	94,1
	Doutorado	16	5,9	5,9	100,0
	Total	**270**	**100,0**	**100,0**	

5.1 Estudo 1 - Perceção dos especialistas sobre a situação do cibercrime na cidade de Luanda

Para o melhor andamento da investigação foram realizadas perguntas com vista a reponderem aos objetivos traçados e a pergunta que norteia a investigação, por intermédio da aplicação de questionário por inquérito dirigido aos especialistas de instituições públicas e privadas.

A cidade de Luanda tem sido palco de crimes desta natureza. Sobre esta temática, dos 115 especialistas que compõem a amostra da população em estudo a descrição

que fazem sobre a atual situação do cibercrime na cidade de Luanda resulta que 78 (67,8%) participantes disseram que a situação é perigosa, 32 (27,8%) intervenientes acreditam que seja regular e 5 (4,3%) dos inqueridos não têm a noção ou são indecisos.

Tabela 6: Situação atual do cibercrime na cidade de Luanda

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Perigosa	78	67,8	67,8	67,8
	Regular	32	27,8	27,8	95,7
	Não sei/Indeciso	5	4,3	4,3	100,0
	Total	**115**	**100,0**	**100,0**	

Analisando os resultados, no entendimento da maioria dos especialistas, 78 (67,8%), a situação atual do cibercrime na cidade de Luanda é perigosa, pois os casos de cibercrimes denunciados tendem a crescer, o que vai em concordância com os dados do relatório da DCCI (Gráfico 1). Assim, ao afirmarem que a situação do cibercrime na cidade de Luanda é perigosa, entende-se que por serem especialistas na matéria e trabalharem em diferentes instituições, públicas e privadas, são conhecedores da realidade sobre a qualidade das infraestruturas tecnológicas existentes capazes de fazerem face ao cibercrime, conhecem dados não tornados público sobre a incidência dos cibercrimes e as vulnerabilidades que têm sido exploradas pelos cibercriminosos de modo a atingirem os seus objetivos, e por conta disso, tornam perigosa a situação do cibercrime em Luanda. Em suma, o atual ambiente do cibercrime na cidade de Luanda é propenso para a degradação e comprometimento da proteção dos dados pessoais, financeiros, desestimulo da economia digital e a frágil proteção da infraestrutura tecnológica.

Definir o principal alvo dos cibercrimes denunciados na cidade de Luanda não é uma tarefa simples, pois os cibercriminosos adaptam os seus *modus operandi* de acordo aos objetivos que desejam alcançar. No entanto, quando questionados os 115 especialistas de instituições públicas e privadas que compõem a amostra da investigação, resultou que 28 (24,3%) dos participantes acreditam que o principal alvo dos cibercrimes na cidade de Luanda são as instituições públicas, 37 (32,2%) consideram que sejam as instituições financeiras, 41 (35,7%) apontam a população como o principal alvo e 9 (7,8%) indicam as empresas petrolíferas como o foco dos ataques.

Tabela 7: Principal alvo dos cibercrimes na cidade de Luanda

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Instituições Públicas	28	24,3	24,3	24,3
	Instituições Financeiras	37	32,2	32,2	56,5
	População	41	35,7	35,7	92,2
	Empresas Petrolíferas	9	7,8	7,8	100,0
	Total	**115**	**100,0**	**100,0**	

Os dados demonstram que a maioria dos especialistas, 41 (35,7%), considera que a população é o principal alvo dos cibercrimes denunciados na cidade de Luanda. Apesar do relatório da DCCI não revelar sobre qual o alvo preferencial dos cibercrimes na cidade de Luanda, os dados resultantes do questionário vão ao encontro com o espelhado no Gráfico 2 (sobre a incidência criminal) na medida que a burla informática tem sido a via pela qual os cibercriminosos têm maioritariamente atingido as suas vítimas, em peculiar a população geral que concomitantemente são os maiores consumidores de conteúdos tecnológicos.

Com o processo da globalização e, mais recentemente, o confinamento imposto pela pandemia da COVID-19, a interação e o trabalho entre a população luandense mudaram significativamente, pois muitos serviços passaram a ser exclusivamente oferecidos de forma digital e outros de forma híbrida. Entretanto, a baixa literacia digital no seio dos habitantes da cidade de Luanda facilita a exploração das vulnerabilidades pelos ciberatacantes, em busca de lucro fácil. Para tal, é urgente o fortalecimento da literacia digital no seio da população de modo a ajudar na diminuição gradual da incidência desses crimes e, consequentemente, reduzir os danos causados pela partilha inadvertida de informações pessoais.

A compreensão da forma mais comum da manifestação do cibercrime na cidade de Luanda é fundamental, pois ajuda no desenvolvimento de estratégias eficazes para o seu combate. Assim, questionados os 115 especialistas que compõem a amostra de diferentes instituições públicas e privadas os resultados mostraram que 33 (28,8%) indicaram o *ransomware*, 17 (14,8%) apontaram clonagem de cartões/*skimming*, 7 (6,1%) destacaram os crimes financeiros, 46 (40,0%) identificaram o *phishing* e 12 (10,4%) mencionaram as transferências ilícitas.

Tabela 8: Tipo mais comum de cibercrime denunciado na cidade de Luanda

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	*Ransomware*	33	28,7	28,7	28,7
	Clonagem de cartões/*Skimming*	17	14,8	14,8	43,5
	Crimes Financeiros	7	6,1	6,1	49,6
	Phishing	46	40,0	40,0	89,6
	Transferências ilícitas	12	10,4	10,4	100,0
	Total	**115**	**100,0**	**100,0**	

Olhando para os dados da tabela, nota-se que a maioria dos especialistas, 46 (40,0%), considera que o *phishing* é o tipo mais comum de cibercrime denunciado na cidade de Luanda, o que representa preocupação acrescida na medida que se assiste maior uso de dispositivos eletrónicos com acesso a diferentes plataformas de compras *online* e físicas bem como a progressiva substituição da moeda física e dos cheques pelos cartões de débito/crédito em diferentes transações e operações bancárias.

Para o sucesso deste tipo de ataque, os cibercriminosos enviam *links* fraudulentos para os *e-mails* e dispositivos eletrónicos das vítimas, como se fossem provenientes das reais instituições, e que tão logo sejam abertos transferem informações para uma base de dados criada pelos criminosos. Com o sucesso desse tipo de ataque, os cibercriminosos conseguem fazer a clonagem os cartões, invadirem SI das instituições e que podem levar a consumação do *ransomware* (consequentemente o bloqueio total ou parcial de um SI e o respetivo pedido de resgate).

Diante desse cenário, é fundamental que se intensifiquem esforços para a consciencialização e educação da população sobre os cuidados necessários para se diminuir o sucesso desse *modus operandi*.

Os cibercrimes hoje representam uma ameaça para qualquer empresa, organização, Estados e pessoas singulares. Contudo, quando questionados os 115 especialistas de diferentes instituições públicas e privadas que participam do estudo sobre o tipo de cibercrime que consideram ameaçador para a sua instituição, redundou que 25 (21,7%) entendem ser o *ransomware,* 48 (41,7%) indigitaram o *phishing*, 22 (19,1%) escolheram a fraude financeira, 19 (16,5%) indicaram a Clonagem de cartões e 1 (0,9%) indicou nenhum.

Tabela 9: Tipo de cibercrime ameaçador para a instituição

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	*Ransomware*	25	21,7%	21,7%	21,7%
	Phishing	48	41,7%	41,7%	63,5%
	Fraude Financeira	22	19,1%	19,1%	82,6%
	Clonagem de cartões	19	16,5%	16,5%	99,1%
	Nenhum	1	0,9%	0,9%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Os resultados da tabela em epígrafe denotam quem a maioria dos especialistas, 48 (41,7%), considera que o ataque por *phishing* é o tipo de cibercrime que maior ameaça representa para as instituições onde trabalham. A avaliação que se pode fazer a este cenário recai sobre o fraco investimento na capacitação dos recursos humanos e na infraestrutura tecnológica (dispositivos físicos, lógicos, protocolos e formações) existente nas instituições para a proteção dos seus SI, mesmo sabendo que na atualidade a internet é quase de uso obrigatório, especialmente para a atualização dos SI e a manutenção das correspondências por *e-mail*, meio pelo qual os cibercriminosos tendem a atrair vítimas de maneiras a pescarem informações confidenciais, por conta do fraco domínio dos funcionários na identificação deste tipo de ataque e a não existência de filtros de bloqueio automático capazes de ativarem alertas.

O sentimento de que os ataques de *phishing* sejam os mais assustadores nas instituições públicas e privadas na cidade de Luanda tem suporte quando analisada a questão das medidas de segurança aplicadas na cidade de Luanda, pois o fator humano e o tecnológico não são tidos como primordiais na defesa contra este fenómeno e que conjugados permite a fácil entrada e sucesso do *phishing*, pois facilmente os funcionários destas instituições fazem a abertura de *links* fraudulentos, confundindo serem provenientes de fontes seguras.

Com relação a natureza dos dados que as instituições manejam e que podem estar vulneráveis aos cibercrimes, indagados os 115 especialistas afetos as instituições públicas e privadas e que participam do estudo, resultou que 10 (8,7%) acreditam que as suas instituições sejam pouco vulneráveis, 59 (51,3%) acreditam que as suas instituições encontram-se muito vulneráveis, 44 (38,3%) são de opinião que as suas instituições estejam moderadamente vulneráveis e 2 (1,7%) afirmam que as suas instituições não estejam vulneráveis.

Tabela 10: Vulnerabilidade aos cibercrimes pelos dados que a instituição maneja

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Pouco vulnerável	10	8,7	8,7	8,7
	Muito vulnerável	59	51,3	51,3	60,0
	Moderadamente vulnerável	44	38,3	38,3	98,3
	Não vulnerável	2	1,7	1,7	100,0
	Total	**115**	**100,0%**	**100,0%**	

Os resultados demonstram que a maioria dos especialistas, 59 (51,3%), considera que em função aos dados que a instituição manipula ela está muito vulnerável aos cibercrimes, podendo-se entender que os dados manipulados pelas empresas são bastante valiosos e desejáveis para os cibercriminosos e por conta disso tentam a todo o custo a cessar aos mais variados SI das organizações para saquearem os dados. Para tal, é necessário que as empresas deem maior importância aos dados que manipulam e invistam na modernização tecnológica (fazendo atualizações constantes de *software*, segmentação da rede, configurações adequadas dos SI e a gestão de acessos), a implementação de políticas de criptografia de dados, definição de políticas claras de recuperação de dados e a elaboração de um plano interno de resposta contra os cibercrimes.

As combinações destes mecanismos permitem maior envolvência humana e tecnológica, mitigação das vulnerabilidades, manutenção e preservação das informações (financeiras, propriedade intelectual, dados pessoais e projetos futuros) que são elementos preponderantes para a segurança e confiança dos clientes e a manutenção do funcionamento da instituição.

Relativamente aos e-crimes, hoje são uma realidade e representam as atividades ilícitas cometidas no mundo virtual e que podem ser dos mais simples aos mais sofisticados. Com relação a isso, no que concerne as medidas de segurança cibernética que são tomadas em resposta aos e-crimes na cidade de Luanda, dos 115 especialistas das instituições públicas e privadas que participam da investigação redundou que 49 (42,6%) consideram a criação de leis ser a medida de segurança cibernética tomada em resposta aos e-crimes na cidade de Luanda, 15 (13,0%) consideram serem as formações, 22 (19,1%) disseram ser a sensibilização da população, 1 (0,9%) afirmou ser o investimento em infraestruturas tecnológicas e 4 (3,5%) entendem não existir nenhuma medida.

Tabela 11: Medidas de segurança cibernética em resposta aos i-crimes

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Criação de Leis	49	42,6	42,6	42,6
	Formações	15	13,0	13,0	55,7
	Cooperação	22	19,1	19,1	74,8
	Sensibilização da População	24	20,9	20,9	95,7
	Investimentos em infraestruturas tecnológicas	1	0,9	0,9	96,5
	Nenhum	4	3,5	3,5	100,0
	Total	**115**	**100,0**	**100,0**	

Perlustrando os resultados da tabela a maioria, 49 (42,6%), considera que a criação de leis tem sido a medida privilegiada para a manutenção da segurança cibernética em resposta aos e-crimes na cidade de Luanda. A opinião dos especialistas é analisada soba a perspetiva de que a criação de leis visa regulamentar o normal funcionamento, defender as vítimas e punir os seus praticantes de formas a desestimular os seus atos. Contudo, o país ainda não possui uma lei específica sobre os cibercrimes e socorre do código penal, livro branco das tecnologias de informação e de comunicação, a Lei nº. 7/17 (sobre a proteção das redes e sistemas informáticos), a convenção de Malabo (adotada pela União Africana) sobre segurança cibernética e proteção de dados pessoais e a Lei n.º 23/11 (sobre as comunicações electrónicas e dos serviços da sociedade da informação).

O entendimento que os especialistas apontam sobre a criação de leis como a medida privilegiada para a manutenção da segurança cibernética em resposta aos e-crimes na cidade de Luanda não corresponde ao que na realidade se vive, uma vez que não se deve confundir a lei dos crimes informáticos como a lei dos cibercrimes, pois os crimes informáticos são uma tipologia específica dos cibercrimes e a lei a si aplicável nem sempre consegue resolver na plenitude dos casos de cibercrimes, razão pela qual o país ainda se esboça na edificação de projetos com vista a criação de uma lei específica aos cibercrimes.

A segurança cibernética é um compromisso de todos e deve ser coberta pela monitorização e detenção de cibercrimes com vista a proteção e manutenção dos dados e dos SI. Quanto a forma como é feita a monitorização e detenção de possíveis atividades de cibercrimes nos SI das instituições onde trabalham os 115 especialistas que fazem parte do estudo em causa, os resultados ilustram que 27 (23,5%) apontaram o fluxo de dados, 23 (20,0%) indigitaram o controlo de acesso lógico, 34 (29,6%) assinalaram o controlo de acesso físico, 1 (0,9%) indicou que não é feita, 29

(25,2%) disseram nenhuma e 1 (0,9%) respondeu serem todas as formas apresentadas.

Tabela 12: Monitorização e detenção de cibercrimes nos SI da instituição

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Análise do fluxo de dados	27	23,5%	23,5%	23,5%
	Controlo de Acesso Lógico	23	20,0%	20,0%	43,5%
	Controlo de Acesso Físico	34	29,6%	29,6%	73,0%
	Não sei	1	0,9%	0,9%	73,9%
	Nenhuma	29	25,2%	25,2%	99,1%
	Todas	1	0,9%	0,9%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Os resultados expõem que a maioria dos especialistas, 34 (29,6%), aponta o controlo de acesso físico (cartões de acesso, leitores biométricos, catracas electrónicas, sistemas de videovigilância e chave eletrónica), como a forma mais utilizada para a controlo e detenção de possíveis atividades de cibercrimes nos SI das instituições onde trabalham. O controlo de acesso físico é um investimento crucial e essencial para qualquer organização que pretenda precaver-se dos cibercrimes, pois elementos internos das organizações constituem potencial ameaça, pois podem ser vítimas de pressões e em função a sua facilidade de acesso as zonas reservadas podem ilicitamente extrair informações importantes da empresa. Para tal, é necessário que seja mantido o controlo de todos os elementos que entram e saem, através da validação da identificação dos usuários por intermédio de programas informáticos desenhados para tal e reduzirem-se os riscos de roubo e sabotagem.

A implementação de medidas de segurança cibernética garante a proteção e valorização dos dados, do negócio, maior confiança na segurança interna da instituição, evita as interrupções de fornecimento de serviços e aumenta a lealdade dos clientes.

Quanto a estratégia de recuperação dos dados utilizada para fazer face aos possíveis ataques de cibercrime nas instituições públicas e privadas onde trabalham os 115 especialistas que participam do estudo, adveio que 22 (19,1%) apontaram o *backup*, 12 (10,4%) indicaram a redundância, 13 (11,3%) disseram ser a política de gestão de dispositivos, 5 (4,3%) apontaram a criptografia, 18 (15,7%) afirmaram ser o *firewall*, 19 (16,5%) declararam ser o controlo de acesso, 25 (21,7%) afirmaram a utilização de duas ou mais estratégias e 1 (0,9%) afirmou não saber.

Tabela 13: Estratégia de proteção e recuperação de dados pela empresa

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Backup	22	19,1%	19,1%	19,1%
	Redundância	12	10,4%	10,4%	29,6%
	Política de Gestão de Dispositivos	13	11,3%	11,3%	40,9%
	Criptografia	5	4,3%	4,3%	45,2%
	Firewall	18	15,7%	15,7%	60,9%
	Controlo de acesso	19	16,5%	16,5%	77,4%
	Duas ou mais estratégias	25	21,7%	21,7%	99,1%
	Não sei	1	0,9%	0,9%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Os dados da tabela em intitule, ilustra que a maior parte dos especialistas, 25 (21,7%), é de opinião que a utilização de duas ou mais estratégias para a proteção e recuperação de dados tem sido o estratagema mais utilizada para se fazer face a possíveis ataques de cibercrime nas instituições onde trabalham. As ameaças cibernéticas estão em constantes mutações (a estratégia hoje tida como infalível pode não responder em curto espaço de tempo) devendo para tal a segurança cibernética ser encarada como um desafio persistente, pois não existe estratégia que isoladamente possa ser apontada como a melhor para a proteção dos SI contra os cibercrimes.

A opinião dos especialistas é suportada no sentido que a combinação de estratégias de proteção permite a elevação dos níveis de segurança e confiança cibernética, pois visam adicionar camadas de segurança que dificultam o processo de invasão dos cibercriminosos. Todavia, nem sempre as empresas optam pela utilização de defesas combinadas, pois envolve custos económicos adicionais.

Em suma, é necessário que em todo este processo seja acompanhado pelo fator humano no seio da organização, na medida que por melhor que sejam os mecanismos de defesa as ações do homem podem comprometer o sistema todo.

Relativamente a existência de políticas de cibersegurança claras e acessíveis a todos os funcionários na instituição, dos 115 especialistas das instituições públicas e privadas que participam do estudo emergiu que 12 (10,4%) disseram que existem, 76 (66,1%) afirmaram que não existem, 16 (13,9%) declararam que existem parcialmente e 11 (9,6%) disseram não saberem.

Tabela 14: Políticas de cibersegurança acessíveis aos funcionários

			Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Sim		12	10,4%	10,4%	10,4%
	Não		76	66,1%	66,1%	76,5%
	Parcialmente		16	13,9%	13,9%	90,4%
	Não sei		11	9,6%	9,6%	100,0%
	Total		**115**	**100,0%**	**100,0%**	

A gestão de acesso as políticas de cibersegurança podem variar em cada instituição e com base a fatores como o nível de maturidade de cibersegurança, o tamanho da empresa e o setor no qual opera. Os resultados da tabela em epígrafe mostram que a maioria dos especialistas, 76 (66,1%), afirma que nas instituições onde trabalham não existem políticas de cibersegurança claras e acessíveis a todos os funcionários. Este cenário é inquietante uma vez que com a não presença dessas políticas, que redonda na falta do seu conhecimento por parte dos funcionários, pode permitir a ilibação de funcionários que cometam cibercrimes voluntários/involuntários uma vez que pode ser alegado o desconhecimento da existência da obrigatoriedade do funcionário na observância de condutas com vista a salvaguarda da instituição. Para além disso, contribui na fraca consciencialização dos funcionários sobre a matéria e aumenta os riscos de incidentes desta natureza.

Em suma, é importante que as organizações criem, disponibilizem e atualizem os regulamentos das suas políticas de cibersegurança de modo a estarem acessíveis a todos os funcionários, com publicações nos portais internos, reuniões, treinos, *e-mails*, *intranet*[32] e outros meios de comunicação interna, contendo informações como: o objetivo geral das políticas, os procedimentos, os encargos individuais, as áreas e as infraestruturas abrangidas.

Com relação a existência de protocolos que visam dar respostas imediatas em caso de ciberataques, quando consultado os 115 especialistas de instituições públicas e privadas que participam do estudo em causa adveio que 13 (11,3%) afirmaram que as suas instituições possuem esse protocolo, 77 (67,0%) defenderam que as suas instituições não possuem este protocolo e 25 (21,7%) não sabem se existe ou não este protocolo nas suas instituições.

[32] Rede de computadores privada que assenta sobre protocolos da i*nternet*, mas de uso exclusivo de um determinado local e que só pode ser a cessada pelos seus utilizadores ou colaboradores internos.

Tabela 15: Protocolo para resposta imediato ao ciberataque na instituição

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Sim	13	11,3%	11,3%	11,3%
	Não	77	67,0%	67,0%	78,3%
	Não sei	25	21,7%	21,7%	100.0%
	Total	**115**	**100,0%**	**100,0%**	

Os dados contidos na tabela acima relevam que a maioria dos especialistas, 77 (67,0%), revelaram não existir um protocolo nas suas instituições que possa servir de guião e facilitar a resposta imediata em casos de ciberataques. A situação afigura-se preocupante uma vez que o cibercrime é um fenómeno em ascensão e a falta de um guião nas instituições, facilita a tardia detenção dos ataques, degradação da reputação da instituição, a propagação dos danos nos SI e a consequente perda de dados.

Um protocolo com respostas rápidas aos ciberataques deve ser um plano bem definido de modo a preparar os funcionários a enfrentarem os desafios inerentes a cibersegurança e assim tornarem-se na primeira barreira de segurança. Contudo, é fundamental que haja a envolvência de todos na elaboração deste protocolo e constantemente procurar-se fazer a sua atualização, fazer-se a consultar regular dos especialistas entendidos na matéria para ser averiguada a sua conformidade e a aplicação regular de testes de simulação para serem identificadas as possíveis falhas existentes no protocolo e a sua rápida conformação.

Sobre a frequência com que são realizados os treinamentos relativos a cibersegurança aos funcionários da instituição, quando questionados os 115 especialistas das instituições públicas e privadas que participam do estudo em mote, resultou que 6 (5,2%) participantes disseram serem feitos diariamente, 10 (8,7%) especialistas afirmam serem feitos mensalmente, 9 (7,8%) inqueridos comentaram serem feitos trimestralmente, 18 (15,7%) participantes declaram serem realizados anualmente e 72 (62,6%) questionados disseram que nunca são feitos estes treinamentos.

Tabela 16: Treinamento de segurança cibernética aos funcionários

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Diariamente	6	5,2%	5,2%	5,2%
	Mensalmente	10	8,7%	8,7%	13,9%
	Trimestralmente	9	7,8%	7,8%	21,7%
	Anualmente	18	15,7%	15,7%	37,4%
	Nunca	72	62,6%	62,6%	100,0%
	Total	**115**	**100.0%**	**100.0%**	

Os resultados contidos na tabela em mote revelam que a maioria dos especialistas, 72 (62,6%), referem que nas suas instituições não são realizados treinamentos de segurança cibernética dirigida aos funcionários. O treinamento sobre a segurança cibernética numa instituição (pequena, média ou grande) é fundamental, pois funciona como um elemento adicional com vista a proteção dos dados e permite a reciclagem regular dos conhecimentos, por parte dos funcionários, sobre matérias de cibersegurança e cibercrimes. Deste modo, urge a necessidade de as instituições públicas e privadas na cidade de Luanda, trabalharem na capacitação contínua dos seus recursos humanos para a manutenção dos níveis de cibersegurança, prevenção dos incidentes, redução dos custos, criação de uma cultura de segurança, proteção da reputação da empresa e o aumento da confiança dos clientes e investidores.

Quanto a frequência com que são feitas as atualizações das políticas de cibersegurança nas instituições onde trabalham os 115 especialistas que participam do estudo, emerge que 13 (11,3%) responderam que são feitas trimestralmente, 13 (11,3%) retorquiram que são realizadas anualmente, 4 (3,5%) disseram ser feitas a cada dois anos e 85 (73,9%) argumentaram que nunca são feitas.

Tabela 17: Atualização das políticas de cibersegurança

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Semestralmente	13	11,3%	11,3%	11,3%
	Anualmente	13	11,3%	11,3%	22,6%
	A cada dois anos	4	3,5%	3,5%	26,1%
	Nunca	85	73,9%	73,9%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Sobre a questão em causa, os resultados da tabela em epígrafe demostram que a maioria dos especialistas, 85 (73,9%), dizem que nas instituições onde prestam serviços não são feitas as atualizações das políticas de cibersegurança, o que revela ser uma situação preocupante, pois patenteiam as vulnerabilidades da instituição aos e ataques cibernéticos.

A atualização das políticas de cibersegurança é um processo que deve ser feito continuamente e alinhado com as melhores práticas. Entende-se que não seja uma situação fácil, pois envolve custos onerosos, mas é fundamental que se trabalha na segurança e revisão constante das atualizações e das políticas de cibersegurança com a implementação de restrições de acesso aos conteúdos não seguros de *internet*, a alteração regular de senhas, o controlo de acesso remoto, o controlo dos dispositivos

conectados a rede, a monitorização do acesso a *cloud computing*, a revisão da base de dados e a realização de *backup*.

Sobre o nível de treinamento e preparação das autoridades locais para lidarem com o cibercrime, a opinião dos 115 especialistas de instituições públicas e privadas adveio que 75 (65,2%) consideram que o treinamento e a preparação são inadequados, 34 (29,6%) afirmaram que sejam moderadamente adequados e 6 (5,2%) são de opinião que o treinamento e a preparação são adequados.

Tabela 18: Treinamento e preparação das autoridades locais

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Inadequado	75	65,2%	65,2%	65,2%
	Moderadamente adequado	34	29,6%	29,6%	94,8%
	Adequado	6	5,2%	5,2%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Os dados da questão em estudo revelam que no entendimento da maioria dos especialistas, 75 (65,2%), o nível de treinamento e preparação das autoridades locais para lidarem com o cibercrime é inadequado. A complexidade no entendimento e combate dos cibercrimes exige das autoridades locais uma melhor e constante preparação para melhor trabalharem em investigações que possam conduzir a raiz da questão e dos seus praticantes. Infelizmente em países subdesenvolvidos, caso de Angola e em particular a cidade de Luanda, ainda é grande a carência de especialistas ligados a matéria de cibercrimes e cibersegurança que muito poderiam contribuir para a melhor preparação de outros especialistas. Em consequência, muitos profissionais que lidam e dirigem setores e departamentos de segurança pública revelam pouco domínio e conhecimentos nesta matéria, o que dificulta no processo de investigação e tomada de decisões.

Dada a complexidade deste fenómeno, à sua investigação exige das autoridades locais e dos profissionais o conhecimento de matérias relacionadas a criptografia, análise forense computacional e legislações. Para tal, é necessário que o poder local trabalhe para o reforço dos saberes nesta matéria e permitir o aumento do poder da prevenção e proteção local.

Com relação ao principal desafio para o combate do cibercrime na cidade de Luanda, na opinião dos 115 especialistas de instituições públicas e privadas que participam do estudo em questão emerge que 28 (24,3%) apontam a falta de legislação específica, 35 (30,4%) acreditam ser a falta de recursos tecnológicos, 45 (39,1%) apontam a falta

de formação especializada, 6 (5,2%) acreditam ser o pouco interesse política e 1 (0,9%) acredita serem todas as opções indicadas.

Tabela 19: Principal desafio para o combate ao cibercrime na cidade de Luanda

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Falta de legislação específica	28	24,3%	24,3%	24,3%
	Falta de recursos tecnológicos	35	30,4%	30,4%	54,8%
	Falta de formação especializada	45	39,1%	39,1%	93,9%
	Pouco interesse política	6	5,2%	5,2%	99,1%
	Todas	1	0,9%	0,9%	100,0%
	Total	**115**	**100,0%**	**100,0%**	

Face a rápida evolução tecnológica mundial, a transnacionalidade dos cibercrimes e a elevada dependência tecnológica retiram a simplicidade do seu combate em qualquer sociedade. No questão em estudo, os dados da tabela em mote demostram que a maioria dos especialistas, 45 (39,1%), convergem na ideia de que a falta de formação especializada seja o principal desafio para o combate ao cibercrime na cidade de Luanda. Infelizmente, existe uma crescente demanda de profissionais com conhecimentos especializados em cibercrimes na cidade de Luanda, pois a sua formação leva tempo e recursos financeiros que nem sempre estão à disposição. Para além do fator humano também deve ser levado a sério o contínuo investimento nas infraestruturas tecnológicas que devem ser adaptadas a realidade atual.

Com base aos fatores mencionados e atendendo a débil situação sócio económico do país, a cidade de Luanda em particular, existe a possibilidade de as instituições públicas e privadas continuarem a enfrentar a escassez da mão de obra qualificada devido a sua fuga para outras latitudes com melhores ofertas e condições de vida.

5.2 Estudo 2 - Perceção do público geral sobre a situação do cibercrime na cidade de Luanda

O questionário é uma ferramenta com vista a coleta de dados e utilizado em diferentes pesquisas. Neste ponto, pretende fazer-se a análise dos dados obtidos através da sua aplicação por inquérito dirigido a amostra do público-geral na cidade de Luanda para a obtenção de informações detalhadas sobre a temática em estudo, sendo os resultados interligados as teorias e aos objetivos traçados para a pesquisa.

Quando questionados as 270 pessoas que fazem parte da amostra relacionada com a população geral na cidade de Luanda, se já ouviram falar sobre o cibercrime,

despontou que 189 (70,0%) alegaram já terem ouvido falar do cibercrime e 81 (30,0%) alegaram nunca terem ouvido falar sobre o cibercrime.

Tabela 20: Existência do cibercrime

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Sim	189	70,0%	70,0%	70,0%
	Não	81	30,0%	30,0%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os resultados contidos na tabela em mote indicam que a maioria dos inqueridos, 189 (70,0%), já ouviram falar sobre o cibercrime. Quanto maior for o número de habitantes da cidade de Luanda com conhecimentos da existência do cibercrime, facilmente se conseguirá tornar o citadino mais cuidadoso aos cibercrimes e na construção de maior segurança com o manuseio dos dispositivos e serviços digitais. Para além disso, também ajuda na educação e consciencialização da população da cidade de Luanda sobre os perigos e as consequências que os crimes desta natureza podem provocar, pois a ausência desse saber pode facilitar o aparecimento de vulnerabilidades e tornar a população um alvo fácil e apetecível.

Em suma, apesar do cibercrime ser uma atividade criminosa surgida no final do século XX, ainda é bastante desconhecida e por conta disso tem causado danos significativos nas suas vítimas graças a evolução, proliferação, produção e utilização em massa da tecnologia (particularmente a nano tecnologia), podendo estes crimes variarem desde os mais pequenos, médios ou grandes.

Relativamente ao grau de conhecimento sobre os cibercrimes, quando averiguado nas 270 pessoas que conformam a amostra do público-alvo em análise, adveio que 146 (54,07%) responderam que o seu grau de conhecimento é baixo, 73 (27,04%) afirmaram ter um grau de conhecimento médio, 41 (15,19%) disseram ter saberes avançados e 10 (3,70%) afirmam não possuírem qualquer conhecimento sobre cibercrime.

Tabela 21: Grau de conhecimento sobre cibercrimes

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Baixo	146	54,07%	54,07%	54,1%
	Médio	73	27,04%	27,04%	81,1%
	Avançado	41	15,19%	15,19%	96,3%
	Nenhum	10	3,70%	3,70%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Face a pergunta em mote, os resultados revelam que a maioria dos inqueridos, 146 (54,07%), possuem um conhecimento baixo sobre os cibercrimes. Este resultado mostra que o grau de conhecimento sobre este fenómeno por parte da população da cidade de Luanda denota ser preocupante na medida que nos dias de hoje quase tudo se processa no mundo digital, sendo por isso basilar ter-se o seu conhecimento.

A segurança digital é uma responsabilidade de todos e deve começa com o seu entendimento e das medidas preventivas para a proteção individual e dos outros. Deste modo, quanto maior for o grau de conhecimento dos cibercrimes por parte da população da cidade de Luanda, melhor preparados estarão para o reconhecimento e estancamento da difusão desse delito.

Com relação aos tipos de cibercrimes que conhecem ou já tenham sido vítimas, quando questionadas as 270 pessoas que fazem parte da amostra do público-geral os resultados revelam que 56 (20,7%) afirmaram conhecer o *phishing*, 69 (25,6%) disseram conhecer o *ransomware*, 112 (41,5%) comentaram conhecer a clonagem de cartões/*skimming*, 24 (8,9%) afirmaram conhecer a engenharia social e 9 (3,3%) asseguraram não serem conhecedores que qualquer tipo de cibercrime.

Tabela 22: Tipos de cibercrimes que conhece

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	*Ransomware*	56	20,7%	20,7%	20,7%
	Phishing	69	25,6%	25,6%	46,3%
	Clonagem de Cartões/*Skimming*	112	41,5%	41,5%	87,8%
	Engenharia Social	24	8,9%	8,9%	96,7%
	Nenhum	9	3,3%	3,3%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os resultados da questão apontam que o tipo de cibercrime que a maioria dos questionados, 112 (41,5%), conhecem ou já tenham sido vítimas é a clonagem de cartões/*skimming*. Infelizmente, face a pouca literacia digital da população e alguma vulnerabilidade dos SI, muitas pessoas têm sofrido com este tipo de crime, pois os cibercriminosos têm encontrado facilidades na implementação de dispositivos eletrónicos em caixas de pagamento automático para a captura de dados contidos em cartões de crédito/débito das suas vítimas. Para além disso, os meliantes também têm conseguido fazer a clonagem de cartões das suas vítimas, por intermédio dos aplicativos do *internet banking*, entrando em contato com as vítimas, via telefónica, fazendo-se passar por funcionários de agências bancárias, alegando estarem a tratar

de questões relacionadas com atualizações de contas bancárias, persuadindo desta forma as suas vítimas a forneceram dados confidenciais, que quando fornecidos os cibercriminosos usam-nos para o proveito próprio, causam deste modo danos que por vezes podem ser irreparáveis.

Diante desta situação, é necessário que sejam levados acabo constantemente campanhas de sensibilização da população sobre os cuidados a terem diante de crimes desta natureza e a promoção da cultura de denúncia para que rapidamente se possa bloquear o uso do seu cartão.

Quanto ao grau de conhecimento das leis existentes para a prevenção e combate ao cibercrime na cidade de Luanda, ao serem questionadas as 270 pessoas que participam do estudo virado a população-geral da cidade de Luanda, resultou que 112 (41,5%) responderam terem conhecimentos baixo, 82 (30,4%) afirmaram terem conhecimentos médio, 35 (13,0%) retorquiram possuírem conhecimentos avançados e 41 (15,2%) declararam não possuírem conhecimentos sobre as leis existentes e que visam a prevenção e combate ao cibercrime na sua urbe.

Tabela 23: Conhecimento das leis para prevenção e combate ao cibercrime

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Baixo	112	41,5%	41,5%	41,5%
	Médio	82	30,4%	30,4%	71,9%
	Avançado	35	13,0%	13,0%	84,8%
	Nenhum	41	15,2%	15,2%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

O conhecimento de leis é elementar para qualquer estrato da sociedade, pois permite que sejam conhecidos os direitos e deveres de cada. Os cibercrimes não fogem a esta realidade e possuem normas que regulam o seu combate e tratamento. Os dados em epígrafe mostram que a maioria dos questionados, 112 (41,5%), dizem possuir conhecimentos baixo relativamente as leis existentes para a prevenção e combate dos cibercrimes na cidade de Luanda.

A pouca familiaridade com as leis contribui na perturbação da população geral na identificação correta, se um ato está ou não tipificado como cibercrime, não facilita a denúncia de casos suspeitos junto as autoridades com informações que facilitam a condução dos processos de investigação criminal. O conhecimento de leis permite que a população entenda os seus direitos e deveres na internet e concomitantemente defendê-los. Desta forma, trabalhar-se-ia melhor na prevenção e conscientização da

população de modos a serem tomadas medidas preventivas para a salvaguarda das informações pessoais e a desincentivarão de falsas informações na *internet*.

Quanto a classificação da gravidade do cibercrime em comparação aos outros tipos de crimes na cidade de Luanda, quando questionados os 270 indivíduos que compõem a amostra da população-geral da cidade de Luanda redundou que 53 (19,6%) responderam ser menos grave, 131 (48,5%) afirmaram ser igualmente grave, 71 (26,3%) asseguraram ser mais grave e 15 (5,6%) retorquiram não terem a certeza.

Tabela 24: Gravidade do cibercrime em relação aos outros crimes em Luanda

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Menos grave	53	19,6%	19,6%	19,6%
	Igualmente grave	131	48,5%	48,5%	68,1%
	Mais grave	71	26,3%	26,3%	94,4%
	Não tenho certeza	15	5,6%	5,6%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

A crescente dependência pelos serviços da *internet* e dos dispositivos eletrónicos a si conectados num mundo cada vez mais digitalizado, tem sido acompanhado nas últimas décadas pelo crescimento dos cibercrimes. A sua gravidade transcende as fronteiras físicas e virtuais dos Estados, num curto espaço de tempo, e vai desde o cometimento de fraudes financeiras, roubo de identidades, ataques a infraestruturas tecnológicas e entre outras formas com vista a obtenção de diversos ganhos.

Apesar do cibercrime ser um fenómeno relativamente novo, mas que se destaca pela sua natureza global e pela rápida propagação, a tabela em epígrafe demostra que a maioria dos inqueridos, 131 (48,5%), equiparam o cibercrime com a mesma gravidade dos outros tipos de crimes na cidade de Luanda uma vez que se configura num ato criminoso que muito tem lesado as suas vítimas.

Equiparando com os outros tipos de crimes, o cibercrime se distingue pelo facto de maioritariamente serem perpetuados por anónimos que utilizam a tecnologia como arma para ferirem às suas vítimas, que podem estar em qualquer parte do mundo (por vezes as vítimas não dão conta de terem sido atacadas). Infelizmente, devido à sua fácil propagação e o alcance global, o cibercrime causa perdas financeiras em qualquer parte do mundo, impacto social (desconfiança e o isolamento), dificuldades na sua investigação (face a volatilidade das suas provas digitais) e à sua transnacionalidade (que dificulta a aplicação da lei entre diferentes ordenamentos jurídicos).

Sobre a frequência de utilização dos serviços de *internet* no seio da população da cidade de Luanda, quando questionados as 270 pessoas que participam da amostra nessa investigação, os resultados indicam que 27 (10,0%) disseram que nunca fazem o uso dos serviços de internet, 64 (23,7%) afirmaram usar pouco os serviços de internet, 115 (42,6%) declararam serem usuários regulares e 64 (23,7%) asseguraram que sempre usam os serviços de internet.

Tabela 25: Frequência de utilização de internet

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Nunca	27	10,0%	10,0%	10,0%
	Pouca	64	23,7%	23,7%	33,7%
	Regular	115	42,6%	42,6%	76,3%
	Sempre	64	23,7%	23,7%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

A *internet* é uma ferramenta quase indispensável nos dias de hoje para a convivência dos humanos, trazendo consigo algumas mudanças na sua comunicação. Quando procurado saber junto do público que compõe a amostra, os resultados apontam que a maioria, 115 (42,6%), afirmam serem usuários regular dos serviços de *internet*, indicando que apesar dos serviços de acesso a *internet* carecerem de melhorias quantitativas e qualitativas, a população não está a parte no acompanhamento dessa tendência tecnológica e que por conta disso ajuda no seu crescimento e socialização nas mais variadas áreas do saber. Contudo, ainda são necessários investimentos para o contínuo crescimento e melhoria da infraestrutura tecnológica de modos a permitir que mais pessoas consigam fazer o uso dos serviços de internet, em qualquer lugar, para os mais variados fins, e assim promover-se a inclusão digital (aproveitando-se dos serviços fornecidos pelo Angosat 2) e a melhoria no acesso à informação.

A digitalização e a dependência tecnológica da sociedade moderna traz consigo vantagens como também desafios com relação a nova forma de delito (o cibercrime) que ganha cada vez mais espaço. Quando questionados os 270 indivíduos que compõem a amostra da população-geral de modos a saber se alguma vez foram vítimas de cibercrime o resultado revela que 195 (72,2%) afirmaram já terem sido alvos de cibercrimes e 75 (27,8%) responderam nunca terem sido alvos de cibercrimes.

Tabela 26: Vítima de cibercrime

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Sim	195	72,2%	72,2%	72,2%
	Não	75	27,8%	27,8%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Apesar da sociedade luandense estar em crescimento, em matéria ligada a tecnologia, os seus habitantes não estão imunes aos cibercrimes e isto é notado no resultado da questão em tratamento uma vez que a maioria dos inqueridos, 195 (72,2%), confirmam já terem sido vítimas do cibercrime. Os números são preocupantes face a fraca literacia digital da população da cidade de Luanda, pois torna-os alvos fáceis dos cibercriminosos.

Para a melhoria da segurança cibernética da população, é essencial ser cultivado o hábito da verificação da autenticidade de sites, incutir-se o hábito de não abertura de *links* suspeitos, manter-se a cultura de bloqueio dos dispositivos utilizados, a mudança periódica das senhas de autenticação, a criação de senhas complexas, tentar ao máximo possível a não utilização de redes *wi-fi* públicas e incentivar a cultura de denúncia perante suspeitas de cibercrimes, junto as autoridades competentes.

A manutenção destas políticas não significa a impossibilidade de continuarem a ser alvos de cibercrimes, mas ajuda na diminuição do sucesso dos mesmos, pois os criminosos tendem a melhorar os seus modos de ataques com técnicas inovadoras e que devem ser sempre acompanhadas com novas técnicas de defesa.

Definir um padrão comportamental para pessoas que tenha sido alva de cibercrimes não é fácil, pois por vezes a reação pode ser momentânea e nem sempre a mais acertada, podendo variar de acordo com a gravidade do dano sofrido e com base as caraterísticas pessoais da vítima. Questionadas os 270 indivíduos que representam a amostra da população em estudo para se perceber sobre a atitude que tomariam caso fossem vítimas de cibercrime, os resultados demostram que 169 (62,6%) afirmaram que denunciariam as autoridades, 90 (33,3%) disseram que pagariam o resgate e 11 (4,1%) disseram que não denunciariam.

Tabela 27: Atitude se fosse vítima de cibercrime

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Denunciaria as autoridades	169	62,6%	62,6%	62,6%
	Pagaria o resgate	90	33,3%	33,3%	95,9%
	Não denunciaria	11	4,1%	4,1%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os dados resultantes da questão em estudo e representados na tabela anterior revelam que a maioria dos participantes, 169 (62,6%), disseram que caso fossem vítimas de cibercrimes, denunciariam junto as autoridades habilitadas (bancos, polícia, empresa responsável pelo serviços e a PGR). Apesar da taxa resultante da maioria dos inqueridos, infelizmente a cultura de denúncia dos cibercrimes ainda se condói com muitos desafios por parte dos lesados por conta de fatores como a descrença nas autoridades, vergonha por terem sido vítimas, medo pela retaliação e a falta de conhecimento.

A denúncia da ocorrência dos cibercrimes é um passo elementar para o seu combate, pois ajuda na proteção individual do denunciante e dos outros, e a construção de um convívio mais criterioso e proativa a favor da cibersegurança.

Relativamente a postura adotada pelos inqueridos para a manutenção e proteção dos seus dados enquanto navegam na *internet*, dos 270 indivíduos que compõem a amostra da população-geral, arrolou-se que 105 (38,9%) disseram usarem senhas fortes, 69 (25,6%) responderam fazerem a mudança periódica das senhas, 76 (28,1%) afirmaram usarem senhas diferentes para cada rede e 20 (7,4%) asseguraram não adotarem qualquer postura.

Tabela 28: Postura adotada para a segurança e proteção dos dados na internet

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Uso de senhas fortes	105	38,9%	38,9%	38,9%
	Mudança periódica de senhas	69	25,6%	25,6%	64,4%
	Uso de senhas diferentes para cada rede	76	28,1%	28,1%	92,6%
	Nenhuma	20	7,4%	7,4%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

A adoção de uma postura que permite a conexão segura aos mais variados serviços oferecidos na *internet* e a forma como são manuseados os dispositivos eletrónicos são variáveis, mas fundamentais na garantia da segurança individual e coletiva. Os dados da tabela anterior, demostram que a maioria dos inqueridos, 105 (38,9%), optam pelo uso de senhas fortes para a proteção dos seus dados na *internet*. Por senha forte, é entendido como o uso combinando de caracteres especiais, números e letras (minúsculas e maiúsculas) com o intuito de dificultar ao máximo possível a descodificação da senha por outrem.

A adoção desta postura, por parte dos inqueridos, representa a aplicação de uma linha ténue de defesa contra o acesso não autorizado das suas contas, pois representa

uma chave de conhecimento pessoal. Apesar disso, é fundamental que os usuários pautem sempre pela mudança rotineira das suas senhas e sempre que existir suspeitas de invasão, pois à sua manutenção por longos períodos pode facilitar a descodificação por parte dos cibercriminosos que a todo o custo tentam roubar e expor dados e informações sigilosas das vítimas.

Sobre a frequência que são feitas as revisões e atualizações das configurações de segurança em dispositivos eletrónicos, na opinião das 270 pessoas que fazem parte da amostra do público-geral desta investigação, ficou fragmentada em 26 (9,6%) que disseram nunca fazerem a revisão das configurações em dispositivos eletrónicos, 137 (50,7%) afirmaram que raramente a fazem, 99 (36,7%) afirmaram que a fazem frequentemente e 8 (3,0%) asseguraram que a fazem sempre.

Tabela 29: Frequência de revisão das configurações de segurança

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Nunca	26	9,6%	9,6%	9,6%
	Raramente	137	50,7%	50,7%	60,4%
	Frequentemente	99	36,7%	36,7%	97,0%
	Sempre	8	3,0%	3,0%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Na era da digitalização tecnológica, a manutenção da segurança cibernética deve ser encarada com rigor, pois são cada vez recorrentes novas formas de ameaças. Os resultados do estudo, indicados na tabela anterior, refletem que a maioria dos questionados, 137 (50,7%), afirmaram que raramente fazem a revisão das configurações de segurança dos seus dispositivos eletrónicos. Essa condição é preocupante, pois permite a fácil exploração das vulnerabilidades e por conta disso podem provocar sérios danos nos seus dispositivos.

A revisão constante das configurações de segurança dos dispositivos eletrónicos não deve ser encarada como um luxo. Para tal, é fundamental que seja incutida essa cultura no seio da população da cidade de Luanda de modos a permitir a melhoria da sua segurança digital, a confiável disponibilidade dos dados por si manuseados e trabalhar-se na recognição e correção precoce das vulnerabilidades.

No que toca a abordagem de questões relacionadas com a cibersegurança por parte população em estudo, a apreciação das 270 pessoas que fazem parte da amostra do público-geral desta investigação saiu segmentada em 32 (11,9%) a afirmarem que nunca o fazem, 124 (45,9%) disseram que raramente têm essas discussões, 97

(35,9%) declararam que frequentemente têm essas discussões e 17 (6,3%) afirmaram que mantêm sempre discussões sobre cibersegurança entre amigos e familiares.

Tabela 30: Abordagem sobre cibersegurança

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Nunca	32	11,9%	11,9%	11,9%
	Raramente	124	45,9%	45,9%	57,8%
	Frequentemente	97	35,9%	35,9%	93,7%
	Sempre	17	6,3%	6,3%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Com a popularização dos serviços da internet e o uso massivo da nano tecnologia, especialmente os telemóveis, torna-se fundamental falar-se de cibersegurança nos mais vários ambientes. Com relação os dados obtidos na aplicação da questão em análise, representados na tabela anterior, demostram que a maioria, 124 (45,9%), afirmam que raramente discutem sobre a cibersegurança no seio dos amigos e familiares, entendendo-se assim que apesar dos danos causados pelos crimes desta natureza ainda não é comum à sua abordagem no meio social luandense, podendo esta situação ser resultado da falta de conhecimento sobre matérias relacionadas a temática ou pela pouca importância dada as consequências negativas deste fenómeno. A falta de interação entre amigos e familiares sobre questões ligadas a cibersegurança pode provocar consequências significativas, do ponto de vista pessoal e das pessoas que compõem o meio envolvente, pois facilita um ambiente vulnerável e obstrui a edificação de uma coletividade virtual instruída e firme. Para tal, é capital que seja abertamente abordada essa temática para que todos ganhem consciência dos riscos a que estão sujeitos.

Confiar nas atividades do governo é capital para a consolidação da segurança digital, validação das suas políticas e da licitude das suas ações. Para a compreensão sobre a confiança da população da cidade de Luanda sobre as atividades levadas pelo governo na investigação e punição dos cibercriminosos, foi aplicado um questionário dirigido a 270, que constituem a amostra do público-alvo em análise, os resultados demostram que 76 (28,1%) disseram acreditar pouco, 134 (49,6%) afirmaram que mantêm confiança razoável, 34 (12,6%) declararam ter confiança alta e 26 (9,6%) comentaram não terem nenhuma confiança sobre essas atividades.

Tabela 31: Confiança na investigação e punição do governo aos cibercriminosos

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Pouco	76	28,1%	28,1%	28,1%
	Razoável	134	49,6%	49,6%	77,8%
	Alto	34	12,6%	12,6%	90,4%
	Nenhuma	26	9,6%	9,6%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os resultados dos dados colhidos na aplicação da questão, espelham que a maioria da população participante, 134 (49,6%), mantêm confiança razoável sobre as atividades governamentais na investigação e punição dos cibercriminosos, deixando a entender que ainda existe ceticismo e que pode refletir-se na falta de cooperação na denúncia e fornecimento de informações vitais que auxiliam nas investigações das ações dos cibercriminosos. Quando existe confiança da população nas políticas tomadas pelo governo para o combate ao cibercrime, ela sente-se motivada a colocar. Para tal, é essencial que exista uma comunicação objetiva e clara, por parte do governo, sobre os resultados e as atividades levadas acabo para o desmantelamento de grupos vocacionados aos cibercrimes, representando deste modo o cumprimento de um dos objetivos da criação da DCCI. No entanto, esta comunicação não implica a exposição dos meios usados para o seu alcance, pois permitiria que os cibercriminosos conhecessem a forma de atuação das autoridades e procuram obter vantagens para a manutenção do seu anonimato.

O combate dos cibercrimes não é tarefa fácil, sendo para tal necessário trabalhar-se arduamente para o garante da cibersegurança na cidade de Luanda. quando questionados os 270 que fazem parte da amostra da população em estudo sobre qual deveria ser o foco do governo para o combate dos cibercrimes na cidade de Luanda, adveio que 60 (22,2%) escolheram a melhoria da legislação, 55 (20,4%) indigitaram o aumento das penas, 84 (31,1%) apontaram o investimento em infraestruturas críticas e 71 (26,3%) indicaram a educação digital da população.

Tabela 32: Foco do governo para o combate ao cibercrime

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Melhorar a legislação	60	22,2%	22,2%	22,2%
	Aumentar as penas	55	20,4%	20,4%	42,6%
	Investimento em infraestruturas críticas	84	31,1%	31,1%	73,7%
	Educação digital da população	71	26,3%	26,3%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os resultados da questão em análise, mostram que a maioria dos inqueridos, 84 (31,1%), entendem que para o combate dos cibercrimes na cidade de Luanda o governo deve concentrar esforços no investimento em infraestruturas críticas no setor das Telecomunicações, energético e serviços financeiros, pois são sensíveis para o fomento das política do Estado e tendem a ser alvos apetecíveis aos ciberataques.

A política de investimento em infraestruturas críticas é relevante para o fortalecimento da resiliência da segurança cibernética na cidade de Luanda, pois permite a continuidade dos serviços essenciais, a proteção da segurança nacional e minimiza o sucesso dos ciberataques. Para tal, é fundamental que este investimento seja acompanhado com programas de formação e capacitação de profissionais em matéria de cibersegurança, criação de planos de resposta contra os ataques cibernéticos e campanhas de sensibilização e educação da população.

Com o crescente uso das TIC, é essencial que desde a mais tenra idade a população da cidade de Luanda, sobretudo os mais jovens, sejam capacitados a enfrentarem os desafios que o cibercrime impõe. Quando questionados os 270 indivíduos que compõem a amostra do público-geral em estudo sobre a importância que representa a inclusão da educação cibernética nos programas escolares na cidade de Luanda, resultou que 77 (28,5%) afirmaram ser pouco importante, 78 (28,9%) disseram ser importante essa inclusão, 111 (41,1%) entendem ser muito importante e 4 (1,5%) asseveraram não ser importante.

Tabela 33: Inclusão da educação cibernética nos programas escolares

		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Pouco importante	77	28,5%	28,5%	28,5%
	Importante	78	28,9%	28,9%	57,4%
	Muito importante	111	41,1%	41,1%	98,5%
	Não Importante	4	1,5%	1,5%	100,0%
	Total	**270**	**100,0%**	**100,0%**	

Os dados obtidos na aplicação da questão, indicam que a maioria dos inqueridos, 111 (41,1%), entendem que a inclusão da educação cibernética nos programas escolares da cidade de Luanda é muito importante. Com essa apreciação percebe-se que apesar da pouca literacia cibernética da população da cidade de Luanda, existe inquietude no seu seio com relação a fraca ou a inexistência de abordagem desta temática em programas escolares, nos mais variados níveis, e que contribui para o contínuo sucesso dos ciberataques.

O investimento numa formação sólida com programas contendo temáticas ligadas a educação cibernética e ensinar desde criança as noções básicas de identificação e proteção contra os cibercrimes, contribuirá para que as gerações presentes e futuras possam estar melhor preparadas a lidarem com um mundo cada vez mais digitalizado, e deste modo estar-se a compor uma sociedade luandense mais próspera e firme. Para além disso, contribui para a potencialização das habilidades digitais dos futuros técnicos para o seu melhor desempenho e permitir a participação ativa de todos no mundo digital.

5.3 Discussão dos resultados

Os resultados obtidos do estudo quantitativo, inerentes estudo sobre o atual cenário dos cibercrimes denunciados na cidade de Luanda, forneceram *insights* valiosos. De modo a facilitar a discussão dos resultados, escolhemos fazê-lo olhando para os objetivos marcados e com a ajuda do marco teórico debruçado ao longo do trabalho. Para tal, foram aplicados dois (2) questionários por inquérito: um (1) direcionado aos especialistas de instituições públicas e privadas da cidade de Luanda e um (1) dirigido a população geral da cidade de Luanda.

Objetivos:

1 – Descrever como se manifestam os cibercrimes denunciados na cidade de Luanda. Em função daquilo que era esperado pela aplicação do questionário por inquérito aos especialistas das instituições públicas e privadas da cidade de Luanda os resultados indicam que o *phishing* e o *ransomware* são as formas que mais se manifestam os cibercrimes.

Entendemos que apesar do uso cada vez massivo dos serviços de *internet* na cidade de Luanda ainda é notória a precariedade de muitas pessoas em terem estes serviços disponíveis nos seus locais de residência, e quando existem nem sempre são dos melhores, e por conta disso procuram fazer o uso da *internet* nos seus locais de trabalho com vista a verificarem variados conteúdos do seu interesse. Assim, os cibercriminosos aproveitam-se das vulnerabilidades e enviam links de e-mail fraudulentos para as suas vítimas e que quando cessados podem permitir a intrusão de vírus que buscam o bloqueio dos SI da instituição e consequentemente a consumação do *ransomware*.

Quanto ao inquérito dirigido a polução da cidade de Luanda, apesar da maioria dos inqueridos terem pouco conhecimento sobre os cibercrimes já ouviram falar sobre os mesmos, mas mesmo assim ainda continuam a ser vítimas desses ataques e com realce para o *phishing* e a clonagem de cartões/*skimming*. Entendemos que apesar do desenvolvimento tecnológico e dos modos de defesa contra os ciberataques o *phishing* ainda é a técnica predileta dos cibercriminosos por permitir maior fluidez na distribuição de mensagens por *e-mail*, entre empresas e os clientes e vice-versa (Rodrigues, 2020). Para além disso, apesar do país ter crescido tecnologicamente e existir maior acesso a informações sobre os ataques por *skimming* ainda existem lacunas que contribuem para a predomínio destes crimes e que leva a muitos usuários continuam a ser vítimas por conta da sua insipiência e pela utilização da ES pelos cibercriminosos. (Júnior, 2012; Tavares, 2017; Fassbinder, 2016)

A alta prevalência de crimes desta natureza são o reflexo da combinação de fatores como o rápido crescimento e fragilidades tecnológicas e as práticas inadequadas de segurança cibernética. Essa manifestação pode ser enquadrada com base a teoria da oportunidade, pois coincidem os três elementos essenciais para que exista um ato: ausência de guardião, alvo vulnerável e um infrator motivado (Felson e Clarke, 1998; Bedendo, 2008; Bezerra, 2017). Contudo, esta tendência também é enquadrável com a teoria do anonimato, pois traz consigo a interpretação de que os criminosos se sentem protegidos e seguros a cometerem delitos desta natureza no mundo virtual, pois dificilmente são descobertos, tornando-se deste modo a característica que mais incentiva a ocorrência dos crimes cibernéticos. (Lima, 2021; Gleicher, 2008; Melo, 2017; Suxberger e Pacheco, 2019; Gleicher, 2008)

Entendemos também que a nova ordem mundial provocada pela pandemia da Covid-19, contribuiu para o aumento exponencial dos crimes desta natureza, pois permitiu que serviços aprovisionados presencialmente fossem transportados para o ciberespaço ou de forma híbrida, o que de certa medida despoletou o uso massivo dos dispositivos eletrónicos para a aquisição de meios e o continuo desenvolvimento das atividades laborais. (Gonçalves, 2021)

2 – Descrever os principais cibercrimes denunciados na cidade de Luanda

Não obstante o cibercrime na cidade de Luanda ainda não ser um fenómeno com proporções aos vistos em cidades mais desenvolvidas, os especialistas consideram a situação como perigosa, tal e qual abordado no capítulo 5, sendo o *phishing* e o

ransomware os que maior ameaça representam e concomitante os mais denunciados nas instituições em que estão ligados. Para além desses crimes os resultados da pesquisam apontam para a existência de crimes como o *skimming*, os crimes financeiros e as transferências ilícitas.

Infelizmente, fatores como a falta de treinamentos sobre a cibersegurança aos funcionários e a falta de atualizações das políticas de cibersegurança nas instituições muito têm contribuído para esse cenário, sendo para tal fundamental que sejam continuamente treinados os funcionários, os técnicos especializados e os gestores para melhor conhecerem e identificarem estes crimes, antes que ocorram os ataques. (Barker et al., 2022; (Silva et al., 2022)

Quanto a população geral, apesar de consideram igualmente grave o cibercrime em comparaçao aos outros crimes, a mioria fazem o uso dos serviços de internet, mas raramente fazem a revisão e atualização das configurações de segurança dos seus dispositivos. Como visto no capítulo 5, apesar do *phishing* e o *skimming* serem os crimes predominantes, também estão presentes a ES e o *ransomware*.

Consultados os dados dos relatórios da DCCI para se apurar sobre a real icidência dos principais cibercrimes denunciados na cidade de Luanda, constatamos existires crimes como a difamação, furto, extorsão, assunção ou atribuição de falsa identidade, dano em dados informáticos e a falsidade informática.

Os crimes financeiros e as transferências ilícitas refletem o crescimento do uso de serviços e plataformas digitais na cidade de Luanda, o que concilia com os resultados de estudos da *African Cybersecurity Report* (2022) que os enquadram nas formas mais comum de cibercrime na África Subsariana. Não obstante, os resultados apresentados conciliam-se com a teoria da anomia, pois está-se perante uma situação social onde existe a falta de integração das normas, os cibercriminosos equilibram as suas faltas com os meios ao seu dispor. (Calhau, 2006; Rego, 2019; Barreiras,2021)

Apesar disso, esperava-se que os relatórios fossem mais esclarecedores, mas infelizmente são genéricos e dificultam a perceção se são relativos a população ou as instituições. No nosso entender, essa não estratificação pode resultar da sua filtragem, antes de serem tornados público, já que o conhecimento técnico muitas das vezes está sujeito as lideranças, podendo com isso ofuscar o conhecimento da real incidência numérica sobre os tipos mais comuns de cibercrimes denunciados na cidade de Luanda.

3 – Descrever os principais alvos dos cibercrimes denunciados na cidade de Luanda

Os resultados da nossa investigação sugerem que os técnicos das instituições públicas e privadas da cidade de Luanda consideram que a população e as instituições financeiras sejam os principais alvos dos cibercrimes denunciados. Contudo, genericamente acreditam que em função aos dados operados pelas suas instituições elas estejam muito vulneráveis, pois poucos possuem protocolos de resposta imediato em caso de ciberataques. Para além dos alvos predominantes, o estudo revela que as instituições públicas, as empresas petrolíferas e as microempresas também têm sido alvas de cibercrimes e que por vezes provoca a paralisação das operações e o comprometimento dos dados guardados nos dispositivos ligados a instituição (Dias, 2019; Mbinza, 2023).

Os principais alvos dos cibercrimes denunciados na cidade de Luanda podem ser analisados a luz das teorias do crime existentes e serem escolhidos com base em fatores como vulnerabilidade, oportunidades e a motivação do criminoso. Contudo, para a questão em causa emergem a teoria da subcultura e a teoria da associação diferencial, que são entendidos como o reflexo de um código cultural que desconsidera as normas e os fatores sociais convencionais e envolve a apreensão de ações a partir de uma realidade venerável com a qual se identifica para a aquisição de status. (Liberati, 2007; Dias e Andrade, 2013; Queiroz e Lavor, 2020)

No nosso entender, era espetável que a população fosse tida como o principal alvo dos ciberataques, pois ainda persiste a fraca literacia digital no seu seio. A facilidade com que as instituições e a população têm sido atingidas colocam a Angola no top cinco (5) dos países africanos que mais ciberataques bem sucedidos sofrem (Afonso, 2021; Matondo, 2024). Contudo é de se estranhar a ausência das empresas de telecomunicações, pois são estas que maioritariamente funcionam como provedores de sinal de internet e que muitas das vezes sofrem ataques desta natureza que por vezes causam a paralização de alguns serviços fornecidos

4 – Descrever as medidas implementadas pelo governo de Angola para o combate aos cibercrimes denunciados na cidade de Luanda

Os resultados da nossa investigação, relativamente ao objetivo em análise, revelam que a maioria dos técnicos questionados acreditam que as suas instituições não possuem políticas de cibersegurança acessíveis a todos, mas, contudo, existem medidas de segurança como a criação de leis e a sensibilização da população que

têm sido usadas para dar resposta aos crimes desta natureza. Contudo, também tem sido utilizada a combinação de estratégias com vista a proteção e recuperação de dados (White, 2012; Reis, 2018).

Relativamente a apreciação da população, sobre a questão em análise, é de entendimento que o foco do governo para o combate dos cibercrimes na cidade de Luanda deveria resumir-se em investimentos em infraestruturas críticas e na educação digital da população, que passarei pela inclusão de temas relacionados com a cibersegurança em programas escolares. Contudo, a população tem pouco conhecimento sobre as leis existentes que visam a prevenção e proteção contra o cibercrime e nutre pouca confiança nas atividades realizadas pelo governo na investigação e punição dos praticantes dos cibercrimes na cidade de Luanda. (Lovatto, 2015; Filho, 2017)

Ao nosso ver ainda não existem tecnologias, recursos humanos suficientes e capazes de fazerem face ao cibercrime e nem tão pouco o controlo dos dispositivos e dos usuários que a cessam ao ciberespaço, o que torna difícil a identificação de quem realmente tenha estado no ciberespaço. Na verdade, ainda não existe uma estratégia bem definida e tornada pública pelo governo para o controlo e proteção do ciberespaço, daí a razão de ainda estar-se a criar condições para a criação de uma legislação capaz de regularizar a utilização e a proteção contra os cibercrimes. Com isso, entende-se que ainda é inadequado o nível de treinamento e preparação das autoridades locais para lidarem com o cibercrime. Assim, percebemos que ainda não existe segurança nacional sobre o ciberespaço.

De modo geral, as medidas implementadas pelo governo de Angola para o combate aos cibercrimes denunciados na cidade de Luanda são suscetíveis de serem analisadas sob as várias perspetivas das teorias do crime na medida que para se combater estes crimes devem envolver a combinação de estratégias preventivas e punitivas. Assim, entre as teorias desenhadas no marco teórico a que mais se aproxima é a teoria da anomia, mas não existem políticas públicas voltadas para a manutenção da segurança cibernética, o robustecimento das infraestruturas e a educação digital com vista a redução das desigualdades sociais que por vezes proporcionam a promoção de oportunidades de crimes desta natureza e assim fortificar as ações do Estado. (Calhau, 2006; Rego, 2019; Barreiras,2021)

CONCLUSÕES

Em função ao tema exposto e aos objetivos traçados, fez-se ao longo deste trabalho uma incursão sobre algumas teorias do crime que nos levam a compreensão do cibercrime e da temática em questão, que permitiu chegar-se ao ponto que para muitos é tido como o culminar de uma investigação e para outros é encarado como o seu início, na medida que a ciência é algo que se encontra em constantes mutações e o que hoje é considerado verdade num futuro breve pode ser refutado parcial ou totalmente.

Com a crescente expansão e evolução da tecnologia, em particular aos serviços fornecidos por via *online*, os Estados vão enfrentando dificuldades para manterem o controlo das suas fronteiras virtuais, por conta da transnacionalidade dos cibercrimes, e como consequência disso assiste-se o seu crescimento no ciberespaço e fora dele. Controlar todas as atividades que acontecem no ciberespaço para se combater integralmente o cibercrime é quase impossível, pois a cada dia surgem novas formas de interação nos ciberespaços conhecidos e em plataformas pouco conhecidas. Contudo, muitas das ações levadas acabo nestes espaços acabam por repercutir-se no mundo físico, comprometendo parcial ou totalmente a infraestrutura tecnológica utilizada para o fornecimento dos serviços fornecidos, fruto da incessante, procura por parte dos cibercriminosos, de informações valiosos ou a prática de ações conducentes ao pagamento de resgate para a restituição do controlo dos dados.

Infelizmente, nos dias de hoje perpetuar um ciberataque tende a ser cada vez mais fácil, pois por vezes com recurso a tecnologia menos sofisticada pode ser atingida qualquer pessoa e instituição, a partir de qualquer lugar do mundo. A nova realidade afeta a todos, em particular a cidade de Luanda, onde todos estão passíveis de sofrerem cibercrimes que pelo seu imediato impacto provocam efeitos disruptivo contra a integridade moral, reputação, infraestrutura tecnológica e perdas económicos avultadas.

Para este trabalho o objetivo geral consiste em descrever como se manifesta o cibercrime denunciado na cidade de Luanda. Para tal, foi necessário a aplicação de dois (2) questionários por inquérito (um dirigido aos especialistas ligados as instituições públicas e privadas e outro direcionado a população-geral) cujo tratamento é feito separadamente. No entender dos especialistas das instituições públicas e privadas, apesar do *ransomware* ser o tipo de cibercrime que quando aplicado contra as instituições causa danos severos, por bloquear o acesso aos SI por parte da

instituição e posteriormente o pedido de resgate para a sua recuperação, na cidade de Luanda o cibercrime se manifesta pelos ataques de *phishing* que consiste no envio de *e-mails* maliciosos na tentativa de busca de alguém que possa facilmente morder a isca enviada. olhando para a realidade local, estes tipos de ataques tendem a ter maior sucesso e abrangência na cidade de Luanda devido ao fraco investimento das instituições nas infraestruturas tecnológicas capazes de filtrarem e detetarem prematuramente ataques do tipo, bem como pela pouca preparação dos recursos humanos para a identificação destes ataques e por conta disso tendem a abrir *links*, sem a devida preocupação de assegurarem a verificação da sua autenticidade. Por vezes, os funcionários são atraídos em ataques do género devido ao limitado acesso dos serviços de *internet* que muitos enfrentam nos seus locais de habitação e quando postos nos locais de trabalho aproveitam usufruir destes serviços, o máximo que podem, utilizando dispositivos da empresa e pessoais, acabando por vezes de forma acidental enviarem informações valiosas das instituições aos criminosos.

Quanto a população-geral, a manifestação do cibercrime reside na clonagem de cartões/*skimming* que diariamente afeta a muitos, pois hoje a maioria das operações bancárias são realizadas com recurso as plataformas digitais ou com recurso aos cartões de débito/crédito. Os cibercriminosos têm investido em dispositivos eletrónicos, instalando-os em caixas de pagamento automático, capazes de copiarem dados contidos na banda magnética dos cartões das suas vítimas para posteriormente causarem danos a estas. Para além disso, os praticantes de crimes desta natureza muitas das vezes infiltram-se em filas de levantamento nos caixas de pagamento automático, com cartões de diferentes bancos, com o intuito de encontrarem pessoas com dificuldades de manuseamento destes caixas, oferecendo ajuda, e num curto espaço de tempo conseguem fazer a troca do cartão da vítima por um dos que se encontra em sua posse e do mesmo banco, alegam as vítimas de que o cartão não esteja operacional e em seguida procuram outro caixa para rapidamente esvaziam as contas das vítimas.

O outra formato de atuação que os cibercriminosos utilizam nos ataques por *skimming* consiste na criação de páginas de internet de venda de produtos *online*, inspiradas de lojas oficiais, que confundem e levam as sua vítimas a acreditarem na compra e que ao introduzirem os dados dos seus cartões e finalizarem a compra imediatamente são clonados pelos criminosos e nunca recebem a referida compra feita.

Uma outra forma de atuação por *skimming* dos cibercriminosos na cidade de Luanda tem consistido no estudo das informações pessoais da vítima a ser atacada e em seguida comunicam-se com as mesmas, por via telefónica, fazendo-se passar por funcionário da instituição bancária onde a vítima tem domiciliada a conta, persuadindo-a a fornecer informações sob pretexto de se estar a fazer atualizações e em seguida pedindo-as a dirigirem-se para um caixa de formas a introduzirem as instruções por eles imanadas. Infelizmente o número de vítimas deste tipo de ataques tende a crescer e a causar consequências morais e económicas devastadoras que por vezes levam muito tempo a serem superadas.

Para o alcance do objetivo geral deste trabalho foi necessário traçarem-se objetivos específicos que na visão de Minayo (2010) devem ser o suporte para que seja possível responder-se aquilo que se pretende com a pesquisa. Assim, o primeiro objetivo traçado neste trabalho consiste em descrever os principais cibercrimes denunciados na cidade de Luanda, e para tal foram estudadas teorias de autores que abordam sobre os mais variados conceitos sobre o cibercrime bem como as suas mais variadas formas de manifestação, tendo sido utilizados dados dos relatórios da DCCI e apoiados com informações oriundas dos questionários aplicados. Deste modo, de forma geral foram descritos e tratados cibercrimes como a burla informática, acesso ilegítimo aos SI, a falsidade informática, a clonagem de cartões/*Skimming*, o *phishing*, os crimes financeiros, as transferências ilícitas e a ES. Com a análise e descrição destes crimes, tenciona-se despertar a população e as instituições sobre a sua perigosidade e permitir que facilmente possam saber identificá-los e agirem para que não surtam os efeitos preconizados pelos cibercriminoso.

O segundo objetivo específico traçado prende-se com a descrição dos principais alvos de cibercrimes denunciados na cidade de Luanda, e para tal foi necessário estudar-se os poucos relatórios existentes com vista a ter-se a visão sobre esta realidade e que foi apoiado com os resultados dos questionários deste estudo. Deste modo, no entender dos especialistas os principais alvos dos cibercrimes denunciados na cidade de Luanda são a população, as instituições financeiras e as instituições públicas. Para a população-geral os principais alvos são considerados as instituições financeiras, as instituições do governo e as instituições comerciais.

Face aos resultados obtidos entende-se que a população, as instituições financeiras, as instituições do governo e as instituições comerciais tendem a ser os alvos prediletos dos cibercriminosos requerendo para tal maior vigilância a estes, não descorando os

outros. Estes alvos, são justificáveis uma vez que com fraco investimento levado acabo nas infraestruturas tecnológicas das mais variadas instituições na cidade de Luanda, a pouca qualificação dos recursos humanos e a fraca educação cibernética contribuem para que sejam alvos vulneráveis, pois não se consegue enfrentar este fenómeno sem os mínimos conhecimentos necessários.

O terceiro objetivo deste trabalho visa a descrição das medidas implementadas pelo governo de Angola para o combate ao cibercrime na cidade de Luanda, que não parece fácil, pois a eficácia de qualquer medida passa pela existência de normas que as guiam. O país ainda não possui uma Lei específica para o tratamento dos cibercrimes e procura trabalhar para o seu alcance, mas que tarde a chegar, atendendo que estes crimes evoluem rapidamente. Existem algumas leis aprovadas e que regulam o tratamento destas matérias, tais como o Livro Branco das Tecnologias de Informação e Comunicação, a Lei 22/11 da proteção dos dados pessoais, a lei n.º 7/17 de proteção das redes e Sistemas Informáticos e o Código Penal. Infelizmente, estas leis são limitadas uma vez focarem-se no tratamento dos crimes informáticos, que são menos abrangentes que os cibercrimes.

Com a transnacionalidade dos cibercrimes, isoladamente os países não conseguem combatê-los e por isso se tem buscado pela cooperação entre os Estados. Quanto a este quesito, Angola adotou e tem trabalhado com a Convenção da União Africana Sobre Cibersegurança e Proteção de Dados Pessoais, quer ao nível regional como continental, e tem cooperado com os países membros da CPLP, mas que por conta de muitos destes países serem signatários de outras convenções não os permite tratarem e cooperarem com Angola em determinadas matérias com maior profundidade.

Apesar de ainda não existir uma convenção mundialmente aceite e aplicada para o combate ao cibercrime, a que mais consenso reúne é a convenção de Budapeste, mas até a esta altura ainda não foi adotada pelo governo de Angola. Por conta disso, muitas vezes torna-se difícil seguir determinados rastos destes crimes, principalmente quando os seus praticantes utilizam o espaço físico ou servidores de computadores alojados em países signatários desta convenção, o que dificulta a recuperação dos ativos, principalmente os que envolvem a transferência ilícita de capitais e crimes financeiros.

De forma geral, entende-se que o cibercrime denunciado na cidade de Luanda tende a aumentar por conta por falta de investimento em infraestruturas tecnológicas,

recursos humanos qualificados, negligencia na observância de cuidados básicos de segurança em plataformas *online* e em dispositivos eletrónicos e regras capazes de travarem estes crimes.

Quanto as leis, entendemos que apesar da entrada em vigor do novo código penal, em novembro de 2020, que consagra no título VIII os crimes informáticos, nos termos dos artigos 437.º a 444.º, contemplando três (3) capítulos, detalhadamente: capítulo I (disposições gerais), capítulo II (crimes contra os dados informáticos) e capítulo III (crimes contra as comunicações e sistemas informáticos), com molduras penais que vão até 2 anos ou com a de multa até 240 dias (sobre a quem, sem autorização, aceder à totalidade ou à parte de um sistema de informação, de que não for titular, art.º 438, n.º1), de 2 a 8 anos de prisão (se o acesso for conseguido através da violação das regras de segurança ou se tiver sido efetuado a um serviço protegido, art.º 438, n.º2) e de 2 a 5 anos (se o dano emergente da perturbação for de valor elevado, art.º 441, n.º2)

No nosso entender, apesar do Código Penal angolano abordar sobre os crimes informáticos, que são menos abrangentes que os cibercrimes, deveria ser mais inclusivo e lançar os cibercrimes, pois os de fórum informático são um tipo específico e que diretamente envolvem a manipulação de SI e dados ao passo que os cibercrimes são mais abrangentes e para além de envolverem os crimes informáticos também envolvem os crimes tradicionais cometidos com auxilio aos meios eletrónicos e os exclusivamente virtuais.

RECOMENDAÇÕES

Pretende-se com esta pesquisa descrever a manifestação do cibercrime na cidade de Luanda e contribuir para o enriquecimento da bibliografia, incentivar a pesquisa pela temática, a sensibilização das autoridades para que se aproxime as melhores práticas de combate ao cibercrime e a conscientização da população sobre os riscos que correm. Contudo, e em função aos objetivos traçados com vista a prevenção contra os cibercrimes na cidade de Luanda, recomenda-se o seguinte:

- Que seja melhorada a infraestrutura tecnológica e a criação de um centro nacional de cibersegurança competente para monitorar, filtrar e bloquear automaticamente e responder em tempo real as tentativas de ataques cibernéticos;
- Que sejam criados e atualizados regularmente os protocolos internos com medidas que norteiam o comportamento a ser seguido pelos funcionários da instituição, em casos suspeitos ou confirmados de ataques cibernéticos, e assim torná-los num primeiro nível de segurança, quer individual como coletivo, e proporcionar um ambiente mais seguro e de confiança;
- A aprovação da lei de combate ao cibercrime, de modo a fazer face a este fenómeno que tende a desenvolver novas formas de atuação e garantir-se uma maior abrangência no seu combate;
- Que a PGR seja a instituição reguladora, que faça cumprir as normas e sempre que possível proceder as propostas para as devidas atualizações, em função ao desenvolvimento do fenómeno em estudo;
- Que a DCCI reforce a divulgação (através de colóquios, seminários, palestras, relatórios periódicas) sobre as atividades levadas acabo para o combate do cibercrime na cidade de Luanda, de modo a poder aumentar a confiança da população nas suas ações e desencorajar a continuidade destes crimes, tal e qual consta no diploma da sua criação;
- A inclusão nos mais variados níveis escolares, temáticas relacionadas com o cibercrime, de modo que desde muito cedo seja incutida a cultura de cibersegurança no seio das pessoas e das instituições;
- Sempre que alguém se dirigir a um terminal de pagamento automático, antes de introduzir o cartão, clique na tecla cancelar para anular qualquer tentativa de clonagem de cartões;

- Que exista a cultura de criação de uma subcontas, a partir da conta principal, onde deve ser adicionado o cartão de débito/crédito de modos a que estejam disponíveis somente os valores que se pretendem alocar e, mesmo que for alvo de clonagem do cartão, os cibercriminosos não consigam ter acesso a conta principal, onde por norma está disponível o ordenado;
- A temática em estudo não se encontra fechada e recomenda-se que seja continuada por outros investigadores de modo a ser ampliada e melhorada, particularmente em pesquisas que visam a confirmação de hipóteses, pois o mundo cibernético é bastante vasto e em constantes mutações.

BIBLIOGRAFIA

Accenture Security. (17 de Agosto de 2019). *The Cost of Cybercrime.* Obtido de Accenture.com: https://newsroom.accenture.com/search?q=The+Cost+of+Cybercrime

Afonso, L. C. (2015). *Métodos de detecção de malware por análise de tráfego* [Dissertação de Mestrado, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança]. Repositório Aberto do Instituto Politécnico de Bragança. http://hdl.handle.net/10198/11951.

Agência Especializada da Organização das Nações Unidas sobre Drogas e Crime (UNODC). (2024). *Atuando para deter o cibercrime.* UNODC.

Alecrim, E. (23 de 08 de 2016). *INFOWESTER.* Obtido de INFOWESTER: https://www.infowester.com/ransomware.php

Almeida, I. F. (2018). *A prova digital.* Almedina.

Almeida, J. M. (2019). *Sistema de Análise e Gestão de Vulnerabilidades: Implementação numa Instituição Bancária* [Trabalho de projecto de mestrado, Faculdade de Ciências da Universidade de Lisboa]. Repositório Aberto da Universidade de Lisboa. http://hdl.handle.net/10451/41682.

Almeida, P. J. (2017). *Criptografia e segurança.* Publindústria, Edições Técnicas.

Almeida, R. N. (2011). *Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais* [Monografia de Licenciatura não publicada]. Faculdade de Tecnologia de São Paulo.

Almeida, R. R. (12 de 08 de 2016). *Local do Crime e a Importância da Preservação das Provas.* Obtido de https://conteudojuridico.com.br/open-pdf/php4PLDCK.pdf/consult/php4PLDCK.pdf

Alvarenga, E. M. (2012). *Metodologia da Investigação Quantitativa e Qualitativa: normas e técnicas de apresentação de trabalhos científicos (2ª ed.).* A4 Diseños.

_____ (2012). *Protocolo de Investigación Científica e informe Final de Tesina Y Tesis.* A4 Diseños.

Alves, A. T. (2021). *Reflexões em torno de Metodologias de Investigação: recolha de dados* [Dissertação de mestrado, Departamento de Educação e Psicologia, Universidade de Aveiro]. Repositório da Univbersidade de Aveiro. http://hdl.handle.net/10773/30772.

Alves, C. B. (2010). *Segurança da informação vs. Engenharia social: como se proteger para não ser mais uma vítima.* Clube de Autores.

Amorim, P. R. (2005). *Biometria* [Tese de doutoramento, Universidade Federal de Pernambuco]. Repositório Aberto da Universidade Federal de Pernambuco. http://hdl.handle.net/bitstream/123456789/38886/1.

Andrade, J. A. (2015). *Gestão de redes e sistemas: estudo de um caso* [Dissetação de mestrado, Instituto Superior de Engenharia do Porto]. Repositório Científico do Instituto Politécnico do Porto. http://hdl.handle.net/10400.22/8216.

Angola, L. /. (06 de Janeiro de 2023). *Ver Angola*. Obtido de Ver Angola: https://www.verangola.net/va/pt/012023/Sociedade/33940/INE-estima-que-Angola-tenha-351-milh%C3%B5es-de-habitantes-em-2024.htm

Aparício, M. S. (2017). *O ciberespaço como dimensão de segurança* [Dissertação de mestrado, Academia da Força Aérea]. Repositório Comum da Academia da Força Aérea. http://hdl.handle.net/10400.26/23108.

Aragão, J. W. (2017). *Metodologia Científica* [Dissertação de mestrado, Universidade Federal da Bahia]. Repositório da Universidade Federal da Bahia. https://repositorio.ufba.br/handle/ri/30900.

Araújo, F. L. (2019). Aspectos jurídicos no combate e prevenção ao ransomware. *Revista do Ministério Público do Estado do Rio de Janeiro*, 26. Obtido de Araújo, F. L. (2019). Aspectos jurídicos no combate e prevenção ao ransomware. Revista do Ministério Público do Estado do Rio de Janeiro, 26.

Ariza, M. A. (2022). *Ataques automatizados de Engenharia Social com o uso de Bots em Redes Sociais Profissionais* [Dissertação de mestrado, Faculdade de Engenharia da Universidade Federal do Rio Grande do Sul]. Repositório da Sociedade Brasileira de Computação. https://doi.org/10.5753/sbseg.2022.225334.

Associação Portuguesa de Apoio à Vítima. (2021). *Manual ROAR - Da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas.* Associação Portuguesa de Apoio à Vítima.

Ayres, N. R. (2015). *A preservação do local do crime e a atuação dos órgãos de segurança pública no Distrito Federal: um estudo em campo* [Monografia de graduação, Faculdade de Ciências Sociais e Jurídicas]. Repositório do Centro Universitário de Brasília. https://repositorio.uniceub.br/jspui/handle/235/8441.

Azevedo, A. H. (2016). *Burlas Informáticas: Modos de Manifestação* [Dissertação de mestrado, Universidade do Minho]. Repositório Aberto da Universidade de Minho. https://hdl.handle.net/1822/44510.

Azevedo, R. M. (2013). *Propagação de vírus informático baseada em modelos biológicos* [Dissertação de mestrado, Instituto Superior de Engenharia do Porto]. Repositório Científico do Instituto Politécnico do Porto. http://hdl.handle.net/10400.22/6519.

Banha, P. (2010). *Sistemas de Armazenamento e Administração de Sistemas Informáticos* [Dissertação de Mestrado não publicada]. Escola Superior de Tecnologia de Abrantes.

Baptista, I. M. (2017). *O Fator Humano na Cibersegurança [Dissertação de mestrado não publicada].* Técnico de Lisboa.

Baratta, A. (2002). *Criminologia crítica e crítica do direito penal (3. ed.).* Revan.

Barker, W. C. (2022). Gestão de risco de ransomware: Um perfil do Framework de segurança cibernética. *National Institute of Standards and Technology*, 31.

Barreiras, M. (2021). *Criminologia: Escolas e Teorias Criminológicas.* Gran Cursos.

Barreto, A. G. (2016). *Preservação da Evidência Eletrónica: Desafios à Polícia Judiciária.* Revista Eletrônica Direito & TI.

Barreto, M. (2018). Identificação, isolamento, coleta e preservação do vestígio cibernético. Vestígios cibernéticos. Identificação Isolamento físico e lógico. Coleta, registro e preservação Coleta de dados voláteis. p. 63.

Batista, L. J. (2018). *O malware como meio de obtenção de prova em processo penal* [Dissertação de mestrado, Faculdade de Direito da Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/37574.

Batistela, C. M. (2018). *Modelo dinâmico de propagação de vírus em redes de computadores* [Tese de doutoramento, Universidade de São Paulo]. Repositório da Universidade de São Paulo. http://www.teses.usp.br/teses/disponiveis/3/3139/tde-28082018-081239/.

Bauman, Z. &. (2010). *Aprendendo a pensar com a sociologia.* Jorge Zahar.

Bedendo, R. (2008). *Teoria das oportunidades e policiamento comunitário: uma combinação contraditória?* [Dissertação de mestrado, Instituto de Ciências Humanas da Universidade Federal de Juíz de Fora]. Repositório Institucional da Universidade Federal de Juíz de Fora. https://repositorio.ufjf.br/jspui/handle/ufjf/2991.

Bergmann, H. M. (10 de 09 de 2014). Ciberespaço e cibercultura: novos cenários para a sociedade, a escola e o ensino de geografia. *Revista Iberoamericana de Educación*, p. 6.

Bezerra, R. R. (2017). *Teorias do Delito: uma análise críticada conduta em face da ontologia e deontologia penal* [Dissertação de mestrado, Instituto Brasiliense de Direito Público]. Repositório do Instituto Brasiliense de Direito Público. https://repositorio.idp.edu.br//handle/123456789/3127.

Branco, I. (2020). *Aplicação de firewall com filtro avançado para aplicações WEB* [Dissertação de mestrado não publicada]. Universidade do Vale do Taquari.

Braz, J. (2016). *Ciência, Tecnologia e Investigação Criminal.* Lisboa: Almedina.

Bressanin, M. (2023). Teoria Geral do Delito. *Trilhante*, 37.

Brito, A. B. (2019). *Teoria do crime.* Universidade Nova de Lisboa.

Brito, D. R. (2016). *Combatendo a ameaça Ransomware aplicando a norma NBR ISO/IEC 27001:2013 na gestão da segurança da informação* [Dissertação de mestrado, Universidade Tecnológica Federal do Paraná]. Repositório Educapes. http://educapes.capes.gov.br/handle/capes/665349.

Brito, I. B. (2015). Catálogo de Fraudes da RNP: 7 anos de experiência no tratamento de fraudes eletrônicas brasileiras. *Conferência Integrada ICCyber ICMédia* (p. 5). ICMédia.

Bryant, W. D. (2016). *International Conflict and Cyberspace.* Routledge.

Burnett, M. T. (2020). *Perícia Forense Computacional: Análise de Vestígios Voláteis e não Voláteis para o Laudo Pericial* [Dissertação de mestrado não publicada]. Universidade Federal do Piauí.

Caiúve, A. M. (2020). *A problemática da regulação dos crimes informáticos no Anteprojeto de Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime* [Dissertação de mestrado, Universidade do Minho]. Repositório da Universidade do Minho. https://hdl.handle.net/1822/76461.

Calhau, L. B. (2006). *Resumo de criminologia.* Impetus.

Câmara, P. (2010). *Segurança dos dados nas empresas: problemas e soluções.* Escola Superior Aberta.

Cambundo, Â. G. (2021). Cibercrime: breve reflexão sobre ciberinvestigação em tempo de pandemia. *JANUS*, 26.

Campos, J. B. (2003). *Como Funcionam os Sistemas de Biometria: Um Estudo Geral.* Faculdades Integradas de Caratinga.

Campos, J. P. (2018). *Computação Forense: Análise e Comparação de Desempenho das Ferramentas Forensic Tooolki 4 e Recoverit 6.* Carantinga.

Canongia, C. &. (2010). *Segurança cibernética: o desafio da nova sociedade da informação.* Parcerias Estratégicas.

Carneiro, A. (2009). *Auditoria e Controlo de Sistemas de Informação.* FCA.

Carvalho, A. A. (2021). *A responsabilidade civíl em casos de clonagem de cartão de crédito* [Dissertação de mestrado, Centro Universitário Nobre]. Repositório Acadêmico do Centro Universitário Nobre. http://unifan.net.br/repositório-academico/.

Cervo, A. L. (2002). *Metodologia científica. 5.ed.* Prentice Hall.

Cleyson, F. A. (2021). *Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos* [Monografia de graduação, Universidade Federal de Ouro Preto]. Biblioteca Digital de TCCS da Universidade Federal de Ouro Preto. http://www.monografias.ufop.br/handle/35400000/3567.

Coelho, I. (03 de 08 de 2023). *Teoria do Crime: compreendendo seus elementos fundamentais*. Obtido de JusBrasil: https://www.jusbrasil.com.br/artigos/teoria-do-crime-compreendendo-seus-elementos-fundamentais/1908699401

Colmenares, F. C. (2002). Virus Informaticos. *Revista iberoamericana de derecho informático*, 22.

Conceição, I. G. (2023). *Ameaças cibernéticas e os seus impactos na segurança humana* [Dissertação de mestrado, Universidade Autónoma de Lisboa]. Repositório da Universidade Autónoma de Lisboa. https://repositorio.ual.pt/entities/publication/d51aab4e-48c9-4acf-9748-86e6e740a50a.

Costa, J. V. (2017). *Análise de Vulnerabilidades de Segurança em Portais de Governos Eletrônicos* [Dissertação de mestrado, Universidade Federal de Uberlândia]. Repositório da Universidade Federal de Uberlândia. https://repositorio.ufu.br/handle/123456789/20400.

Costa, V. T. (2014). *Controle e isolamento de recursos em ambientes de redes virtuais openflow.* Universidade Federal do Rio de Janeiro.

Coutinho, C. P. (2018). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática.* Almedina.

Couto, J. C. (2018). *Auditoria de Cibersegurança: um caso de estudo* [Dissertação de mestrado, Instituto Superior de Contabilidade e Administração do Porto]. Repositório Científico do Instituto Politécnico do Porto. http://hdl.handle.net/10400.22/13242.

Cunha, L. C. (2020). *Redes neurais convulsionais e segmentação de imagens – uma revisão bibliográfica.* Universidade Federal de Ouro Preto.

Cybersecurity Ventures. (2 de Novembro de 2023). *Cybercrime Report 2023.* Obtido de Esentire: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

Dias, J. F. (2013). *Criminologia: o homem delinquente e a sociedade criminógena.* Coimbra Editora.

Dias, M. V. (07 de 06 de 2019). *Sonangol atacada por piratas cibernéticos*. Obtido de Novo Jornal: https://www.novojornal.co.ao/economia/interior/sonangol-atacada-por-piratas-ciberneticos-71141.html

Dias, P. R. (2021). *Prevenir um ataque de phishing* [Dissertação de mestrado, Instituto Superior de Tecnologias Avançadas de Lisboa]. Repositório Comum. http://hdl.handle.net/10400.26/39283.

Diniz, E. H. (2014). Relacionamento virtual via internet banking: uma análise de respostas de e-mail. *RAC-Eletrônica*, 99.

Eiras, M. C. (2004). *Engenharia Social e Estelionato Eletrônico.* Instituto Brasileiro de Propriedade Intelectual.

Escrivão, A. (16 de Maio de 2021). *Angola – Percurso cronológico no domínio das telecomunicações*. Obtido de angop: https://angop.ao/noticias/tecnologia/angola-percurso-cronologico-no-dominio-das-telecomunicacoes/

Faria, E. C. (2013). *A Aplicação da teoria das subculturas aos usuários de crack no Distrito Federal.* Centro Universitário de Brasília.

Faria, N. C. (2022). *Estratégia de Cibersegurança* [Dissertação de mestrado, Universidade do Minho]. Repositório da Universidade do Minho. https://hdl.handle.net/1822/84478.

Fassbinder, N. (2016). *A responsabilidade civil pelo fato do serviço de crédito* [Dissertação de mestrado, Universidade Federal do Paraná]. Repositório da Universidade Federal do Paraná. https://www.acervodigital.ufpr.br/bitstream/handle/1884/46293/89.

Félix, T. M. (2022). *IoT (Internet of Things) Podemos Confiar?* [Dissertação de mestrado, Instituto Superior de Tecnologias Avançadas de Lisboa]. Repositório comum. http://hdl.handle.net/10400.26/42250.

Felson, M. &. (1998). *Opportunity makes the thief: pratical theory for crime prevention.* Barry webb.

Fernandes, F. G. (2019). *Desenvolvimento de um processo automático de gestão de vulnerabilidades de ciber segurança em ambientes de grande dimensão* [Dissertação de mestrado, Faculdade de Ciências da Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/39578.

Fernandes, J. P. (2012). *Cibersegurança.* Nação e Defesa.

Fernandes, N. &. (2002). *Criminologia Integrada (2. ed.).* Revista dos Tribunais.

Fernandes, S. (2015). *Ciencia.ao - O portal de ciência, tecnologia e inovação de Angola* [Dissertação de mestrado, Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa]. Repositório da Universidade Nova de Lisboa. http://hdl.handle.net/10362/15901.

Fernández, M. P. (2019). *Rede de Computadores.* Eduece.

Ferreira, T. R. (2022). *ZeroDays v2 Sistema de Gestão de Ameaças de Cibersegurança Dia-Zero (Exploits e Software Malicioso Dia-Zero)* [Dissertação de mestrado, Faculdade de Ciências]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/56844.

Ferro, A. L. (2008). A teoria da associação diferencial e o crime de colarinho branco. *De Jure - Revista jurídica do ministério público de Minas Gerais*, 92.

Filho, J. E. (2017). *Análise de tráfego em redes TCP/IP.* Novatec.

Fonseca, A. C. (2021). *Fraude ao consumidor online: variáveis explicativas da vitimação e reportação [Dissertação de mestrado, Faculdade de Direito da Universidade do Porto].* Repositório Aberto da Universidade do Porto. https://hdl.handle.net/10216/138209.

Fontes, E. L. (2012). *Segurança da informação (1ª ed.).* Saraiva.

Francisco, G. E. (2016). *Processo de Awareness dos Utilizadores nas Redes Militares* [Dissertação de mestrado da Academia Militar]. Repositório comum. http://hdl.handle.net/10400.26/11367.

Franzese, L. F. (2023). *Um estudo das vulnerabilidades do OWASP top 10 na plataforma Moodle* [Dissertação de mestrado, Universidade Federal de

Uberlândia]. Repositório da Universidade Federal de Uberlândia. https://repositorio.ufu.br/handle/123456789/38406.

Giddens, A. (2008). *Sociologia (6ª ed.).* Fundação Calouste Gulbenkian.

Gil, A. (2008). *Métodos e técnicas de pesquisa social (6ª ed.).* Atlas.

Gleicher, N. (2008). *John Doe Subpoenas: Toward a Consistent Legal Standard.* 118 Yale L.J.

Gonçalves, F. J. (2023). *Análise e proposta de melhorias em simulacros de Phishing* [Dissertação de mestrado, Faculdade de Ciências da Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/62503.

Gonçalves, G. V. (2022). *Engenharia Social e a Segurança da Informação* [Dissertação de mestrado, Centro Universitário do Planalto Central Aparecido dos Santos]. Repositório do Centro Universitário do Planalto Central Aparecido dos Santos. https://dspace.uniceplac.edu.br/handle/123456789/2099.

Gonçalves, L. (2021). *Responsabilidade civil em casos de fraudes digitais no setor bancário* [Dissertação de mestrado, Centro Universitário de Curitiba]. Repositório do Centro Universitário de Curitiba. https://repositorio.animaeducacao.com.br/handle/ANIMA/17830.

Gonçalves, M. R. (2015). *Proposta de reestruturação física e lógica de rede: estudo de caso em uma empresa de confecções* [Dissertação de mestrado, Universidade Tecnológica Federal do Paraná]. Repositório da Universidade Tecnológica Federal do Paraná. http://repositorio.utfpr.edu.br/jspui/handle/1/23130.

Gonçalves, R. S. (2019). *O fator humano da cibersegurança nas organizações* [Dissertação de mestrado, Instituto Superior de Economia e Gestão da Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10400.5/19248.

Gontijo, C. R. (2016). Ciberespaço: que território é esse? *Centro Federal de Educação Tecnológica de Minas Gerais*, 8.

Gouveia, J. T. (16 de 2 de 2016). A escola clássica de criminologia = The classical school of criminology. *A escola clássica de criminologia = The classical school of criminology*, p. 26.

Gouveia, L. B. (2017). *Gestão da segurança da informação: conceitos básicos e introdução ao tema* [Dissertação de mestrado, Faculdade de Ciência e

Tecnologia da Universidade Fernando Pessoa]. Repositório Institucional da Universidade Fernando Pessoa. http://hdl.handle.net/10284/5954.

Guedes, I. S. (2021). *Cibercriminalidade: novos desafios, ofensas e soluções.* Edições de Ciências Sociais, Forenses e da Educação.

Ifanger, F. C. (2010). *A teoricrimiinológica do Labelling Approach e as medidas socioeducativas* [Dissertação de mestrado, Faculdade de direito da Universidade de São Paulo]. Biblioteca digital da Universidade de São Paulo. https://doi.org/10.11606/D.2.2010.tde-06072011-111256.

Instituto Nacional de Estatística. (2016). *Resultados definitivos: recenseamento geral da população e habitação - 2014.* Instituto Nacional de Estatística.

International Information System Security Certification Consortium. (14 de Setembro de 2020). *Building a Cybersecurity Workforce.* Obtido de (ISC: https://www.isc2.org/research

Isoni, M. M. (02 de 04 de 2007). E - crime em ambientes digitais informacionais da Internet. *DataGramaZero - Revista de Ciência da Informação*, p. 17.

Jorge, A. D. (2021). *Segurança e Integridade da Informação em contexto organizacional* [Dissertação de mestrado, Instituto Superior de Tecnologias Avançadas de Lisboa]. Repositório comum. http://hdl.handle.net/10400.26/39282.

Júnior, E. M. (2014). *Raid via software como solução de backup para prestação de serviço.* Centro Estadual de Educação Tecnológica Paula Souza.

Júnior, J. C. (1 de 06 de 2019). Cibercrime: Um Estudo Acerca do Conceito de Crimes Informáticos. *Revista Eletrônica da Faculdade de Direito de Franca*, p. 11.

Júnior, J. F. (2012). *Mineração de Dados para Detecção de Fraudes em Transações Eletrônicas* [Dissertação de mestrado, Universidade Federal de Minas Gerais]. Repositório da Universidade Federal de Minas Gerais. https://repositorio.ufmg.br/bitstream/1843/.

Júnior, M. F. (2016). *Uso da Técnica de Duplicação para Armazenamento de Dados Biológicos em Storage* [Dissertação de mestrado não puiblicado]. Universidade de Brasília.

Kim, D. &. (2018). *Fundamentals of information systems security (3rd ed.).* Jones & Bartlett Learning.

Klauberg, A. F. (2016). *Isolamento das redes virtuais (VLAN) em uma infraestrutura em nuvem usando uma abordagem SDN/openflow [Dissertação de mestrado não publicada].* Instituto Federal de Santa Catarina.

Lelo, S. (18 de Outubro de 2021). *Angola é um dos cinco países mais atacados por hackers*. Obtido de DW: https://www.dw.com/pt-002/angola-governo-admite-que-%C3%A9-preciso-um-centro-para-combater-o-cibercrime-no-pa%C3%ADs/a-59536562

Lemos, A. (2006). Processos de territorialização e desterritorialização na cibercultura. *Ciberpesquisa*, 17.

Lento, L. O. (2016). *Governança e gestão da segurança de informação* [Dissertação de mestrado não publicada]. Universidade do Sul de Santa Catarina.

Lévy, P. (1999). *Cibercultura.* Loyola.

Lévy, P. (2010). *Cibercultura (3ª ed.).* Editora 34.

Lewis, J. A. (21 de Fevereiro de 2018). *The Economic Impact of Cybercrime.* Obtido de Center for Strategic and International Studies: https://www.csis.org/analysis/economic-impact-cybercrime

Liberati, W. D. (2007). *Teoria da subcultura delinquente* [Dissertação de mestrado não publicada]. Pontifícia Universidade Católica de São Paulo.

Lima, E. M. (2021). *O anônimato nos crimes cibernéticos e a ocultação delitiva* [Dissertação de mestrado, Centro Universitário Luterano de Palmas]. Repositório do Centro Universitário Luterano de Palmas. https://ulbra-to.br/bibliotecadigital/publico/home/documento/2703.

Liska, A. &. (2017). *Ransomware: Defending Against Digital Extortion. 1ª ed.* O'Reilly Media.

Lobato, D. C. (2015). *Proposta de um Ambiente de Simulação e Aprendizado Inteligente para RAID* [Dissertação de mestrado, Instituto de Ciências Matemáticas e de Computação da Universidadade de São Paulo]. Biblioteca Virtual da Universidade de São Paulo. https://doi.org/10.11606/D.55.2000.tde-26072001-181852.

Lovatto, M. (2015). *Gerenciamento e segmentação de redes: estudo de caso em empresa do setor alimentício* [Dissertação de mestrado, Universidade Tecnológica Federal do Paraná]. Repositório Institucional da Universidade Tecnológica Federal do Paraná. http://repositorio.utfpr.edu.br/jspui/handle/1/23135.

Lyra, M. R. (2015). *Governança da Segurança da Informação (1ª ed.).* Novatec.

Machado, F. N. (2014). *Segurança da informação - princípios e controle de ameaças (1ª ed.).* Saraiva.

Machado, H. (2008). *Manual de Sociologia do Crime.* Afrontamento.

Machado, P. D. (2015). *O papel da GNR no contexto da cibersegurança nacional* [Dissertação de mestrado, Instituto Universitário Militar]. Repositório Comum. http://hdl.handle.net/10400.26/17403.

Machado, T. J. (2017). *Cibercrime e o crime no mundo informático: A especial vulnerabilidade das crianças e dos adolescentes* [Dissertação de mestrado, Universidade Fernando Pessoa]. Repositório Institucional da Universidade Fernando Pessoa. http://hdl.handle.net/10284/6089.

Madi, M. S. (2022). *Avaliação de vulnerabilidades em sistemas web de órgãos públicos da região da estrada de ferro em Goiás* [Dissertação de mestrado, Instituto Federal Goiano]. Repositório do Instituto Federal Goiano. https://repositorio.ifgoiano.edu.br/handle/prefix/2633.

Magalhães, J. (2020). *Espaço cibernético e a nova espionagem: análise das políticas públicas e a capacidade defensiva do Brasil* [Dissertação de mestrado, Centro Universitário de Brasília]. Publicações académicas. https://doi.org/10.5102/pic.n0.2019.7489.

Maia, R. L. (2016). *Dicionário - Crime, Justiça e Sociedade (1.ª ed.).* Edições Sílabo.

Manfio, J. (2016). *Implantação de uma infraestrutura de segurança da informação utilizando UTM firewall* [Dissertação de mestrado, Antonio Meneghetti Faculdade]. Repositório Acadêmico. http://hdl.handle.net/123456789/196.

Marconi, M. &. (2003). *Fundamentos de metodologia científica. 5ª Ed.* Atlas.

Marques, P. P. (2013). *Informática Forense: Recolha e preservação da prova digital* [Dissertação de mestrado, Universidade Católica Portuguesa]. Repositório Institucional da Universidade Católica Portuguesa. http://hdl.handle.net/10400.14/13191.

Martins, D. N. (2015). *Conjunto de diretrizes para o ciclo de vida do e-mail em organizações corporativas* [Dissertação de mestrado não publicada]. Universidade do Sul de Santa Catarina.

Matondo, M. (15 de 01 de 2024). *Ataque Cibrnético no Banco Nacional de Angola*. Obtido de Maka Angola: https://www.makaangola.org/2024/01/ataque-cibernetico-no-banco-nacional-de-angola/

Matos, O. P. (2017). *Um estudo sobre ataques de phishing e suas medidas de contenção* [Disssertação de mestrado, Universidade Federal do Pará]. Repositório da Universidade Federal do Pará. https://bdm.ufpa.br/jspui/handle/prefix/3001.

Mauser, D. &. (2014). *Certificação Security + - (2ª ed.).* Novatec.

Mbinza, P. (11 de 10 de 2023). *Sector bancário angolano registou sete ataques cibernéticos este ano – APD*. Obtido de Forbes África Lusófona: https://www.forbesafricalusofona.com/sector-bancario-angolano-registou-sete-ataques-ciberneticos-este-ano-apd/

Meier, L. F. (2018). *Engenharia Social: estudo de caso sobre os riscos de um ataque efetuado por um ex-funcionário*+ [Dissertação de mestrado, Universidade Tecnológica Federal do Paraná]. Repositório Institucional da Universidade Tecnológica Federal do Paraná. http://repositorio.utfpr.edu.br/jspui/handle/1/19429.

Mello, L. G. (2021). *Aplicação da teoria do domínio do fato a crimes cibernéticos do tipo ransomware* [Dissertação de mestrado, Universidade Federal do Rio Grande do Sul]. Repositório Digital, https://lume.ufrgs.br/handle/10183/237599.

Melo, M. C. (2017). *Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil [Dissertação de mestrado, Instituto de Tecnologia e Sociedade do Rio de Janeiro].* Repositório do Instituto de Tecnologia e Sociedade do Rio de Janeiro. https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf.

Melo, R. C. (2023). *Modelo para mapeamento de ameaças cibernéticas.* Universidade de Brasília.

Mendes, A. V. (2007). *Estudo de criptografia co chave pública baseada em curvas elípticas* [Dissertação de mestrado não publicada]. Universidade Estadual de Montes Claros.

Menezes, U. T. (2016). *O papel das forças e serviços de segurança no combate aos crimes cibernéticos em Angola* [Dissertação de mestrado não publicada]. Instituto Superior Técnico.

Miala, M. (06 de Fevereiro de 2022). *O Impacto das TIC's em Angola*. Obtido de linkedin: https://www.linkedin.com/pulse/o-impacto-das-tics-em-angola-manuel-miala/

Minayo, M. C. (2010). *Pesquisa social: teoria, método e criatividade. (29ª ed.).* Petrópolis.

Mitnick, K. D. (2003). *A arte e de enganar.* Pearson.

Mitshashi, R. A. (2011). *Segurança de Redes [Dissertação de mestrado não publicada].* Faculdade de Tecnologia de São Paulo.

Mocinho, T. O. (2023). *Teoria do Crime e seus Elementos.* Forense.

Molina, A. G. (2012). *Criminologia.* Revista dos Tribunais.

Monteiro, N. M. (2015). *Estudo de vulnerabilidades em aplicações web e o seu reflexo em domínios Portugueses* [Dissertação de mestrado, Instituto Superior de Engenharia do Porto]. Repositório Científico do Instituto Superior de Engenharia do Porto. https://recipp.ipp.pt/bitstream/10400.22/8224/1/.

Monteiro, S. D. (3 de 05 de 2007). O Ciberespaço: o termo, a definição e o conceito. *DataGramaZero - Revista de Ciência da Informação* , p. 20.

Morais, C. H. (2021). *Ransomware: segurança da informação e prevenção* [Dissertação de mestrado, Pontifícia Universidade Católica de Goiás]. Repositório Acadêmico da Pontifícia Universidade Católica de Goiás. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1619.

Morais, V. M. (2022). *O ecossistema de cibersegurança em Portugal* [Dissertação de mestrado, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria]. IC-Online. http://hdl.handle.net/10400.8/8077.

Moreira, E. S. (2019). O uso de ataques diretos e pessoais da engenharia social para a obtenção de informações de uma corporação. *Revista Inteligência Competitiva*, 18.

Moreira, F. (2019). *Cibercriminalidade e Cibersegurança* [Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Comum . http://hdl.handle.net/10400.26/34934.

Moreno, N. K. (2012). *Projecto de Rede de Computadores: Edifício D da UniPiaget* [Dissertação de mestrado,Universidade Jean Piaget de Cabo Verde]. Universidade Jean Piaget de Cabo Verde. https://core.ac.uk/download/pdf/38682602.

Nakamura, E. T. (2016). *Segurança da informação e de redes.* Educacional S.A.

National Institute of Standards and Technology. (19 de Abril de 2020). *Cybersecurity Awareness and Education.* Obtido de NIST:

https://csrc.nist.gov/pubs/itlb/2003/10/information-technology-security-awareness-training/final

Neves, R. A. (2022). *Vitimação por Phishing: um estudo empírico* [Dissertação de mestrado, Faculdade de Direito da Universidade do Porto]. Repositório Aberto da Universidade do Porto. https://hdl.handle.net/10216/145534.

Novaes, M. A. (2011). *Auditoria de Sistemas: a Importância da Segurança da Informação para as Demonstrações Financeiras.* [Dissertação de mestrado não publicada]. Universidade Federal de Pernambuco.

Oliveira, A. D. (2011). *Arquitetura de Segurança do IPL* [Dissertação de mestrado, Escola Superior de Tecnologia e Gestão]. Instituto Politécnico de Leiria. https://iconline.ipleiria.pt/bitstream/10400.8/1319/1.

Oliveira, B. P. (2019). *Construção de Conjuntos de Dados para Análise de Ransomware* [Dissertação de mestrado, Universidade Federal de Uberlândia]. Repositório da Universidade Federal de Uberlândia. https://repositorio.ufu.br/handle/123456789/27982.

Oliveira, D. S. (2016). *A estratégia de engenharia social e o sequestro dos dados por ransomware [Dissertação de mestrado, Universidade Católica de Brasília].* Repositório da Universidade Católica de Brasília. https://repositorio.ucb.br:9443/jspui/handle/123456789/11019.

Oliveira, J. C. (2018). *Ransomware - Laboratório de Ataque do WannaCry* [Dissertação de mestrado, Universidade de Brasília]. Repositório da Universidade de Brasília. https://bdm.unb.br/bitstream/10483/23052/1/2018.

Oliveira, L. A. (2021). A inserção da teoria do Labelling Approach na criminologia e sua aplicação na sociedade brasileira. *Revista Jurídica do Nordeste Mineiro*, 24.

Oliveira, R. R. (2012). Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. *Segurança Digital*, 12.

Oliveira, V. F. (2021). *Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação* [Dissertação de mestrado, Universidade Nova de Lisboa]. Repositório da Universidade Nova. http://hdl.handle.net/10362/117660 .

Organisation for Economic Co-operation and Development. (17 de Julho de 2012). *Cybersecurity: Threats, Challenges, Opportunities.* Obtido de OECD: https://www.oecd.org/fr/sti/publicationsdocuments/37/

Paulino, G. C. (2022). *Técnicas avançadas de investigação: perspectivas prática e jurisprudencial. 2ª ed.* Escola Superior do Ministério Público da União.

Pedro, F. P. (2022). *Estado dos Crimes Informáticos em Angola (Breve relatório).* Luanda: Direção de Combate aos Crimes Informáticos.

Pereira, A. F. (2022). *Cibercrime & A problemática da prova ilicitamente obtida por particulares no processo penal português* [Dissertação de mestrado, Universidade Católica Portuguesa]. Repositório Institucional da Universidade Católica Portuguesa. http://hdl.handle.net/10400.14/39837.

Pereira, S. M. (2022). *Cibersegurança: o Papel da Polícia de Segurança Pública na Prevenção do Cibercrime* [Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Comum. http://hdl.handle.net/10400.26/41482.

Philot, D. R. (2021). *Segurança da informação: ataques ransomware e proteção de dados* [Dissertação de mestrado, Universidade do Sul de Santa Catarina]. Repositório Universitário da Ânima. https://repositorio.animaeducacao.com.br/handle/ANIMA/17754.

Piekarski, J. I. (2018). *Vulnerabilidade digital de novas tecnologias: técnicas utilizadas através do meio digital que podem ser aplicadas em processo de espionagem e no cybercrime* [Dissertação de mestrado, Universidade do Sul de Santa Catarina]. Repositório Universitário da Ânima. https://repositorio.animaeducacao.com.br/handle/ANIMA/3702.

Pocinho, M. (2009). *Estatística: Teoria e Exercícios Resolvidos. Tese de Licenciatura não publicada* [Dissertação de mestrado, Universidade do Minho]. Research Gate. https://www.researchgate.net/profile/Margarida-Pocinho/publication/315762853.

Queiroz, E. G. (2020). Teoria da subcultura delinquente e a criminalização seletiva. *Revista Diálogos Acadêmicos*, 4.

Quintão, P. (2022). *Tecnologia da Informação: Segurança da Informação – Parte I.* Gran Cursos Online.

Rego, M. R. (2019). A Teoria da anomia social no estudo criminal: uma abordagem a partir das socialogias de Durkheim e Merton. *Revista Transgressões*, 25.

Reis, G. L. (2018). *Controlos de Cibersegurança em Ambientes MS Windows de Grandes Empresas: Modelo de Risco para Priorização de Atualizações de*

Segurança [Dissertação de mestrado, Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/36263.

Ribeiro, L. F. (2023). *Padões visuais na identificação de Phishing: abordagem multimetodológica* [Dissertação de mestrado, Universidade do Porto]. Repositório Aberto da Universidade do Porto. https://hdl.handle.net/10216/154906.

Ribeiro, M. C. (2015). *Cibercrime e a prova digital* [Dissertação de mesttrado, Instituto Superior Bissaya Barreto]. Repositório Comum. http://hdl.handle.net/10400.26/28946.

Rodrigues, I. A. (2020). *Robophish: um sistema de robos de software (RPA) para agilizar e automatizar o tratamento do Phishimg* [Dissertação de mestrado, Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/48246.

Rostirolla, A. P. (2021). Teoria Geral Do Crime: Conceito e Elementos. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 937-944.

Santos, A. F. (2016). *O Cibercrime: desafios e respostas do direito* [Dissertação de mestrado, Universidade Autónoma de Lisboa]. Repositório da Universidade Autónoma de Lisboa. http://hdl.handle.net/11144/2640.

Santos, B. A. (2021). *Comunicação sobre cibersegurança em contexto de teletrabalho nas agências de marketing digital* [Dissertação de mestrado, Instituto Universitário de Lisboa]. Repositório do Iscte – Instituto Universitário de Lisboa. http://hdl.handle.net/10071/24252.

Santos, F. H. (2010). *O Twitter como ferramenta de marketing em bibliotecas nacionais ibero-americanas* [Dissertação de mestrado, Universidade Federal do Rio Grande do Sul]. Repositorio Digital. http://hdl.handle.net/10183/27828.

Santos, J. P. (2017). *Deteção de malware de nova geração e sua mitigação* [Dissertação de mestrado, Universidade de Lisboa]. Repositório da Universidade de Lisboa. http://hdl.handle.net/10451/31173.

Santos, K. A. (2016). *Um estudo comparativo entre os firewalls IPFW E PF* [Dissertação de mestrado não publicada]. Centro Paula Sousa.

Santos, P. B. (2008). *Cyberwar - O fenómeno, as tecnologias e os actores.* FCA.

Severino, A. J. (2013). *Metodologia do trabalho científico. 1. ed.* Cortez.

Shecaira, S. S. (2004). *Criminologia.* Revista dos Tribunais.

Silva, A. B. (2022). *Conhecendo os crimes cibernéticos praticados no Brasil e como se proteger* [Dissertação de mestrado não publicada]. Centro Universitário Brasileiro.

Silva, E. W. (2012). *Sociologia Jurídica.* Unijuí.

Silva, I. P. (2019). *Engenharia socialcomo ameaça ao setor bancário: uso do phishing para coletar informações dos correntistas e a necessidade de estratégias de segurança* [Dissertação de mestrado, Universidade Federal do Ceará]. Repositório da Universidade Federal do Ceará. http://repositorio.ufc.br/handle/riufc/49703.

Silva, M. I. (2020). *Mecanismos internos de controlo de fraude nas Instituições de Crédito: Estudo de caso* [Dissertação de mestrado, Instituto Politécnico de Lisboa]. Repositório do Instituto Politécnico de Lisboa. https://repositorio.ipl.pt/bitstream/10400.21/12911/1/.

Silva, S. M. (2014). *A Ciberespionagem no contexto Português* [Dissertação de mestrado, Academia Militar]. Repositório Comum. http://hdl.handle.net/10400.26/8750.

Silva, T. J. (2020). *Análise de segurança à aplicação Autenticação.gov* [Dissertação de mestrado, Instituto Politécnico de Leiria]. IC-Online. http://hdl.handle.net/10400.8/5830.

Silva, T. M. (2012). *Segurança Informática - Vulnerabilidades Aplicacionais* [Dissertação de mestrado, Universidade Católica Portuguesa]. Veritati - Repositório Institucional da Universidade Católica Portuguesa. http://hdl.handle.net/10400.14/12040.

Silva, T. M. (2015). Ciberespaço: uma nova configuração do ser no mundo. *Periódicos Eletrônicos de Psicologia*, 7.

Silva, W. W. (2019). *A evolução da criptografia e suas técnicas ao longo da história* [Dissertação de mestrado, Instituto Federal Goiano]. Repositório do Instituto Federal Goiano. https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1.

Sousa, C. M. (2023). *Avaliação de Segurança Informática numa Instituição Pública* [Dissertação de mestrado não publicada]. Universidade da Madeira.

Stallings, W. (2015). *Criptografia e segurança de redes: princípios e práticas (6. ed.).* Pearson Education do Brasil.

Suxberger, A. H. (2019). A teoria da anomia nos crimes cibernéticos. *Delictae*, 22.

Tanenbaum, A. S. (2015). *Redes de computadores.* Campus.

Tavares, M. F. (2016). *Análise dos benefícios de implementação de um servidor com sistema raid nível 10 no instituto médio de administração e gestão do Kuito-Bié / Angola* [Dissertação de mestrado não publicada]. Universidad San Lorenzo.

Tavares, T. K. (2017). *O Fator Humano na Segurança de Informação nas Organizações* [Dissertação de mestrado, Instituto Superior Técnico]. Repositório do Instituto Superior Técnico. https://www.repository.utl.pt/bitstream/10400.5/19248/1.

Teixeira, C. F. (2021). *Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos* [Dissertação de mestrado, Universidade Federal de Ouro Preto]. Biblioteca Digital dos TCCS. http://www.monografias.ufop.br/handle/35400000/3567.

Teles, T. M. (2015). *Cibersegurança: Deteção de outliers* [Dissetação de mestrado, Escola Naval]. Repositório Comum, http://hdl.handle.net/10400.26/10860.

Testoni, A. G. (2016). *Soluções Raid para prevenção de falhas ocorridas em discos rígidos de computador* [Dissertação de mestrado não publicada]. Instituto Superior Tupy.

U.S. Department of Homeland Security. (28 de Outubro de 2021). *Critical Infrastructure Protection.* Obtido de DHS: https://www.dhs.gov/sites/default/files/2022-06/ST%20-%20Critical%20Infrastructure%20Security%20and%20Resilience%20RDTE%20Spend%20Plan.pdf

Velloso, R. V. (2018). O ciberespaço como ágora eletrônica na sociedade contemporânea. *Ciência da Informação*, 7.

Vilaça, M. L. (2016). *Tecnologia, Sociedade e Educação na era Digital.* Duque de Caxias.

Voz da América. (14 de Dezembro de 2014). *Crime cibernético chega a Angola*. Obtido de VOA Portugues: https://www.voaportugues.com/a/crime-cibernetico-chega-a-angola/2558363.html

White, C. (2012). *Redes de Computadores e Comunicação de Dados.* Cengage Learning.

Zalana, S. H. (2016). *Cibersegurança nas Infraestruturas Críticas Angolanas do Sector das Tecnologias de Informação e Comunicação* [Dissertação de mestrado não publicada]. Instituto Superior Técnico.

Legislação

Decreto Presidencial n.º 202/11, de 22 de Julho. *Diário da República*, n.º 139, I Série – **Aprova o Regulamento das Tecnologias e dos Serviços da Sociedade da Informação.**https://www.inacom.gov.ao/fotos/frontend_1/editor2/lei_225_de_2011-3_de_outubro_de_2017.pdf

Despacho Presidencial n.º 71/11, de 12 de Setembro. *Diário da República*, n.º 175, I Série – **Aprova o Livro Branco das Tecnologias de Informação e Comunicação.** https://www.inacom.gov.ao/fotos/frontend_1/editor2/despacho_presidencial_no_71_11-12_de_novembro_de_2011.pdf

Decreto Presidencial n.º 179/17, de 09 de agosto. *Diário da República*, n.º 135, I Série – **Aprova o Estatuto Orgânico do Ministério do Interior, consagra o Serviço de Investigação Criminal como um novo Órgão Executivo Central**. https://uif.persistec.com/upload_media/upload/documentos/legislacao/Decreto%20Presidencial%20n%C2%BA%20179_17,%20Estatuto%20Orga%CC%82nico%20do%20SIC.pdf

Lei n.º 22/11, de 17 de Junho. *Diário da República*, n.º 114, I Série – **Lei da Protecção de Dados Pessoais.** https://apd.ao/fotos/frontend_1/editor2/110617_lei_22-11_de_17_junho-proteccao_dados_pessoais.pdf

Lei n.º 23/11, de 20 de Junho. *Diário da República*, n.º 115, I Série – **Lei das Comunicações Electrónicas e dos Serviços da Sociedade de Informação.** https://apd.ao/fotos/frontend_1/editor2/110620_lei_23-11_de_20_junho-das_comunicacoes_electronicas_e_dos_servicos.pdf

Lei n.º 29/11, de 1 de Setembro. *Diário da República*, n.º 168, I Série – **Lei de alteração da divisão político-administrativa das províncias de Luanda e Bengo.** https://dw.angonet.org/wp-content/uploads/20110901_-_lei_n.o_29-11_-_divisao_politico-administrativa_das_provincias_de_luanda_e_bengo.pdf

Lei n.º 7/17, de 16 de Fevereiro. *Diário da República*, n.º 27, I Série – **Lei de Protecção das Redes e Sistemas Informáticos.** https://minttics.gov.ao/fotos/frontend_10/gov_documentos/redes_e_sistemas_informaticos_20864175955f109a14374be.pdf

Lei n.º 38/20, de 11 de Novembro. *Diário da República*, n.º 179, I Série – **Lei que aprova o Código Penal Angolano.** https://tribunalsupremo.ao/wp-

content/uploads/2023/03/C%C3%B3digo-Penal-e-do-Processo-Penal-Angolanos-2020-DRI-179_11-Novembro-176_230110_151357-1.pdf

Resolução n.º 33/19, de 09 de julho. *Diário da República*, n.º 91, I Série – **Convenção da União Africana sobre a cibersegurança e proteção de dados pessoais.** https://www.apd.ao/fotos/frontend_1/editor2/190709_resolucao_33-19_de_9_julho-convencao_ciberseguranca_proteccao_dados.pdf

ANEXOS

Anexo I – INSTITUCIONAL
Tema: Cibercrime

Título: Estudo sobre o atual cenário dos cibercrimes denunciados na cidade de Luanda

Sexo: Masculino ☐ Feminino ☐

Público-alvo: Instituições Financeiras (Bancos Privados, Finanças e BNA); Especialistas em TIC; Polícias; Magistrados; Instituições de Ensino

Grau Académico: Médio (12° Ano) ☐ Licenciatura ☐ Mestrado ☐ Doutorado ☐

Idade: 18-27 ☐ 28-37 ☐ 38-47 ☐ >=48 ☐

Pesquisador: Matias Francisco Sanches Tavares **Tipo de questionário**: Fechado

1. **Como descreve a situação atual do cibercrime na cidade de Luanda?**
   - Perigosa; Regular; Boa; Excelente; Não sei/Indeciso

2. **Qual o principal alvo dos cibercrimes denunciados na cidade de Luanda?**
   - Instituições Públicas; Instituições Financeiras; População; Empresas Petrolíferas; Outro

3. **Qual o tipo mais comum de cibercrime denunciado na cidade de Luanda?**
   - *Phishing* (e-mail com conteúdo fraudulento para roubo de senhas e outras informações)
   - Crimes Financeiros (fraude, lavagem de dinheiro, corrupção, evasão fiscal, manipulação de mercado)
   - Ransomware (*software* que bloqueia dispositivos e que exigem pagamento de resgate)
   - Clonagem de cartões/*Skimming* (Roubo de dados que constam na banda magnética de um cartão)
   - Transferências ilícitas (movimento de fundos de forma ilegal como dinheiro de tráfico de drogas, corrupção, terrorismo e contrabando)
   - Outro.

4. **Que tipo de cibercrime consideras ameaçador para a sua instituição?**
   - *Ransomware*; *Phishing*; Fraude Financeira; Clonagem de cartões/*Skimming*; Nenhum

5. **Face a natureza dos dados que a instituição maneja, acreditas ser vulnerável a cibercrimes?**
   - Pouco vulnerável; Muito vulnerável; Moderadamente vulnerável; Não vulnerável

6. **Que medidas de segurança cibernética têm sido tomadas em resposta aos e-crimes na cidade de Luanda?**
   - Criação de Leis; Formações; Cooperação; Sensibilização da População; Investimentos em infraestruturas tecnológicas; Nenhuma

7. **Como é feita a monitorização e detenção de possíveis atividades de cibercrimes nos Sistemas Informáticos da Instituição?**
   - Análise do fluxo de dados; Controlo de Acesso Físico; Controlo de Acesso Lógico; Não sei; Nenhuma; Todas

8. **Face a possíveis ataques de cibercrimes, qual a estratégia de proteção e recuperação de dados utilizada na empresa?**

- *Backup*; Redundância; Política de Gestão de Dispositivos; Criptografia; *Firewall*; Controlo de acesso; Duas ou mais estratégias; Não sei

9. **A sua instituição possui um protocolo de resposta imediato em caso de ciberataques?**

- Sim; Não; Não sei

10. **Com que frequência são realizados treinamentos sobre cibersegurança aos funcionários da instituição?**

- Diariamente; Mensalmente; Trimestralmente; Anualmente; Nunca

11. **Com que frequência são feitas as atualizações das políticas de cibersegurança na instituição?**

- Nunca; Anualmente; Semestralmente; A cada dois anos

12. **Existem políticas de cibersegurança claras e acessíveis a todos os funcionários na instituição?**

- Sim; Não; Parcialmente; Não sei

13. **Como classificas o nível de treinamento e preparação das autoridades locais para lidarem com o cibercrime?**

- Inadequado; Moderadamente adequado; Adequado; Excelente

14. **Na sua opinião, qual o principal desafio para o combate do cibercrime na cidade de Luanda?**

- Falta de legislação específica; Falta de recursos tecnológicos; Falta de formação especializada; Maior interesse político; Todas

Anexo II - **POPULAÇÃO GERAL**
Tema: Cibercrime

Título: Estudo sobre o atual cenário dos cibercrimes denunciados em Angola

Idade: ☐ Sexo: Masculino ☐ Feminino ☐

Público-alvo: População geral ☐

Grau Académica: Básico (9° Ano) ☐ Médio (12° Ano) ☐ Licenciatura ☐ Mestrado ☐ Doutorado ☐

Idade: 8-17 ☐ 18-27 ☐ 28-37 ☐ 38-47 ☐ >=48 ☐

Pesquisador: Matias Francisco Sanches Tavares **Tipo de questionário**: Fechado

1. **Já ouviu falar de Cibercrimes?**
   - Sim; Não
2. **Relativamente aos cibercrimes, qual o seu grau de conhecimento?**
   - Baixo; Médio; Avançado; Nenhum
3. **Que tipos de cibercrimes conheces ou já foi vítima?**
   - *Phishing* (e-mail com conteúdo fraudulento para roubo de senhas e outras informações);
   - *Ransomware* (software que bloqueia dispositivos e que exigem pagamento de resgate);
   - Clonagem de cartões/*Skimming* (Roubo de dados que constam na banda magnética de um cartão);
   - Engenharia Social (manipulação de pessoas para obtenção de dados como senhas, número de cartões);
   - Nenhum;
   - Outro.
4. **Já alguma vez foi vítima de Cibercrime?**
   - Sim; Não
5. **Se fosses vítima de cibercrimes, qual seria a sua atitude?**
   - Denunciaria as autoridades; Pagaria o resgate; Não denunciaria; Outra.
6. **Como classificas a gravidade do cibercrime comparado com os outros tipos de crimes na cidade de Luanda?**
   - Menos grave; Igualmente grave; Mais grave; Não tenho certeza
7. **Discutes sobre cibersegurança com amigos e familiares?**
   - Nunca; Raramente; Frequentemente; Sempre
8. **Qual à sua frequência de utilização dos serviços de Internet?**
   - Nunca; Pouca; Regular; Sempre
9. **Que postura adotas para a manutenção da segurança e proteção dos seus dados enquanto navegas na *internet*?**
   - Uso de senhas fortes (combinando caracteres especiais, números e letras); Mudança período de senhas; Uso de senhas diferentes para cada rede; Nenhuma; Outra

10. **Com que frequência fazes a revisão e atualização das configurações de segurança em dispositivos eletrónicos?**

- Nunca; Raramente; Frequentemente; Sempre

11. **Qual o seu grau de conhecimento relativamente as leis existentes para a prevenção e combate ao cibercrime na cidade de Luanda?**

- Baixo; Médio; Avançado; Nenhum

12. **Confias nas atividades conduzidas pelo governo na investigação e punição dos praticantes dos cibercrimes na cidade de Luanda?**

- Pouco; Razoável; Alto; Nenhum

13. **Na sua opinião, qual deveria ser o foco do governo para o combate dos cibercrimes na cidade de Luanda?**

- Melhorar a legislação; Aumentar as penas; Investimento em infraestruturas críticas (Telecomunicações, setor energético e serviços financeiros); Educação digital da população; Outro

14. **Que importância representa a inclusão da educação cibernética nos programas escolares na cidade de Luanda?**

- Pouco importante; Importante; Muito Importante; Não Importante