UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

ENGENHARIA INFORMÁTICA

PROPOSTA DE MODELO DE INTEROPERABILIDADE PARA O CADASTRO ÚNICO MÓVEL ENTRE OS SERVIÇOS DE COMUNICAÇÃO COM OS DE TELEFONIA MÓVEL E IDENTIFICAÇÃO CÍVIL DE MOÇAMBIQUE

CASO DE ESTUDO: Operadores de Telefonia Móveis Nacionais

Autor:

Langa, Nactividade Estêvão

Supervisor:

Eng.º Délcio Arnaldo Chadreca

Maputo, Dezembro 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

ENGENHARIA INFORMÁTICA

PROPOSTA DE MODELO DE INTEROPERABILIDADE PARA O CADASTRO ÚNICO MÓVEL ENTRE OS SERVIÇOS DE COMUNICAÇÃO COM OS DE TELEFONIA MÓVEL E IDENTIFICAÇÃO CÍVIL DE MOÇAMBIQUE

CASO DE ESTUDO: Operadores de Telefonia Móveis Nacionais

Autor:

Langa, Nactividade Estêvão

Supervisora:

Eng.º Délcio Arnaldo Chadreca

Maputo, Dezembro de 2023

UNIVERSIDADE
EDUARDO
MONDLANE

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

ENGENHARIA INFORMÁTICA

TERMO DE ENTREGA DO RELATÓRIO DE TRABALHO DE LICENCIATURA

Declaro que o estudante **Nactividade Estêvão Langa**, entregou no dia 08/12/2023 as 03 cópias do relatório do seu Trabalho de Licenciatura com a referência 2020EITLN202, intitulado: **PROPOSTA DE MODELO DE INTEROPERABILIDADE PARA O CADASTRO ÚNICO MÓVEL ENTRE OS SERVIÇOS DE COMUNICAÇÃO COM OS DE TELEFONIA MÓVEL E IDENTIFICAÇÃO CÍVIL DE MOÇAMBIQUE**. Caso de Estudo: Operadoras de Telefonia Movel Nacionais

Maputo, aos 08 de Dezembro de 2023

O (A) Chefe da Secretaria

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

ENGENHARIA INFORMÁTICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, 08 de Dezembro de 2023

O Autor

_____

(Nactividade Estêvão Langa)

Dedicatória

A minha mãe Madalena Azevedo

A meu pai Estêvão Carlos Langa

Agradecimentos

Agradeço, primeiramente, a Deus, pelo dom da vida, pela oportunidade de poder tido essa trajetória académica até ao momento actual junto a Ele.

Agradeço aos meus criadores, Estêvão Langa e Madalena Azevedo, pelo investimento irretornável depositado em mim não só como estudante, mas também com pessoa, agradeço-os também pelos imensos e irretribuíveis ensinos, pela persistência e paciência, por terem sido o alicerce em momentos de tribulação e por acreditarem que seria capaz mesmo quando havia dúvidas em mim.

Aos meus estimados irmãos, Ibraimo, Tasmira, Alima e Estêvão agradeço-os por sempre me fazerem sentir aparada, pelo suporte, pela força, por acreditarem que poderia tornar sonhos em realidade. Agradeço-os por serem meus fiéis intercessores de vida e pela visão externa em meio a dificuldades.

De forma carinhosa agradeço aos Docentes e aos Funcionários da Faculdade de Engenharia da Universidade Eduardo Mondlane (UEM), pelo profissionalismo de forma directa ou indirecta cada contribuiu par tornar possível esse desafio. Agradeço pelos conselhos, orientações, ensinamentos partilhados de forma sabia. Em especial quero render a minha gratidão a meu Supervisor Eng.º Délcio Chadreca, ao Eng.º Felizardo, Eng.º Albino Cuinhane, Eng.º Ruben Manhiça, Dr. Sergio Mavie, Dr. Vali Issufo, Eng.ª Ivone Cipriano, Eng.ª Leila Omar, Eng.ª Tatiana Kovalenko, Eng.ª Nilza Collinson, Eng.º Edson Cossa *(In memoriam)*, cada semente de ensino profissional e de vida vem brotando em mim.

Por último, mas não menos importantes agradecimentos estendidos aos meus superiores hierarquios, a todos amigos, colegas, familiares não mencionados.

Epígrafe

"*Na vida ninguém é substituível, releve sempre"*

Estêvão Carlos Langa *(In memoriam)*

RESUMO

De igual modo como observa-se um crescimento no mercado tecnológico verifica-se também um crescimento de crimes que caracterizam-se por fraturar o bom desenvolvimento das instituições que gerem as tecnologias. Uma das áreas mais "sensíveis" e que vê-se naturalmente ameaçada com este crimes, é a área de telefonia móvel que constantemente busca por soluções tecnológicas inovadoras para fazer "frente" as exigências dos consumidores dos seus serviços, rumo a maior fidelização e crescimento da sua carteira de clientes. Assim o presente trabalho, que caracteriza-se por ter uma abordagem exploratória e descritiva procura usar uma solução de interoperabilidade dos sistemas de registo das carteiras de telefonia móvel com os de serviços de identificação, tributação civil e a entidade reguladora de comunicação que é o Instituto Nacional de Comunicação de Moçambique (INCM), a fim de contribuir para o delineamento de estratégias para por fim aos constrangimentos técnicos e operacionais consequentes da ocorrência dos crimes cibernéticos. Pelos resultados do levantamento dos modelos de rastreio a nível das operadoras de telefonia móveis nacionais existentes foram entrevistadas nomeadamente: Vodacom, TMcel e Movitel pôde-se concluir que, estas não possuem um protocolo estabelecido com instituições do estado particularmente as de registo civil ou alternativamente alguma que possa fazer a identificação sumária dos infractores. Deste modo, foi feita a proposta de um modelo de interoperabilidade que contempla no seu mecanismo de rastreio a integração entre os serviços de atribuição do Número Único de Identificação Tributária (NUIT), as redes de telefonia móvel, os serviços de identificação civil e o INCM, de modo que a chave primária de identificação seja mesmo o NUIT. Considerando-se esta solução recomendou-se a interoperabilidade como mecanismo proposto no presente estudo percebendo-se que os operadores de telefonia móvel teriam maior flexibilidade, eficácia e eficiência na prevenção e resposta tanto para os crimes cibernéticos que podem ocorrer dentro dos sistemas de informação internos a nível das operadoras móveis (crimes cibernéticos puros) assim como os externos via dispositivos electrónicos que são comuns em banca móvel.

Palavras-chave: Interoperabilidade; Sistemas de Informação; Operadores de Telefonia Móvel.

ABSTRACT

Just as there has been growth in the technology market, there has also been a rise in crimes that are characterized by disrupting the smooth development of the institutions that manage technology. One of the most "sensitive" areas, which is naturally threatened by these crimes, is the mobile telephony sector, which is constantly looking for innovative technological solutions to meet the demands of the consumers of its services, to increase the loyalty and growth of its customer base. This work, which is characterized by having an exploratory and descriptive approach, seeks to use a solution for the interoperability of mobile phone card registration systems with those of identification services, civil taxation and the communication regulator, the National Communication Institute of Mozambique (INCM), to contribute to the design of strategies to put an end to the technical and operational constraints resulting from the occurrence of cybercrime. From the results of the survey of tracing models at the level of the existing national mobile phone operators interviewed, namely Vodacom, TMcel and Movitel, it was concluded that they do not have an established protocol with state institutions, of the state, particularly civil registry offices, or alternatively, one that can make a summary identification of offenders. In this way, an interoperability model was proposed which includes in its tracking mechanism integration between the services for assigning the Unique Tax Identification Number (NUIT), the mobile telephone networks, the civil identification services and the INCM, so that the primary identification key is the NUIT. Considering this solution, we recommend integrating the mechanism proposed in this study, realizing that mobile phone operators would have greater flexibility, effectiveness, and efficiency in preventing and responding to both cybercrime that can occur within internal information systems at mobile operator level (pure cybercrime) as well as external cybercrime via electronic devices, which is common in mobile banking.

Keywords: Interoperability; Information Systems; Mobile Telephony Services.

Índice

Índice de Figuras

Índice de Tabela

LISTA DE ABREVIATURAS E ACRÓNIMOS

API	Interface de Programação de Aplicativos
A.T	Autoridade Tributária de Moçambique
B.I	Bilhete de Identidade
GSM	Sistema Global para Comunicações Móveis
HTTP	Protocolo de Transferência de Hipertexto
HTTP	Protocolo de Transferência de Hipertexto Seguro
INCM	Instituto Nacional de Comunicação de Moçambique
INAGE	Instituto Nacional de Governo Eletrônico
NUIT	Número Único de Identificação Tributária
SGBD	Sistema de Gerenciamento de Banco de Dados
S.I	Sistema de Informação
T.I	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
UOP	Unidade Operacional da Polícia

Glossarial de Termos

Autenticação	Processo de segurança para verificação da veracidade e autenticidade de uma identidade ou objetos
Integração	Inclusão de novos elementos, processo de interligar componentes heterogéneos de forma que funcionem como se fossem um único
Interoperabilidade	Capacidade de um sistema (informatizado ou não) de se comunicar de forma transparente
Internet	Rede de conexões globais que permitem o compartilhamento instantâneo de dados entre dispositivos
Sistema	Conjunto de elementos interdependentes de modo a formar um todo organizado
Módulo	Parte do sistema responsável por uma tarefa definida
Protocolo	Conjunto de informações, normas ou regras específicas que os elementos finais de uma comunicação usam para conectar-se ou comunicarem-se
Stakeholders	Todos grupos de pessoas ou organizações que podem ter algum tipo de interesse pelas ações de uma determinada empresa

1. CAPÍTULO I - INTRODUÇÃO

1. Introdução

1.1. Contextualização

Ao longo dos últimos anos, as organizações têm vindo a fazer um esforço no sentido de se adaptarem e de acompanharem as transformações e as necessidades da sociedade, desenvolvendo novos meios de resposta para os cidadãos, novas vias de comunicação e de transmissão da informação, sustentados por sistemas tecnológicos estruturados. Nestes termos, os Sistemas de Informação (S.I.) associados às Tecnologias de Informação e Comunicação (TIC's) conheceram um avanço e dominam quase todo o mundo, facilitando a comunicação, de tal forma que as pessoas conseguem se comunicar de diversas formas sem precisar de deslocarem-se Laudon e Laudon (2004).

Não obstante, a facilidade de comunicação por via dos S.I existe alguma vulnerabilidade que os meios informáticos expõem aos utilizadores, de acordo com Simon et al. (2014), devido à facilidade de comunicação das pessoas e do desenvolvimento das tecnologias, torna os crimes praticados com uso de computadores ou via internet mais danosos do que a décadas atrás, uma vez que dificilmente é possível controlar e até mesmo identificar a sua origem, pois não existem fronteiras.

Madni et al (2014), afirma que incidentes cibernéticos tendem a aumentar diante da ausência ou fragilidade de políticas de prevenção e controle, observando-se que tais incidentes causam prejuízos e insegurança. Por outro lado, os mesmos autores enfatizam que quando organizações estatais e privadas desenvolvem políticas e acções para aumentar a segurança, elas também incorrem em custos de oportunidade e de transação, inclusive o risco de abusos e violações de direitos. Isso ocorre por causa da dinâmica dos processos de securitização da informação empresarial.

Em Moçambique existem normas acordadas vigentes na Estratégia Nacional de Segrança Cibernetica (ENSC, 2021-2024), desenvolvidas pelo Instituto Nacional de Tecnologias de Informação e comunicação (INTIC) que visam a responder vigorosamente às ameaças presentes no ciberespaço. Tal como referenciado no relatório anual de 2017 do INAGE (2017), actualmente, existe uma variedade de ameaças e riscos de crimes cibernéticos que podem prejudicar o bom funcionamento do ciberespaço moçambicano, incluindo os sistemas e serviços de Tecnologias de

Informação e Comunicação (TIC) em Moçambique, que por consequência podem provocar um impacto negativo nos esforços para o aproveitamento das TICs no desenvolvimento socioeconómico.

Os crimes cibernéticos cometidos em Moçambique têm incidido particularmente em utilizadores de operadoras de telefonia móvel, o que tem sustentado sobre as instituições a sujeitos ou corporações. Portanto, as operadoras de telefonia móvel verificam a necessidade de aprimorarem os mecanismos de segurança. O que se propõe no presente estudo é que estas instituições possam adoptar estratégias que permitam a intercomunicação entre diferentes sistemas de informação para facilitar o controlo das operações realizadas pelos consumidores dos serviços de telefonia móvel como forma de prevenção e de resposta aos crimes observados no país.

1.2. Justificativa de Estudo

A interoperabilidade de sistemas de informação é um tema muito abordado na gestão de sistemas de informação, sobretudo quando se explicita questões como segurança, confidencialidade e disponibilidade de informação. Observando o actual contexto moçambicano onde se constata de forma “tímida”, mas crescente os crimes cibernéticos, há necessidade de adoptar estratégias para a sua prevenção.

Portanto, os resultados do presente estudo envolvem na sua pertinência aspectos que acomodarão os seguintes contributos:

- No âmbito organizacional para o sector de telefonia móvel poderá reduzir os constrangimentos técnicos, operacionais, logísticos e melhorar de forma complementar os mecanismos já existentes a cobertura dos casos de crimes cibernéticos;
- No âmbito de satisfação de serviços de telefonia móvel a implementação do mecanismo proposto poderá reduzir a incidência de crimes cibernéticos e, nesse caso, poderá dar maior credibilidade no contexto de segurança das operadoras móveis para os utilizadores dos mesmos serviços;
- No âmbito do estado como os crimes cibernéticos apresentam uma legislação ainda muito “Embrionária” será um complemento adicional as normas que visam o combate aos crimes cibernéticos;

- No âmbito académico será uma contribuição significativa com exemplo pratico da actual legislação vigente que visa sobre a aplicabilidade da interoperabilidade a nível das instituições do estado moçambicano.

1.3. Problematização

Com o crescimento acesso a meios informáticos em Moçambique e dos serviços bancários móveis o número de casos de crimes cibernéticos tenderá a crescer a medida que a sofisticação destes meios vai se verificando. Portanto, vem constituir um desafio maior das operadoras de telefonia móvel conferir maior segurança a informação dos consumidores dos seus serviços e, como tal, assiste-se no contexto de aprimoramento de estratégias de segurança de informação verte-se naturalmente a necessidade de implementar mecanismos de interoperabilidade de sistemas de informação.

As empresas ligadas aos serviços de telefonia móvel enfrentam uma realidade dura: antecipar, responder e reagir à riscos de ataques cibernéticos, o que implica que, num ambiente de competitividade intensa, a estratégia de reacção a estes ataques não determina apenas o sucesso, mas a sobrevivência das empresas, pelo que uma boa estratégia de segurança de dados centra-se na agressividade e utilização eficiente dos sistemas de informação (Gilman, 2013).

Como descrito no paragrafo anterior a interoperabilidade de sistemas de informação traz também desafios às organizações que a promovem sendo que partes destes desafios surgem durante o desenho e desenvolvimento dos projectos de interoperabilidade de sistemas de informação. Assim sendo, como compreende-se a interoperabilidade de sistemas de informação de telefonia móvel como mecanismo viável de segurança de informação para mais eficiente cobertura a resposta dos incidentes ligados a crimes cibernéticos a partir do rastreio de informação atinente aos praticantes destes crimes, a presente pesquisa incide-se no esboço de um modelo que permite a interoperabilidade entre os sistemas de informação de telefonia móvel com os serviços de identificação e tributação civil assim como com dos mesmos serviços com a entidade reguladora de comunicação em Moçambique que é o Instituto Nacional de Comunicação de Moçambique (INCM).

1.4. Pergunta de pesquisa

Para materialização da pesquisa o presente estudo propõe-se as seguintes questões de investigação:

a) Quais são os componentes e as directrizes que permitem um modelo de sistema interoperável entre os sistemas de informação governamentais com os das operadoras de telefonia móvel?
b) De que forma a introdução do modelo de interoperabilidade proposto poderá servir de mecanismo de prevenção de crimes cibernéticos?

1.5. Objectivos

1.5.1. Objectivo Geral

Propor a Implementação da Interoperabilidade entre os Sistemas de Informação da carteira móvel e os dos serviços de identificação civil como mecanismo de prevenção de crimes cibernéticos.

1.5.2. Objectivos Específicos

- Descrever os mecanismos de prevenção e reposta das operadoras de telefonia móvel em Moçambique no que se refere aos crimes cibernéticos baseados em engenharia social;
- Retratar a representação do modelo de cadastro único móvel identificando os fluxos de comunicação entre os diferentes intervenientes do mesmo modelo;
- Caracterizar as principais recomendações e requisitos associados a implementação do mecanismo de interoperabilidade proposto para a prevenção de crimes cibernéticos em Moçambique.

1.6. Metodologia

1.6.1. Processo de investigação

Para responder os objectivos preconizados para o presente estudo conduzir-se-á uma investigação regida por três fases, nomeadamente: conceptual, metodológica e empírica (Lakatos & Marconi, 2012). As etapas previstas para cada fase são de seguida delineadas no esquema abaixo:

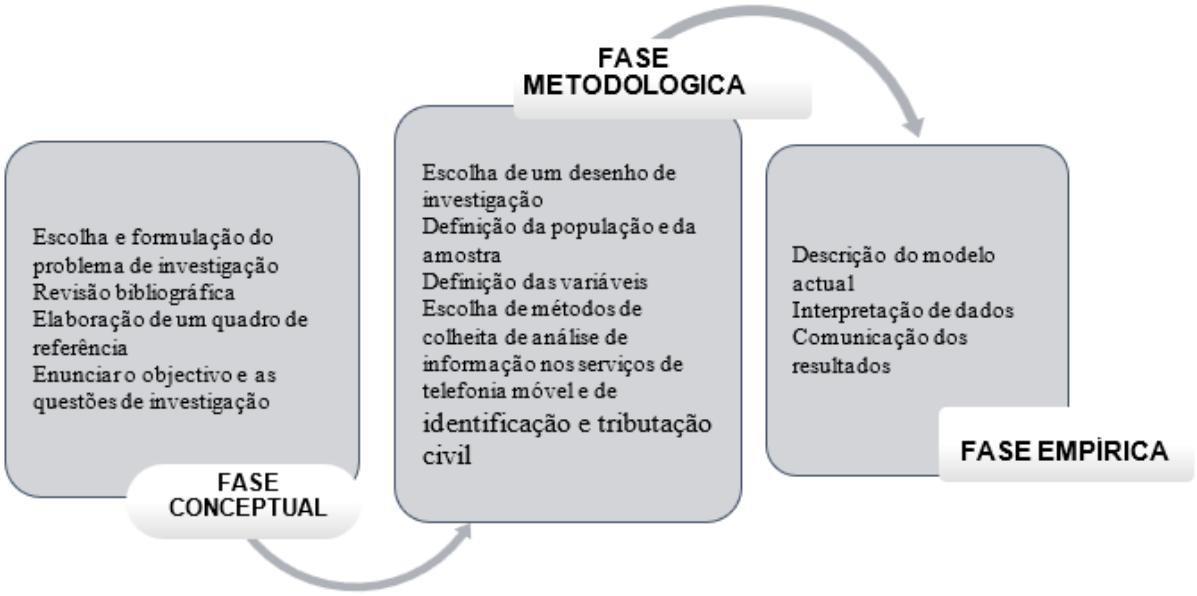

Figura 1.Etapas do Processo Metodológico de Trabalho Científico

Fonte: adaptado pela autora extraído da obra de Lakatos & Marconi (2003)

1.6.2. Métodos de pesquisa

A metodologia da pesquisa ocupar-se-á de um estudo de caso, método empírico, aplicado-descritivo, com combinação de metodologias qualitativa e quantitativa, apoiado nas técnicas de observação directa, revisão bibliográfica, documental indirecta publicado em livros, revistas e material acessíveis ao público e colectados em fontes primárias (site do Governo Electrónico) e secundárias (Documentos oficiais dos Serviços de Identificação Civil, relatório do INAGE e Estratégia Nacional de Segurança Cibernética), estruturado da seguinte forma:

- Em relação aos procedimentos metodológicos, o trabalho irá apresentar-se mediante um estudo de caso que, por seu turno, se caracteriza de acordo com Wagner (1999) pelo estudo concentrado de um único caso, o qual é preferido pelos pesquisadores que desejam aprofundar seus conhecimentos de um determinado caso específico. Portanto, como o contexto é de interoperabilidade de Sistemas de Informação dos serviços bancários moveis e os de identificação civil, o autor cingiu-se em focar em 3 entidades bancárias como caso de estudo e os próprios serviços de identificação civil da Cidade de Maputo;

- A pesquisa desenvolvida foi de campo, por ser uma investigação empírica realizada dentro do próprio local onde ocorre o fenómeno do objecto de pesquisa, por isso a pesquisa foi realizada tomando a entrevista a agentes bancários e funcionários dos serviços de identificação civil, para ter se entendimento do funcionamento dos mesmos serviços;
- A referida pesquisa é de natureza aplicada, segundo Vergara (2003), fundamentalmente motivada pela necessidade de resolver problemas, mais imediatos, e, possui finalidade prática. A pesquisa visa identificar elementos a partir de um modelo de interoperabilidade como forma de elevar a eficiência na identificação dos praticantes dos crimes cibernéticos.

1.6.3. Processo de recolha de dados

O processo de recolha de dados é feito o levantamento e avaliação de informação recolhida no campo (variáveis de interesse), em concordância com metodologia estabelecida, que permitem responder as perguntas de pesquisas e avaliar resultados.

1.6.3.1. Descrição das entidades de recolha de informação

Os dados e a informação foram recolhidos nas 3 redes de telefonia móveis nacionais nomeadamente Vodacom, TMcel e Movitel assim como foi recolhida nos serviços de identificação e tributação civil de Maputo. A nível dos serviços de identificação e tributação civil foram feitas questões relacionadas com a informação presente na base de dados destes serviços e possíveis “focos” que a instituição almeja ter em termos de outras variáveis de identificação.

De forma indiferente as questões que foram abordadas as agências focalizaram nos formatos de pesquisa para identificação de crimes cibernéticos e possíveis protocolos que as operadoras móveis com as autoridades civis para a facilitação da cobertura e resposta a estes casos com base na experiência de cada operadora.

1.6.3.2. Considerações éticas

Para não ferir os interesses das operadoras móveis que foram consultados para dar efeito ao presente estudo, não serão citados os referidos nomes e cargos das pessoas envolvidas no processo de inquirição como forma de proteger os seus compromissos e respeitar a sua atuação.

1.6.3.3. Metodologia de desenvolvimento do Sistema de Informação

Software de modelação dos diagramas de caso uso (Draw.io)

Segundo Vazquez e Guilherme (2015), o **Draw.io** é um editor gráfico online no qual é possível desenvolver desenhos, gráficos e outros sem a necessidade de usar um software caro e pesado. Ele disponibiliza recursos para criação de qualquer tipo de desenho, porém, possui uma parte dedicada à arquitectura da informação.

Linguagens de Programação

Segundo Debastini (2015), as linguagens JavaScript, HTML e CSS constituem as três principais linguagens da *World Wide Web* (WWW):

- **JavaScript-** é uma linguagem de programação de Scripts na web que se caracteriza por uma linguagem de programação interpretada estruturada, de script em alto nível com tipagem dinâmica fraca e multiparadigma (protótipos, orientado a objeto, imperativo e, funcional);
- **HTML**- (*Hyper Text Markup Language)* é uma linguagem de marcação utilizada na construção de páginas na Web. Documentos HTML podem ser interpretados por navegadores. A tecnologia é fruto da junção entre os padrões HyTime e SGML. HyTime é um padrão para a representação estruturada de hipermídia e conteúdo baseado em tempo;
- **CSS**- (*Cascading Style Sheet)* é usado para estilizar elementos escritos em uma linguagem de marcação como HTML.

1.6.3.4. Conceitos gerais da modelação

Segundo Daniela (2017), os requisitos para a modelação de um sistema em Javascript incluem dois requisitos a conhecer: os requisitos do sistema e os requisitos funcionais. Abaixo são apresentadas ambas definições na abordagem de Daniela (2017).

(a) Requisitos do Sistema: são descrições acerca do que o sistema deverá fazer, tanto a nível de serviços que ele fornece como a nível das suas restrições operacionais.

(b) Requisitos Funcionais: são declarações de serviços que o sistema deve fornecer, de como o sistema deve reagir a entradas específicas e de como o sistema deve se comportar em determinadas situações e que em alguns casos os requisitos funcionais também podem explicitar o que o sistema não deve fazer.

De acordo com Daniela (2017), para requisitos funcionais são “requisitos relacionados ao resultado de algum comportamento a ser fornecido por uma função do sistema”. Com base nessas duas definições temos que requisitos funcionais são descrições de um comportamento que o sistema exibirá atendendo certas condições.

Diagrama de Casos de uso

Primeiramente antes de debruçar sobre os diagramas de caso de uso faz sentido definir os casos de uso. Segundo Vazquez e Guilhermen (2015), um caso de uso é um tipo de classificador representando uma unidade funcional coerente provida pelo sistema, subsistema, ou classe manifestada por sequências de mensagens intercambiáveis entre os sistemas e um ou mais actores.

De acordo com Debastiani (2015), um caso de uso capta as interações que ocorrem entre produtores e consumidores de informação e o sistema em si. O mesmo autor secunda que os diagramas de caso de uso são simples modelos que documentam de uma maneira esquemática as funcionalidades de um sistema no diapasão do utilizador e também as inter-relações das funcionalidades de uma aplicação e as relações entre elas e o seu ambiente.

Segundo Vazquez e Guilherme (2016), existem basicamente 4 elementos que compõem um diagrama de requisitos:

- **Actores:** Representam pessoas ou sistemas que interagem com o sistema modelado;
- **Caso de uso:** Representam as funcionalidades esperadas pelo sistema;
- **Associações/Relações:** Representam as relações entre os actores e os casos de uso;

- **Limite do Sistema:** Representa o limite que separa as partes do caso de uso que pertencem ao sistema, das partes (pessoas ou sistemas) que estão fora do limite do sistema.

Diagrama de Componentes e Implantação

Daniela (2017), explica sobre a existência dos diagramas de componentes, diagramas de implantação e diagramas de sequência. A mesma autora diferencia ambos explicando que:

- **Diagrama de Componentes -** "O diagrama de componentes apresenta uma visão estática de como o sistema será implementado e quais os seus módulos de software, ou seja, os seus componentes".

  Assim sendo o diagrama de componentes apresenta os seguintes elementos:

  - Componentes: representam arquivos, módulos, bibliotecas que os sistemas detêm;
  - Dependência: Representa a relação de dependência entre os diversos componentes;
  - Interface: Representa um serviço realizado por uma Classe ou Componente.

- **Diagrama de Implantação -** "O diagrama de implantação é aquele com a visão mais física da UML. Trata-se do diagrama que enfoca a questão da organização da estrutura física sobre o qual o software irá ser implantado e executado em termos de hardware". Assim sendo o diagrama de implantação apresenta os seguintes elementos:

  - **Nós**: Representam uma máquina, servidor, etc., em que um ou mais módulos do software são executados;
  - **Associações**: Representam as ligações entre os nós.

1.7. Motivação

O crescimento no número operadoras móveis e provedores de serviços na área de comunicação, permitem a interação por meio eletrónico. Segundo a INCM, de 1992 a 2017, passou-se de um único operador de telefonia fixa para três de telefonia móvel celular, registando mais 13 milhões de subscritores de telefonia móvel celular e mais de 83 mil de telefonia fixa, com 69 provedores de serviços que cobrem 11 províncias. Porém esse crescimento traz consigo ataques cibernéticos cada vez mais sofisticados, golpes e inconvenientes para os consumidores o que torna um desafio as operadoras móveis.

Sendo a segurança de informação fundamental no valor não só das telefonias moveis nacionais bem como dos potenciais clientes "usuários" aplicado em todos aspectos

de proteção de informações e dados, o que motiva a autora a realizar o presente trabalho monográfico por forma a minimizar o impacto de crimes cibernéticos incididos sobre as telefonias moveis.

1.8. Estrutura do Trabalho

O presente trabalho é composto por cinco (5) capítulos, sequencialmente enumerados e uma (1) secção não enumerada, composta pela bibliografia. A sua organização é apresentada do seguinte modo:

- **Capítulo I: Introdução** – consiste da parte introdutória, onde é feita a contextualização do estudo, são apresentadas os objectivos, o problema de estudo a pergunta de pesquisa e a relevância do estudo;
- **Capítulo II: Revisão da Literatura –** neste capítulo são apresentados a fundamentação teórica dos principais conceitos a volta do tema em estudo nomeadamente: os crimes cibernéticos, definição, históricas do surgimento, tipologias e mecanismos de prevenção e resposta e por fim o tratamento dos crimes cibernéticos em Moçambique (estratégia, normas, estatísticas de incidência e mecanismos de prevenção e resposta);
- **Capítulo III: Caso de Estudo** – neste capítulo aborda-se de forma detalhada a incides predominante nas operadoras de telefonia movel, bem como sobre o a utilização de um modelo de interoperabilidade de sistemas de informação;
- **Capítulo IV: Resultados e discussão** – este capítulo consiste em apresentar o modelo actual implementado pelas operadoras móveis no registo de clientes, o modelo proposto de cadastro único proposto com os fluxos de informação entre os diferentes sistemas de informação dos intervenientes do processo de cadastro único móvel;
- **Capítulo V: Conclusões e recomendações**– são apresentadas as principais conclusões em conformidade com os objectivos propostos e são apresentadas as recomendações;
- **Secção de Bibliografias** – por fim são apresentadas todas as referências de autores, obras constantes na narrativa do texto.

2. CAPÍTULO II - REVISÃO DA LITERATURA

2. Revisão da Literatura

O presente capítulo apresenta os principais conceitos que norteiam o presente trabalho, nomeadamente a interoperabilidade a diferença entre interoperabilidade e integração, segurança de informação, crimes cibernéticos e as políticas de prevenção e resposta implementadas em Moçambique.

2.1. Interoperabilidade

Segundo a Comissão Europeia (2004) a interoperabilidade consiste na habilidade de sistemas informáticos e processos de negócios suportados por estes garantirem o compartilhamento de informação de maneira eficaz, eficiente e coordernada e se utilizarem desta para melhor realização de suas actividade e processos.

De acordo com Novakousk e Lewis (2012), várias definições capturam a ideia geral por detrás da interoperabilidade, porém, estas tendem a focar apenas nos aspectos técnicos, muitas vezes reflectindo a crença de que a interoperabilidade é primariamente um desafio técnico, como resultado, muitos esforços para construção de sistemas interoperáveis focam apenas em tais desafios técnicos.

Porém, ultimamente, de acordo com Novakousk e Lewis (2012), vários projectistas de sistemas têm reconhecido o facto de a interoperabilidade total consistir em muito mais do que aspectos técnicos. É neste contexto que várias organizações têm estado empenhadas em ampliar o seu escopo, tal é o caso da Comissão Europeia (2004) que propõe a definição apresentada no parágrafo a seguir.

A interoperabilidade é a habilidade de diferentes organizações interagirem em torno de um objectivo comum e mutuamente benéfico, envolvendo compartilhamento de informação e conhecimento por meio dos processos de negócio que estas suportam através da troca de dados entre os seus sistemas informáticos.

Para Novakousk e Lewis (2012), apesar de não existir uma definição de interoperabilidade universalmente aceite, a última é mais completa que a anterior, pois delineia o seu amplo escopo, e reconhece a existência de factores não técnicos capazes de influenciá-la.

É importante referir que a interoperabilidade no seu conceito não é o mesmo que integração entre sistemas, eis que a interoperabilidade tem um conceito mais restrito a comunicação entre sistemas sem quaisquer tipos de dependência tecnológica, enquanto a integração confere este conceito de comunicação mais de forma

dependente. Em Moçambique a interoperabilidade ainda é um conceito “embrionário” não existem sistemas a nível da Administração Pública interoperáveis, contudo existem alguns sistemas integrados (ex: as plataformas que “correm” no E-SISTAFE geridas pelo CEDSIF, o sistema de registo de bilhetes de identidade e o sistema de registo de passaportes estão integrados na mesma plataforma).

2.1.1. Modelos de Interoperabilidade

Tanto quanto a quantidade de definições existentes, existem também vários modelos de interoperabilidade. Os modelos de interoperabilidade dividem o problema de interoperabilidade em diferentes tipos, níveis ou dimensões. Novakousk e Lewis (2012) apresentam os seguintes modelos de interoperabilidade:

- Nível de Sistema de Informação de Interoperabilidade-*Level of Information System Interoperability (LISI)*;
- Modelo de Maturidade de Interoperabilidade Organizacional-*Organizational Interoperability Maturity Model* (OIMM);
- Níveis de interoperabilidade Conceptual-*Levels of Conceptual Interoperability Model (LCIM)*;
- Quadro Modelo de Interoperabilidade Europeia-*European Interoperability Framework (EIF);*
- Quadro Modelo de Interoperabilidade em Governança-*Government Interoperability Framework (GIF)*.

Para Novakousk e Lewis (2012), embora a forma como os modelos mencionados são definidos e estruturados seja similar, os mesmos não são adequados para um modelo de interoperabilidade genérico pelo facto de serem dependentes a um domínio específico. Os mesmos autores apresentam um modelo genérico derivado dos modelos acima. O modelo apresenta inicialmente os objectivos básicos da interoperabilidade e, em seguida mapeia-os aos níveis de integração, onde os objectivos mais complexos são mapeados a níveis de interoperabilidade mais altos. Por fim, descrevem-se os factores que influenciam a interoperabilidade entre sistema.

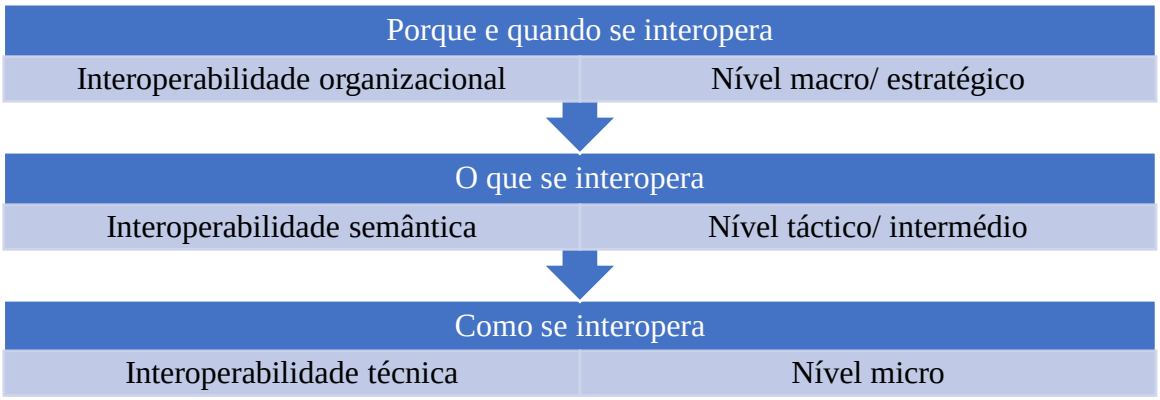

Figura 2. Dimensões/Modelos de Interoperabilidade

Fonte: adaptado pela autora

Organizacional	**Políticas de cooperação**
	Processos de trabalho, estratégias
Semântica	Intenção, significado e entendimento
	Contexto, taxonomia e semântica
	Linguagem, figura e fotos
Técnica	Dispositivos, fotos
	Interface
	Foramto dos dados
	Entrega dos dados
	Aplicação de protocolos
	Banco de dados
	Plataforma
	Segurança
	Redes

Tabela 1. Camadas de interoperabilidade

Fonte: adaptado pela autora

2.2. Objectivos da Interoperabilidade

Novakousk e Lewis (2012) apresentam três objectivos principais associados ao alcance da interoperabilidade entre sistemas (informáticos ou não), nomeadamente: (a) intercâmbio de dados; (b) intercâmbio de semântica; e (c) acordo de processos.

2.2.1. Intercâmbio de Dados

Este é o primeiro objectivo, e nele, visa-se apenas garantir o facto de haver troca de dados entre as partes da comunicação, não importando o seu significado.

2.2.2. Intercâmbio de Semântica

Este é o segundo objectivo, e nele, além do facto de garantir-se a troca de dados entre as partes da comunicação, visa-se também assegurar que as mesmas atribuem o mesmo significado aos dados que trocam. De acordo com Novakousk e Lewis (2012), este objectivo difere do primeiro devido ao aspecto da interpretação, isto é, no primeiro objectivo, a troca de dados simplesmente existe ou não, não existe meio-termo, porém, a troca de significado é mais complicada pois não existem garantias implícitas de que as partes irão interpretar os dados da mesma forma.

2.2.3. Harmonia entre Processos

Este é o terceiro objectivo, e nele, visa-se garantir um acordo sobre como deve-se agir sobre a informação trocada entre as partes da comunicação. De acordo com Novakousk e Lewis (2012), este objectivo difere dos dois anteriores pelo facto de mudar o foco, da transferência de dados para as acções que podem ser tomadas sobre os dados uma vez que estes tenham sido trocados.

Para garantir este objectivo, todos os participantes da comunicação devem acordar de antemão sobre o que deve ser feito em relação aos dados que recebem. Muitas vezes, a ausência de harmonia entre processos caracteriza-se pelo facto de um consumidor de um serviço dever fornecer a mesma informação a várias unidades da mesma organização, no decurso de um mesmo evento.

2.3. Níveis de Interoperabilidade

A ideia fundamental por detrás dos níveis de interoperabilidade é, como relacionar os objectivos básicos da interoperabilidade para atingir objectivos mais complexo. A

interoperabilidade no seio de TIC pode ser classificada em três categorias, nomeadamente: (a) interoperabilidade técnica; (b) interoperabilidade semântica; e (c) interoperabilidade organizacional.

2.3.1. Interoperabilidade Técnica

A interoperabilidade técnica está directamente mapeada ao objectivo de intercâmbio de dados. Esta é posicionada na base pelo simples facto de a troca de dados constituir a base para qualquer comunicação.

Vários modelos de interoperabilidade subdividem este nível em vários subníveis com o objectivo de abordar modos específicos de comunicação bem como separar os dados do meio de comunicação.

A interoperabilidade técnica por sua vez está subdividida em pelo menos quatro camadas ou categorias, nomeadamente:

- **Interconexão -** volve padrões relacionados com a rede de computadores e o desenvolvimento de sistemas. Esta camada garante a comunicação entre diferentes sistemas;
- **Integração de dados -** contém padrões usados para a descrição dos dados trocados entre sistemas distintos;
- **Acesso à Informação e Apresentação -** refere-se à apresentação dos dados ao utilizador final em vários meios de acesso;
- **Gestão de Conteúdo e Metadados -** envolve os padrões usados para o acesso e gestão o funcionamento de toda a plataforma de interoperabilidade.

2.3.2. Interoperabilidade Semântica

A interoperabilidade semântica é mapeada ao objectivo do intercâmbio de significado. Esta é posicionada sobre o nível de interoperabilidade técnica pelo facto de ser necessário garantir a troca de dados para que haja troca de sentido.

2.3.3. Interoperabilidade Organizacional

A interoperabilidade organizacional é mapeada ao objectivo de harmonia entre processos. A mesma é posicionada no nível mais elevado pelo facto de ser impossível harmonizar processos sem antes garantir a troca de dados e, em seguida o entendimento do seu significado entre as partes da comunicação.

2.4. Componentes do Modelo de Interoperabilidade

Segundo a Alves & Moreira (2004), ao se estabelecer um modelo de interoperabilidade deve-se ter em consideração os múltiplos componentes que se referem a cada uma das áreas que serão afectadas pelo desenvolvimento do modelo.

Os modelos de interoperabilidade de acordo com Novakousk & Lewis (2012), englobam uma série de padrões e especificações técnica de forma a uniformizar as práticas dos órgãos estatais e alcançar a interoperabilidade irrestrita dos serviços de governo electrónico.

Conforme os autores acima citados existem pelo menos cinco componentes básico que devem integrar um modelo de interoperabilidade, abaixo a especificação de cada um dos componentes, nomeadamente:

- **Infra-estrutura Tecnológica**: corresponde às componentes tecnológicas necessárias para que seja colocado em marcha o modelo escolhido, ou seja, a plataforma através da qual ocorre o intercâmbio, os conectores de ponta que ligam provedores e consumidores de informação, bem como definições técnicas e semânticas para o intercâmbio de dados;
- **Processos de Atenção**: correspondem aos modelos de gerenciamento de processos de negócios, *business process management* que devem ser desenvolvidos e implicam o mapeamento dos serviços e processos de negócios que serão suportados pela infra-estrutura tecnológica, tais processos englobam a adopção de acordos relativos aos níveis de serviço para a operação entre consumidores e provedores de informação;
- **Standards**: desenho e definição de padrões a serem observados no desenvolvimento dos dois itens anteriores. No caso concreto os padrões são determinados no contexto da interoperabilidade em Moçambique pelo e GIF4M, que cobre todos os elementos técnicos envolvidos. Os *Standards* devem assegurar a evolução necessária e prever mecanismos que permitam dar conta de novos requerimentos de intercâmbio;
- **Marco Jurídico**: tendo em conta os limites da ordem jurídica de um país, em relação a questões como dentre inúmeras outras, a aplicação de TIC pela Administração Pública, o intercâmbio de informações, a privacidade e a salvaguarda de dados, as formas de relacionamento entre a Administração Pública e demais actores sociais. O modelo de interoperabilidade deve contar

com um arcabouço jurídico-normativo que delimite, de forma inovadora ou que de acordo com o ordenamento jurídico vigente: a responsabilidade pela implementação e desenvolvimento do projecto, o alcance de iniciativas, os trâmites e procedimentos comuns desenhados para o intercâmbio de dados, bem como a forma de relacionamento entre o papel e as responsabilidades de cada, um dos actores envolvidos na iniciativa;

- **Marco Institucional**: para garantir a viabilidade e a sustentabilidade do modelo de plataforma de interoperabilidade selecionado, é preciso que se estabeleçam levando-se em conta as características dos f*rameworks* institucionais formais e informais existentes os arranjos institucionais apropriados com a delimitação do papel de cada um dos actores responsáveis pelo desenvolvimento, pela implementação e pelo funcionamento da plataforma de interoperabilidade (operação tecnológica, pela gestão das operações de rotina, bem como pela gestão reguladora de tramites de acesso/adesão e processos de troca de informação através da plataforma).

2.5. Diferença de Interoperabilidade e Integração

Na literatura são várias as definições para integração de sistemas. Madni (2014), descreve a integração de sistemas como “o foco na formação de um todo coerente a partir de componentes de sistemas (incluindo humanos) capaz de satisfazer as necessidades de diferentes *stakeholders*”. Na mesma linha, Madni (2014) definem que “a integração de sistemas de informação engloba sistemas distribuídos (com múltiplos módulos de *software* ou componentes que correm em dois ou mais computadores/servidores) ou heterogéneos para que possam interagir entre si e potenciar a integração de múltiplas aplicações individuais numa única”.

A integração envolve dois ou mais sistemas conectados, sendo que há entre eles uma relação de dependência tecnológica.

Por outro lado, Glenny (2011), afirmam que de forma resumida, a interoperabilidade encontra-se entre a compatibilidade e a integração total, pelo que é importante distinguir os conceitos de compatibilidade, interoperabilidade e integração, uma vez que a incapacidade de o fazer pode muitas vezes complicar o debate sobre como atingir cada um deles.

A interoperabilidade pode ser definida como a capacidade de dois ou mais sistemas estabelecerem uma comunicação de forma eficaz, garantindo a integridade dos dados e os resultados almejados pelos stakeholders sem que haja entre eles dependência tecnológica.

Interoperabilidade	Integração
Coexistência	Unificação
Autonomia	Assimilação
Fraca interdependência	Forte dependência

Tabela 2. Diferença entre os conceitos de Interoperabilidade e Integração

Fonte: (Alves & Moreira, 2004)

Segundo Alves & Moreira (2004), os sistemas interoperáveis não têm de estar necessariamente integrados, ao contrário do que sucede na integração, em que as conexões estabelecidas entre os sistemas são rígidas e fixas, as conexões entre sistemas interoperáveis são mais flexíveis, sendo fáceis de estabelecer e alterar.

2.6. Segurança de informação, fundamentação teórica

Para Bravo (2014), a segurança da informação é “prevenção e detecção de acções não autorizadas por utilizadores de um sistema de computadores”.

De acordo com Sêmola (2014), “podemos definir segurança da informação com uma área de conhecimento dedicada a protecção de activos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Como pode-se verificar os conceitos acima apresentados, pode-se concluir que todos conceitos tem a sua razão de ser, contudo para o autor o conceito apresentado por Galvão (2015), é o mais consistente, pois percebe-se ter uma informação segura dentro da organização e necessário ter uma área de conhecimento dedicada de conhecimentos específicos por parte dos profissionais que nele representa. Esses profissionais terão de garantir que a informação não sofrerá nenhuma alteração ou acesso não autorizado, garantindo sempre a disponibilidade das informações para o acesso autorizado.

Segundo Bravo (2014), existem outras áreas que estudam a segurança da informação, porém cada uma delas se dedica mais detalhadamente aos aspectos próprios da sua área e não de forma abrangente, com a preocupação de agrupar os vários aspectos que envolvem a segurança. O mesmo autor refere que a ciência da computação, por exemplo, dedica-se mais aprofundadamente aos aspectos tecnológicos da segurança da informação; na administração se estudam, com muita propriedade, os aspectos relacionados aos processos. Já os aspectos relacionados a pessoas são estudados por várias áreas, como administração, psicologia, pedagogia, dentre outras. O autor ainda afirma que o estudo com visão multidisciplinar é próprio da ciência da informação, pois isso está em sua gênese.

Para Bolt (2013), parece ser apropriado que a segurança da informação seja objecto de interesse também da ciência da informação, a qual poderia estudá-la com uma visão mais holística, de modo a reunir os diversos aspectos que a envolvem, bem como a inter-relação existente entre eles.

Dados mais detalhados acerca do mapa apresentado por Bravo (2014), são referenciados no resultado do estudo por Sêmola (2014), que afirma que o mapa *basehouse* é o resultado de um estudo conduzido de 2003 a 2005, que foi publicado em uma série de quatro artigos no qual o autor utiliza a metodologia Delphi. O estudo contemplou as respostas de 57 líderes acadêmicos em ciência da informação de 16 países, para as seguintes questões: 1) definições de conceitos fundamentais de dados, de informação, de conhecimento e de mensagem; 2) concepções alternativas em relação ao domínio da ciência da informação; 3) diferentes mapeamentos classificatórios da área; e 4) mapeamento compreensivo da ciência da informação. O autor propõe a organização da área em uma taxonomia com dez facetas, a saber: fundamentos multidisciplinares, fontes, trabalhadores do conhecimento, conteúdos, aplicações, operações e processos, tecnologias, ambientem, organizações e usuários.

Segundo Bolt (2014), que abrange a origem, a colecta, a organização, o armazenamento, a recuperação, a interpretação, a transmissão, a transformação e a utilização da informação. Esses aspectos dão suporte, para que a informação gerada ou capturada possa ser guardada e preservada com integridade, pelo período necessário, a fim de que possa ser recuperada e utilizada posteriormente. Porém, a informação está sob constante risco, em qualquer uma das etapas de seu ciclo de vida, razão pela qual deve ser protegida contra vários tipos de ameaças. O principal

objetivo da segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação. Além disso, se preocupa com a identificação de vulnerabilidades e a gestão dos riscos associados aos diversos ativos informacionais, independentemente da forma ou do meio em que são compartilhados ou armazenados. Dessa forma, a segurança da informação deve contemplar todos os itens que compõem o corpo de conhecimento da informação, para que, ao ser utilizada no futuro, a informação seja a mesma gerada no passado, com suas propriedades e suas características preservadas.

2.6.1. Características básicas de segurança informação

As características básicas da segurança da informação são representadas pela tríade conhecida por CIA (Confidencialidade, integridade e Disponibilidade), demonstrados na figura 3.

Figura 3. Segurança de informação-Tríade CIA

Fonte: Segurança de informação-Tríade CIA Fonte: Abreu (2011)

2.6.2. Confidencialidade

De acordo com Galvão (2015),” a informação apenas deve ser utilizada e acessada exclusivamente por quem necessita da informação e por quem tem permissão de acesso e uso dentro das organizações”. Para Galvão (2015), “confidencialidade representa a garantia que a informação estará acessível somente para a pessoa

autorizada. Se uma pessoa sem autorização tem conhecimento, ocorre uma violação de privacidade". Em outras palavras, privacidade esta relacionada com a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

2.6.3. Integridade

De acordo com Galvão (2015), a integridade pode ser entendida como "a detecção de alterações como sejam adições ao conteúdo, eliminação parcial ou qualquer outra modificação por pessoas não autorizadas a fazê-lo.". De acordo com o mesmo autor, a integridade refere-se à indicação inequívoca de quem as mensagens transmitidas entre emissor e receptor não tenham sido adulteradas acidentalmente ou por terceiros ao longo do trajecto entre estes nós.

Segundo Galvão (2015), "integridade visa garantir que as informações armazenadas estejam corretas, verdadeiras e não sofreram nenhum tipo de alteração e violação. É a garantia de que os dados armazenados coincidem com os incluídos".

2.6.4. Disponibilidade

De acordo com Galvão (2015), "disponibilidade é a garantia de que, quando as pessoas autorizadas solicitem alguma informação. Estas estejam disponíveis". De outra forma, é a propriedade da informação estar acessível e utilizável quando solicitada por uma pessoa autorizada. De acordo com o mesmo autor de forma simplificada pode-se afirmar que a disponibilidade é a garantia de que os usuários autorizados tenham acesso a informações e activos associados quando necessário.

2.7. Ameaças a segurança da informação

Segundo Sêmola (2014), "ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus activos por meio da exploração de vulnerabilidades, gerando incidentes de perda de confidencialidade e impactos aos negócios da empresa". De acordo com o autor as ameaças da segurança da informação são todas acções que impossibilitam o funcionamento das características básicas da segurança da informação.

Vulnerabilidade é definida como uma falha no projecto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Sêmola (2014), afirma que "vulnerabilidades são fragilidades presentes ou associadas a activos que manipulam e/ou processam dados. Elas não provocam incidentes, por serem dados passivos, necessitando de um agente causador ou condição favorável, vazamento ou incêndio".

De acordo com Galvão (2015), "fraqueza e fragilidade estão relacionados ao activo da empresa e podem ser compreendidos como vulnerabilidade na estrutura organizacional, facilitando uma ameaça, causando um incidente".

Compreende-se a necessidade de citar a diferença entre a segurança de informação e a segurança cibernética, mas vale considerar ambos conceitos porque para o contexto do presente estudo existe uma ligação estreita entre estes conceitos. Ambos conceitos têm a ver com segurança e proteção de sistemas de computador contra violações de informações e ameaças, mas também são diferentes. A segurança cibernética tem a ver com a proteção de dados do ciberespaço, enquanto o outro trata da proteção de dados em geral. As estratégias e normas implementadas pelo INAGE visam garantir a prevenção e a prontidão aos crimes cibernéticos, mas não descartam a necessidade de os sistemas de informação dentro da Administração Pública apresentarem o preceito "CIA ou CID" para garantir a eficácia da implementação destas normas. Portanto de seguida são apresentados os conceitos ligados a segurança cibernética.

2.8. Segurança Cibernética

Antes de introduzir o conceito de segurança cibernética interessa indagar (informar-se/averiguar) acerca do ciberespaço. Segundo Sêmola (2014), o ciberespaço (ou espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens electrónicas, salas de bate-papo, grupos de discussão, dentre outros. O termo foi criado por Willian Gibson em seu romance "Neuromancer". (Sêmola, 2014). Em relação aos conceitos tanto de Segurança Cibernética quanto de Defesa Cibernética, cabe colocar que estes vêm sendo construídos com a presença de diferentes e importantes agentes, no país.

Entende-se que o escopo de actuação da Segurança Cibernética compreende aspectos e atitudes tanto de prevenção quanto de repressão. E para a Defesa Cibernética entende-se que a mesma compreende acções operacionais de combates ofensivos.

Falando da origem do termo Bravo (2014), o termo Ciberespaço pretende caracterizar o “mundo paralelo” que se desenvolve na, e através, de redes digitais, sendo uma das mais comuns e conhecidas a Internet. O termo surgiu em 1984, pela mão de William Gibson, caracterizando precisamente a vivência e experiências das pessoas na rede. Actualmente é de certa forma vulgar associar o termo Ciberespaço à Internet ou, como é por vezes referida, à "rede de redes", embora, como se refere anteriormente, tal associação não represente, de facto, a totalidade do Ciberespaço.

Galvão (2015), afirma que acrescenta-se que o conceito, em inglês, de Cybersecurity inclui, segundo o *Department of Homeland Security (DHS)*, a prevenção aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e respectiva informação neles contida, visando assegurar a confidencialidade, integridade, e disponibilidade, incluindo, também, ações para restaurar a informação eletrônica e os sistemas de comunicações no caso de um ataque terrorista ou de um desastre natural.”

Como um ponto de partida para a constituição de uma base conceitual nesta temática, ainda em construção, a seguinte conceituação de segurança cibernética, vem sendo adoptada na esfera pública, mais focada na comunidade de segurança da informação e comunicações, qual seja, definida por Sêmola (2014), “segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas”. É, portanto, maior que segurança em TI, pois envolve pessoas e processos.

De acordo com Galvão (2015), conceito colocado na perspectiva da *International Communications Union* (ITU) em que Cybersecurity significa basicamente prover proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens. Tais recursos e bens variam e dependem do nível de desenvolvimento dos países. Dependem, também, do que cada país considera como sendo recurso crítico, os esforços que podem e estão dispostos a realizar, bem como da avaliação do risco que estão dispostos a aceitar em consequência das inadequadas medidas de segurança cibernética. Adicionalmente, para certo número de países

desenvolvidos, há outras ameaças tais como fraude, proteção do consumidor, e privacidade, as quais consideram também como soluções da cybersecurity, forma de proteger e manter a integridade das infraestruturas críticas nos setores financeiro, de saúde, da energia, do transporte, das telecomunicações, da defesa, e de outros".

Percebe-se a partir da dissecação apresentada pelos autores acima que na actualidade que somos capazes de criar, actualizar e armazenar mais informação do que alguma vez fomos capazes no passado, mas nunca essa informação foi tão ameaçada como é hoje. Nesta senda, o autor Bolt (2013), afirma que para manter as infraestruturas sustentáveis e competitivas, vitais para a sobrevivência de nações em todo o mundo, tem-se procurado investir em mecanismos e processos que derivam da necessidade de envidar todos os esforços possíveis para garantir recursos digitais seguros. O mesmo autor ainda salienta que vivemos, de facto, num mundo interconectado, com recursos interligados em estruturas e redes e, assim, uma das principais preocupações para assegurar uma forte protecção e salvaguarda da informação tem sido a segurança dos sistemas de informação nacionais, públicos e privados, e da informação, essenciais ou importantes o suficiente para suportar as actividades de que um Estado, uma organização ou um particular depende.

2.8.1 Conceito de crimes cibernéticos

Os crimes cibernéticos são entendidos por Galvão (2015), como todo conjunto de actividades ilícitas praticadas com a utilização de computadores ou todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar.

Segundo Madni (2014), os crimes cibernéticos classificam-se em puros (próprios) e impuros (impróprios). Os crimes cibernéticos puros ocorrem quando o agente quer atacar o sistema de informática de um terceiro, seja este sistema um software, hardware, sistema e meios de armazenamento de dados.

De acordo com Galvão (2015), crimes electrónicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Segundo Galvão (2015), nota-se, que esta categoria de crime caracteriza-se quando um individuo, principalmente o *hacker* e o *cracker*, utiliza-se de um computador e/ou

internet para invadir a máquina de um terceiro, sendo que o crime se consome no próprio meio virtual, não produzindo efeitos fora deste ambiente.

Madni (2014), afirma que destaca-se a presença de duas figuras nesta mesma conjuntura: Os hackers e os crackers. Segundo a mesma autora, um dos significados do termo hacker é: “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”. Fazendo uma análise sobre a acepção desta palavra, podemos concluir que esta é a pessoa que detém um conhecimento singular acerca do assunto e que não necessariamente o use com o propósito de atuar na ilegalidade porque a partir desse discernimento conclui-se que o domínio no referido assunto pode ser visto de forma positiva e negativa. Já os crackers são pessoas que agem focando a vantagem ilícita. Eles invadem e destroem sites, sejam eles quais forem, fazem quebra de senhas, desenvolvem softwares capazes destruir várias máquinas ao mesmo tempo (Madni, 2014).

O crime cibernético impuro diferente dos crimes cibernéticos puros, esta forma de delito usa o computador como um mero instrumento para a realização deste. Numa definição aceite como consensual e pragmática é a de Galvão (2015), que afirma “os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática.” Desta forma, os crimes impuros são aqueles em que o agente utiliza-se do computador e da internet como ferramenta meio para produzir um resultado que afeta outros bens tutelados pelo nosso ordenamento jurídico que não sejam relacionados aos meios virtuais.

Ainda segundo Galvão (2015), após uma década, mais precisamente no ano 2000, a ONU relacionou outros tipos de crimes cibernéticos, elaborados no 10º Congresso sobre Prevenção de Delito e Tratamento de Delinquente, realizado em Viena, os quais seguem abaixo:

- Espionagem industrial para descoberta de segredos comerciais, técnicas e estratégias; sabotagem de sistemas;
- Sabotagem e vandalismo de dados;
- Lavagem de dinheiro;
- Jogos de azar; fraudes, principalmente contra consumidores;
- Pornografia infantil;

- Estratagemas, com intuito de buscar sistemas restritos;
- Averiguação de senhas secretas.

2.8.2. Factores que favorecem a ocorrência de crimes cibernéticos

Nos últimos anos o desenvolvimento tecnológico ganhou significativa importância nos domínios políticos, sociais e económicos, sendo a Internet actualmente o maior fenómeno social conhecido e aquele que produz um grande impacto na vida diária das sociedades, das organizações e dos Estados.

Segundo Bravo (2014), o acesso fácil e intuitivo, muitas vezes anónimo, a milhões de sites em todo o mundo, com praticamente todo o tipo de informação necessária, tornam o Ciberespaço um espaço flexível e abrangente de comunicação, ou, numa perspectiva um pouco mais crítica e como bem refere o autor "(…) a uma lógica do espectáculo que leva a um consumo em excesso de imagens e de informações sem qualquer efeito numa melhor compreensão das coisas do mundo". Por esse motivo, o autor fundamenta que da mesma forma como acontece no relacionamento entre seres humanos, o Ciberespaço tem sido usado também para satisfazer interesses ilícitos de indivíduos e grupos, que encontram na Internet a oportunidade de satisfazer os seus interesses e potenciar o impacto e abrangência das suas acções.

Segundo Fernandes (2010), a própria natureza pública da Internet, anárquica e potencialmente insegura, constitui paradoxalmente um dos factores mais relevantes para o seu sucesso, razão pela qual é neste momento "terreno fértil" para as interacções diárias entre as pessoas e as organizações, assim como para o desenvolvimento de acções pouco éticas, ilícitas e criminais. A respeito deste fenómeno importa salientar também o factor humano como uma das fontes de insegurança na utilização dos recursos tecnológicos, factor esse amplamente explorado através de métodos por vezes ilícitos ou de moral duvidosa, como por exemplo publicidade encoberta ou ataques de Engenharia Social, que procuram tirar partido da apetência natural do ser humano para ser crédulo, curioso e social.

De acordo com Bravo (2014), actualmente, estar ligado à Internet tornou-se uma necessidade diária para as pessoas enquanto indivíduos ou enquanto colaboradores de uma organização, independentemente da sua dimensão e influência, moldando a forma como apreendem e percepcionam a realidade. A extrema dependência de soluções que agora nos parecem simples, como o correio electrónico, compras online,

interacção com organizações e com o próprio Estado, ou soluções de videovigilância, encontra-se sustentada normalmente na Internet e em tecnologias associadas, sendo difícil imaginar a vivência das sociedades desenvolvidas sem estes recursos.

Segundo Bolt (2013), o crescimento de ataques resulta essencialmente do exponencial crescimento e desenvolvimento das tecnologias associadas à Internet e à computação. Este crescimento tem provocado uma espiral de oferta e procura difícil de acompanhar pelas organizações responsáveis pelo desenvolvimento de soluções computacionais de Cibersegurança, uma vez que a demanda e ritmo.

Segundo Glenny (2011), há elevados a que os artefactos de *software* são disponibilizados que inviabilizam por vezes a capacidade de se testar eficazmente esses artefactos no que respeita à sua segurança e vulnerabilidades. São precisamente estas vulnerabilidades que são depois amplamente exploradas com diferentes finalidades, encontrando-se entre elas as finalidades criminais.

Fernandes (2010), afirma que a grande maioria dos ataques e acções ilícitas desenvolvidas na e pela Internet não se revestem de grande complexidade, antes resultando o seu sucesso, em maior proporção, da fragilidade do factor humano na sua interacção com as tecnologias do que das fragilidades endógenas dessas mesmas tecnologias. Segundo o mesmo autor é de facto reconhecido que um grande ataque cibernético requer tempo, por vezes dinheiro, conhecimentos e inteligência, mas é também um facto que estes recursos estão, cada vez mais, disponíveis para a generalidade das pessoas. O autor ainda secunda que por esse motivo tem também sido reconhecida a utilização da generalidade das ferramentas disponibilizadas na Internet pelas organizações criminais ou grupos activistas, como forma de manifestarem os seus intentos ou como forma de recrutar apoiantes, angariar fundos, coordenar e comunicar acções, assegurar a logística necessária e promover campanhas de intimidação.

Bravo (2014), disseca que no conjunto de interações que entroncam diferentes agentes que acedem aos serviços de internet também as realidades da cibercriminalidade e do ciberterrorismo (enquanto exemplo extremo de cibercriminalidade com propósitos de intimidação e terror estatal ou coletivo), ilícitas na sua natureza e com fundamentos e propósitos criminais, considerando-se a cibercriminalidade a atividade sustentadora e financiadora do ciberterrorismo através, por exemplo, dos proveitos provenientes da criminalidade organizada, branqueamento de capitais, extorsão, etc. O autor secunda que são vários,

recorrentes e diários os exemplos destas atividades, como por exemplo as acções levadas a efeito pelo grupo *Anonymous* contra várias agências de inteligência, organizações e empresas ligadas aos órgãos de comunicação social.

Sêmola (2014), apresenta uma explicação com fundamento mais "holístico" afirmando que da mesma forma que as fronteiras físicas e históricas dos Estados há muito foram extravasadas pelo poder da comunicação e pela necessidade de interação entre as organizações, o mesmo sucede, por inerência ao próprio espaço onde se desenvolve, com o Ciberespaço. O autor secunda que ainda assim e de um certo ponto de vista, pode-se, contudo, afirmar que a interação social digital mantem na sua metodologia os mesmos pressupostos, embora aplicados nas realidades, possibilidades, recursos tecnológicos e, também, vulnerabilidades da nova era tecnológica e do Ciberespaço. Por fim o autor afirma que assiste-se agora, de facto, a uma sofisticação na comunicação no Ciberespaço, alicerçada em inteligência e processos de planeamento e desenvolvimento complexos onde um utilizador supera facilmente e de forma anónima as questões da unicidade do ser humano e mesmo as fronteiras dos Estados onde se encontra, permitindo-lhe assim considerar qualquer Estado, organização ou indivíduo como o seu interlocutor para a comunicação.

2.8.3 Soluções para prevenção de crimes cibernéticos: a integração de sistemas de informação

Ao longo das últimas décadas, as Tecnologias de Informação e Comunicação têm provocado profundas mudanças de paradigmas nas sociedades, edificando uma cultura globalizada ligando toda a Humanidade (Bravo, 2014). Esta dinâmica, alavancada pela integração da tecnologia nos mais variados aspetos das nossas vidas, de uma forma transversal a toda a sociedade e afetando indivíduos, organizações e o Estado, vêm permitindo o acesso a melhores e mais diversificados serviços tecnológicos.

Como afirma Sêmola (2014), com o exponencial crescimento da utilização das tecnologias e do Ciberespaço, a sociedade ficou também mais vulnerável, as ameaças aos sistemas de informação aumentaram e os ataques vêm provocando danos com impactos cada vez mais significativos. Nos últimos anos, os impactos potenciais e reais das ameaças à segurança no Ciberespaço tornaram-se também evidentes devido a um conjunto de incidentes com repercussões diretas na segurança dos Estados, pelo seu potencial de afetarem as infraestruturas críticas nacionais de

alguns desses Estados. O autor secunda que de facto, a tecnologia e o Ciberespaço não são apenas recursos e espaço onde se pode fazer melhor e de forma mais eficiente aquilo que outrora era difícil, demorado e dispendioso fazer. Em muitos casos esta nova realidade criou o potencial de alterar significativamente a influência de diferentes grupos ou atores nos cenários internacional e nacional, social ou empresarial, tornando-se assim assunto de debate também político, muito para além do que são as suas considerações meramente técnicas (Sêmola, 2014).

Observados os aspectos dissecados por Sêmola (2014), o autor Galvão (2015) considera assim, no que respeita à Segurança da Informação e Cibersegurança, que não podem ser desconsideradas as necessidades atuais de integração e interoperabilidade (para certos casos) entre os sistemas de informação no Ciberespaço (ao nível organizacional, semântico e também técnico). O mesmo autor fundamenta que a necessidade de sistemas de informação interligados e interoperáveis, que permitem assim alcançar uma partilha de informação eficaz e eficiente, representa hoje uma das tendências mais desejadas e desenvolvidas para alcançar os níveis desejados de competitividade e capacidade de resistência efetiva entre infraestruturas tecnológicas críticas.

Madni (2014), afirma que a questão da integração de sistemas é, de algum modo, simples de entender e gerir no contexto isolado de uma única organização, mas quando se transpõe esta realidade e necessidade para um Estado ou grupo de Estados (interoperabilidade transfronteiriça), consideramos que a questão deve ser abordada como um desafio para uma condição necessária e um elemento-chave em vários aspetos da governação dos Estados envolvidos.

Segundo Sêmola (2014), o sucesso das nações no futuro será, portanto, caracterizado pela sua capacidade de colaborar, a sua capacidade de se adaptar e sua capacidade de operar de forma interligada. Em grande parte dos casos a questão-chave não será certamente a capacidade de acesso à tecnologia adequada ou a capacidade de produzir a tecnologia necessária, mas sim a implementação dessas tecnologias que compreendem a integração de sistemas, afetando e beneficiando deste modo um número cada vez maior de pessoas. Esta é claramente uma questão que extravasa o âmbito puramente tecnológico, devendo por isso ser pensada e dirimida ao nível da decisão política, que é aquela que tem a capacidade de produzir alterações estruturais na sociedade e na forma como a mesma se desenvolve (Sêmola, 2014).

2.9. Crimes cibernéticos em Moçambique e na região austral

O crime cibernético não tem apenas impacto nas organizações, mas também no país e no continente, são necessárias estratégicas para proteger as infraestruturas do país, a segurança dos cidadãos e a integridade dos sistemas de informação (pública e privada).

2.9.1. A nível da região austral

Segundo o relatório do Ministério dos Negócio Estrangeiros de Cooperação (2020), esforços a nível da SADC iniciaram em novembro de 2012, quando os Ministros das Tecnologias de Informação e Comunicação dos países membros da SADC aprovaram as seguintes três Leis Modelo Harmonizadas para a Segurança Cibernética a nível da SADC: Lei de Comércio Electrónico, Protecção de Dados e Cibercriminalidade. Importa referir que estas leis-modelo foram desenvolvidas no âmbito do projecto HIPSSA (Harmonização das Políticas de TIC na África Subsariana) da União Internacional das Telecomunicações (UIT) e estão alinhadas com a Convenção da União Africana sobre Segurança Cibernética e Protecção de Dados Pessoais.

Dados apresentados pelo INAGE (2021), atestam que dos países membros, todos já iniciaram a domesticação das Leis Modeladas Harmonizadas da SADC e tem como compromisso concluírem o processo até dezembro de 2019, inclusive a criação dos CERTs nacionais. Com a assistência da UIT, países como Angola, Zimbabué e Moçambique iniciariam a elaboração dos termos de referência para o seus CERT, enquanto assistência técnica da CTO tem ajudado países como o Botswana a elaborar a sua estratégia nacional de segurança cibernética. Assim, apenas as Maurícias e África do Sul concluíram este processo de criação de um quadro legal para proteger o espaço cibernético. As Maurícias já aprovaram a Lei de Uso Indevido de Computadores e Cibercriminalidade (CMCA) 2003; Lei de TICs em 2001; Lei de Transações Electrónicas em 2000 e Lei de Proteção de Dados em 2004 (INAGE, 2021).

De acordo com o INAGE (2021), a Equipa de Resposta a Emergências Informáticas das Maurícias (CERT-MU) é o CERT nacional e coordena e trata as questões de segurança da informação a nível nacional desde 2008. Semelhantemente, na África do Sul foi aprovado o Quadro Nacional de Política de Segurança Cibernética (NCPF)

da África do Sul em 2012. O objetivo do NCPF é de criar um ambiente cibernético seguro, confiável que facilite a proteção de infra-estrutura crítica de informações, de segurança cibernética em apoio dos imperativos de segurança nacional e da economia.

2.9.2. Espaço cibernético e políticas de prevenção de crimes cibernéticos em Moçambique

Segunda a Resolução n.º 69/2021, 31 de Dezembro 2021, a PENSC vai ao encontro dos anseios dos moçambicanos no sentido de criarem uma visão nacional que lhes permita desenvolverem uma plataforma comum de resiliência a ataques cibernéticos ou a quaisquer outras formas de perturbação da ordem pública, com recurso às Tecnologias de Informação e Comunicação (TIC).

2.9.2.1. Políticas e Regulamentação

O Governo Electrónico fornece dados e informações aos diversos utilizadores que interagem com o sistema, por essa razão, existe a necessidade de definir privilégios de autoridade, níveis de acesso dos utilizadores a informação que cada um, destes pode manipular. Conforme a Estratégia do Governo Electrónico de Moçambique (2005), são necessários dispositivos legais como assinaturas digitais, sistemas de verificação de autenticação de terceiros e evidência electrónica.

De modo a proteger a privacidade e os interesses dos cidadãos e do empresariado, é necessário que existam bases legais no país responsáveis por regular e para facilitar o uso amplo e autorizado da informação fornecida. Actualmente o país dispõem de leis que regulam o envolvendo o uso das TIC em diferentes contextos destacando-se:

- **Lei n. º3/2017 de 9 de Janeiro (Lei das Transações Electrónicas)** – promulgada no dia 09 de janeiro de 2017, a lei das transacções electrónicas regula as transacções electrónicas, o comercio electrónico e o governo electrónico. A lei, também visa garantir a protecção, segurança dos provedores e utilizadores das TIC;
- **Lei nº35/2014 de 31 de Dezembro (Código Penal Moçambicano)** – aborda das penas referentes aos crimes informáticos, no titulo III no seu capítulo I,

ou seja, o código penal moçambicano trata das penalizações decorrentes do uso das TIC na prática de crimes tipificados pela lei;

- **Estratégia Nacional de Cibersegurança (ainda em consolidação)** – inserido no plano de acções dos países-membros da CTO, a elaboração da Estratégia Nacional de Segurança Cibernética em Moçambique visa adoptar medidas que garantam um ambiente *online* seguro, ou seja, onde utentes, negócios e o Governo estão devidamente protegidos, permitindo ao país usufruir dos benefícios das TIC em prol do desenvolvimento social e económico.

Acções a diferentes níveis tem contribuído para um crescente acesso a Internet e desenvolvimento de um ambiente em que o TIC é considerado um instrumento que contribui para uma melhor prestação de serviço tanto a nível do Governo bem como a nível do sector privado. Como parte da implementação das estratégias de TIC e da administração pública acima referidas foram implementados muitos projectos no país. Abaixo são indicados alguns destes projectos que muito impulsionaram a Governação Electrónica em Moçambique em conformidade com os dados do INAGE (2021):

- Projecto de Governo Electrónico e de Infra-estruturas de Comunicação de Moçambique (Mozambique Electronic Government and Communications Infrastructure –MEGCIP); Rede Electrónica do Governo (GovNet);
- Sistema de Informação do Pessoal do Estado (SIP);
- e-SISTAF (Sistema de Informação de Administração Financeira do Estado);
- Centros Provinciais de Recursos Digitais (CPRDs);
- Centros Multimédia Comunitários;
- Projecto e-BAU (Plataforma Integrada de Prestação de Serviços ao Cidadão)
- Projecto de Apoio a Melhoria de Qualidade e Proximidade dos Serviços Públicos dos PALOPs e Timor-Leste;
- Projecto de Formulários Electrónicos; e
- Projecto de Plataforma de Interoperabilidade.

Segundo o Ministério de Ciências, Tecnologias e Ensino Superior (MCTES, 2021), é com a visão da criação dos diferentes projectos que incluem a informatização e interoperabilidade entre sistemas que o Governo tem estado a desenvolver estratégias que garantam que o cidadão possa tirar um maior proveito das tecnologia

e beneficiar-se de um serviço mais direccionado e de qualidade, através da implementação de sistemas e disponibilização de infraestruturas tecnológicas de prestação de serviço, desenvolvimento de políticas, leis, estratégias, e regulamentos no sector das TIC, que focalizam no desenvolvimento, modernização, cobertura geográfica, e redução de custos de acesso as infra-estruturas e serviços de telecomunicações nacionais (MCTES, 2021).

O INAGE (2021), disseca no seu relatório que o crescente acesso aos serviços das TIC, incluindo a Internet, é também acompanhado de crescentes vulnerabilidades a que o cidadão está sujeito e com isto também o crescimento dos crimes cibernéticos. O governo de Moçambique está também plenamente consciente da ameaça e dos efeitos negativos do crime cibernético sobre a sua nação e por isso tem sido feito esforços para garantir que haja instrumentos que possam proteger o cidadão e penalizar os que cometem estes crimes com recurso as TIC. Estes esforços incluem:

- O novo Código Penal, Lei n.º 24/2019 (Boletim da República, 2019), em Dezembro de 2019, que cobre os crimes informáticos nos seus artigos 256, 253,289,336,337, 3338, 339,, A Lei 3/2017, a Lei das Transacções Electrónicas, promulgada em Janeiro de 2017, que visa proteger os consumidores e regular o uso de sistemas electrónicos no governo, sector privado e sociedade civil;
- Regulamento de controlo de Tráfego de Telecomunicações, decreto n.º 75/214, de 12 de Dezembro;
- Regulamento de Registo de Cartões SIM, Decreto 18/2015;
- Lei de Telecomunicações, Lei n.º 4/2016, de 3 de Junho.

A Estratégia Nacional de Segurança Cibernética de Moçambique (2017 - 2021), descreve a abordagem para assegurar que o país garanta um ciberespaço seguro e resiliente que seja utilizado com segurança pelo Governo, sector privado, sociedade civil e demais instituições. Actualmente, existe uma multiplicidade de ameaças e riscos que podem prejudicar o bom funcionamento do ciberespaço, incluindo os sistemas e serviços de TIC em Moçambique que podem provocar um impacto negativo nos esforços para o aproveitamento das TICs para o desenvolvimento socioeconómico. Esta estratégia estabelece o compromisso do Governo de Moçambique em garantir um ciberespaço seguro e que contribua para o desenvolvimento socioeconómico (ENSC, 2017-2021).

2.9.3. Crimes cibernéticos registados em Moçambique

Em Janeiro de 2022, o país contava com 7.54 Milhões de usuários de internet. No total de 50% da população que tem acesso de serviços de telecomunicações apenas 23,1% da população (opais.co.mz 2022). A maioria dos usuários no país acessa a internet por meio de telefonia celular, como ocorre em outros países do Sul Global. Segundo os resultados do inquérito sobre utilização de telefonia móvel em Moçambique, Publicado em 26 Maio 2023 realizado pelo INCM, cerca de 12.510.571 pessoas que possuem telefone celular, com idade mínima de 16 anos, a média de utilização dos serviços de telefonia móvel é de 54,5% da população nas zonas rurais e 45,5% nas zonas urbanas. Deste número a percentagem maior é de homens, numa cifra de cerca de 59,2% e 40,8% para as mulheres. A população jovem constitui a maioria dos utilizadores dos serviços de telefonia móvel, sendo que a faixa etária entre dos 20 a 24 anos aparece como a maioria, em cerca de 14,1%, seguida da faixa 25 a 29 anos, com cerca de 12,2%.

Segundo os dados divulgados em 20 de Setembro de 2023 no âmbito do seminário de Legislação sobre cibercriminalidade e prova electronica que decorreu em Maputo, da conta de que Moçambique está enfrentando uma ameaça crescente de cibercriminalidade com uma media de 1.5 milhões de ataques cibernéticos por mês. Orgãos governamentais e universidades sofreram ataques tipo DDoS (negação de serviços) e *web defacement*. Em 2019 e 2020, além do aumento de ataques não-direcionados, foram detectados ataques persistentes, incluindo ransomware, spyware e quebras de chaves criptográficas, em redes governamentais, empresas e no sistema financeiro (Moçambique INAGE 2020). A falta de educação e planeamento financeiro ocasiona como uma das consequências o consumo compulsivo, isso é provocado pelo deslumbramento de crianças, jovens e adultos frente às campanhas publicitárias levando a falsa impressão de bem-estar ao adquirir sempre mais produtos (Wisniewski, 2011). Diante desse excesso de consumo e suas consequências, estudos relacionados a educação financeira e como ela pode minimizar esses factores, têm-se tornado a base de vários estudos.

2.9.3.1. Quadro Legal e Aplicabilidade da Interoperabilidade em Moçambique

O desafio da Administração Pública em construir uma gestão mais eficiente e, com isso, melhorar os serviços entregues ao cidadão faz com que o uso das Tecnologias

da Informação e da Comunicação (TICs) e, principalmente, a interoperabilidade entre sistemas de governo estejam no centro desse processo de melhoria.

O regulamento do quadro de interoperabilidade do Governo electrónico que foi aprovada no decreto 67/2017, que generaliza a sua aplicação em todas as instituições da função pública em Moçambique reforça o uso da interoperabilidade na busca pela publicidade dos dados. Ao garantir, virtualmente, um maior acesso aos direitos do cidadão e aumentar a sua parcela de participação na gestão do Estado, a interoperabilidade possibilita a expansão do exercício da cidadania, permitindo, ao menos tecnicamente, o acesso, pelo cidadão, a serviços e informações, atualmente, pulverizados e inacessíveis. Com mais informações disponíveis, é possível minimizar o número de interações do cidadão com o governo, ou seja, quanto mais informações o cidadão tem a sua disposição, menos contato, teoricamente, o cidadão precisaria ter com o governo.

Deste modo o Regulamento do quadro de interoperabilidade do Governo Electrónico de Moçambique assenta-se nos seguintes princípios:

- Princípio da Legalidade;
- Princípio da Transparência;
- Princípio da Prossecução do Interesse Público e Protecção dos Direitos e Deveres do Cidadão;
- Princípio a Confidencialidade;
- Princípio da Integridade de Dados e Informação;
- Princípio da Autenticidade;
- Princípio de Partilha de Dados entre as entidades da Administração Pública para a prossecução de uma actividade do Estado;
- Princípio de Recolha de dados entre as entidades da Administração Pública para a prossecução de uma actividade do Estado;
- Princípio de Recolha de Dados do Cidadão Única Vez pela Administração Pública;
- Princípio de Dados Autoritários;
- Princípio de Celeridade dos Processos Administrativos.

Apesar do marco legal estabelecido que versa a ideia da implementação da interoperabilidade de forma generalizada entre todas as instituições da Administração Pública moçambicana, persistem vários desafios na sua implementação, dentre os

quais a requalificação dos sistemas de informação e a sua adaptação por criação de extensões para permitir que haja comunicação entre os mesmos. O INAGE assume que nesta fase sejam necessárias iniciativas “independentes” entre as instituições para permitir uma implementação gradual da interoperabilidade entre os sistemas em Moçambique. Portanto, o modelo proposto na presente monografia visará contribuir para o desencadeamento de acções que culminem na implementação do quadro legal sobre interoperabilidade em Moçambique.

Ao abrigo do artigo 2 do Decreto n.º 30/2001, de 15 de Outubro, a Administração Pública é um conjunto de órgãos, serviços e funcionários e agentes do Estado, bem como as demais pessoas colectivas públicas que asseguram a prestação de serviços públicos ao cidadão.

Segundo a Estratégia da Reforma e Desenvolvimento da Administração Pública (2012, 2025, p. 19), a Administração Pública de Moçambique, resulta do amplo processo em curso no sector público iniciado em 2001 com o lançamento pelo Governo, da Estratégia Global da Reforma do Sector Público (EGRSP), o qual orienta as instituições públicas para a melhoria da qualidade dos seus serviços e respostas do Estado, visando obter uma cultura pública direcionada para a integridade, transparência, eficiência e eficácia.

3. CAPÍTULO III - CASO DE ESTUDO

3. Caso de Estudo

O presente capítulo apresenta todas as etapas metodológicas, de forma resumida a estrutura do caso de estudo, experiências internacionais de mecanismos para a prevenção de crimes cibernéticos e comparação com o contexto Moçambicano.

3.1. TMcel

A TMcel – Moçambique Celular, S.A., foi constituída aos 22 de Abril de 1997. O capital social é de 1.500.000.000 meticais distribuído pelos seguintes sócios: Telecomunicações de Moçambique, S.A (TDM) com 74% do capital social e o Instituto de Gestão das Participações do Estado (IGEPE) com a percentagem remanescente. A sua sede social está localizada na cidade de Maputo e tem como objecto social a prestação de serviços no domínio das telecomunicações móveis em Moçambique no âmbito do qual foi atribuída uma licença GSM em 2003 com duração de 15 anos e, em 2011 foram iniciadas as negociações com o regulador para a unificação das licenças 2G e 3G. Até o final do mesmo ano, a instituição contava com 801 colaboradores.

A TMcel foi a empresa pioneira no mercado de telefonia móvel em Moçambique e, em 2010 e 2011 permaneceu como líder na categoria da “Melhor Marca de Telecomunicações” na pesquisa independente das “Melhores Marcas de Moçambique” levada a cabo pela empresa Intercampus do Grupo GfK, apesar da entrada de novos concorrentes (Idem).

Tem como missão “Ser o operador e a marca preferida em Moçambique através do fornecimento de produtos e serviços de voz, dados e banda larga de qualidade e padrão mundial, fáceis de utilizar, a preços atractivos e com elevado profissionalismo e competitividade e, para esse fim, a TMcel tornar-se-á a empresa moçambicana mais orientada ao cliente e, actuando de uma forma social e ambientalmente responsável, agregando simultaneamente valor aos seus parceiros” (idem)

3.2. Vodacom

A Vodacom é uma empresa de origem sul-africana, que opera no ramo de telecomunicações, mais especificamente na prestação de serviços de telefonia móvel.

As actividades desta empresa tiveram o seu início no dia 1 de Junho de 1994, registando no primeiro mês a aderência de 50.000 clientes, e no final de cinco meses, a aderência de um total de aproximadamente 100.000 clientes. Neste período, a Vodacom liderou o ranking internacional de empresas de telefonia móvel, no que concerne à rapidez de crescimento em menor espaço temporal.

Tendo em vista a sua expansão em território africano, em Junho de 1995 a Vodacom abriu a primeira filial em Lesotho a título experimental, e iniciou as suas actividades em Maio de 1996.

Em Julho de 1999 a Vodacom atingiu cobertura a nível mundial, por meio de parceria com a empresa *Globalstar Southern Africa Ltd*.

Inicialmente, a Vodacom foi gerida pela empresa sul-africana Telkom e pela britânica Vodafone, compartilhando cada um destes 50% das acções existentes. Contudo, em 6 de Novembro de 2008 a Vodafone anuncia o seu aumento de participações para 65%, o que culminou com a substituição da cor azul inicial da empresa para a cor vermelha, tendo este processo de substituição o seu término em Abril de 2011.

A Vodacom actualmente fornece serviços de telefonia móvel para mais de 35 milhões de clientes nos seguintes países: África do Sul, Tanzânia, Lesoto, Moçambique, e a República Democrática do Congo.

No contexto moçambicano a empresa Vodacom iniciou a sua operação em Moçambique em Dezembro de 2003. Os accionistas da Vodacom Moçambique incluem a *Vodacom International Limited* (85%); e parceiros locais como a EMOTEL – Empresa Moçambicana de Telecomunicações, SARL (5%), a *Intelec Holdings*, Limitada (5%) e a *Whatana Investments,* Limitada (5%).

O Presidente do Conselho de Administração é nomeado numa base bianual, sendo a posição rotativa entre todos os accionistas.

Em Março de 2010, a Vodacom atinge uma quota de mercado de 45%, sendo que nos dias de hoje estima-se que apresente uma percentagem acima a 2/3 (66%) do mercado.

3.3. Movitel

A Movitel é uma operadora de telecomunicações móveis com sede na cidade de Maputo em Moçambique. Conta com 12 agências distribuídas pelas 11 províncias do país, 127 centros distritais e mais de 1.500 colaboradores. O empreendimento é

resultado da parceria entre a empresa vietnamita Viettel e a moçambicana SPI (Gestão e Investimento). O seu funcionamento iniciou-se depois de vencer um concurso público em 2010 para operar como empresa de telecomunicações móveis no mercado moçambicano.

A Movitel começou a montar a sua infra-estrutura em 2011, no início com o total de 12.500 quilómetros de extensão em fibra óptica e 1.800 antenas que suportassem serviços em 2G e 3G. Em Julho de 2019 a empresa lançou em Maputo o serviço de 4,5G LTE, na altura o mais rápido do país.

A Movitel apresenta uma estrutura muito consolidada e, apesar de, ser a operadora com menor tempo de operação no mercado de telefonia móvel é a que apresenta maior número de clientes actualmente. A operadora MOVITEL é a preferida dos utilizadores da zona rural em Moçambique, com uma taxa de 72% da população nestas zonas, segundo o primeiro inquérito nacional, por amostragem, aos utilizadores de telefonia móvel celular no país.

O estudo feito pelo INCM ressalta ainda que a utilização destes serviços varia na razão inversa da idade, sendo maioritária na faixa etária de 20 a 24 anos de idade com 14.1%, seguida da faixa de 25 a 29 anos, com 12.2%.

3.4. Experiências internacionais de mecanismos para a prevenção de crimes cibernéticos e comparação com o contexto Moçambicano

De seguida são apresentados alguns exemplos de mecanismos implementados para a prevenção de crimes cibernéticos segundo a informação existente. De referir que a gestão de sistemas de informação enquadra-se em alguns países em organismos de informação classificada, portanto a exploração bibliográfica abaixo descrita apresenta algumas limitações em termos de pormenorização.

3.4.1. Experiência de implementação do mecanismo de interoperabilidade dos Estados Unidos da América

De forma consentânea ao supracitado a gestão da interoperabilidade nos Estados Unidos da América (EUA) é feita por um organismo específico denominado CISA que significa Cybersecurity and Infrastructure Security Agency que traduzindo é Agência de Cibersegurança e segurança de Infra-estruturas electrónicas. A CISA desenvolve uma variedade de serviços, publicações e programas de segurança cibernética e de

infraestrutura para o governo federal, governos SLTT, indústria, pequenas e médias empresas, instituições educacionais e o público americano.

A CISA definiu plataformas específicas para a gestão de serviços por área de aplicação, portanto os serviços de telefonia movél não são exclusos dessas plataformas. McCoy (2017), refere que nos EUA existiam até 2017 cerca de 47 operadoras móveis e que pela estrutura autonóma dos governos federais haveria muito espaço para a criação de novas operadoras nos diferentes estados existentes. Para poder combater os crimes cibernéticos a CISA faz uma inspecção nas tecnologias implementadas pelas operadoras e obriga que todos os registos de novos clientes sejam interoperáveis com as bases de dados de identificação civil e de outros dados demográficos do país. Deste modo, assim que o consumidor dos serviços de telefonia móvel acede a um dos serviços automaticamente é registado e identificado nas bases de dados dos serviços civis de forma integrada a outros serviços gerais (registos em escolas, hospitais, etc.).

A informação apresentada permite apresentar um diagnóstico que põe Moçambique com desafios muito “alargados” para poder ter uma política no geral idêntica aos dos EUA. O primeiro aspecto observado é que apesar de existir uma entidade com a responsabilidade de tutelar este processo de interoperabilidade que é o INAGE, persistem “mazelas” na sua implementação, tais como: (a) necessidade de disseminar e enquadrar este quadro legal perante as instituições da função pública; (b) necessidade de definir tecnologias mais compatíveis o possível para garantir que existam extensões tecnológicas que permitam a materialização da interoperabilidade; (c.1) Como consequência do aspecto apresentado na alínea anterior a necessidade de se fazer um diagnóstico aprofundado das tecnologias existentes; (c.2) E por outro lado, definir um modelo de integração de todas as tecnologias existentes na função pública para uma única plataforma.

3.4.2. Experiência de implementação do mecanismo de interoperabilidade em Portugal

Para o caso de Portugal foi definido mecanismo de interoperabilidade para a gestão de sistemas de informação na Administração Pública denominado Interoperabilidade na Administração Pública (IAP). Este mecanismo é gerido pelo Governo Central

português e pela entidade que tutela a gestão dos sistemas de informação o que seria o homólogo do INTIC em Moçambique.

A IAP foi criada em 2007 tendo sido desenvolvido por um grupo de trabalho do Conselho para as Tecnologias de Informação e Comunicação (CTIC), abrangendo a Agência para a Modernização Administrativa (AMA), a Secretária-geral do Ambiente e Ação Climática, a Secretaria-Geral da Economia e o Centro de Gestão da Rede Informática do Governo (CEGER). O IAP sendo que disponibiliza serviços de orquestração e troca de mensagens entre sistemas aplicacionais (através da Plataforma de Integração), de comunicação de mensagens SMS com cidadãos (através da Plataforma de Mensagens) e de facilitação de pagamentos (através da Plataforma de Pagamentos). Neste período, foram trocadas mais de 1,5 mil milhões de mensagens de dados, enviados 190 milhões de SMS e foram suportados pagamentos de mais de mil milhões de euros. Ao todo, desde 2007, foram realizadas mais de 1,7 mil milhões de interações na IAP

A título de exemplo, a IAP garante de forma segura a troca de informação entre todas as entidades que participam no ciclo de vida do Cartão de Cidadão (IRN, AT, SS, Saúde, INCM, MAI, etc.), permite a atribuição automática de bolsas de estudo aos alunos do ensino superior e a abertura de conta bancária desmaterializada (online e sem papéis).

A IAP permite ainda a prescrição médica eletrónica para levantamento de medicamentos em farmácias sem necessidade da receita física e a validação de faturas para a ADSE, que obtém da AT dados sobre as despesas médicas dos beneficiários para facilitar a comparticipação de despesas médicas.

Estima-se que a IAP já tenha permitido poupanças superiores 5 mil milhões de euros, tendo também poupado mais de 380 milhões de horas a cidadãos e empresas e 66 milhões de horas aos serviços da Administração Pública. Quanto ao impacto ambiental, estima-se que tenham sido neutralizadas mais de 445 milhões de toneladas de carbono e que tenham sido poupadas mais de 70 mil toneladas de emissões de CO2.

A IAP, que conta com 123 entidades públicas e privadas, é uma plataforma segura que preserva todos os direitos de privacidade e proteção dos dados pessoais, tendo obtido em dezembro de 2019 a certificação ISO 2700, que atesta a conformidade do Sistema de Gestão de Segurança da Informação da AMA.

Para Moçambique poder implementar um modelo semelhante ao IAP prevaleceria a premissa apresentada acerca da necessidade de criação de um novo portal administrado pelo INTIC ou mesmo pelo INAGE, onde ficariam criadas as condições tecnológicas de base para disponibilizar um novo *backoffice* com melhores ferramentas de monitorização e a implementação dos novos sistemas implementados tal como feito a nível do IAP, que pudesse acelerar e automatizar a integração das entidades interessadas.

3.4.3. Experiência de implementação de mecanismo de interoperabilidade na África do Sul

Diferentemente dos EUA e de Portugal a África do Sul não possuí uma plataforma central que integra de forma interoperável todos os sistemas da função pública e, por consequente a sua gestão não é centralizada a entidade responsável pela gestão de sistemas de informação.

As instituições da Função Pública na África do Sul possuem modelos autónomos de gestão, parte delas interoperam mas não é sob o modelo centralizado e existem muitas “brechas” a segurança de informação.

Como resultado da autonomia da gestão de sistemas de informação e da sua não centralização há reportes de crimes cibernéticos com alguma frequência em particular os crimes impuros. Portanto, Moçambique não apresenta muitas diferenças e possui alguns avanços em termos do quadro legal para administração da interoperabilidade relativamente a África do Sul. Porém, a África do Sul possui mecanismos mais avançados de prevenção e de resposta a crimes cibernéticos, tendo serviços privados integrados que criam *firewall* e colaboram directamente com os serviços competentes na identificação dos infractores. Fora deste factor, a África do Sul possui maior “capacidade humana”, “capacidade material” “capacidade tecnológica” com alguma perícia para fazer frente, mas tem maior peso a resposta relativamente a prevenção a crimes cibernéticos nos ambientes das operadoras móveis concretamente no que se refere aos crimes cibernéticos. Os consumidores das operadoras não apresentam qualquer registo, apenas são auscultados a tomarem algumas medidas para a prevenção dos crimes cibernéticos que essencialmente se baseia em aderirem em redes de firewall de entidades privadas.

Os 3 exemplos dos países apresentados permitem aferir que Moçambique encontra-se no melhor “caminho” que iniciou pela definição de um quadro legal de regulamentação da interoperabilidade, mas que deverá certamente ainda ultrapassar os desafios previamente apresentados.

4. CAPÍTULO IV. PROPOSTA DE SOLUÇÃO

4. Análise e Discussão Dos Resultados

No presente capítulo é feita a descrição dos modelos de prevenção e resposta[1] a crimes cibernéticos em função das políticas das redes de telefonia móvel e a posterior é apresentada uma proposta de um modelo funcional para mitigar os casos de crimes cibernéticos.

4.1 Caracterização da prevenção e resposta a crimes cibernéticos

Vodacom

O agente da rede de telefonia móvel, a Vodacom afirmou não existir necessariamente um protocolo com os serviços de identificação civil, mas que já existem protocolos classificados com as autoridades competentes para o rastreio dos casos de crimes cibernéticos. Contudo, nenhum destes protocolos envolve a comunicação entre o sistema de informação da Vodacom com os sistemas de informação destas entidades competentes.

Os crimes cibernéticos classificados como “puros” que ocorrem com meios informáticos dentro do sistema da Vodacom ainda não se verificaram até ao momento, apenas já foram verificados alguns constrangimentos na gestão interna de informação, mas nada que tenha ocorrido por intervenção externa.

Os crimes cibernéticos classificados como “impuros” que ocorrem com mecanismo a meios electrónicos mas não dentro do sistema de informação da Vodacom já ocorreu a um número considerável, onde já foram reportados casos fraudulentos de uso dos serviços em nuvem web para desviar valores por descuido do cliente e também já se verificaram casos de algumas fraudes que envolveram o acesso a algum meio electrónico para apurar dados de clientes e posterior furto com uso do serviço de banca móvel *M-pesa*. Para mitigar estes casos a resposta que a operadora predispôs são os alertas por meio de *SMS* e outros mecanismos para persuadir os clientes a terem atenção com este tipo de fraude.

Por fim, a Vodacom mostra-se disponível para aderir a protocolos com as entidades de identificação cívil para além das entidades já envolvidas, considerando um aspecto critico para mitigar os possíveis casos e uma solução que futuramente servirá para

[1] Não existe uma informação sumária que possa ser exposta dos mecanismos específicos que as operadoras usam em termos de protocolo, uma vez que é algo classificado. As respostas apresentadas vão em função da proposta de solução exposta pelo autor do trabalho monográfico.

melhor controlar e responder eficientemente para estes casos de fraudes por crimes cibernéticos.

TMcel

O agente da TMcel unanimemente ao agente da Vodacom afirmou que a TMcel não tem quaisquer protocolos com as entidades de registo civil, mas que tem com as autoridades competentes. Adiantou também que estes protocolos não passam por alguma solução de comunicação de sistemas, mas sim dos serviços de contra-inteligência definidos pelas autoridades policiais para o tratamento destes casos.

A TMcel tem o reporte de algumas tentativas de invasão ao sistema considerando deste modo a possibilidade de ocorrência de crimes cibernéticos “puros” em que registaram-se algumas violações a rede de sistemas mas que tais casos não repercutiram em perdas em valores pela acção imediata de bloqueio operacional do sistema. Apesar de se terem verificado percebeu-se que pela modalidade dos crimes cibernéticos “puros” ocorridos muito possivelmente os agentes envolvidos não se encontravam em território nacional, pelo que, não há muita informação dos mesmos e nenhum sinal de que tenham usado alguma rede de sistema de informação nacional.

Os crimes cibernéticos “impuros” já foram observados uma vez que aquando da criação do serviço de conta móvel, mas boa parte dos casos envolveu as operadoras e houve responsabilidade dividida. Os casos que se observaram foram de desvio de valores com recurso a meios electrónicos.

A TMcel também mostra-se aberto a cooperar com entidades de identificação civil para melhorar a prevenção e resposta aos casos já reportados e os futuros que possam ocorrer.

Movitel

A rede de telefonia móvel, a Movitel não tem protocolos estabelecidos com as entidades de identificação civil, porém pela natureza dos serviços tem protocolos estabelecidos com instituições de estado e autoridades competentes para o caso de fraudes futuras.

Assim, observados os mecanismos das redes de telefonia móvel e a sua abertura para aderirem a um protocolo com os serviços de identificação civil, propõe-se o modelo de interoperabilidade que aborda os componentes descritos de seguida.

4.2 Apresentação do modelo proposto

4.2.1 Processo de registo único móvel

Abaixo são apresentados os requisitos funcionais no esquema abaixo. Essencialmente os clientes fazem o registo dos cartões nas operadoras de telefonia móvel, onde devem apresentar o Bilhete de Identidade (B.I) e o Número Único de Identificação Tributária (NUIT).

De seguida a operadora de telefonia móvel deverá comunicar com a Autoridade Tributária e em paralelo com o Ministério de Interior. No caso da Autoridade Tributária tem a função de "dar conformidade" ao NUIT comunicado.

O Ministério de Interior armazena os dados na sua base de dados e canaliza aos Serviços de Identificação Cívil, comunicando que o número de B.I em causa está associado ao NUIT enviado. Por outro lado, a operadora de telefonia móvel faz o envio dos dados com a confirmação do NUIT e o B.I fazem a comunicação ao INCM. Pode-se, portanto, visualizar abaixo os requisitos funcionais:

[RF01] Consultar NUIT

O sistema deve fornecer ao usuário da operadora a capacidade de consultar NUIT.

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

[RF02] Enviar novo registo

O sistema deve fornecer ao usuário da operadora, ministério do interior e INCM, a capacidade de enviar novos registos.

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

[RF03] Listar novos registos

O sistema deve fornecer aos usuários do Ministério do Interior, INCM a listarem todos novos registos.

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

[RF04]	**Reportar Suspeita de Burla**

O sistema deve fornecer aos usuários das operadoras, INCM a capacidade de reportar suspeita de burla.

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

Tabela 3. Requisitos funcionais do modelo proposto

Fonte: adaptado pela autora

Requisitos de Qualidade

Um requisito de qualidade é um requisito relacionado a uma questão de qualidade não coberta por um requisito funcional. Estes requisitos definem a qualidade desejada por um sistema e muitas vezes influenciam a arquitectura do sistema mais do que requistos funcionais.

A tabela abaixo apresenta os requisitos de qualidade desejáveis para o sistema proposto.

[RF01]	**Usabilidade**

O sistema deverá apresentar uma interface amigável, facil de manuzear e reativa.

A implementação a API será baseada na arquitectura RESTful.

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

[RF02]	**Segurança**

O sistema deverá reconhecer apenas a requisições devidamente autenticadas, todas as requisições ao sistema serão *stateless*. A autentição ao sistema será feita via *Json Web Tokens*

Prioridade:	☑	Essencial	☐	Importante	☐	Desejável

Tabela 4. Requisitos de Qualidade do modelo proposto

Fonte: adaptado pela autora

Diagrama de Componentes

O diagrama de componentes apresenta uma visão estática de como o sistema será implementado e quais os seus módulos de software, ou seja, os seus componentes. Assim sendo o diagrama de componentes apresenta os seguintes elementos:

- **Componentes**: representam arquivos, módulos, bibliotecas que os sistemas detêm;
- **Dependência**: Representa a relação de dependência entre os diversos componentes**;**
- **Interface**: Representa um serviço realizado por uma Classe ou Componente.

Diagrama de Implantação

O diagrama de implantação é aquele com a visão mais física da UML. Trata-se do diagrama que enfoca a questão da organização da estrutura física sobre o qual o software irá ser implantado e executado em termos de hardware. Assim sendo o diagrama de implantação apresenta os seguintes elementos:

- **Nós**: Representa uma máquina, servidor, etc., em que um ou mais módulos do software são executados;
- **Associações**: Representam as ligações entre os nós.

Abaixo é apresentado o diagrama de componentes e implantação para o problema em questão.

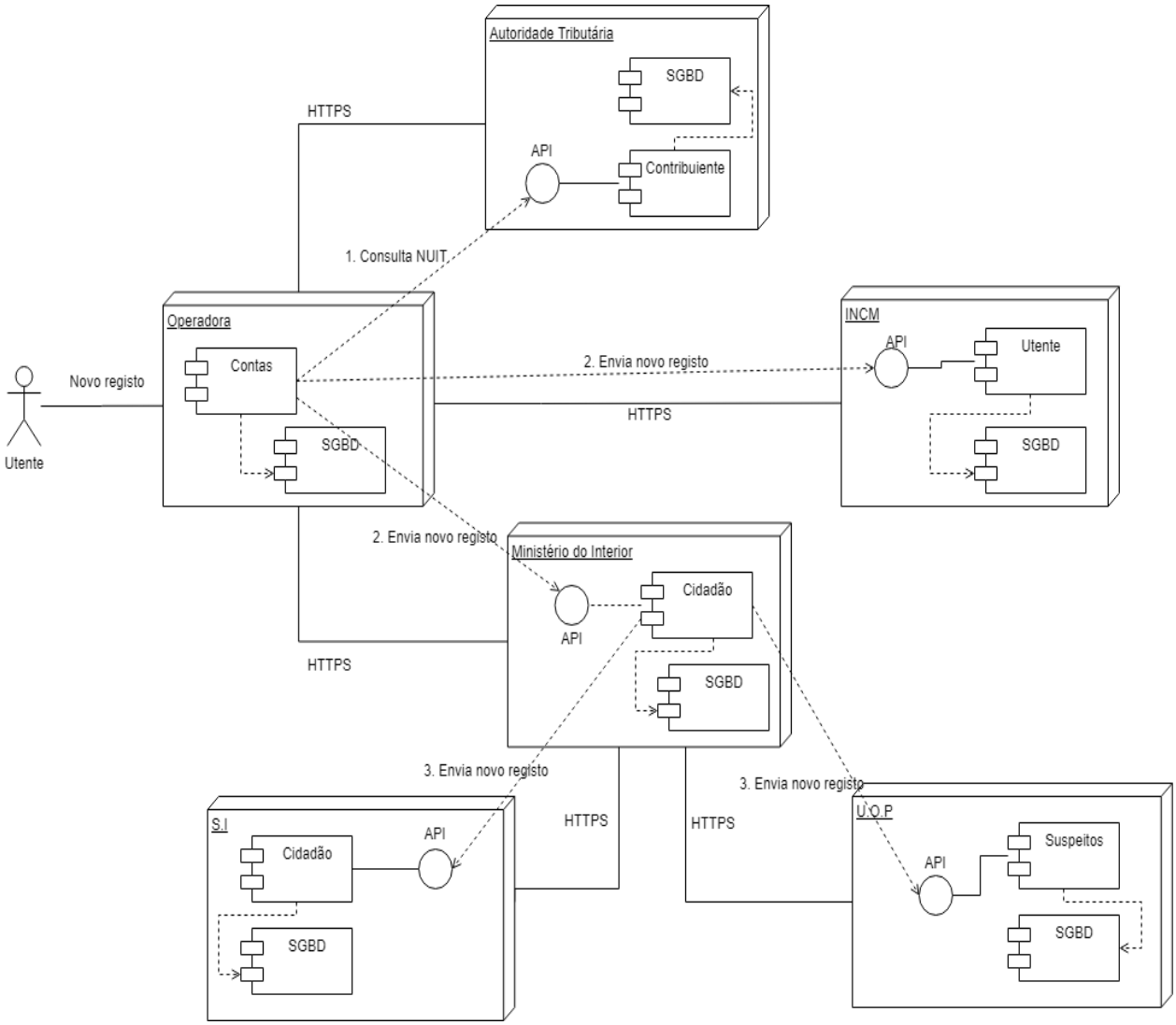

Figura 4.Diagrama de componentes e implantação

Fonte: adaptado pela autora

Diagrama de sequências

O diagrama de sequências apresenta a sequência de cada um dos intervenientes e "denuncia" cada actividade intrínseca a estes mesmos intervenientes. As sequências apresentadas demonstram que há fluxos que alimentam e retroalimentam entre os intervenientes.

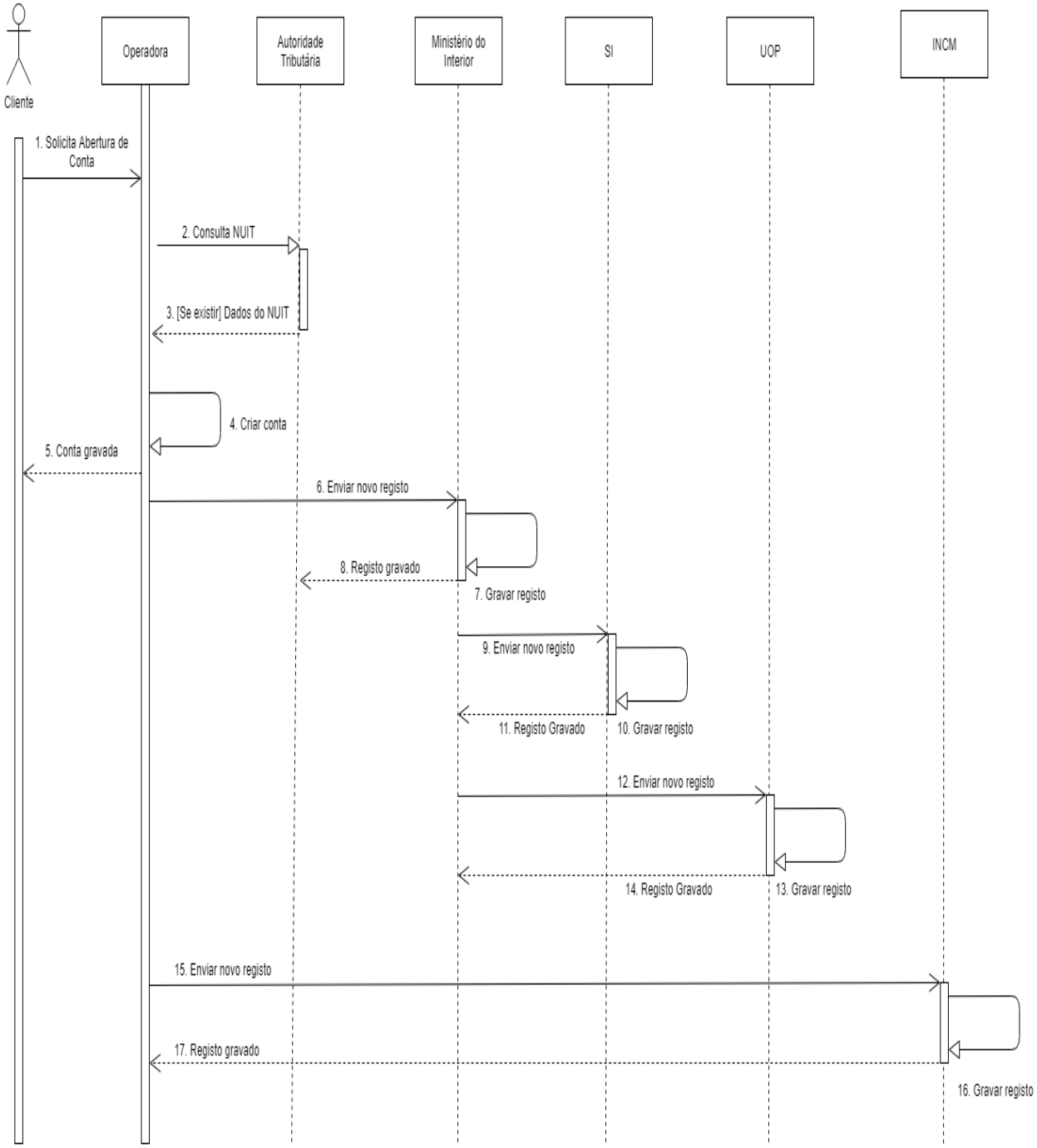

Figura 5. Diagrama de sequências

Fonte: adaptado pela autora

Em complementaridade com o diagrama de sequências acima apresentado é também descrita a especificação do API do modelo proposto para uma melhor percepção do tipo e estado dos dados ao serem inseridos.

Requisição	
Terminal	/api/v1/citizen/:nuit
Método	GET
Cabeçalho	Content-Type: application/json Authorization: Bearer Token
Resposta Esperada	
Estado	*Success*
Código de Estado	200
Dados	Nome apelido dataNascimento numeroBI localEmissao dataEmissao provincial distrito localidade bairro residência quarteirão casaNr nomePai nomeMãe photoUrl nuit
Exceção	Não encontrado
Estado	*failed*
Código de Estado	404
Error	NUIT não encontrado

Requisição	
Terminal	/api/v1/new_record/
Método	POST
Cabeçalho	Content-Type: application/json Authorization: Bearer Token
Dados	numero_bi nuit contacto data_de_registo
Resposta Esperada	
Estado	*Success*
Código de Estado	201
Exceção	Falha ao registar
Estado	*Failed*
Código de Estado	500
Error	NUIT não encontrado

Requisição	
Terminal	/api/v1/report_scam /
Método	POST
Cabeçalho	Content-Type: application/json Authorization: Bearer Token
Dados	Contacto data_de_actividade
Resposta Esperada	
Estado	*Success*

Código de Estado	201
Exceção	Falha ao registar
Estado	*failed*
Código de Estado	500
Error	NUIT não encontrado

Tabela 5. Especificação da API

Fonte: adaptado pela autora

Diagrama de caso de Uso

O diagrama de caso de uso é apresentado abaixo, com a descrição sumária dos papéis que cada um dos usuários apresenta na rede de fluxos do sistema. Os 3 usuários do sistema são o usuário da operadora, o usuário do Ministério do Interior e o usuário do INCM.

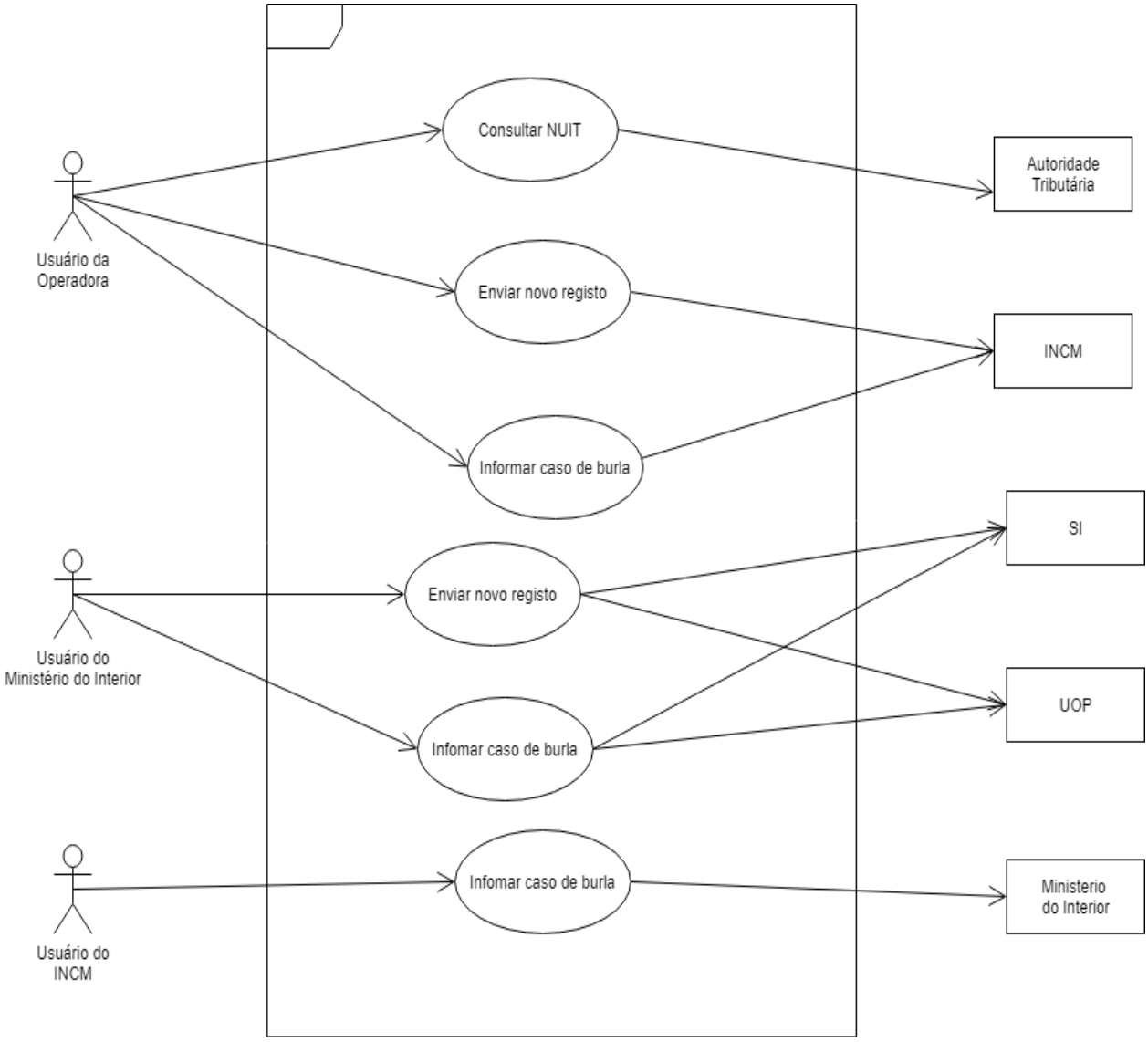

Figura 6. Diagrama de caso de uso

Fonte: adaptado pela autora

Actor	Casos de Uso
Usuário da Operadora	Consultar NUIT
	Enviar novo registo
	Reportar suspeita de burla
Usuário do Ministério Do Interior	Enviar novos registos
	Reportar suspeita de burla
Usuário do INCM	Enviar novos registos
	Reportar suspeita de burla

Tabela 6. Actores e os seus respectivos casos de uso

Fonte: adaptado pela autora

Nome:	**1 – Consultar NUIT**		
Ator Principal:	Operador	Actor Secundário:	
Objetivo:	OB_01 – Obter informações sobre um determinado cidadão		
Pré-condição:	PE_01– O NUIT deve existir na base de dados da AT		
Pós-condições:	Nenhuma		
Fluxo Principal:	FP_01: O actor introduz o NUIT na caixa de pesquisa e clica em pesquisar O sistema exibe tela de espera O sistema retorna com informações relacionadas ao NUIT e preenche os campos de identificação do usuário Caso de uso encerrado		
Exceções	Ex_01: O actor não forneceu dado X (nuit O sistema exibe a seguinte mensagem: “O dado X é obrigatório” O nuit não esta cadastrado no sistema da AT O sistema exibe a seguinte mensagem: “NUIT não encontrado” O actor introduz um nuit com formato incorrecto O sistema exibe a seguinte mensagem: “NUIT inválido”		

Tabela 7. Caso de uso para o caso de consulta de NUIT

Fonte: adaptado pela autora

Nome:	**2 – Enviar novo registo**		
Ator Principal:	Usuário da operadora	Actor Secundário:	
Objetivo:	OB_01 – Enviar registo de novo cliente ao Ministério do Interior e INCM		
Pré-condição:	PE_01– O usuário deve estar devidamente autenticado PE_02– O novo cliente deve estar registado no sistema		
Pós-condições:	Nenhuma		
Fluxo Principal:	FP_01: O actor seleciona o novo cliente O sistema exibe uma tela contendo todos os dados do cliente e botão “Enviar” O actor pressiona o botão enviar O sistema exibe uma caixa de diálogo com as seguintes informações: Título: Confirmar envio Mensagem: Tem certeza que deseja enviar este registo para o Ministério do Interior e INCM? Botão de confirmação: Sim Botão de cancelamento: Não O actor pressiona o botão de confirmação O sistema processa os dados Dados enviados [ex1] Caso de uso encerrado		
Exceções	Ex_01: Um dos servidores retorna um erro O sistema exibe a seguinte mensagem: “Falha no envio de dados”		

Tabela 8. Caso de Uso para o envio de novos registos a nível do Ministério do Interior

Fonte: adaptado pela autora

Nome:	**3 – Reportar suspeita de burla**		
Ator Principal:	Usuário da operadora	Actor Secundário:	INCM
Objetivo:	OB_01 – Reportar suspeita de burla		
Pré-condição:	PE_01– O usuário deve estar devidamente autenticado		
Pós-condições:	Nenhuma		
Fluxo Principal:	FP_01: O actor pressiona “Reportar Suspeita” O sistema exibe uma caixa de diálogo com as seguintes informações: Título: Confirmar envio Mensagem: Tem certeza que deseja reportar suspeita de burla ao INCM? Botão de confirmação: Sim Botão de cancelamento: Não O actor pressiona o botão de confirmação O sistema processa os dados Dados enviados [ex1] Caso de uso encerrado		
Exceções	Ex_01: Um dos servidores retorna um erro O sistema exibe a seguinte mensagem: “Falha no envio de dados”		

Tabela 9. Caso de Uso para o reporte de suspeita de burla

Fonte: adaptado pela autora

4.2.2 Processo de reporte no caso de suspeita de infracção

Para o caso de suspeita ou mesmo materialização de alguma infracção/crime cibernético, o cliente reporta a operadora e por sua vez a operadora reporta ao Ministério do Interior que por sua via deverá participar a sua unidade operacional que nesse caso são os serviços da polícia civil. Abaixo é apresentado o diagrama descrito.

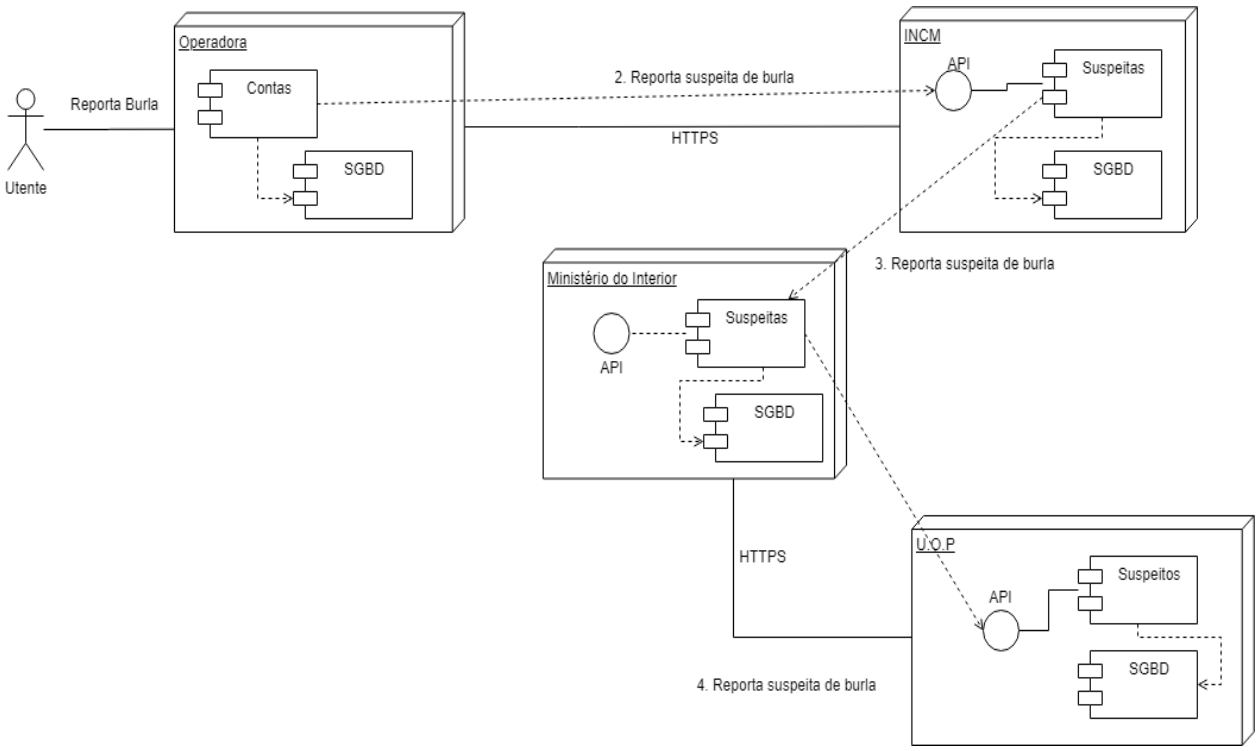

Figura 7.Diagrama do processo de reporte para o caso de suspeita de infracção

Fonte: adaptado pela autora

4.2.3 Comparação do modelo actual e o modelo proposto

Na tabela abaixo são apresentados pontos críticos para a comparação do modelo actual e o modelo proposto, e possível através dela analisar fraquezas e lacunas no modelo actual bem como, apresentar melhorias e robustez do modelo proposto.

Dimensão/ Factor	Modelo actual	Modelo proposto
Existência de protocolos com os serviços de identificação civil	Nenhum protocolo estabelecido	Protocolo estabelecido e devidamente definido
Existência de protocolos com os serviços de tributação civil para criação de uma identificação como "chave-primária"	Nenhum protocolo estabelecido	O modelo prevê a definição da chave-primária o NUIT, o que permitirá ter um maior controlo em aspectos ligados a tributação no geral e em serviços de telefonia móvel
Existência de protocolos com o Ministério do Interior ou Unidade subordinada ao mesmo	Existência de protocolo com os serviços de investigação criminal, contudo para os casos do desconhecimento da referência IMEI (Identificação Internacional do Equipamento Móvel) não é possível garantir o rastreamento do dispositivo móvel	O Modelo prevê que haja registo num formato de cadastro único que interopera com os serviços de Ministério de Interior e as referidas Unidades de Policiamento assim como os Servios de Identificação Cívil, por isso o protocolo estabelecido neste modelo é muito mais eficaz e eficiente
Chances de ocorrência de crimes puros	Baixo e controlado, existência de mecanismos de rastreamento interno muito consistentes	Baixo e controlado, porque embora exista comunicação com outros sistemas os dados intercomunicados por outras instituições não afectam o sistema interno

Chances de ocorrência de crimes impuros	Alto e associado principalmente a banca móvel	Altas mas com possibilidade igualmente alta de recuperação do dispositivo devido ao rápido rastreamento do dispositivo e da informação automaticamente disponibilizada as entidades policiais
Nível de comunicação de dados com a entidade reguladora das comunicações (INCM)	Regular mas prevalecem desafios na “purificação” da associação entre o contacto e os dados dos clientes das operadoras móveis	Extremamente regular, mecanismo automático de comunicação e alta fluência de dados e informações dos dados dos clientes das operadoras móveis
Nível de integridade dos dados e informações comunicados a entidade reguladora de telecomunicações (INCM)	Médio com necessidade de acompanhamento constante da carteira dos clientes das operadoras	Alto e sem necessidade de monitoria da carteira dos clientes das carteiras das operadoras móveis, dados mais sólidos e que requisitam menor esforço humano, material e financeiro por parte da entidade reguladora das comunicações
Nível de adesão e cumprimento das normas do Instituto Nacional de Governo Electrónico	Médio com muitos desafios relativos a prevenção dos crimes cibernéticos e com fraca capacidade de resposta a estes mesmos desafios	Alto e com contributo na robustez da melhoria das normas uma vez que o modelo permite que sejam implementadas algumas normas que se encontram no momento em “desuso”

Table 10. Tabela comparativa entre o modelo actual e o modelo proposto

Fonte: Elaborado pela autora

5. CAPÍTULO V. CONCLUSÕES E RECOMENDAÇÕES

5.1. Conclusão

O presente estudo teve como objectivo desenvolver um modelo de interoperabilidade dos serviços de carteira móvel com os serviços de identificação e tributação civil assim como os mesmos serviços de telefonia com o INCM, isto para definir um mecanismo de prevenção e resposta a crimes cibernéticos. Observando a necessidade de aumentar a eficiência e a eficácia prevenção e resposta a casos de fraudes bancárias considerou-se pertinente “abraçar” a interoperabilidade dos sistemas, mas considerando as possíveis restrições no tipo de dados, as funcionalidades adaptadas para o modelo de interoperabilidade em causa são especificamente para reportar a identificação detalhada do operador bancário. Como tal, inicialmente fez-se o diagnóstico dos protocolos de prevenção e resposta das operadoras móveis podendo-se concluir que:

- Os crimes cibernéticos puros ainda são incomuns para as operadoras móveis Vodacom e TMcel e, apesar da Movitel já ter registado invasões dentro do seu sistema não teve qualquer registo de desvio de valores. Não obstante a Vodacom não tem informação detalhada dos infractores dos estas acções por falta de mecanismos mais avançados para detecção desses casos;
- Os crimes cibernéticos impuros são comuns na Vodacom e TMcel mas não na Movitel. Para as redes de telefonia móvel nomeadamente Vodacom e TMcel é feito o uso do sistema de internet banking para apurar dados, mas a fraude concreta é efectuada por meio dos serviços de banca móvel M-pesa e conta móvel respectivamente;
- Existem dificuldades no rastreio de casos de crimes cibernéticos “impuros” para todas as redes de telefonia móvel. Não existe um protocolo de prevenção e os protocolos de resposta são dependentes das autoridades policiais, e do modelo de coordenação entre as redes de telefonia móvel e as autoridades e outros possíveis agentes com alguma fonte de informação.
- O modelo proposto de integração deveria ter uma chave de identificação primária a partir de um sistema único para o rastreio. Observando as entidades percebe-se a viabilidade de usar o NUIT como identificador primário, considerando a possibilidade de um cliente poder ter mais de um documento de identificação pela vulnerabilidade sujeita dos serviços de identificação civil;
- O actor principal ao qual se designa o operador da rede de telefonia móvel que estiver a fazer a pesquisa sobre a identificação de determinado sujeito bancário

tem os privilégios no sistema de autenticar e fazer a pesquisa do NUIT. Para poder aceder aos dados de identificação deve obrigatoriamente solicitar autorização a Autoridade Tributária na circunstância para não tirar a autonomia dos agentes do estado e posteriormente por solicitação interoperável entre a AT e os Serviços de Identificação Civil tem o retorno com os dados do sujeito bancário em tempo real;

- Os dados de registo do sistema integrado permitem em tempo real ter as datas de registo documental do sujeito do cliente e todos os seus dados pessoais automatizados num mecanismo “robusto” que pode ser considerado viável para o rastreio e com isto contribuir para mitigar as possíveis ocorrências de crimes cibernéticos.

Assim, com o modelo de interoperabilidade entre as operadoras nacionais e os sistemas de identificação civil funcional espera-se que haja maior flexibilidade, eficácia e eficiência no processo de rastreio de casos de fraudes bancária e permitir uma maior “pureza” no processo de registo civil e atribuição do número único de identificação tributária, aumentando deste modo a sua utilidade e pertinência para os cidadãos.

5.2. Recomendações

Mediante os resultados apresentados recomenda-se:

a) As redes de telefonia móvel a implantação do modelo integrado de sistemas de informação de serviços bancários e os de identificação civil seguindo a proposta do modelo apresentado no presente trabalho;

b) O estabelecimento de protocolos de interoperabilidade conjunto a outros sistemas de informação que possam fornecer mais informações.

Bibliografia

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, José Moreira. 2004 – *Cidadania Digital e Democratização Electrónica,* 2ª ed., Portugal, cidade do Porto.

BOLT, Raphael (2013) *Criminologia midiática: do discurso punitivo a corosão simbólica do garantismo.*

BRAVO, Rogério (2014) *"Open Sources" na investigação de cibercrimes: conceito e implicações.*

DEBASTIANI, Carlos A. (2015), *Definindo Escopo em Projetos de Software*. São Paulo: Novatec.

CHAPMAN, C.S., Kihn, L.A., (2009), *Information system integration, enabling control and performance. Accounting, Organizations and Society*, 34(2).

FERNANDES, Jorge H.C. (2010), *Segurança da informação: Nova disciplina na ciência da informação?* XI Encontro Nacional de Pesquisa em ciência da informação. Rio de Janeiro, 2010.

GALVÃO, Michele da C. (2015), *Fundamentos em Segurança da Informação* São Paulo: Person Education do Brasil.

GASPAR, Ana "Desafios à integração de sistemas de informação: um estudo de caso no setor da banca" and *Engineering. IEEE*.

GLENNY, Misha (2011), *Dark Market cyberthieves cybercops and you*, Nova York.

GLENNY, Misha (2011), *Dark Market cyberthieves cybercops and you*, Nova York.

GILMAN, Rick (2013) *Cloud Computer Evolves*, American Agent & Broker, Vol 83.

LAKATOS, E. M.; Marconi, M. de A. (2002), *Fundamentos de metodologia científica*. 4.ª Ed. São Paulo: Atlas.

LANGA, C. V. A. (2021). Implementação da Interoperabilidade entre os Sistemas de Informação da Administração Pública de Moçambique. Universidade Eduardo Mondlane.

MASSUNGUINE, G. P. (2022). Segurança Cibernética: Proposta de Implementação de uma Plataforma SIEM. Universidade Eduardo Mondlane.

MADNI, A.M., Sievers, M., (2014), *Systems integration: Key perspectives, experiences, and challenges. Systems Engineering*, 17(1).

MICHAQUE. E. A. (2017). Proposta De Um Modelo de Interoperabilidade Entre Os Sistemas De Informação Usados Na UEM. Universidade Eduardo Mondlane.

MONJANA, A. Z. (2021). Influência Das Práticas De Shadow IT na Exposição A Riscos De Segurança. Universidade Eduardo Mondlane.

NOVAKOUSK, M. & Lewis, G. 2012*. Interoperability in the e-Government Context*, S.I: Software Engineering Institute.

NIU, Y., (2010), *An empirical analysis of accounting information integration in integrated systems*. In *2010 2nd IEEE International Conference on Information Managemen*t.

SÊMOLA, M. (2014*), Gestão da Segurança da Informação* - Uma Visão Executiva - 2 ed. São Paulo: Elsevier.

SILVA, Daniela Rocha (2017). *A linguagem JavaScript». Um Estudo em Larga Escala sobre a Estrutura do Código-fonte de Pacotes JavaScript* (PDF) (Tese de Bacharel). Universidade Federal do Estado do Rio de Janeiro (UNIRIO).

SILVA, Jonathas Luiz Carvalho; Freire, Gustavo Henrique de Araújo (2012), *Um olhar sobre a origem da ciência da informação: indícios embrionários para sua caracterização identitária.* Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, v. 17, n. 33.

SIMON, A., Yaya, L.H., Karapetrovic, S., Casadesus, M. (2014), *Can integration difficulties affect innovation and satisfaction?* Industrial Management & Data Systems.

TOMICIC-Pupek, K., DOBROVIC, Z., Furjan, M.T., (2012), *Strategies for Information Systems Integration.* In Information Technology Interfaces (ITI), Proceedings of the ITI 2012 34th International Conference.

VAZQUEZ, Carlos; Simões, Guilherme (2016), *Engenharia de Requisitos: Software Orientado ao Negócio*. [S.l.]: Brasport.

VOM Brocke, M., 2010. *The Six Core Elements of Business Process Management*, Handbook on Business Process Management 2, Springer.

ZINS, C. (2007), *Mapa do conhecimento da ciência da informação: implicações para o futuro da área*. BJIS, v.1, n.1.

Bibliografia consultada

Legislação:

MOÇAMBIQUE. 2017. Decreto n.º 60/2017 de 6 de Novembro*. Boletim da República*.

MOÇAMBIQUE. 2017. Decreto n.º 03/2017 de 09 de Janeiro. *Lei das Transacções Electrónicas.*

MOÇAMBIQUE. 2017. Decreto n.º 61/2017, 06 de Novembro. *Lei de Criação do Instituto Nacional de Governo Electrónico*.

MOÇAMBIQUE. 2018. Resolução n. º17/2018, de 21 de Junho. *Lei da Política para a Sociedade de Informação de Moçambique*, publicado no Boletim da República n.º 122

MOÇAMBIQUE. Decreto n.º 67/2017 de 01 de Dezembro, Normas de implementação e funcionamento do Quadro de Interoperabilidade de Governo Electrónico, como um dos instrumentos de operacionalização da Lei de Transacções Electrónicas, Maputo, 2017.

MOÇAMBIQUE. Resolução nº 69/2021, 31 de Dezembro, Política de Segurança Cibernética e Estratégia da sua Implementação publicado no 12º Suplento do Boletim da Republica n.º 253

Sites:

https://pt.scribd.com/document/340190668/Importancia-Das-TIC-Na-Sociedade-Actualhttps://seer.ufs.br/index.php/eptic/article/viewFile/104/78 15 de Agosto de 2023

https://www.incm.gov.mz/ 15 de Agosto de 2023

https://opais.co.mz/so-23-da-populacao-tem-acesso-a-internet-no-pais/ 01 de Setembro de 2023

- https://www.intic.gov.mz/criancas-cada-vez-mais-expostas-a-crimes-cibernetico s/ 13 de Setembro de 2023
- https://www.incm.gov.mz/index.php/sala-de-imprensa/noticias/563-divulgados-resultados-do-inquerito-sobre-utilizacao-de-telefonia-movel-em-mocambique, 10 de Setembro de 2023
- https://www.tmcel.mz/ , 07 de Setembro de 2023
- https://vm.co.mz/ ,07 de Setembro de 2023

- https://movitel.co.mz/about, 07 de Setembro de 2023