UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

ANÁLISE DAS VULNERABILIDADES EM SISTEMAS DE CERTIFICAÇÃO DIGITAL CENTRALIZADOS

Caso de estudo: **Instituto Nacional de Tecnologias de Informação e Comunicação**

Autor:

MADABULA, Pedro António

Supervisor:

MSc. Sérgio Eduardo Mavie

Co-Supervisor:

Engº. Délcio Arnaldo Chadreca

Supervisor da Instituição:

Prof. Doutor. Engº. Lourino Alberto Chemane

Maputo, Julho de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

ANÁLISE DAS VULNERABILIDADES EM SISTEMAS DE CERTIFICAÇÃO DIGITAL CENTRALIZADOS

Caso de estudo: **Instituto Nacional de Tecnologias de Informação e Comunicação**

Autor:

MADABULA, Pedro António

Supervisor:

MSc. Sérgio Eduardo Mavie

Co-Supervisor:

Engº. Délcio Arnaldo Chadreca

Supervisor da Instituição:

Prof. Doutor. Engº. Lourino Alberto Chemane

Maputo, Julho de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

TERMO DE ENTREGA DO RELATÓRIO DE ESTÁGIO PROFISSIONAL

Declaro que o estudante **Pedro António Madabula** entregou no dia ___/___/_____, ___ cópias do relatório do seu Relatório de Estágio Profissional com a referência 2021EIEPD224, intitulado: Análise das Vulnerabilidades em Sistemas de Certificação Digital Centralizados.

Maputo, ___ de _____ de _____

A Chefe da Secretaria

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE 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 obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, ___ de _____ de _____

O Autor

_____

(Pedro António Madabula)

Dedicatória

Ao meu pai, António Pedro Madabula

A minha mãe, Carla Marlú Lazaro Massango

Aos meus irmãos, Frederico António Madabula e António Pedro Madabula Júnior

A minha bisavó, Tereza

Agradecimentos

Inicio esta secção reconhecendo que o temor do Senhor é o princípio da sabedoria. Agradeço a Deus pela oportunidade de usufruir da vida e por não ter me permitido desaminar durante a realização deste trabalho.

Agradeço aos meus pais pelo esforços que têm realizado para que não me faltasse nada, por me apoiarem nas minhas decisões de vida dando-me conselhos sempre que possível e por terem me educado da melhor forma possível para que me tornasse na pessoa que sou hoje.

Agradeço aos meus tios Frederico Madabula e Alfredo Nhanale por sempre terem me mostrado que a escola é essencial na educação de um indivíduo. Um obrigado a todos os meus familiares pelo apoio imensurável no meu crescimento e educação, em especial ao meu avô Pedro Madabula pelos ensinamentos valiosos de vida que têm me dado.

Agradeço aos funcionários da UEM pela gestão de todo o processo educativo, em particular aos docentes por terem me enriquecido de conhecimento técnico para de alguma forma resolver os problemas da sociedade. No mesmo sentido faço um agradecimento especial aos meus supervisores MSc. Sérgio Eduardo Mavie, Engº. Délcio Arnaldo Chadreca, Prof. Doutor. Engº. Lourino Alberto Chemane e ao coordenador da disciplina Eng.º Cristiano Maculuve pela confiança demonstrada em mim ao aceitar este desafio, sem a qual este trabalho não teria sido feito e por terem me orientado na realização da presente pesquisa.

Ainda relativo ao auxílio na realização deste trabalho, agradeço a Eng.ª Ivone Cipriano pelas várias oportunidades que me deu durante os estudos e por acreditar no meu potencial. Agradeço a Eng.ª Leila Omar, drª. Bhavika Rugnath, pela oportunidade dada de monitorar as cadeiras de Introdução à Programação e Programação Orientada a Objectos I e ao Eng.º Rúben Manhiça, no qual me inspiro bastante, pelo auxilio na escolha do tema de pesquisa.

Em especial agradeço a minha namorada Fátima Francisco Massicame, por sempre ter se mostrado disponível a apoiar-me incondicionalmente nos momentos bons e difíceis da minha vida, sem ela o percurso na faculdade não teria sido tão incrível.

Igualmente importante, meus sinceros agradecimentos aos meus colegas de turma que se tornaram amigos próximos, que juntos batalhamos na promessa de um dia nos tornarmos engenheiros, em especial ao António João Cossa, Gilvaldo Massunguine, Hélio Chaúque, Tomás Mondlane, Cany Mangue, Alexandre Rabeca, Lourenco Nelson, Télvio Sheldon, Luís Macuvele, Manuel Novela, Sara Tivane, Stoner Naiene, Carson Ribeiro, Luís Cossa e aos demais. A todos amigos e companheiros de vida, em especial, Anivel Mateus, Cripton Baloi, Jéssica Nhassengo, Dinércia Buce, Yuran Salomão, Hortêncio Pereira, Geraldo Carlos, António Samuel e Calisto Adelino.

Agradeço a todos funcionários do INTIC por me terem recebido de boa forma e por terem me auxiliado na realização do relatório de estágio. Em especial ao Engº. Sérgio Guivala, Engº. Helder Fernando e ao Engº. Jeremias Zunguza. De igual modo agradeço aos colegas e amigos no estágio Carlos Mussa, Kelvin Lukanga, Catarina Maxieie, Esselina Mangadane, Maria Mucombo e Sérgio Mussica.

Agradeço a equipa do Laboratório de Segurança da Universidade Federal de Santa Catarina, em especifico, o Frederico Shardong, o Lucas Mayr e o Prof. Custódio pelo apoio prestado na compreensão das matérias sobre o tema de pesquisa.

Por fim, agradeço a todos que directa ou indirectamente contribuíram para a realização deste trabalho e pelo apoio dado na minha jornada de vida.

Epigrafe

"*Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.*"

Sun Tzu Wu

Resumo

A análise de vulnerabilidades em Sistemas de Certificação Digital Centralizados consiste na identificação, avaliação e na aplicação de possíveis técnicas de controle dos riscos em ameaças de segurança cibernética identificadas nesses sistemas. Com isso, o objectivo do presente trabalho foi justamente elaborar um plano de gestão de riscos para o Sistema de Certificação Digital de Moçambique gerido pelo Instituto Nacional de Tecnologias de Informação e Comunicação com recurso a princípios, politicas, estratégias, ferramentas e boas práticas de segurança cibernética. A gestão de Sistemas de Certificação Digital é um desafio que afecta diferentes instituições públicas e privadas em vários países pois estes sistemas possuem aplicações críticas, como o caso da assinatura digital de documentos electrónicos, que podem ser críticos para os seus utilizadores, trazendo dessa forma consequências como a exploração das vulnerabilidades nestes sistemas por invasores informáticos com o objectivo de comprometer a sua segurança. Dessa forma torna-se importante a elaboração de um plano de gestão de riscos pois este tornará possível evitar perdas futuras nos activos de informação na gestão do Sistemas de Certificação Digital de Moçambique. Para atingir o objectivo explicou-se os principais conceitos de segurança em Sistemas de Certificação Digital Centralizados e em seguida fez-se uma análise das vulnerabilidades e das técnicas utilizadas na redução e mitigação de riscos de segurança cibernética nesses sistemas. Sendo que a utilização desses sistemas é relativamente nova em Moçambique, a pesquisa visa não só em identificar as suas vulnerabilidades, mas também na exploração da sua literatura com o intuito de clarificar o impacto da sua utilização para a sociedade.

Palavras-chave: Sistemas de Certificação Digital, Plano de Gestão de Riscos, Segurança da Informação, Infra-estruturas de Chaves Públicas

Abstract

The analysis of vulnerabilities in Centralized Digital Certification Systems consists of the identification, assessment and the application of possible risk control techniques in cybersecurity threats identified in these systems. With this, the objective of the present work is precisely to elaborate a risk management plan for the Digital Certification System of Mozambique managed by the National Institute of Information and Communication Technologies using principles, policies, strategies, tools and good security practices. The management of Digital Certification Systems is a challenge that affects different public and private institutions in several countries, as these systems have critical applications, such as the case of digital signature of electronic documents, which may be critical for their users, bringing consequences such as the exploitation of vulnerabilities in these systems by computer attackers with the aim of compromising their security. In this way, it is important to elaborate a risk management plan, as it will make it possible to avoid future losses in information assets in the management of Mozambique's Digital Certification System. In order to achieve the objective, the main security concepts in Centralized Digital Certification Systems were explained and then an analysis of the vulnerabilities and the techniques used in the reduction and mitigation of cybersecurity risks in these systems was carried out. Since the use of these systems is relatively new in Mozambique, the research aims not only to identify vulnerabilities in Centralized Digital Certification Systems but also to explore their literature in order to clarify the impact of their use on society.

Key words: Digital Certification Systems, Risk Management Plan, Information Security, Public Key Infrastructures

Índice

Lista de figuras

Lista de tabelas

Lista de abreviaturas e acrónimos

AC	Autoridade Certificadora
AR	Autoridade de Registo
CertAU	Certificado de Assinatura Única
DoS	*Denial of Service*
DPC	Declaração de Práticas de Certificação
FISP	*Federal Information Systems*
HSM	*Hardware Security Module*
HTTP	*Hipertext Transfer Protocol*
ICP	Infra-estruturas de Chaves Públicas
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
ITU-T	*International Telegraph Union*
ISO	*International Organization for Standardization*
IMA	*Institute of Management Accountants*
LabSEC	Laboratório de Segurança
MiTM	*Man-in-The-Middle*
NTTP	*Network News Transfer Protocol*
PDF	*Portable Document Format*
PIE	Provedores de Identidade Electrónica
SCD	Sistemas de Certificação Digital
SCDM	Sistema de Certificação Digital de Moçambique
SI	Sistema de Informação
SMTP	*Simple Mail Transfer Protocol*
SSL	*Secure Socket Layer*
SRAT	*Security Risk Assessment Tool*
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
TLS	*Transport Layer Security*
UFSC	Universidade Federal de Santa Catarina
VPN	*Virtual Private Network*

Glossário de termos

Dados – são elementos que constituem a matéria-prima da informação. Podendo, também ser definidos, como conhecimento bruto, ainda não devidamente tratado.

E-mail – é um método que permite compor, enviar e receber mensagens através de sistemas electrónicos de comunicação.

Framework - é uma série de acções e estratégias que visam solucionar um problema bem específico.

Hardware – parte física de computadores e outros sistemas electrónicos.

Informação – são os dados devidamente tratados e analisados, produzindo conhecimento relevante.

Infra-estrutura - conjunto de serviços e instalações necessários para o funcionamento de uma organização.

Internet – é um sistema público e global de redes de computadores interligadas com o propósito de servir progressivamente utilizadores no mundo inteiro.

Log – é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema informático.

Online – é o termo utilizado para referenciar o estado de activação relativo a ligado de um determinado sistema.

Protocolo – é o conjunto das informações, decisões, normas ou regras definidas a partir de um acto oficial, como audiência, conferência ou negociação para uma certa finalidade.

Sistema – é um conjunto de elementos interdependentes de modo a formar um todo organizado.

Script – é uma série de instruções escritas para que um computador execute determinadas tarefas segundo o programado.

Software – sequência de instruções a serem seguidas e/ou executadas, na manipulação, redireccionamento ou modificação de um dados.

Utilizador – é o termo utilizado para referenciar a qualquer um que utiliza determinado recurso ou serviço.

Website – é um endereço electrónico, contendo é um conjunto de páginas *web*, isto é, de hipertextos acessíveis geralmente pelo protocolo HTTP na *Internet*.

Web – uma abreviação utilizada para referir a *World Wide Web.*

Open-source - *software* de código aberto, com o seu código fonte disponibilizado e licenciado com uma licença de código aberto no qual o direito autoral fornece a possibilidade de estudar, modificar e distribuir o *software* gratuitamente para qualquer um e para qualquer finalidade.

1. Capítulo I – Introdução

1.1. Contextualização

O governo é o sector chave na gestão de um pais, pois vários processos que envolvem os cidadãos de uma sociedade são geridos por instituições do governo. A gestão manual de inúmeros processos dos cidadãos torna-se um desafio, é nesse contexto que a utilização de Tecnologias de Informação e Comunicação (TIC) tem facilitado imensamente na gestão informatizada e eficiente de processos dos cidadãos.

Segundo a *Internet World Stats* (2020) citada por Cepik & Marcelino (2021, p. 3) , em dezembro de 2019, Moçambique contava com 6.523.613 usuários de *Internet*. Cerca de 20,9% de uma população total de mais de 30 milhões, com isso verificou-se um crescimento constante nas transacções electrónicas e a segurança da informação digital tem se tornado uma preocupação real para empresas privadas e o governo. Uma forma de aumentar a segurança da informação digital é através da utilização de Sistemas de Certificação Digital (SCD), pois estes são desenvolvidos com o objectivo de garantir a autenticidade, confidencialidade, integridade e o não repúdio às informações digitais. Contudo, a gestão de dados de forma digital torna-se um desafio devido a presença de vulnerabilidades em sistemas digitais que são susceptíveis a exploração e ataques cibernéticos.

A necessidade de segurança do computador, isto é, a necessidade de proteger locais físicos, *hardware* e *software* contra ameaças, surgiu durante a Segunda Guerra Mundial, quando os primeiros *mainframes*[1], desenvolvidos para auxiliar os cálculos para a quebra de códigos de comunicação foram colocados em uso (Whitman & Mattord, 2012).

Durante a realização do estágio profissional foi possível perceber que o SCD implementado em Moçambique possui uma arquitectura centralizada e é constituído por uma ICP (Infra-estrutura de Chaves Públicas) e um PIE (Provedor de Identidade Electrónica), sendo o INTIC é a Autoridade Certificadora (AC) Raiz do Estado, como definido no decreto n.º 59/2019, com possibilidade de emitir certificados confiáveis para entidades certificadoras dos sectores público e privado e regulando os tipos de certificados que estas entidades podem emitir para o público. Para que o Sistema de Certificação Digital de Moçambique

[1] São computadores de grande porte, geralmente utilizados na gestão de um elevado número de dados.

(SCDM) seja utilizado pela maioria dos moçambicanos deve ser inclusivo. A inclusão será garantida com a utilização de diferentes atributos na identidade electrónica dos cidadãos. O SCDM irá possibilitar a realização de assinaturas digitais, emissão e revogação de certificados digitais entre outros benefícios.

As assinaturas digitais, asseguram a autenticidade, integridade e não repúdio nos documentos digitais assinados pelo seu autor. Tratando-se de documentos digitais existem vulnerabilidades presentes nos sistemas que fazem a gestão de assinaturas digitais e que podem ser exploradas por atacantes causando impactos negativos para os utilizadores desses sistemas. É dessa forma que um plano de gestão de riscos cibernéticos é importante numa organização para identificar as ameaças e vulnerabilidades de segurança cibernética e encontrar as melhores formas de reduzir os seus impactos.

De acordo com Wheeler (2011, p. 24), o objetivo dum plano de gestão de risco é maximizar a saída da organização (em termos de serviços, produtos e receita), minimizando a chance de resultados negativos inesperados. É nesse contexto que o presente trabalho descreve os princípios, politicas, estratégias, ferramentas e boas práticas de segurança cibernética para a redução do impacto dos riscos na gestão de SCD centralizados.

1.2. Definição do Problema

Mais do que olhar, o engenheiro tem a obrigação de reconhecer certas necessidades que consistem em observar o mundo ao seu redor, saber quais são os problemas de sua comunidade, quais são as necessidades, e o que poderia ser melhorado (Conselho, 2018). Este trabalho preocupa-se em acções que podem ser tomadas para a mitigação e redução de riscos cibernéticos no SCDM, dessa forma aumentando o nível sua segurança.

De acordo com o estudo feito pelo Instituto Ponemon (2021), onde entrevistou 6.610 profissionais de Tecnologias de Informação (TI) e segurança em 17 países sobre as práticas, aplicativos e pontos problemáticos de ICP de suas organizações, concluiu-se que, com o aumento da demanda por identidades electrónicas e proteção de formas de trabalho híbridas, isto é, presencial e remotamente, o número médio de certificados emitidos pela

ICP de uma organização aumentou em 50% desde 2019, de 39.197 para 58.639. Mas ainda faltam recursos e experiência para gerir esses certificados. De acordo com o mesmo estudo, 46% dizem que suas organizações não têm as habilidades necessárias para utilizar as ICP e apenas 41% das organizações têm especialistas em ICP na equipe.

De acordo com Cepik & Marcelino (2021), o facto de não existirem avaliações sistemáticas de riscos cibernéticos no país torna difícil estimar a probabilidade de ocorrência de ataques catastróficos.

O real problema consiste na inexistência de um plano de gestão de riscos com a identificação das ameaças e vulnerabilidades dos SCD centralizados com as estratégias e procedimentos a serem tomados em casos de ocorrência de ataques cibernéticos como forma de reduzir os seus impactos. Alguns dos factores que tornam os SCD centralizados vulneráveis a ataques cibernéticos são:

- A necessidade de utilização de *softwares* para tornar possível a gestão de documentos digitais pela transferência de dados, assinatura digital de documentos oficiais do governo, contratos comerciais, entre outras aplicações, associados a computadores e/ou *smartphones* cujo seu funcionamento é baseado na utilização da *Internet* que o é principal recurso para a realização de ataques cibernéticos;
- Uma implementação fraca de ICP pode ser susceptível a ataques devido a vulnerabilidades presentes na infra-estrutura em que a ICP é instalada.
- A falta de treinamento e adaptação na utilização de SCD pelos usuários para manipulação de documentos electrónicos pode ser alvo de exploração desses sistemas, pois o factor humano é o mais vulnerável e possui maior probabilidade de sofrer ataques cibernéticos de engenharia social;
- A falta de profissionais qualificados na gestão de SCD torna-os em risco pois esses sistemas fazem a gestão de informações críticas, cuja sua exposição pode causar danos elevados nas instituições.

O objectivo da implementação dum plano de gestão de riscos é fazer com que o INTIC como instituição reguladora das TIC no pais, evite perdas futuras nos activos de informação, se proteja contra ataques cibernéticos e minimize o impacto em caso de ocorrência.

1.3. Pergunta de pesquisa

De acordo com Gil (2002, p. 27), o problema de pesquisa deve ser formulado como uma pergunta, esta é a maneira mais fácil e directa de formular um problema. Além disso, facilita sua identificação por parte de quem consulta o projeto ou o relatório da pesquisa. A presente pesquisa visa responder a seguinte pergunta de pesquisa:

- De que forma princípios, politicas, estratégias, ferramentas e boas práticas de segurança cibernética aplicados num plano de gestão de riscos podem auxiliar na mitigação e redução de riscos no SCDM gerido pelo INTIC?

1.4. Motivação

Segundo o estudo realizado pelo Instituto Nacional de Governo Electrónico – INAGE (2020) citado por Cepik & Marcelino (2021), em 2018, Moçambique registrou mais de 1.5 milhão de ataques por mês. Mais de 90% foram ataques não-direcionados, principalmente *phishing*, *spam* e *malware*[2] (vírus, *worms*, *trojans* e *bots*). Mas órgãos governamentais e universidades sofreram ataques do tipo DDoS (negação de serviços distribuída) e *web defacement*[3]. Entre 2019 e 2020, além do aumento de ataques não-direcionados, foram detectados ataques persistentes, incluindo *ransomware*[4], *spyware*[5] e quebras de chaves criptográficas, em redes governamentais, empresas e no sistema financeiro. Inclusive na presença da pandemia do *Covid-19*, verificou-se um aumento significativo no uso da *Internet*, pois a pandemia reforçou o uso do trabalho remoto em diversas instituições pelo uso de aplicações que possibilitassem o trabalho remoto.

Segundo o jornal Global Voices Lusofonia (2022), Moçambique foi alvo de um ataque cibernético em *websites* do governo no dia 21 de fevereiro de 2022, entre os *websites* alvo estavam os do Instituto Nacional de Transportes Terrestres – INATTER, Instituto Nacional de Gestão de Desastres – INGD, entre outros. Segundo o jornal Global Voices Lusofonia

[2] Termo utilizado de forma genérica para referir qualquer *software* criado com o intuito de prejudicar SI.
[3] Ataques com o objectivo de modificar a aparência de um objecto, exemplo uma página *web*.
[4] Ataques com o objectivo de inibir o acesso a um Sistema e os atacantes exigem dinheiro como forma de resgate.
[5] É um tipo de *malware* que tenta se esconder enquanto registra secretamente informações e rastreia actividades de utilizadores de SI.

(2022), sobre o assunto, o dirigente da Empresa Nacional de Parques de Ciência e Tecnologias – ENPCT, no momento, referiu que este problema deriva da falta de preparo das instituições moçambicanas na segurança dos seus dados.

Figura 1: Ataque de *hackers* em portais moçambicanos

Fonte: Global Voices Lusofonia (2022)

Com isso, é possível notar que o aumento de utilizadores de *Internet* e aplicações digitais proporciona uma elevação no número de ataques cibernéticos devido as vulnerabilidades presentes em sistemas digitais. Há necessidade de implementação de estratégias de segurança cibernética para a mitigação e redução de riscos cibernéticos.

A realização deste trabalho é de extrema relevância pois surge como uma tentativa de aumentar a segurança no SCDM para que os utilizadores deste sistema usufruam de forma segura pois SCD são usados na gestão de documentos electrónicos que podem ser de extrema importância e críticos para os seus utilizadores e que o seu comprometimento pode causar enormes danos ao pais.

1.5. Objectivos

1.5.1. Objectivo geral

Elaborar um plano de gestão de riscos para o SCDM gerido pelo INTIC com recurso a princípios, politicas, estratégias, ferramentas e boas práticas de segurança cibernética.

1.5.2. Objectivos específicos

- Explicar conceitos relacionados à Segurança Cibernética e SCD;
- Identificar as principais vulnerabilidades e o impacto dos riscos de segurança cibernética em SCD centralizados;
- Descrever a situação actual do INTIC como AC Raiz do Estado no que concerne aos procedimentos de segurança cibernética;
- Apresentar uma proposta do Plano de Gestão de Riscos.

1.6. Metodologia

No estudo realizado por Oliveira afirma que

> Na verdade, método, em ciência, não se reduz a uma apresentação dos passos de uma pesquisa. Não é, portanto, apenas a descrição dos procedimentos, dos caminhos traçados pelo pesquisador para a obtenção de determinados resultados. Quando se fala em método, busca-se explicitar quais são os motivos pelos quais o pesquisador escolheu determinados caminhos e não outros. São estes motivos que determinam a escolha de certa forma de fazer ciência. (Oliveira, 2011)

É dessa forma que não só são apresentados os critérios e as escolhas, mas também o porquê dessas escolhas.

1.6.1. Classificação da metodologia

Geralmente, a classificação da metodologia é feita mediante critérios. O presente trabalho pode ser classificado da seguinte forma:

- **Quanto à abordagem**

Para Fonseca (2002, p. 20), a pesquisa pode ser classificada sendo quantitativa ou qualitativa. Segundo Gerhardt & Silveira (2009, p. 31), a pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, entre outras.

De acordo com Fonseca (2002, p. 20), a pesquisa quantitativa considera que a realidade só pode ser compreendida com a análise de dados brutos, recolhidos com auxílio de instrumentos padronizados e neutros. A presente pesquisa pode ser classificada como sendo qualitativa.

- ✓ Qualitativa: Pois a solução para os problemas identificadas baseou-se na análise e interpretação de princípios, politicas, estratégias, ferramentas e boas práticas de segurança cibernética, tendo se feito observações críticas das ideias abordadas no corpo do trabalho.

- **Quanto à natureza**

Para Gerhardt & Silveira (2009), quanto a natureza a pesquisa pode ser classificada sendo:

- ✓ Pesquisa básica: objetiva gerar conhecimentos novos, úteis para o avanço da ciência, sem aplicação prática prevista. Envolve verdades e interesses universais.
- ✓ Pesquisa aplicada: objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais.

Quanto a natureza a presente pesquisa é classificada sendo aplicada, pois objectiva identificar vulnerabilidades e riscos específicos de SCD de forma a elaborar as respectivas medidas de controle para o INTIC.

- **Quanto aos objectivos**

Segundo Gil (2002), quanto aos objectivos a pesquisa pode ser classificada sendo:

- ✓ Exploratória: Estas pesquisas têm como objectivo proporcionar maior familiaridade com o problema, com vista a torná-lo mais explícito ou construir hipóteses.
- ✓ Descritiva: As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis.
- ✓ Explicativa: Essas pesquisas têm como preocupação central identificar os factores que determinam ou que contribuem para a ocorrência dos fenómenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade porque explica a razão ou o porquê das coisas.

No entanto, a presente pesquisa pode ser classificada como exploratória pois o SCDM é novo para realidade moçambicana não existindo muito conhecimento acerca da sua utilização e para obtenção das informações o autor associou-se à AC Raiz do Estado – INTIC.

- **Quanto aos procedimentos**

Para Gil (2002, p. 43), delineamento refere-se ao planejamento da pesquisa em sua dimensão mais ampla, que envolve tanto a diagramação quanto a previsão de análise e interpretação de colecta de dados. O elemento mais importante para a identificação de um delineamento é o procedimento adoptado para a colecta de dados. Os procedimentos utilizados na presente pesquisa são:

- Pesquisa bibliográfica: Para Gil (2002, p. 44), a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Desta forma, o presente trabalho consistiu na utilização de livros, artigos científicos e páginas *web* para a colecta de todo material teórico sobre SCD e sobre a aplicação da segurança cibernética no contexto de certificados digitais.
- Pesquisa documental: Segundo o estudo realizado por Gil (2002)

> A pesquisa documental assemelha-se muito à pesquisa bibliográfica. A diferença essencial entre ambas está na natureza das fontes. Enquanto a pesquisa bibliográfica utiliza fundamentalmente das contribuições dos diversos autores sobre determinado assunto, a pesquisa documental vale de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa. Incluem-se aqui inúmeros outros documentos como cartas pessoais, diários, fotografias, gravações, memorandos, regulamentos, ofícios e boletins.

Através da pesquisa documental foram utilizadas informações além da pesquisa bibliográfica como entrevistas, regulamentos e aulas sobre o SCDM fornecidos pelo INTIC.

- Estudo de caso: no estudo realizado por Fonseca (2002, p. 33) , um estudo de caso pode ser caracterizado de acordo com um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social. A pesquisa foi realizada no INTIC, onde foi possível descrever o instituto, com o objectivo de saber a sua composição no geral e aspectos relevantes para o estudo do SCDM.
- Pesquisa participante: este tipo de pesquisa caracteriza-se pelo envolvimento e identificação do pesquisador com as pessoas investigadas (Gerhardt & Silveira, 2009, p. 40). Pelo facto do pesquisador ter frequentado um estágio profissional no INTIC, tornou-se mais acessível a identificação de informações relevantes para a realização da pesquisa.

1.6.2. Técnicas de colecta de dados

Durante a colecta de dados, diferentes técnicas podem ser empregadas, sendo mais utilizadas as seguintes: a entrevista, o questionário, a observação e a pesquisa documental (Oliveira, 2011, p. 35).

- Entrevista: Para Lakatos e Marconi (2007) citados por Zanella (2013, p. 115), a entrevista é um encontro entre duas pessoas, a fim de que uma delas obtenha informações a respeito de determinado assunto. Essa técnica foi utilizada para recolha de dados sobre a situação actual do INTIC em termos de segurança no INTIC.
- Questionário: De acordo com Lakatos & Marconi (2003, p. 201), questionário é um instrumento de coleta de dados, constituído por uma série ordenada de perguntas, que devem ser respondidas por escrito e sem a presença do entrevistador. Através dessa técnica foram colectadas informações para avaliar o nível de capacitação na gestão de SCD a equipe técnica na implementação do SCDM.
- Observação: Como diz Triviños (1987) citado por Zanella (2013, p. 121), a observação não é simplesmente olhar, mas destacar de um conjunto, objectos, pessoas, animais,

por exemplo, algo específico, prestando atenção em suas características. Sendo que o pesquisador realizou um estágio profissional no INTIC, através dessa técnica identificou a arquitectura do SCDM e aprofundou mais sobre o assunto através de formações fornecidas pelas instituição.

- Pesquisa documental: Segundo Lakatos e Marconi (2001) citado por Oliveira (2011, p. 40), a pesquisa documental é a colecta de dados em fontes primárias, como documentos escritos ou não, pertencentes a arquivos públicos, arquivos particulares de instituições, domicílios e fontes estatísticas. Através de livros e artigos científicos encontrados em fontes electrónicas foi possível realizar uma recolha de dados confiáveis sobre os SCD centralizados e sobre as técnicas utilizadas para a mitigação dos riscos das vulnerabilidades identificadas.

1.6.3. Técnicas de análise de dados

A análise segundo Lakatos & Marconi (2003, p. 168), é realizada em três níveis, sendo a interpretação, a explicação e a especificação. No presente trabalho os níveis foram utilizados da seguinte forma:

- Intepretação: Fez-se um estudo das vulnerabilidades e dos riscos presentes em SCD centralizados de forma a verificar de que maneira as diferentes soluções podem ser implementadas no SCDM.
- Explicação: Realizou-se uma explanação de como funciona um plano de gestão de riscos no contexto de segurança cibernética e como este pode ser aplicado no INTIC.
- Especificação: Procurou-se perceber como e de que forma ocorrem os principais ataques ou exploração em SCD centralizados com o intuito de perceber o impacto dessas acções para colocar no plano de gestão de riscos.

1.6.4. Metodologia de elaboração do plano de gestão de riscos

A metodologia para a elaboração da solução dos problemas identificados no ponto 1.2 resume-se na elaboração de um plano de gestão de riscos. Nesse sentido, o plano de

gestão de riscos foi elaborado tendo em conta as fases da metodologia de gestão riscos apresentada no Whitman & Mattord (2012), contendo as seguintes fases:

i. Identificação do risco: onde realizou-se um estudo dos activos de informação do INTIC, ou seja, identificou-se, classificou-se e priorizou-se.
ii. Avaliação de risco: depois de se ter identificado os ativos de informações do INTIC, as ameaças e vulnerabilidades, fez-se uma avaliação de riscos relativa de cada uma das vulnerabilidades.
iii. Controle de risco: onde foram elaboradas as estratégias que podem ser usadas no controle do risco, de forma a evitar, transferir ou mitigar os riscos.

Para a compreensão genérica da gestão de riscos em organizações utilizou-se o padrão ISO 31000 que especifica normas internacionais sobre a gestão de riscos e fez-se consultas regulares aos supervisores.

1.6.5. Ferramentas utilizadas

A ferramenta utilizada para a elaboração da solução para o problema consistiu na utilização de uma ferramenta cuja sua descrição é apresentada na tabela abaixo.

Tabela 1: Descrição da ferramenta utilizada na elaboração da solução

Ferramenta	Denominação	Descrição	Justificativa
SRAT versão 1.0.0	*Security Risk Assessment Tool* (Ferramenta de gestão de riscos)	Segundo a Open Briefing SART é uma ferramenta de avaliação de riscos de segurança gratuita e essencial para gestores de segurança para avaliações de risco.	Muito bem documentada, gratuita, calcula automaticamente as classificações de risco e outros parâmetros, tendo a empresa mais de com 10 anos de experiência na gestão de riscos cibernéticos.

Fonte: Elaborada pelo autor

1.7. Estrutura do Trabalho

O presente trabalho é composto por seis capítulos, devidamente enumerados e duas secções não enumeradas referentes a bibliografia e aos anexos. A seguir é apresentada a descrição de cada uma das partes constituintes do trabalho:

- **Capitulo I – Introdução**

Este capitulo é referente a introdução do trabalho, onde foi feita a contextualização do tema de pesquisa, definição do problema, motivação, definição dos objectivos a serem alcançados e a metodologia utilizada na realização do trabalho.

- **Capitulo II - Revisão de Literatura**

Neste capitulo reuniu-se as informações necessárias para servirem de referencial teórico para a realização da pesquisa, utilizando uma sequência lógica com aspectos relacionados à segurança cibernética, SCD e provedores de identidade electrónica.

- **Capitulo III – Caso de Estudo**

Neste capítulo foi feita uma descrição do INTIC como caso de estudo, da sua situação actual, dos constrangimentos enfrentados e colecta dos dados através das técnicas de colecta de dados descritas na metodologia do trabalho.

- **Capitulo IV – Proposta de Solução**

Este capítulo diz respeito aos procedimentos, aspectos técnicos e a metodologia utilizada para elaboração do plano de gestão de riscos.

- **Capitulo V – Discussão de Resultados**

Apresenta-se a análise dos resultados obtidos na revisão de literatura, no caso de estudo e na proposta de solução.

- **Capitulo VI - Considerações Finais**

Nesta parte, apresentou-se de forma conclusiva os resultados obtidos pela pesquisa, verificou-se o cumprimento ou incumprimento dos objectivos inicialmente propostos para elaboração da solução proposta. Pelos constrangimentos encontrados na realização do

trabalho, recomendou-se medidas que podem ser tomadas para a melhoria de próximas pesquisas relacionadas com o tema.

- **Secção das Bibliografias**

Tratando-se de um trabalho de pesquisa, é necessário fazer menção das fontes bibliográficas utilizadas para a obtenção da informação utilizada no trabalho, tendo sido estas devidamente citadas, bem como as que não foram citadas, mas ajudaram na compreensão das matérias abordadas no trabalho.

- **Anexos**

Nesta secção, faz-se a apresentação de todos os elementos que fundamentam e comprovam aspectos que foram apresentados no corpo do trabalho.

2. Capítulo II – Revisão da Literatura

2.1. Segurança da Informação

Em geral, **segurança** é a qualidade ou estado de estar seguro, estar livre de perigo. Em outras palavras, a proteção contra adversários, daqueles que causariam danos, intencionalmente ou de outra forma (Whitman & Mattord, 2012, p. 8).

Conforme destacam Canabarro, Borne e Leal (2014) citados por Cepik (2018, p. 4), o **ciberespaço** é formado pelas diversas estruturas, equipamentos, códigos, agentes e interações que utilizam o espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas.

Dessa forma pode se perceber que a **segurança cibernética** é um conjunto de políticas, estratégias, técnicas ou procedimentos para protecção do ciberespaço, que é constituído por equipamentos e dados computacionais com o objectivo de preservar a integridade, confidencialidade e disponibilidade da informação digital.

2.1.1. Principais Conceitos de Segurança da Informação

O ramo da segurança de informação é bastante vasto e existem diversos conceitos que são essenciais para a sua percepção. Segundo Whitman & Mattord (2012), os principais conceitos de segurança da informação são descritos da seguinte forma:

- **Acesso:** a capacidade de um sujeito ou objecto de usar, manipular, modificar ou afectar outro sujeito ou objecto. Os utilizadores autorizados têm acesso legal a um sistema, enquanto que os *hackers* têm acesso ilegal ao sistema. Os controles de acesso regulam essa capacidade.
- **Activo:** o recurso organizacional que deve ser protegido. Um activo pode ser lógico, como um *website*, informações ou dados ou físico, como uma pessoa, um computador ou outro objecto tangível. Os activos de informação são o foco dos esforços de segurança, eles são o que esses esforços tentam proteger.
- **Ataque:** um acto intencional que pode causar danos ou comprometer informações e/ou os sistemas que as suportam. Os ataques podem ser activos ou passivos, intencionais ou não intencionais, diretos ou indiretos.

- ✓ **Ataque passivo** – ocorre quando alguém que lê casualmente informações confidenciais não destinadas ao seu uso.
- ✓ **Ataque intencional e não intencional** – pode ser exemplificado, por um *hacker* tentando invadir um sistema de informação é um ataque intencional. Um relâmpago que causa um incêndio em um prédio é um ataque não intencional.
- ✓ Um **ataque directo** pode ser exemplificado, por é um *hacker* utilizando um computador pessoal para invadir um sistema. Os ataques directos se originam da própria ameaça.
- ✓ Um **ataque indirecto** pode ser exemplificado, por um *hacker* que compromete um sistema, utilizando outros sistemas, por exemplo, como parte de uma *botnet* (rede de robôs).

- **Controle, proteção ou contramedida:** mecanismos de segurança, políticas ou procedimentos que podem combater ataques com sucesso, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização.
- **Exploração:** uma técnica usada para comprometer um sistema. Os agentes de ameaças podem tentar explorar um sistema ou outro activo de informação usando-o ilegalmente para ganho pessoal.
- **Exposição:** uma condição ou estado de ser exposto. Na segurança da informação, a exposição existe quando uma vulnerabilidade conhecida por um invasor está presente.
- **Perda:** uma única instância de um activo de informação que sofre danos ou modificação ou divulgação não intencional ou não autorizada.
- **Perfil de proteção ou postura de segurança:** todo o conjunto de controles e salvaguardas, incluindo política, educação, treinamento e conscientização e tecnologia, que a organização implementa (ou deixa de implementar) para proteger um activo.
- **Risco:** a probabilidade de que algo indesejado aconteça. As organizações devem minimizar o risco para corresponder ao sua posição ao risco.
- **Sujeitos e objectos:** sujeito - um agente ou entidade usado para conduzir o ataque, objecto – a entidade alvo. Um computador pode ser tanto o sujeito quanto o objecto de um ataque, quando, por exemplo, é comprometido por um ataque (objecto), e então é usado para atacar outros sistemas (sujeito).

- **Ameaça:** uma categoria de objetos, pessoas ou outras entidades que representam um perigo para um activo.
- **Agente de ameaça:** a instância específica ou um componente de uma ameaça. Por exemplo, todos os *hackers* do mundo apresentam uma ameaça coletiva, enquanto Kevin Mitnick, que foi condenado por invadir sistemas telefónicos, é um agente de ameaças específico.
- **Vulnerabilidade:** uma fraqueza ou falha em um sistema ou mecanismo de protecção que o abre porta para ataques ou danos.

2.1.2. Características Críticas da Informação

Segundo Whitman & Mattord (2012), o valor da informação vem das características que ela possui. Quando uma característica da informação muda, o valor dessa informação aumenta ou, mais comumente, diminui.

O padrão NIST FIPS 199 publicado em 2004 (*Standards for Security Categorization of Federal Information and Information Systems*) citado por Stallings (2017) lista confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informações e para SI. Para Ferreira (2008), a tríade CIA (*Confidentiality, Integrity and Availability*) – Confidencialidade, Integridade e Disponibilidade – representa os três principais atributos que, actualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. O FIPS 199 (2004) citado por Stallings (2017, p. 22), fornece uma caracterização útil desses três objetivos em termos de requisitos e a definição de uma perda de segurança em cada categoria.

- **Confidencialidade:** Preservar as restrições autorizadas de acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias. Uma perda de confidencialidade é a divulgação não autorizada de informações.

- **Integridade:** protecção contra modificação ou destruição imprópria de informações, incluindo a garantia de não repúdio e autenticidade das informações. Uma perda de integridade é a modificação ou destruição não autorizada de informações.
- **Disponibilidade:** Garantir o acesso e o uso oportuno e confiável das informações. Uma perda de disponibilidade é a interrupção do acesso da informação ou de um SI.

Figura 2: Tríade CIA

Fonte: Purcell (2018)

2.1.3. Componentes de Sistemas de Informação

Para Whitman & Mattord (2012), um sistema de informação (SI) é muito mais do que *hardware* de computador; é todo o conjunto de *software*, *hardware*, dados, pessoas, procedimentos e redes que possibilitam o uso dos recursos de informação na organização. Segundo os mesmos autores os componentes de SI podem ser descritos da seguinte forma:

- ***Software*:** compreende aplicativos, sistemas operacionais e utilizadores de comando variados. O *software* é talvez o componente SI mais difícil de proteger. A exploração de erros na programação de *software* é responsável por uma parcela substancial dos ataques às informações.

- ***Hardware*:** é a tecnologia física que abriga e executa o *software*, armazena e transporta os dados e fornece interfaces para entrada e remoção de informações do sistema. As políticas de segurança física lidam com o *hardware* como um activo físico e com a protecção de activos físicos contra danos ou roubo.
- **Dados:** os dados armazenados, processados e transmitidos por um sistema de computador devem ser protegidos. Os dados costumam ser o activo mais valioso de uma organização e são o principal alvo de ataques intencionais.
- **Pessoas**: Embora muitas vezes é negligenciado nas considerações de segurança do computador, as pessoas sempre foram uma ameaça à segurança da informação. As pessoas podem ser o elo mais fraco no programa de segurança da informação de uma organização. E, a menos que políticas, educação e treinamento, conscientização e tecnologia sejam empregadas adequadamente para evitar que as pessoas danifiquem ou percam informações acidentalmente ou intencionalmente, elas continuarão sendo o elo mais fraco.
- **Procedimentos**: Procedimentos são instruções escritas para realizar uma tarefa específica. Quando um usuário não autorizado obtém os procedimentos de uma organização, isso representa uma ameaça à integridade das informações. Educar os funcionários sobre os procedimentos de protecção é tão importante quanto proteger fisicamente o sistema de informações.
- **Rede:** Quando os sistemas de informação são conectados uns aos outros para formar redes locais, e essas redes são conectadas a outras redes, como a *Internet*, novos desafios de segurança surgem rapidamente. Ainda é importante aplicar as ferramentas tradicionais de segurança física, como fechaduras e chaves, para restringir o acesso e a interação com os componentes de *hardware* de um sistema de informação, mas quando os sistemas de computador estão em rede, essa abordagem não é mais suficiente. Etapas para fornecer segurança em redes são essenciais, assim como a implementação de sistemas de alarme e intrusão para conscientizar os proprietários do sistema sobre os comprometimentos contínuos.

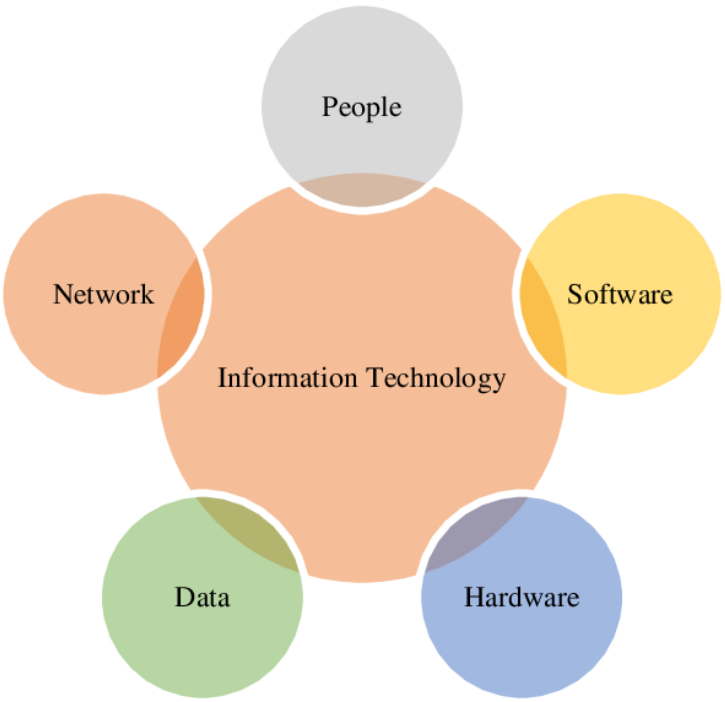

Figura 3: Componentes de SI

Fonte: Rashid (2018)

2.2. Sistemas de Certificação Digital

Certificação Digital – para Casagrande (2011, p. 10), a Certificação Digital é uma forma de confirmar a autenticidade de documentos electrónicos, a identidade de seus emitentes e segurança quanto ao seu sigilo durante o tráfego via conexões remotas.

Sistemas de Certificação Digital – conforme o decreto n.º 59/2019, que define o Regulamento do SCDM, pode-se perceber que SCD são sistemas que englobam serviços de certificação digital, como a realização de transacções electrónicas seguras, a autenticação segura, a autenticidade, integridade, confidencialidade, validade jurídica e não repúdio das assinaturas electrónicas de transacções ou informações em documentos electrónicos de entidades públicas e privadas.

Documentos físicos, isto é, no formato de papel são demasiadamente utilizados no registo de diferentes tipos de informações. Em Moçambique diferentes documentos são ainda geridos no formato físico e para autenticar esses documentos os cidadãos recorrem ao notário. Notários são instituições reconhecidas pelo governo e que garantem a autenticidade

dos documentos físicos, como forma de comprovar que os documentos realmente pertencem a um determinado indivíduo.

Essa solução funciona mas possui algumas limitações pois é necessário que as pessoas se dirijam-se a notários o que de alguma forma pode ser desvantajoso, pelo custo, pela gestão manual de documentos que possui diversas desvantagens. Com a presença da pandemia do *Covid-19* a interação física das pessoas foi de alguma forma limitada, novas oportunidades e formas de trabalho surgiram que utilizam documentos electrónicos em substituição aos documentos físicos. Para Casagrande (2011, p. 9) na busca por soluções, novas tecnologias tem sido empregadas. A Certificação Digital se apresenta como uma das alternativa viáveis.

2.2.1. Conceitos gerais de Criptografia

De acordo com Whitman & Mattord (2012, p. 353), actualmente, muitas ferramentas de TI comuns usam tecnologias de criptografia incorporadas para proteger informações confidenciais nos aplicativos. Por exemplo, todos os navegadores da *web* populares usam recursos de criptografia integrados para permitir o comércio electrónico seguro, como serviços bancários on-line e compras na *web*.

É inegável que a *Internet* revolucionou a forma como as pessoas se relacionam em diferentes partes do mundo. Com o uso da internet a comunicação tornou-se fácil e de grande alcance para os utilizadores desta rede. Desta forma torna-se necessário o uso de técnicas de encriptação de dados para a realização de transações mais seguras.

Criptografia – a palavra criptografia é originaria dos gregos *kryptus*, que quer dizer oculto e *graph*, escrever. É o processo de fazer e usar códigos para garantir a transmissão de informações (Casagrande, 2011, p. 21). Para compreender os fundamentos da criptografia, é necessário conhecer os principais conceitos. Para Whitman & Mattord (2012), os principais conceitos podem ser descritos da seguinte forma:

- **Texto plano:** a mensagem original não criptografada ou uma mensagem que foi decifrada com sucesso.

- **Chave:** As informações usadas em conjunto com um algoritmo para criar o texto cifrado do texto simples ou derivar o texto simples do texto cifrado, a chave pode ser uma série de *bits* usados por um programa de computador, ou pode ser uma senha usada por humanos que é então convertida em uma série de *bits.*
- **Texto cifrado:** a mensagem codificada resultante de uma cifragem.
- **Encriptação:** significa codificar ou converter o texto simples no texto cifrado equivalente.
- **Decriptação:** significa decodificar ou converter o texto cifrado no texto simples equivalente.
- **Criptoanálise:** as técnicas usadas para decifrar uma mensagem sem nenhum conhecimento dos detalhes de codificação.
- **Algoritmo:** as etapas programáticas usadas para converter uma mensagem não criptografada em uma sequência criptografada de *bits* que representam a mensagem ou para fazer o processo inverso (decifrar).

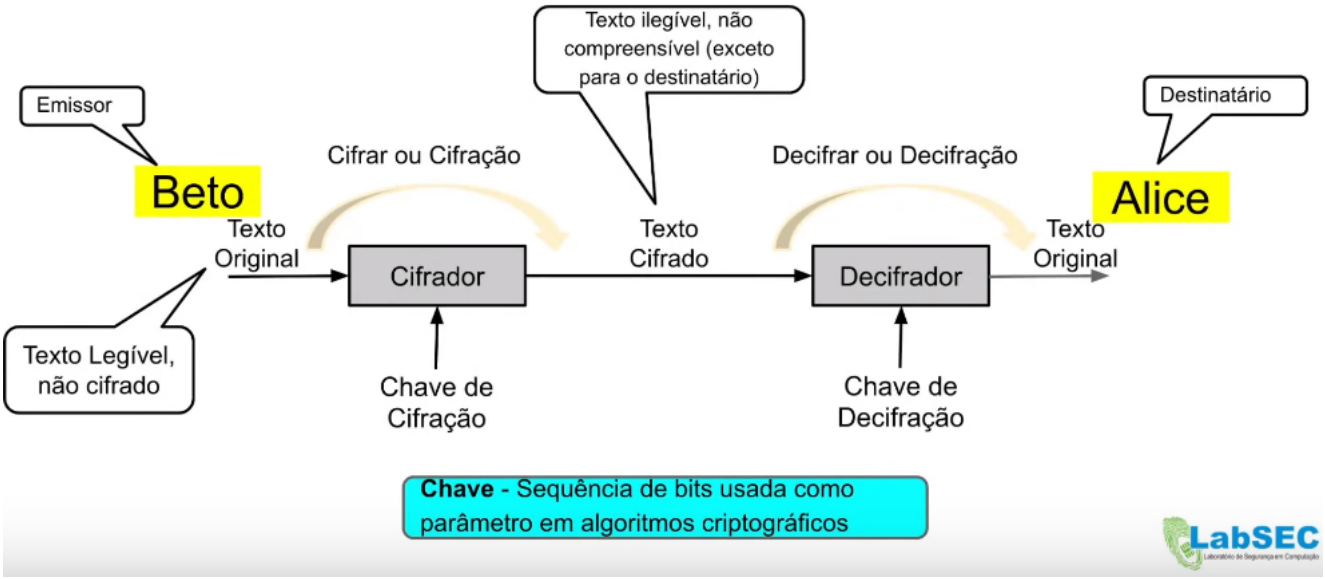

Figura 4: Conceitos fundamentais de criptografia

Fonte: UFSC LabSEC (2022)

A figura acima é uma ilustração simplificada do processo de criptografia, onde um emissor (Beto) envia uma mensagem a um destinatário (Alice), nesse processo a mensagem é cifrada para um texto ininteligível e enviada a partir de um canal utilizando chaves e algoritmos de encriptação e em seguida é decifrada para um texto inteligível.

2.2.2. Comparação de documentos físicos e electrónicos em requisitos de segurança

Para Dias (2004), o uso do documento electrónico é viável, com o uso de novas tecnologias desenvolvidas para o atendimento de requisitos de segurança e funcionais deste tipo de documento. Tendo demonstrado a importância do uso do documento electrónico conforme consta na tabela abaixo.

Tabela 2: Comparação de documentos físicos e electrónicos em requisitos de segurança

Requisitos	Documento em Papel	Documento Electrónico
Autenticidade	Assinatura manuscrita atrelada a um substrato físico contendo as informações que se deseja transmitir ou expressar concordância.	Assinaturas digitais, que dependem dos requisitos irrefutabilidade e irretratabilidade.
Integridade	O documento não deve ter seu conteúdo e formato alterados, sendo qualquer tentativa de fraude identificada. É garantida através da integridade do substrato físico para os documentos em papel.	A integridade de documentos electrónicos é garantida através do uso de funções de resumo criptográfico.
Tempestividade	Requisito relacionado com o estabelecimento de referência temporal, criando evidencias da existência do documento em determinado instante do tempo. Terceiras Partes Confiáveis como Cartórios garantem este requisito para documentos em papel.	Terceiras Partes Confiáveis como Autoridades de Datação garantem este requisito para documentos electrónicos.
Sigilo	O conteúdo do documento deve ser mantido oculto até a ocorrência de um determinado evento.	Encriptação do documento
Privacidade	Classificação dos documentos aos quais o acesso é restrito.	Encriptação com a chave pública, utilizando algoritmos de encriptação simétricos ou assimétricos. Uma

		entidade comprova que somente esta entidade tem acesso à informação, sendo a divulgação prova da quebra de privacidade.
Irrefutabilidade	Requisito no qual o autor de um documento não pode negar a autoria do mesmo. Obtida através da assinatura manuscrita.	Uso da chave privada expressando o consentimento por parte do assinante.
Irretratabilidade	Requisito no qual o autor de um documento não pode negar os termos contidos no documento. Atendido pela assinatura manuscrita que expressa a aprovação do conteúdo visualizado directamente.	Uso de plataformas confiáveis garante o acesso ao conteúdo, sendo a assinatura digital responsável pela expressão da concordância.
Disponibilidade	O aspecto de segurança que está ligado ao armazenamento seguro do documento. O aspecto disponibilidade está relacionado à forma de acesso ao documento ou cópia autenticada.	Esse aspecto está relacionado com o armazenamento seguro e controle de acesso. O aspecto disponibilidade é relacionado ao uso de plataformas computacionais com recursos suficientes para acesso ao documento local ou remotamente.
Auditoria	A auditoria com a relação ao acesso aos documentos não é facilmente obtida sendo necessário mecanismos externos para o controle de acesso. Uma entidade depende de recursos próprios para armazenar dados sobre documentos ou assinaturas geradas anteriormente.	A auditoria com relação ao controle de acesso pode ser obtida através de aplicativos ou então fornecida pelos sistemas operacionais, parte componente das plataformas computacionais utilizadas.

Fonte: Dias (2004)

2.2.3. Criptografia Simétrica

Conforme Oliveira (2012, p. 2), é o modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra. O mesmo autor descreve **a) Algoritmos de Criptografia Simétrica, b) Vantagens e c) Desvantagens**.

a) Algoritmos de Criptografia Simétrica

Os principais algoritmos de criptografia simétrica são:

Tabela 3: Principais algoritmos de criptografia simétrica

Algoritmo	Descrição
AES	O AES tem um tamanho de bloco fixo em 128 *bits* e uma chave com tamanho de 128, 192 ou 256 *bits*, é relativamente fácil de executar e requer pouca memória.
DES	Apesar de permitir cerca de 72 quadrilhões de combinações, seu tamanho de chave (56 *bits*) é considerado pequeno, tendo sido quebrado por (força bruta) em 1997 em um desafio lançado na *Internet*.
3DES	Permite 112 ou 168 *bits*, 3DES é uma simples variação do DES, utilizando em três encriptações sucessivas, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	Tem um tamanho fixo de 128 *bits*, é muito utilizado na criptografia de *e-mails.*
Blowfish	Permite 32 a 448 *bits*, que oferece a escolha, entre maior segurança ou desempenho através de chaves de tamanho variável.
Twofish	O *Twofish* é uma chave simétrica que emprega a cifra de bloco de 128 *bits*, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 *bits*. Ele realiza 16 interações durante a criptografia, sendo um algoritmo bastante rápido.

RC2	Permite de 8 a 1024 *bits*, voltado para criptografia de *e-mails* corporativos e possui tamanho variável.
CAST	É um algoritmo de cifra de bloco. O CAST-128 é um algoritmo com 12 a 16 iterações da etapa principal, tamanho de bloco de 64 *bits* e chave de tamanho variável (40 a 128 *bits*, com acréscimos de 8 *bits*). As 16 etapas de iteração são usadas quando a chave tem comprimento maior que 80 *bits*.

Fonte: Adaptado de Oliveira (2012)

b) Vantagens

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.

c) Desvantagens

O principal problema residente na utilização deste sistema de criptografia é que quando a chave de encriptação é a mesma utilizada para decriptação, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento (o que nem sempre é fácil de ser garantido), qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem.

- Não garante os princípios de autenticidade e não repúdio.

d) Princípio de funcionamento

A figura abaixo descreve o funcionamento da criptografia simétrica. A explicação é baseada na compreensão do autor.

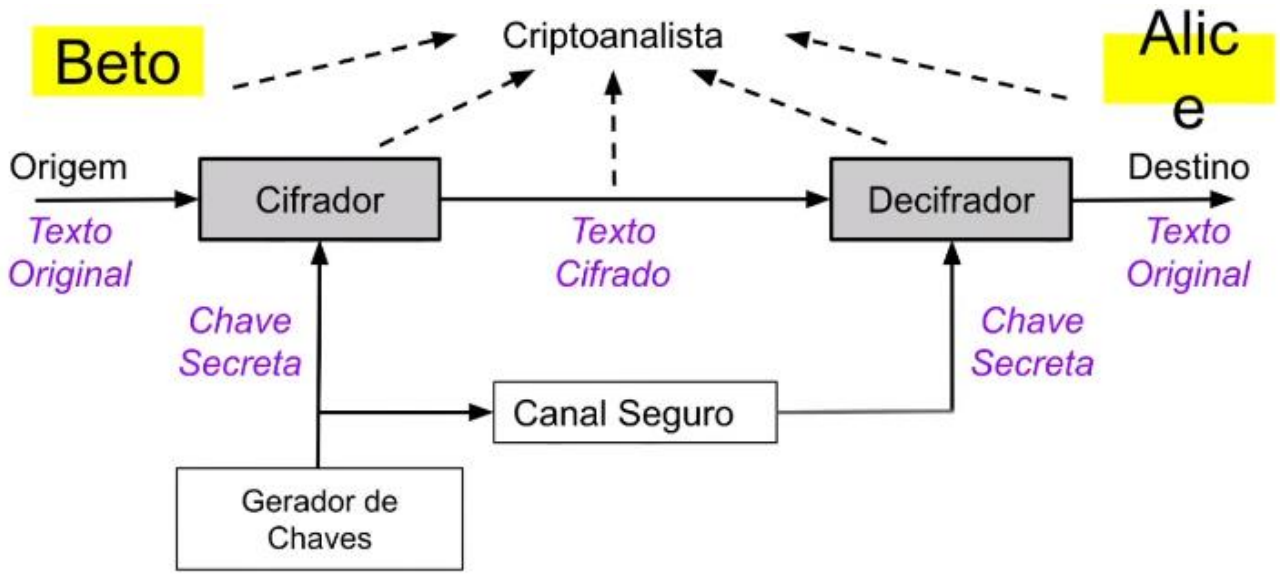

Figura 5: Princípio de funcionamento da Criptografia Simétrica

Fonte: UFSC LabSEC (2022)

A chave privada é utilizada para cifrar e decifrar, primeiro é gerada por um gerador de chaves, que é responsável por gerar a chave que é uma sequência aleatória gerada por um algoritmo, a chave pode ser gerada pelo Beto, pela Alice ou por uma terceira entidade que deve fornecer as cópias a Alice e ao Beto. O canal seguro de comunicação funciona como um túnel e precisa de uma série de requisitos para o compartilhamento de informação de forma segura. O cifrador é responsável por cifrar a mensagem e o decifrador é responsável por decifrar a mensagem utilizando a mesma chave privada.

2.2.4. Criptografia Assimétrica

Segundo Oliveira (2012, p. 3), cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública.

O mesmo autor descreve **a) Algoritmos de Criptografia Assimétrica, b) Vantagens e c) Desvantagens**.

a) Algoritmos de Criptografia Assimétrica

Tabela 4: Algoritmos de Criptografia Assimétrica

Algoritmos	Descrição
RSA	O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como factoração. Por exemplo, os factores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve factorar um grande número. Se o número for grande o suficiente e bem escolhido, então dificilmente pode-se fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de factoração de números grandes. Deste modo, a factoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 *bits* foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países.
ElGamal	O *ElGamal* é outro algoritmo assimétrico utilizado para a gestão de chaves. Sua matemática difere da utilizada no RSA, mas também é um procedimento comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o *ElGamal* obtém sua segurança da dificuldade de calcular logaritmos discretos em um tempo finito, o que se assemelha ao problema da factoração.
Curvas Elípticas	Os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o *ElGamal*, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos

	corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho.

Fonte: Adaptado de Oliveira (2012)

b) Vantagens

A grande vantagem da criptografia assimétrica é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio da chave privada como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens.

c) Desvantagens

O óbice deste sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional.

d) Princípio de funcionamento

A figura abaixo descreve o funcionamento da criptografia assimétrica. A explicação é baseada na compreensão do autor.

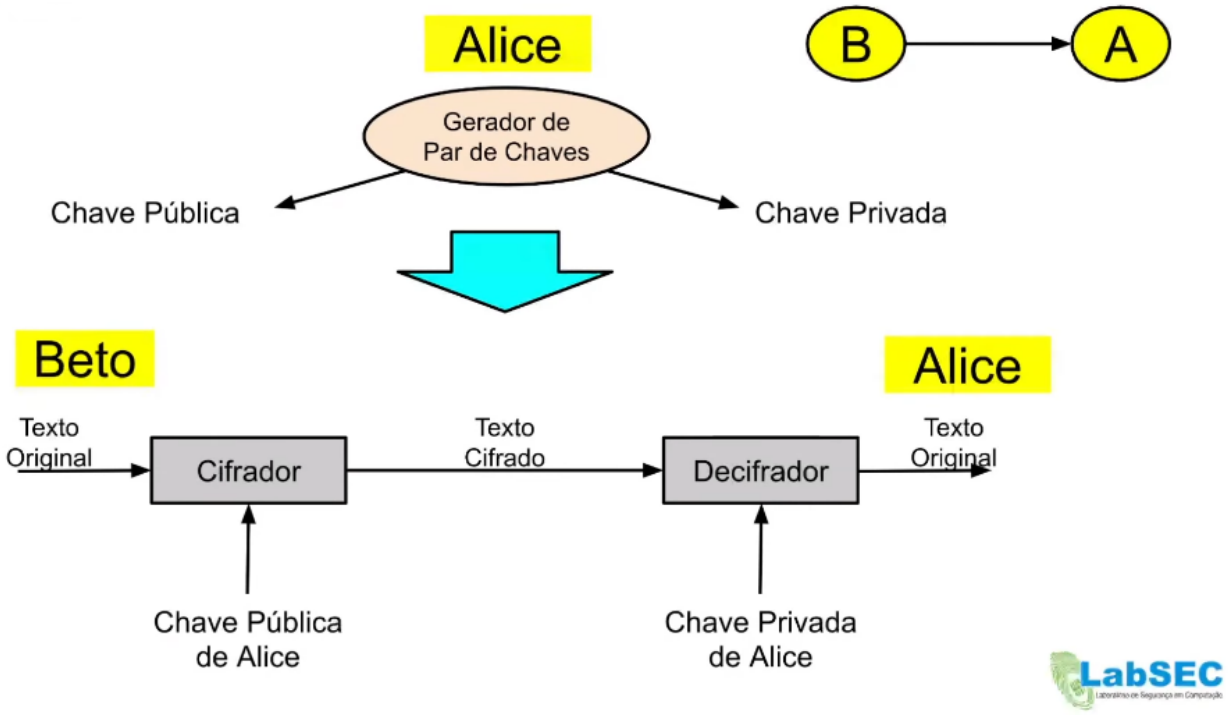

Figura 6: Principio funcionamento da criptografia assimétrica

Fonte: UFSC LabSEC (2022)

Na criptografia assimétrica o gerador de chaves gera um par de chaves, uma pública e uma privada. A chave pública é de acesso público, qualquer um pode ter acesso. Primeiramente a Alice gera um par de chaves e ela divulga a sua chave pública ao Beto. O cifrador de texto original, cifra com a chave pública da Alice, no fim a Alice com a sua chave privada decifra a mensagem enviada pelo Beto. Dessa forma não é necessário o compartilhamento da chave privada na comunicação.

2.2.5. Certificados Digitais

Tendo sido abordados conceitos essenciais sobre a criptografia nos pontos 2.1, 2.2, 2.4 e 2.5, uma questão que pode surgir seria: na comunicação, de que forma podia-se garantir que uma chave pública pertence a um determinado sujeito? Para responder a essa questão é necessário perceber o que é um certificado digital.

Certificado digital, também chamado certificado de chave pública, pode ser conceituado como um documento electrónico que associa, de maneira segura, uma entidade a uma chave pública (Ardigo, 2004, p. 52).

Segundo o ITU-T (2000) citado por Ardigo (2004, p. 52)

> O formato de certificados digitais mais aceito e adotado atualmente tem como base o modelo especificado na recomendação ITU-T X.509 Versão 3. Estas especificações permitem que diferentes aplicações que possuem mecanismos de certificação digital sejam capazes de manipular e extrair dados de certificados digitais e listas de certificados revogados, bem como interagir com os componentes de uma ICP.

Com isso é possível notar que essa versão dos certificados X.509 surgiu com a intenção de reduzir os esforços realizados por diferentes aplicações na gestão de certificados digitais. Os certificados digitais não só contém a chave pública de uma entidade, mas também apresentam outras informações importantes e opcionais de utilizadores como mostrado na figura abaixo.

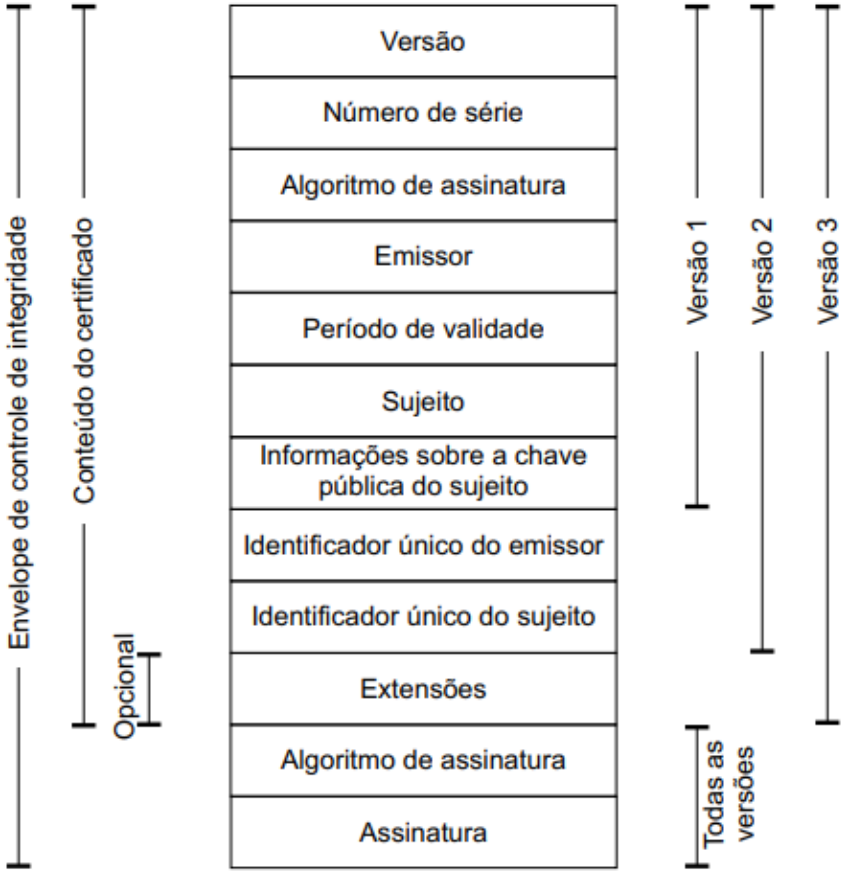

Figura 7: Certificado X.509

Fonte: Ardigo (2004)

Com a figura acima pode-se notar que a versão 3 dos certificados X.509 apresentam o campo (Extensões). As extensões são campos adicionais dos certificados, que permitem

incluir informações nos certificados não suportadas pelo conteúdo básico (Ardigo, 2004, p. 55).

Segundo o mesmo autor, um exemplo da necessidades do campo extensão ocorre em um cenário onde um Banco deseja emitir certificados para todos os seus clientes, e estes certificados devem conter o número da agência e da conta corrente do respectivo cliente. Os campos básicos do certificado não suportam tais informações, portanto a solução foi criar o campo de extensão para conter estas informações.

2.2.5.1. Ciclo de Vida do Certificado Digital

Os certificados digitais apresentam um ciclo de vida, é necessário possuir um prazo de validade devido à evolução dos dispositivos de processamento (Cordeiro, 2011).

Como visto que a principal função do certificado digital é associar as chaves públicas das entidades em operações que envolvem a certificação digital, é necessário que haja um período de validade desses certificados como forma de evitar falhas de segurança.

Nos estudos realizados por Ardigo, afirma que

> A fase inicial compreende a criação da requisição e o seu envio para a entidade validadora. Estas acções são, usualmente, realizadas pelo próprio requerente do certificado. A validação da requisição é feita por uma Autoridade de Registro ou pela própria Autoridade Certificadora que emitirá o certificado, seguindo uma política previamente estabelecida. A entidade validadora é determinada pela política que rege a ICP. Após a validação da requisição, a Autoridade Certificadora emite, com base nesta, o certificado digital e posteriormente o disponibiliza ao requerente para que este possa avaliá-lo. Caso o requerente aprove o certificado, inicia-se a fase de uso deste. A suspensão de um certificado é uma acção preventiva que visa impedir o uso do certificado durante um determinado período de tempo, ou até que uma determinada situação seja resolvida, como por exemplo durante a tramitação de um processo administrativo em que o funcionário deve ficar impedido de executar acções utilizando o certificado emitido pela empresa. A revogação de um certificado pode ser motivada por um situação específica, por exemplo, por uma solicitação do proprietário do certificado sob a alegação de que sua chave privada foi comprometida. (Ardigo, 2004)

Figura 8: Ciclo de vida um certificado digital

Fonte: Ardigo (2004)

2.2.6. Infra-estruturas de Chaves Públicas

Segundo Bhattarai (2020), PKI (*Public Key Infrastructure*) ou ICP é uma *framework* de pessoas, processos, políticas, protocolos, *hardware*, *software*, entre outros usada para gerar, gerir, armazenar, implantar e revogar os certificados de chave pública.

Sendo que vários processos podem ser realizados através da utilização de certificados digitais associados a chaves que identificam diferentes entidades, uma ICP surge com a intenção de gerir as chaves de forma segura.

Segundo Whitman & Mattord (2012, p. 375), uma solução PKI típica protege a transmissão e recepção de informações seguras integrando os seguintes componentes:

- **Autoridade de Certificadora (AC):** emite, gerencia, autentica, assina e revoga os certificados digitais dos utilizadores, que normalmente contêm o nome do utilizador, a chave pública e outras informações de identificação.

- **Autoridade de Registro (AR):** opera sob a colaboração confiável da autoridade de certificação e pode lidar com funções de certificação diárias, como verificar informações de registro, gerar chaves de utilizadores finais, revogar certificados e validar certificados de usuário.
- **Directórios públicos:** são locais centrais para armazenamento de certificados que fornecem um único ponto de acesso para administração e distribuição.
- **Protocolos de gestão:** organizam e gerenciam as comunicações entre ACs, ARs e usuários finais. Isso inclui as funções e procedimentos para configurar novos usuários, emitir chaves, recuperar chaves, actualizar chaves, revogar chaves e permitir a transferência de certificados e informações de status entre as partes envolvidas na área de autoridade da PKI.
- **Políticas e procedimentos:** auxiliam uma organização na aplicação e gestão de certificados, na formalização de responsabilidades e limitações legais e no uso comercial real.

2.2.6.1. Modelos de Confiança

Para (HOUSLEY; POLK, 2001; LLOYD et al., 2001) citados por Ardigo (2004, p. 64), a constituição de uma ICP pode conter várias ACs, e estas necessitam estabelecer relações de confiança entre si. Esta necessidade também existe no relacionamento entre ACs de ICPs distintas.

Segundo Ardigo (2004), os modelos de confiança podem ser classificados e descritos da seguinte forma:

a) Modelo Hierárquico

Este modelo apresenta a organização das ACs relacionadas entre si de forma hierárquica. A relação de confiança entre as ACs é estabelecida automaticamente na emissão dos seus certificados. ACs superiores emitem os certificados para as ACs inferiores, que, por sua vez, os utilizam para assinar os certificados que emitem. Este facto, implica directamente na confiança da AC inferior na AC superior.

Ainda segundo Hunt (2001) citado por Ardigo (2004, p. 65), uma AC superior, localizada no topo da hierarquia, possui seu certificado auto-assinado, ou seja, na geração do seu certificado, a própria AC realiza a assinatura. Estas ACs são denominadas AC raiz.

A AC Raiz quando credencia entidades privadas ou públicas e tem o certificado auto-assinado que torna as outras entidades confiáveis, neste caso o certificado raiz é ancora de confiança.

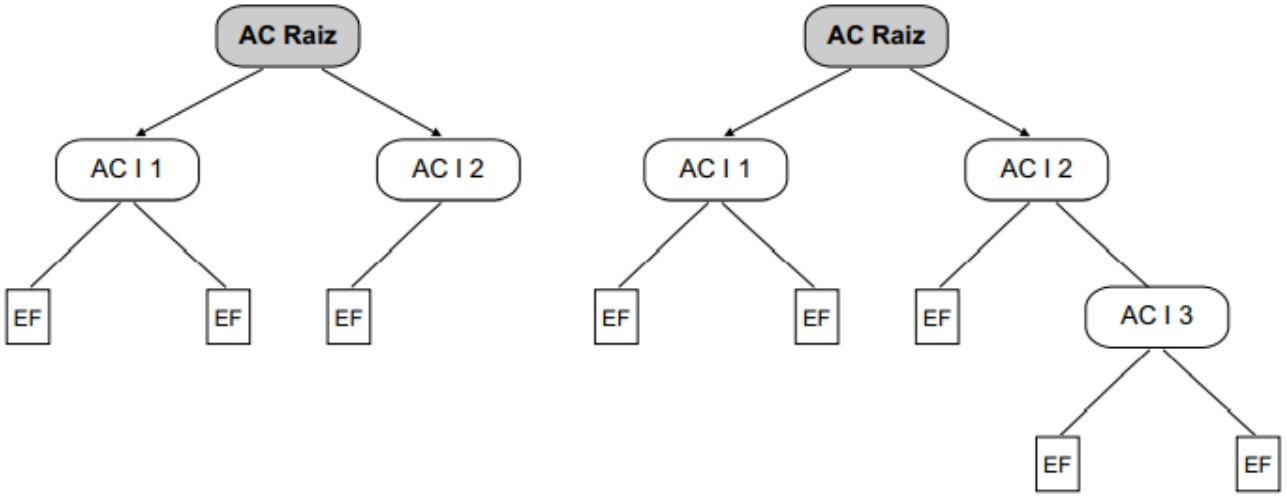

Figura 9: Modelo confiança hierárquico

Fonte: Ardigo (2004)

Segundo Moses (2002) citado por Ardigo (2004), uma ICP pode ser constituída por várias ACs raiz, sendo que estas podem emitir certificados para entidades ou utilizadores finais, ou para outras ACs, isto depende da política adoptada. Normalmente as ACs raiz emitem certificados apenas para ACs inferiores, as chamadas ACs intermediárias (ACI) ou finais. As intermediárias são as que possuem ACs subordinadas a ela, enquanto as finais emitem certificados apenas para usuários.

Vantagens

Segundo Polk & Hastings (2000) citado por Ardigo (2004), o modelo hierárquico possui algumas vantagens que são listadas abaixo:

- A primeira se refere a escalabilidade, pois é fácil a inserção de uma nova AC dentro da hierarquia;

- Facilidade de construção do caminho de certificação, pois a confiança é unidirecional;
- Possui caminhos de certificação relativamente curtos, uma vez, que o maior caminho é igual a profundidade da árvore mais um;
- Facilidade do utilizador conhecer qual aplicação dos certificados emitidos por uma AC, dado sua localização hierarquia.

Desvantagens

Ainda segundo Polk & Hastings (2000) citado por Ardigo (2004, p. 65), a desvantagem deste modelo, é que o comprometimento da AC raiz, implica no com prometimento da hierarquia inteira, pois a característica deste modelo está na concentração da confiança nas ACs raiz.

b) Modelo em Malha

Segundo Lloyd et al. (2001) citado por (Ardigo, 2004), o modelo de confiança em malha, conecta as ACs através de relacionamentos ponto-a-ponto. Estes relacionamentos são criados através da emissão mútua de certificados, onde cada AC emite o certificado para outra, estabelecendo um relacionamento bidirecional, também chamada de certificação cruzada.

Porém, a forma do estabelecimento destes relacionamentos não permitem que ACs imponham condições para gerenciar os tipos de certificados que outra AC pode emitir. Entretanto, a relação de confiança pode ser condicionada através da sua especificação nas extensões do certificado emitido.

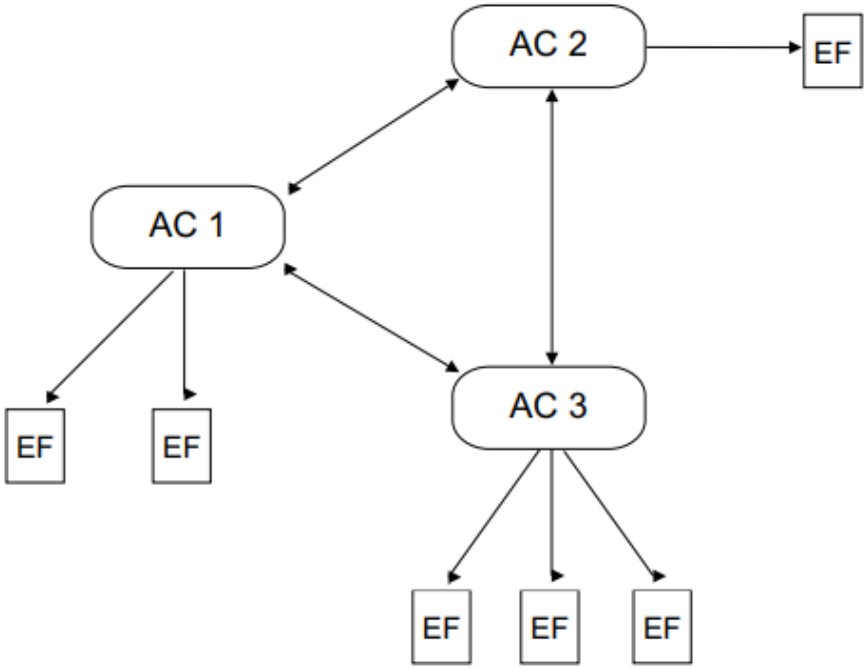

Figura 10: Modelo de confiança em malha

Fonte: (Ardigo, 2004)

Vantagens

- Facilidade de incorporar uma AC de outra ICP, bastando estabelecer um relacionamento ponto-a-ponto entre ACs de ambas ICP;
- O comprometimento de qualquer AC não se propaga para a cadeia inteira, como ocorre na hierárquica;

Desvantagens

- O caminho de certificação é não determinístico, e assim, mais complexo que o hierárquico;
- O número máximo de um caminho de certificação é igual ao número de ACs pertencentes a cadeia de confiança.

c) Modelo em Ponte

Para Alterman (2001) citado por Ardigo (2004, p. 67), o modelo em ponte permite ligar ICPs que implementam diferentes modelos de confiança através de uma entidade denominada ponte.

A ponte é utilizada como um ponto central de confiança, o qual as ACs estabelecem confiança através da certificação cruzada. Este modelo reduz a quantidade de relacionamentos de confiança entre ACs, pois a confiança em uma ponte resulta na confiança em todas as entidades que estabeleceram relacionamento com a ponte, não necessitando constituir confiança com cada AC individualmente.

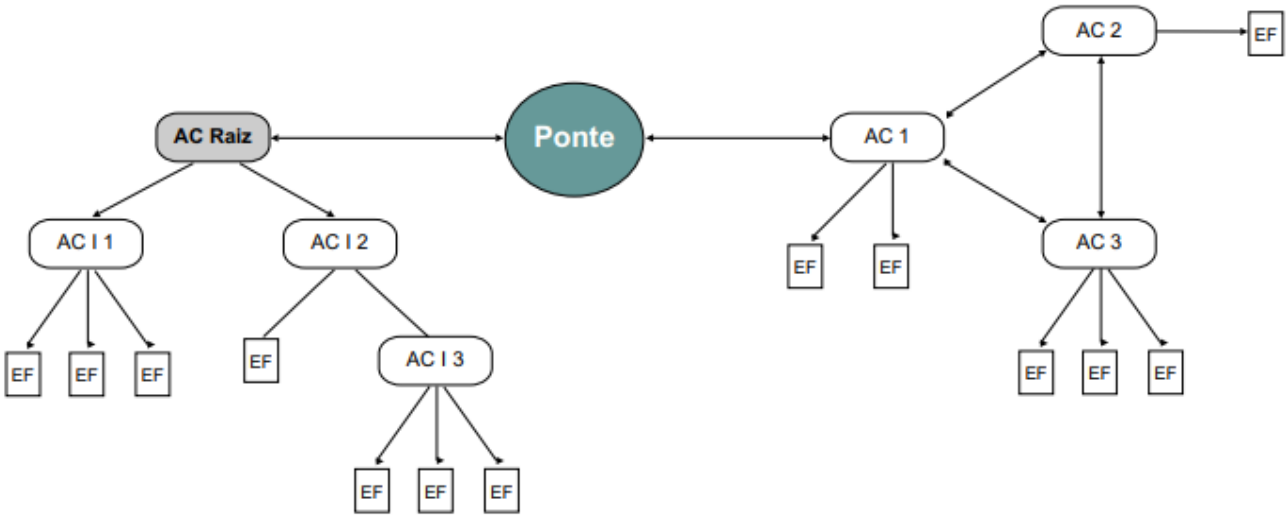

Figura 11: Modelo de confiança em ponte

Fonte: Ardigo (2004)

De acordo com Polk & Hastings (2000) citado por Ardigo (2004, p. 67), a ponte é um ponto de confiança apenas para ACs, pois esta não emite certificados directamente a usuários.

Vantagem

Nos estudos feitos por Alterman (2001) citado por Ardigo (2004), a ponte permite que instituições com infra-estruturas de chave pública próprias interoperem através de uma arquitetura simplificada, que minimiza o gerenciamento da certificação cruzada e melhora a interoperabilidade técnica.

Desvantagem

De acordo com o mesmo autor, utilizadores de uma determinada AC tem a necessidade de confiar em uma determinada que ponte que mantém relacionamento com a AC desejada.

2.2.7. Assinatura Digital

De acordo com SABOONCHI (2014, p. 15), uma assinatura digital é um esquema matemático usado para fornecer uma série de garantias, como privacidade de uma conversa, integridade de dados, autenticidade de uma mensagem ou remetente digital e não repúdio do remetente. Nos casos em que se possa estar preocupado com a segurança de documentos sensíveis como recibos, contratos, acordos ou outros documentos semelhantes em que os utilizadores estejam preocupados com o acesso não autorizado ou roubo de dados, a melhor solução é a aplicação de uma assinatura digital.

a) Princípio de funcionamento

Segundo Whitman & Mattord (2012), processos de criptografia assimétrica são usados para criar assinaturas digitais. Quando um processo criptográfico assimétrico usa a chave privada do emissor para cifrar uma mensagem, a chave pública do emissor deve ser usada para decifrar a mensagem. Quando a decriptação é bem sucedida, o processo verifica se a mensagem foi enviada pelo emissor e, portanto, não pode ser refutada. Esse processo é conhecido como **não repúdio**.

De acordo com o explicado acima é possível perceber que a assinatura digital não garante a confidencialidade nas mensagens pois com a utilização da chave pública do emissor é possível ter acesso ao conteúdo da mensagem. Além do não repúdio, um dos princípios fundamentais para a assinatura digital é a autenticidade.

Autenticidade: A propriedade de ser genuíno e poder ser verificado e confiável. Isso significa verificar se os utilizadores são quem dizem ser e se cada entrada que chega ao sistema veio de uma fonte confiável (Stallings, 2017, p. 23).

No entanto a dúvida que surge é, de que forma pode-se garantir a integridade dos documentos assinados digitalmente? Para responder a essa questão é necessário abordar conceitos que envolvem algoritmos e funções de *Hash* como referido no alínea c).

b) Principais Algoritmos da Assinatura Digital

Segundo Oliveira (2012), os principais algoritmos da assinatura digital são: RSA, *ElGamal* e DAS. Os algoritmos são caracterizados no ponto referente a criptografia assimétrica.

c) Função *Hashing*

Segundo o estudo realizado por Oliveira (2012, p. 7)

> Na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente cifradas com a chave privada de alguém, ao invés disso, é empregada uma função *hashing*, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho, para oferecer agilidade nas assinaturas digitais, além de integridade confiável. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa, por isto, após o valor *hash* de uma mensagem ter sido calculado através do emprego de uma função *hashing*, qualquer modificação em seu conteúdo - mesmo em apenas um *bit* da mensagem - será detectada, pois um novo cálculo do valor *hash* sobre o conteúdo modificado resultará em um valor *hash* bastante distinto.

Entretanto existem alguns algoritmos de *hashing* cujo o mesmo autor descreve da seguinte forma:

Tabela 5: Algoritmos de *hashing*

Algoritmo	Explicação
SHA2	*Secure Hash Algorithm* (SHA-2) é uma família de duas funções *hash* similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512. Eles diferem no tamanho, o SHA-256 utiliza 256 bits e o SHA-512 utiliza 512 bits. Há também versões truncadas de cada padrão, conhecidos como SHA-224 e SHA-384.
SHA1	O *Secure Hash Algorithm* (SHA-1), gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem.
MD5	*Message Digest* (MD), produz um valor *hash* de 128 bits, para uma mensagem de entrada de tamanho arbitrário. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Entretanto, o facto de produzir uma valor *hash* de somente 128 bits é o que causa maior preocupação, é preferível uma função *hashing* que produza um valor maior.

Fonte: Adaptado de Oliveira (2012)

2.2.8. Sistemas híbridos

Para Oliveira (2012), os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o encriptação, a assinatura e o *hashing*. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio electrónico.

Com a combinação dos três mecanismos básicos da criptografia surge uma variedade de aplicações feitas baseando-se em diferentes protocolos baseados na criptografia.

Segundo o mesmo autor Oliveira (2012), alguns desses protocolos podem ser descritos da seguinte forma:

- **IPSec:** Padrão de protocolos criptográficos desenvolvidos para o IPv6[6]. Realiza também o tunelamento[7] de IPs. É composto de três mecanismos criptográficos: *Authentication Header* (define a função *hashing* para assinatura digital), *Encapsulation Security Payload* (define o algoritmo simétrico para encriptação) e ISAKMP (define o algoritmo assimétrico para gestão e troca de chaves de criptografia).
- **SSL e TLS:** Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, *message digest* (*hashing*) e métodos de autenticação e gerência de chaves (assimétricos).

2.3. Provedores de Identidade Electrónica

Como uma identidade física, uma identidade electrónica geralmente é definida como um conjunto de atributos que ajudam a descrever ou qualificar uma entidade em contextos específicos (Schardong et al., 2021).

Conforme a empresa de Segurança de TI Entrust dos Estados Unidos da América, um Provedor de Identidade Electrónica (PIE) é um sistema que cria, armazena e gerencia identidades digitais. O PIE pode oferecer serviços de autenticação a outros provedores de serviços (aplicativos, sites ou outros serviços digitais).

[6] https://pt.wikipedia.org/wiki/IPv6
[7] https://pt.wikipedia.org/wiki/T%C3%BAnel_IP

Basicamente são sistemas para autenticação de utilizadores que possuem requisitos prontos e disponíveis para a utilização directa por parte de desenvolvedores sem a necessidade de desenvolver do zero. A tabela abaixo ilustra alguns provedores de forma comparativa, onde na extremidade esquerda são indicados os critérios e na extremidade superior os PIE.

2.3.1. Comparação de PIE

Tabela 6: Comparação de alguns Provedores de Identidade Electrónica

	Okta	***ForgeRock***	***Keycloak***	***Gluu***
Monitoramento das actividades dos usuários na organização	Sim	Não	Sim	Sim
Suporte para uso em grandes empresas	Sim	Sim	Não	Sim
Open-source	Não	Não	Sim	Não
Integração	*Slack* *Salesforce*	Não disponível	Não disponível	Não disponível
Gestão de APIs[8]	Sim	Não	Sim	Sim
Autenticação multi-factor	Sim	Sim	Sim	Sim

Fonte: *SaaS Worthy* (2022)

2.4. Dispositivos de armazenamento de chaves criptográficas

2.4.1. *Hardware Security Modules*

De acordo com SABOONCHI (2014, p. 17), um HSM é um processador criptográfico projectado especificamente para ser usado para a protecção de uma chave criptográfica ao

[8] https://pt.wikipedia.org/wiki/Interface_de_programa%C3%A7%C3%A3o_de_aplica%C3%A7%C3%B5es

longo de seu ciclo de vida. Os HSMs actuam como âncoras confiáveis para proteger uma PKI. Essa protecção é alcançada gerindo, processando e armazenando chaves criptográficas com segurança dentro de um dispositivo reforçado e resistente a adulterações. Um HSM é capaz de executar várias funções importantes relacionadas à segurança, incluindo:

- Operações criptográficas, como criptografia, assinaturas digitais, *hashing* e computação de *Message Authentication Codes*[9] (MACs);
- Funções de gerenciamento de chaves, como geração de chaves e armazenamento seguro de chaves;
- Autenticação verificando assinaturas digitais.

O mesmo autor SABOONCHI (2014), especifica as vantagens e desvantagens da utilização de HSMs como especificado abaixo:

a) Vantagens

Um HSM possui uma área física protegida por sensores, área chamada de perímetro criptográfico. Um HSM possui sensores capazes de detectar tentativas de intrusão e acesso ao perímetro criptográfico, ou variações atípicas de temperatura e tensão. Se os sensores do HSM detectarem a tentativa de intrusão no perímetro criptográfico, todo o conteúdo do HSM é destruído, para evitar o comprometimento das chaves criptográficas contidas no dispositivo.

b) Desvantagens

A maior desvantagem da utilização destes dispositivos está no preço. O seu preço depende do nível das funcionalidades e os requisitos de segurança requeridos pelo utilizador. Os HSM também requerem manutenção o que influencia directamente no seu custo.

2.4.2. *Smartcard*

De acordo com Bereza (2013, p. 17), s*martcards* ou cartões inteligentes, tem como uma das formas de utilização a autenticação onde é necessária a posse de algo. Os cartões de banco

[9] https://pt.wikipedia.org/wiki/Autenticador_de_mensagem

são um exemplo dessa forma de autenticação. A utilização de um *smartcard* está condicionada à utilização de um leitor de *smartcards*, que é responsável por enviar e receber dados do cartão. Outra função do leitor é a alimentação elétrica do *smartcard*, pois esta é a única interface existente para alimentação do cartão. O mesmo autor Bereza (2013), especifica as vantagens e desvantagens conforme explicado abaixo:

a) Desvantagens

As proteções físicas de um *smartcard* são bastante limitadas quando comparadas com as protecções de outros dispositivos criptográficos.

- *Smartcards* não possuem sensores de acesso físico, variações de temperatura, tensão, entre outros tipos de ataques.
- A performance de um *smartcard* também é prejudicada pelo seu tamanho, pois o processador tem um *clock*[10] limitado e realiza um número baixo de operações por segundo.

Além dessas desvantagens, *smartcards* são desvantajosos pelo factor custo de aquisição e manutenção do mesmos e pelo facto de requerem um leitor de *smartcards* para a sua utilização.

b) Vantagens

A vantagem deste dispositivo é a sua portabilidade, pois ele é pequeno o suficiente para ser carregado para qualquer lugar. Alguns exemplos de sectores onde é comum a utilização de *smartcards* é no controle de acesso de funcionários, no transporte público e no sector bancário (cartões de crédito).

[10] É a frequência com que um processador é capaz de executar as tarefas que o são direccionadas.

3. Capítulo III – Caso de Estudo

3.1. Apresentação do INTIC

Conforme o decreto n.º 9/2011 criou-se o Instituto Nacional de Tecnologias de Informação e Comunicação, abreviadamente designado por INTIC, e extingue a Unidade Técnica de Implementação da Política de Informática UTICT, criada pelo Decreto n.º 50/2002, de 26 de Dezembro.

O Decreto n° 60/2017 de 6 de Novembro, redefine as atribuições do INTIC para regular, supervisionar e fiscalizar o sector de TICs. Por sua vez, o Decreto n° 90/2020 de 9 de Outubro revoga o Decreto n° 60/2017 e estabelece o INTIC como um Instituto Público regulador de TIC e coordena a governação digital e da Internet.

De acordo com Chilundo (2018), no âmbito Decreto n° 60/2017, compete ao INTIC garantir a proteção e segurança:

- ✓ Nas transacções electrónicas;
- ✓ No comercio electrónico; e
- ✓ No governo electrónico.

3.1.1. Áreas Operacionais

Como apresentado no *website* oficial do INTIC a estrutura operativa compreende as seguintes áreas:

- Divisão de Regulação e Fiscalização;
- Divisão de Licenciamento e Certificação;
- Divisão de Segurança Cibernética e Protecção de Dados; e
- Divisão de Governação Digital.

De acordo com as informações do *website*, a Divisão de Licenciamento e Certificação é a área responsável por processos de licenciamento, registo, certificação e fiscalização de operadores do sector de TIC, que abrange provedores intermediários de serviços de Internet, Agentes de Registo de nomes sob o domínio “-mz”, entidades certificadoras no âmbito do Sistema Certificação Digital de Moçambique (SCDM).

3.1.2. Organograma

Um organograma é uma representação gráfica da estrutura organizacional de uma organização. Conforme apresentado no *website* oficial do INTIC, o organograma da instituição é apresentado na figura abaixo.

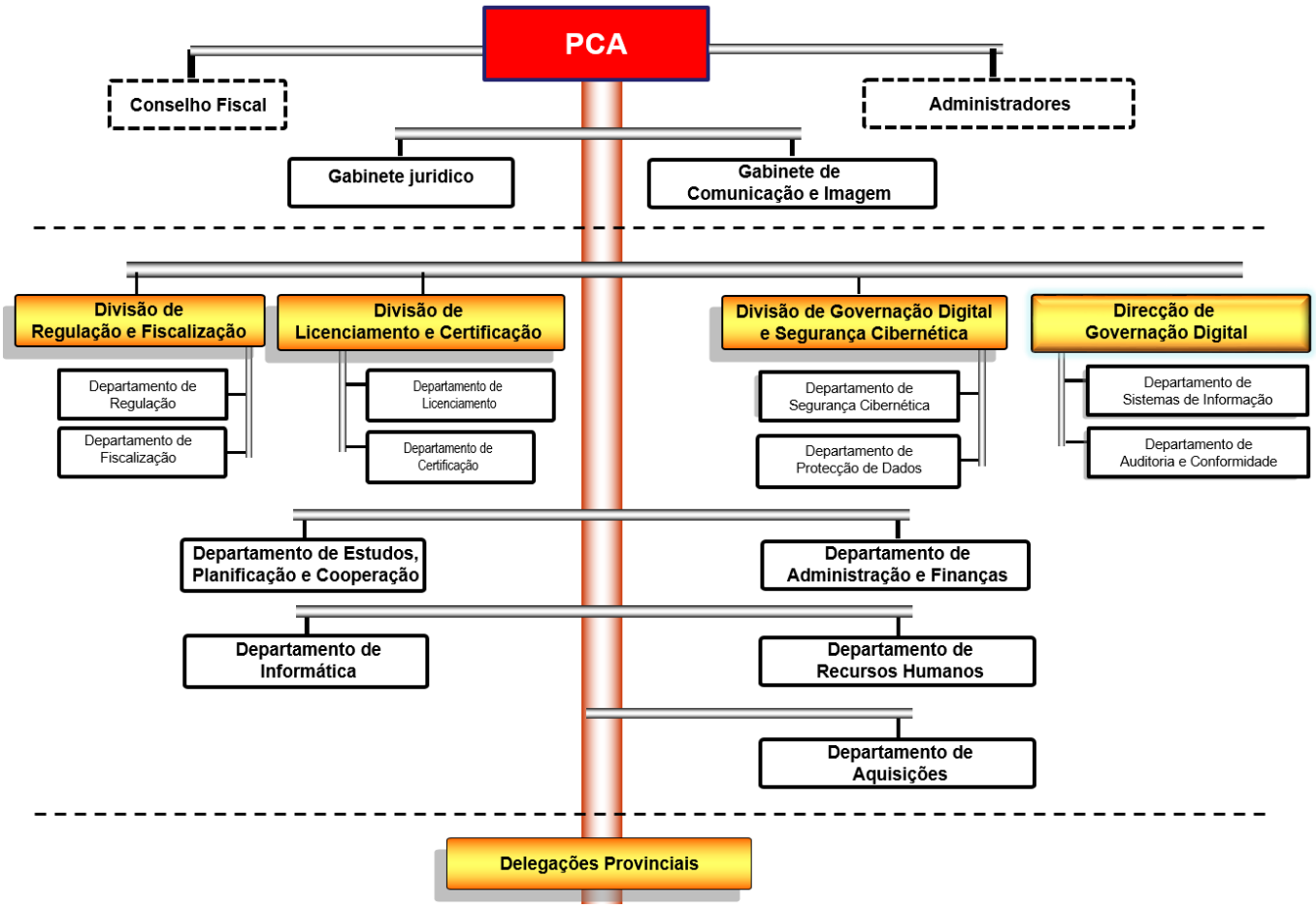

Figura 12: Organograma do INTIC

Fonte: INTIC (2022)

A solução proposta pelo autor actua na departamento da Divisão de Governação Digital e Segurança Cibernética pois estão directamente relacionados na implementação do SCDM.

3.2. Analise da Situação Actual

Nesse ponto é apresentado o cenário actual do INTIC no que concerne aos procedimentos de segurança cibernética utilizados na instituição e na implementação do SCDM. Na busca

de informação foram entrevistados funcionários da área de TI do INTIC no sentido de poder saber qual é o estado actual do INTIC em termos de segurança cibernética.

Como forma de garantir a segurança na instituição a instituição contém os mecanismos listados abaixo:

- **Agentes de Segurança:** Pessoas que fazem a gestão da segurança física do INTIC, controlando o acesso dos trabalhadores a instituição e registando os dispositivos electrónicos que estes trazem na instituição.
- **Câmeras CCTV:** São câmeras de segurança que fazem a monitoria dos movimentos realizados em certas partes da instituição.
- **IDS:** Detecção de Intrusão é o processo de monitorar os eventos que ocorrem em um sistema de computador ou rede e analisá-los em busca de sinais de possíveis incidentes, que são violações ou ameaças iminentes de violação de políticas de segurança de computadores, políticas de uso aceitável ou práticas de segurança padrão (Mahendiran & Appusamy 2015). Dessa forma é possível constatar que um *software* IDS é um mecanismo informatizado de detecção de intrusão.
- ***Firewall*:** O firewall actua como um filtro de pacotes. Ele inspeciona todo e qualquer pacote que entra e que sai. Os pacotes que atenderem a algum critério descrito nas regras formuladas pelo administrador da rede serão remetidos normalmente, mas os que falharem no teste serão descartados sem cerimônia (Tanenbaum & Wetherall, 2011). As regras de controlo de acessos são geralmente listas em tabelas contendo informações necessárias sobre as redes ou usuários na rede e que são bloqueados a outras ou são aceitados por outras redes.
- **DPC:** Segundo INTIC (2022), o DPC pretende apresentar procedimentos e práticas utilizadas pela Autoridade Certificadora Raiz do Estado de Moçambique, no suporte à sua actividade de certificação digital. No entanto este documento descreve duma forma geral as práticas que devem ser seguidas na gestão de SCD.
- **Decreto do SCDM:** O Decreto n.º 59/2019 especifica a legislação do SCDM e as normas que devem ser seguidas no âmbito da sua gestão.

3.2.1. Sistema de Certificação Digital de Moçambique

Conforme o Decreto n.º 59/2019 foi criada a legislação para o Sistema de Certificação Digital de Moçambique e aprova o Regulamento do Sistema de Certificação Digital de Moçambique. Conforme o artigo 2 do mesmo decreto, o SCDM visa garantir um ambiente electrónico seguro de transacções electrónicas no País. O SCDM é de âmbito nacional e aplica-se as pessoas singulares, colectivas públicas ou privadas.

O SCDM é constituído por um PIE e uma ICP. O INTIC é a AC Raiz do Estado possuindo um certificado auto-assinado, ou seja, o primeiro na hierarquia de certificados.

Um certificado é Raiz se é de confiança, não importando se é ou não auto-assinado.

Segundo a DPC (2020) do INTIC, os titulares de certificados podem ser: pessoa singular, pessoa colectiva e sistema ou equipamento tecnológico.

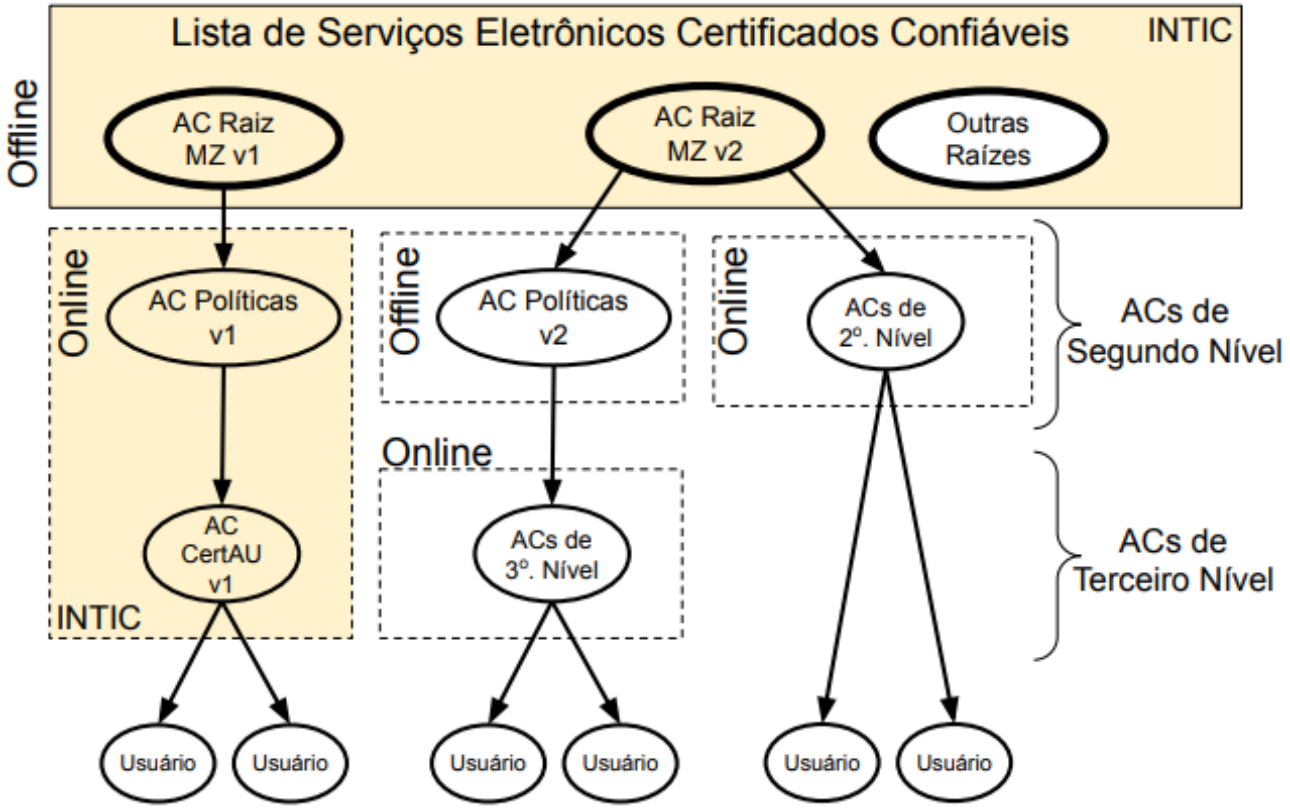

Figura 13: Arquitectura da ICP do SCDM

Fonte: INTIC (2022)

Como pode-se verificar na figura o modelo de confiança adoptado é hierárquico pois ACs presentes no nível superior emitem certificados para as ACs em níveis inferiores, que, por sua vez, os utilizam para assinar os certificados que emitem. Este facto, implica directamente na confiança da AC inferior na AC superior. Conforme a DPC (2022) do SCDM do INTIC, a ICP do Estado de Moçambique está estruturada em 2 e 3 níveis de Autoridades Certificadoras, sendo elas hierarquicamente dependentes.

- **Autoridade Certificadora de Assinatura Única**: a AC emissora de certificados de assinatura única (AC CertAU) é um serviço online de emissão de certificados de assinaturas de documentos electrónicos. Sempre que um usuário final necessitar assinar um documento, um certificado é gerado e utilizado para assinar o referido documento. Assim que o documento for assinado, a chave privada associada ao certificado é destruída.
- **Autoridade Certificadora de Segundo Nível**: a autoridade certificadora de segundo nível (AC de Segundo Nível) é criada pela AC Raiz MZ para a emissão de certificados para os utilizadores finais.
- **Autoridade Certificadora de Terceiro Nível**: a autoridade certificadora de Terceiro Nível (AC de Terceiro Nível) é criada por ACs de Políticas. Esta AC emite certificados para os utilizadores finais.
- **Outras Autoridades Certificadoras**: O SCDM pode integrar, após avaliação e acreditação pela Autoridade Supervisora e Acreditação, de outras ACs que não fazem parte, directamente, da cadeia de certificados da AC Raiz MZ. Diferentemente das entidades acima listada, os titulares de certificados digitais podem ser pessoa singular, pessoa colectiva.

3.2.2. Constrangimentos enfrentados

Os constrangimentos da situação actual do INTIC referente ao SCDM são:

- O DPC especifica os procedimentos a serem seguidos pelos usuários do SCDM mas não especifica as principais ameaças e vulnerabilidades que os SCD tradicionais estão sujeitos o que causa a falta de conscientização sobre as ameaças e vulnerabilidades destes sistemas na equipa técnica de gestão de SCD.

- O decreto do SCDM especifica regras burocráticas sobre a gestão deste sistema e os aspectos legais da sua existência em Moçambique, de forma geral indica como o SCDM irá funcionar para o público mas não aprofunda aspectos relacionados com a segurança desses sistemas.
- No âmbito da implementação do primeiro SCD em Moçambique desde 2018, não existia a capacidade de recursos humanos, dificuldade na retenção de quadros e o sistema não possuía muitas formas de utilização, sendo que este baseava-se no uso de *Tokens* (Sistemas tradicionais) em que devia-se instalar um *software* no computador para a utilização dos serviços do SCDM, enquanto que novo sistema existe a possibilidade do uso de *Tokens*, *SmartCards* e telemóveis o que torna o sistema mais acessível aos utilizadores pois os outros meios adoptados são mais intuitivos quanto sua a usabilidade porém é mais susceptível a exploração.
- A falta de um programa de avaliação do nível de conscientização sobre segurança cibernética contendo as fases de educação, treinamento e conscientização sobre segurança cibernética nos diferentes serviços fornecidos pela instituição. Segundo Whitman & Mattord (2012), os programas referidos anteriormente são uma medida de controle projetada para reduzir a incidência de violações acidentais de segurança por parte dos funcionários.
- Um dos desafios na implementação do SCDM é a inclusão da maioria da população moçambicana para utilização do sistema. A identidade do utilizador seria uma relação de unicidade entre uma ou mais entidades em um contexto especifico. A razão do contexto é devido a existência de várias identidades electrónicas dum único usuário em diferentes sistemas. No contexto do SCDM existe uma relação de unicidade entre o PIE do SCDM e cada um dos seus utilizadores. O problema é que deve existir um mecanismo que garanta que cada utilizador possua apenas uma identidade electrónica com o SCDM. Em sistemas digitais com utilizadores que possuem meios de identificação digital mais sofisticados como por exemplo e-mail garantir a unicidade de utilizadores é uma tarefa relativamente fácil, mas no caso da existência de uma população no universo de utilizadores que não faz a utilização destes meios sofisticados, garantir a unicidade dos utilizadores no sistema torna-se um desafio.

4. Capítulo IV – Proposta de Solução

Como solução para os problemas identificados no capitulo I propõe-se a elaboração de um plano de gestão de riscos.

4.1. Descrição do Plano de Gestão de Riscos

Conforme o padrão ISO 31000 citado pela Associação Brasileira de Normas Técnicas – ABNT (2009), um plano de gestão de riscos é um esquema dentro da estrutura da gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerir riscos.

A gestão de riscos é o processo de identificar riscos, representados por vulnerabilidades, aos activos e infra-estrutura de informações de uma organização e tomar medidas para reduzir esse risco a um nível aceitável (Whitman & Mattord, 2012, p. 119). Segundo os mesmos autores Whitman & Mattord (2012), o processo de gestão de riscos compreende três fases que são Identificação dos Riscos, Avaliação de Riscos e Controle de Risco. A figura abaixo ilustra os componentes de um plano de gestão de riscos de forma genérica.

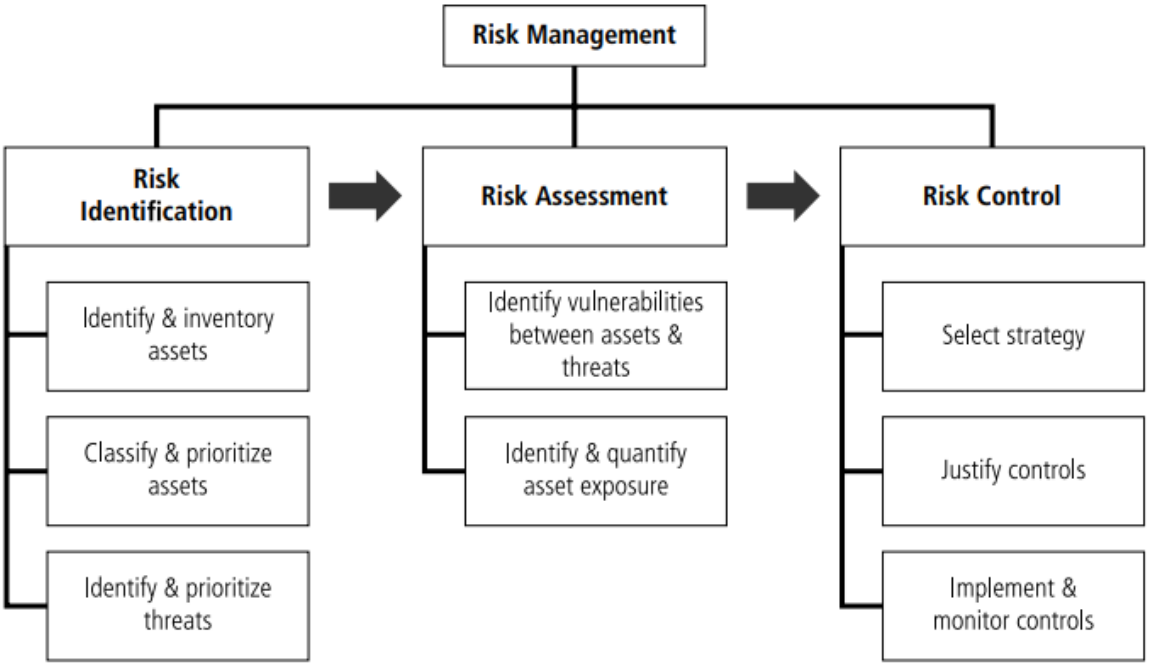

Figura 14: Diagrama de elaboração dum Plano de Gestão de Riscos

Fonte: Whitman & Mattord (2012)

4.1.1. Identificação dos Riscos

Segundo Whitman & Mattord (2012), uma estratégia de gestão de risco exige que os profissionais de segurança da informação conheçam os activos de informação de sua organização, ou seja, identifique-os, classifique-os e priorize-os. Uma vez identificados os ativos organizacionais, um processo de avaliação de ameaças identifica e quantifica os riscos enfrentados por cada activo.

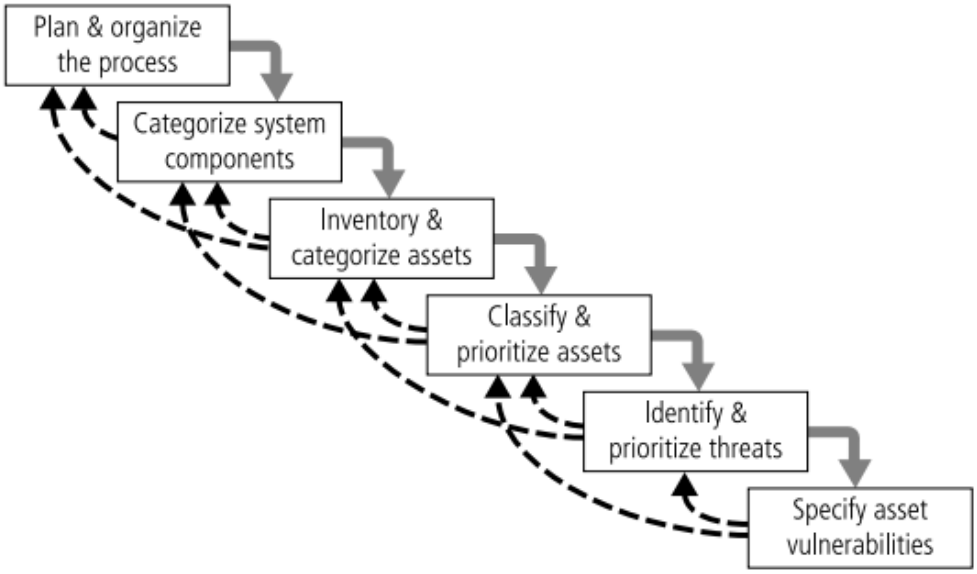

Figura 15: Passos para identificação de riscos

Fonte: Whitman & Mattord (2012)

Utilizando técnicas como entrevistas, questionários, análise do cenário, cursos fornecidos pelo INTIC, a identificação de riscos iniciou pela organização dos tipos de riscos que pretendeu analisar, os componentes do SCDM, os principais activos de informação, as ameaças até e por fim as vulnerabilidades que os SCD centralizados estão sujeitos na sua implementação e operacionalização.

4.1.2. Avaliação de Riscos

De acordo com Whitman & Mattord (2012), após identificar-se os activos de informação da organização e as ameaças e vulnerabilidades, avalia-se o risco de cada uma das vulnerabilidades. Esse processo é chamado de avaliação de risco. A avaliação de risco atribui uma classificação ou pontuação de risco a cada activo de informação. Embora esse

número não signifique nada em termos absolutos, é útil para aferir o risco relativo de cada activo de informação vulnerável e facilita o desenvolvimento de classificações comparativas posteriormente no processo de controle de risco. Ainda de acordo com o mesmo autor, a **probabilidade** refere-se ao estado que uma vulnerabilidade específica seja objecto de um ataque bem-sucedido. Na avaliação de risco, atribui-se um valor numérico à probabilidade. Por sua vez, o **impacto** refere às consequências do risco caso este ocorra, ou seja, a descrição do prejuízo da ocorrência do risco.

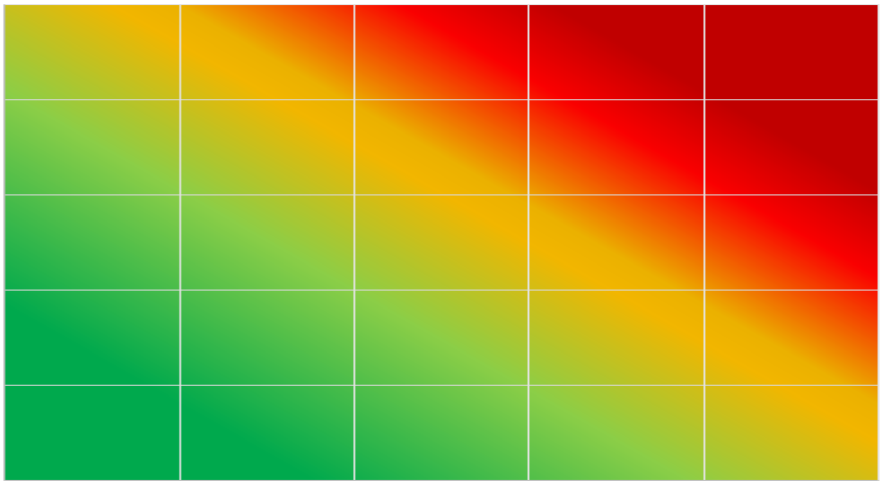

Figura 16: Matriz da probabilidade e impacto de riscos

Fonte: SRAT (2017)

O funcionamento da matriz de probabilidade e impacto do risco pode ser compreendido da seguinte forma: (1) a probabilidade e o impacto do risco aumentam da esquerda para direita e de baixo para cima e (2) as cores indicam a criticidade do risco de forma visual.

Limites de Risco – para o Departamento NTRSA (*National Treasure Republic of South Africa*), limite de risco é um parâmetro quantificado dentro do qual o risco pode ser assumido ou gerido. O nome Limite de Risco é para a tolerância ao risco e capacidade de suporte ao risco. No anexo 4 foi calculado o limite de risco.

Risco Residual – ocorre quando mesmo as vulnerabilidades tendo sido controladas o máximo possível, muitas vezes ainda há algum risco que não foi completamente removido, deslocado ou planejado (Whitman & Mattord, 2012, p. 164).

Risco inerente – o nível de risco que reside em um evento ou processo antes da administração tomar uma acção de mitigação (IMA, 2007). Pode-se perceber que, este risco é o nível de risco em existente antes de serem tomadas medidas de mitigação.

As tabelas abaixo descrevem de forma qualitativa e quantitativa a variação da probabilidade e do impacto dos riscos.

Tabela 7: Probabilidade de ocorrência de riscos

PROBABILIDADE				
Pontuação	**Descrição**	**Probabilidade**	**Diretriz**	**Prazo**
1	Muito improvável	Irrealista	<10%	5+ anos
2	Improvável	Duvidosa	10-30%	2-3 anos
3	Moderadamente provável	Razoável	30-60%	Uma vez por ano ou uma vez por mês
4	Provável	Alto	60-90%	Uma vez por semana
5	Muito provável	Esperada	>90%	Diariamente

Fonte: SART (2017)

Tabela 8: Impacto de ocorrência de riscos

Impacto			
Pontuação	**Descrição**	**Impacto nos activos**	**Impacto no programa**
1	Insignificante	Perda ou dano mínimo	Sem atrasos
2	Menor	Alguma perda ou dano	Alguns atrasos
3	Moderada	Perda ou dano	Alguns atrasos e interrupções
4	Forte	Grande destruição	Interrupção grave
5	Crítica	Destruição completa	Perda ou encerramento

Fonte: SRAT (2017)

4.1.3. Controle de Riscos

Conforme *Project Management Institute* (2013), controlar riscos é o processo de acompanhar os riscos identificados, garantir que os planos de resposta aos riscos sejam implementados, avaliar a eficácia das respostas aos riscos, monitorar os riscos residuais e

identificar novos riscos. Existem quatro estratégias de controlar os riscos como o detalhado abaixo:

- **Evitar:** essa estratégia tenta eliminar uma ameaça, se possível. Uma abordagem possível é adoptar uma estratégia alternativa de uma das seguintes maneiras: 1) reduzir o escopo ou alterar os objetivos do projeto, 2) permitir que o cronograma avance, 3) adoptar uma abordagem técnica comprovada em vez de uma mais inovadora, arriscada ou 4) usar um componente substituto que não tem o mesmo risco.
- **Transferir:** enviar ou alocar um risco para outra parte. Transferir um risco não elimina o risco, meramente dá a outra pessoa a responsabilidade de gerir esse risco.
- **Mitigar:** acções tomadas para reduzir a probabilidade ou o impacto de um risco. As abordagens preventivas anteriores são geralmente mais produtivas do que reparar o dano depois que ele ocorre.
- **Aceitar:** a aceitação passiva é não agir e lidar com os problemas (ou oportunidades) se e quando eles ocorrerem.

4.2. Elaboração do Plano de Gestão de Riscos

Aplicando todos os conceitos abordados no plano gestão de riscos SRAT v1.0.0 elaborou-se através da análise das vulnerabilidades em SCD centralizados e das técnicas utilizadas na redução e mitigação de riscos de segurança cibernética no Anexo 1 do mesmo trabalho o plano de gestão de riscos, este foi subdivido em duas tabelas para que fosse possível anexar no trabalho. Contudo, para uma melhor compreensão das vulnerabilidades de Sistemas de Certificação Digital não é suficiente identifica-las, é necessário a percepção de como os diferentes tipos de ataques ocorrem em SCD, de forma superficial o autor explicou o princípio de funcionamento de alguns ataques pois a explicação mais profunda dos mesmos não abrange o escopo do trabalho.

Para relacionar as duas tabelas apresentadas (1) a segunda tabela é continuação da primeira (2) através do Identificador do Risco (ID) pode-se correlacionar as duas tabelas, sendo que na primeira faz-se uma classificação do risco inerente e na segunda faz-se menção das medidas que podem ser utilizadas para evitar ou mitigar os riscos.

5. Capitulo V – Discussão de Resultados

5.1. Revisão de Literatura

Para a extração do material para a elaboração do presente trabalho utilizou-se 12 livros, 23 artigos científicos, 8 trabalhos académicos e 18 fontes de diversas proveniências detalhadas na bibliografia do trabalho. A figura abaixo ilustra em termos percentuais o material utilizado.

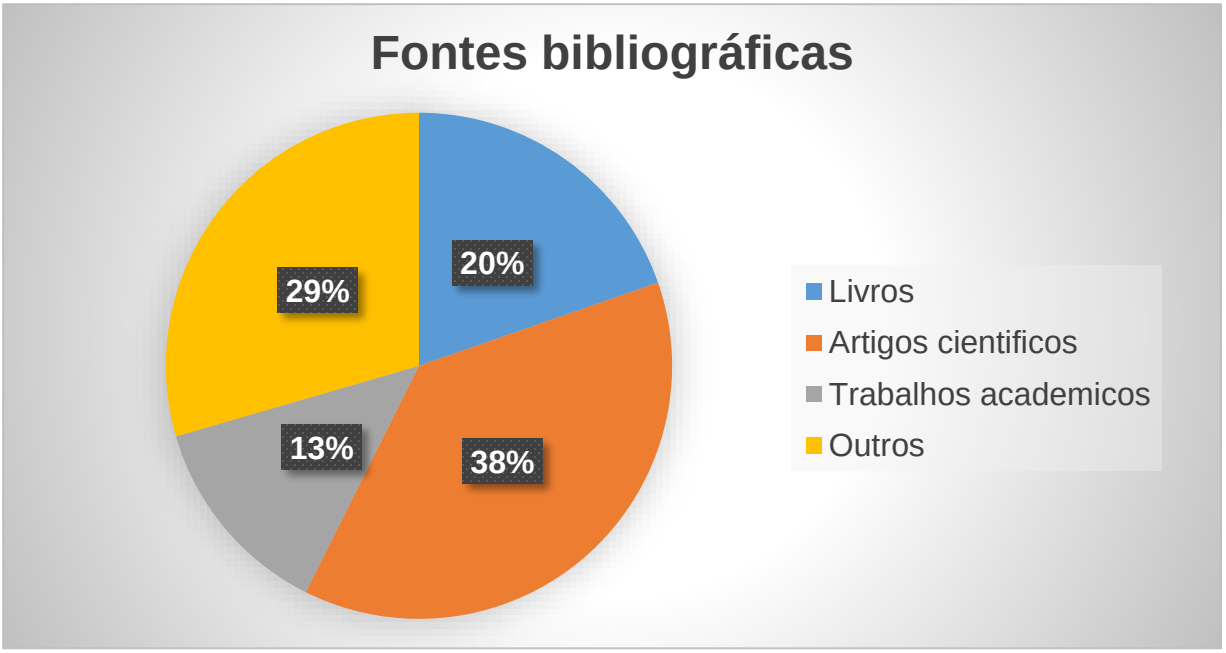

Figura 17: Fontes bibliográficas

Fonte: Elaborada pelo autor

Foram desse modo utilizadas fontes de 1995 a 2022. No caso de conceitos foram utilizados materiais mais antigos, mas para a elaboração do plano de gestão de riscos optou-se por utilizar materiais mais recentes pois representam a situação actual no que tange a segurança de SCD no mundo. Como destacou Kshetri (2019) citado por Cepik & Marcelino (2021), ataques cibernéticos causam bilhões de dólares de prejuízo para as economias africanas anualmente. De acordo com Broadhurst (2006) citado por Cepik & Marcelino (2021), muitos ataques são originados em outros países, inclusive da própria África. Existe, portanto, a necessidade de cooperação multi-lateral e multi-sectorial para lidar com o problema. Tendo isso como base percebe-se que o conhecimento das vulnerabilidades de

sistema informáticos pode possibilitar a sua exploração não dependendo da localização do invasor, para a redução desses factos é necessária a adopção de estratégias.

Numa época em que a coexistência de formas de trabalho hibridas (presenciais e remotas) é uma realidade, a realização de assinaturas digitais de documentos torna-se importante pois minimiza os esforços que são feitos por cidadãos no seu dia-a-dia evitando a dependência de notários para a autenticação de documentos. SCD surgem como uma tentativa de fortalecer o governo electrónico. Segundo Frank & Westervelt (2021), ICP é a espinha dorsal de muitas organizações que valorizam a resiliência da segurança cibernética porque permite que as organizações automatizem o processo de aplicação de políticas e procedimentos de segurança de dados usando certificados digitais e criptografia de chave pública. Contudo para que haja uma implementação segura de aplicações envolvendo ICPs é necessário ter em conta o facto de realizarem a gestão de documentos críticos de cidadãos.

5.2. Caso de Estudo

Foram inquiridos 9 funcionários do INTIC no que concerne ao nível de capacitação na gestão de Sistemas de Certificação Digital. Verificou-se que 55,6% não fizeram parte dum projecto terminado de implementação dum SCD, 33,3% não possui conhecimentos necessários para a gestão de SCD, 33,3% não possui conhecimento dos ataques feitos em Autoridades de Certificação, 77,8% nunca participou de um processo de recuperação ou defesa de um incidente cibernético e 55,6% não possui capacidade técnica para a gestão de SCD. O facto de mais de 50% dos inquiridos nunca ter participado dum processo de recuperação ou de defesa de um incidente cibernético e não possuir capacidade técnica para a gestão de SCD torna-se notável a necessidade de conscientização, educação e treinamento sobre a segurança cibernética em SCD.

Verificou-se que o plano de gestão de riscos irá afectar todos os funcionários do INTIC directa e indirectamente pois os programas de conscientização sobre segurança cibernética devem ser seguidos não só pelos funcionários da parte técnica mas como também das outras áreas pois todos fazem a gestão de processos da instituição.

5.3. Proposta de Solução

Na elaboração dum plano de gestão de riscos é essencial a compreensão dos principais conceitos relacionados utilizados num plano de gestão de riscos. Dessa forma foram abordados conceitos baseando-se no autor Whitman & Mattord (2012), na norma ISO 31000, no PMI e em outros autores que melhor abordam conceitos relevantes dum plano de gestão de riscos. O processo de elaboração dum plano de gestão de riscos numa organização passa por três fases essências (1) a identificação do risco (2) a avaliação do risco e (3) o controle do risco (Whitman & Mattord, 2012). Essa metodologia torna o processo de avaliação de riscos facilmente compreensível pois com a identificação dos riscos, a indicação da probabilidade de ocorrência e o impacto deste risco caso ocorra torna possível a classificação do risco em aceitável ou não. Caso não seja aceitável, medidas de mitigação podem ser tomadas como forma de redução do seu impacto na organização. A norma ISO 31000 aborda de forma geral as directrizes a serem tomadas pelas organizações no processo de análise de riscos, mas não especifica quais ferramentas ou estratégias especificas podem ser utilizadas a elaboração dum plano de gestão de riscos. No entanto a ferramenta SRAT identificada na pesquisa contêm a estrutura da matriz de gestão de riscos com as respectivas fórmulas no caso de uma análise quantitativa de riscos e as directrizes em caso de uma análise qualitativa dos riscos.

De acordo com os estudos realizados entre os meses novembro e dezembro de 2017 citados pela empresa Klynveld Peat Marwick Goerdeler (KPMG) sobre o grau de maturidade na Gestão de Riscos em 204 empresas brasileiras, das quais 42% tinham mais de 3 mil funcionários e 45% facturavam anualmente mais de 1 bilhão de reais. O trabalho atribuiu às empresas pesquisadas 5 graus de maturidade de gestão de risco: fraca, sustentável, madura, integrada e avançada. O resultado geral da maturidade da Gestão de Risco: 29% fraco, 27% sustentável, 40% maduro, 2% integrado e 2% avançado. Obstáculos para implementação do plano de gestão de riscos: 65% - ausência de cultura de gestão de riscos, 56% - existência de outras prioridades e 52% - benefícios potenciais não são visíveis. Com isso percebe-se que ainda existe um grande número de instituições que não possuem a cultura de realizar um plano de gestão riscos nos seus projectos o que tem causado enormes perdas monetárias e físicas em projectos que envolvem até riscos de vida.

6. Capítulo VI – Considerações Finais

6.1. Conclusões

Quando iniciou-se o trabalho de pesquisa constatou-se que vários processos que envolvem os cidadãos de uma sociedade são geridos por instituições do governo porém as TICs utilizadas no governo são alvo de ataques cibernéticos. O INTIC tem como umas das suas áreas a segurança cibernética e a certificação digital, que lidam directamente com a necessidade de manter as transacções electrónicas mais seguras para os cidadãos moçambicanos. Nesse âmbito é implementado o SCDM, que servirá como um avanço tecnológico na área da certificação digital e segurança cibernética no pais. Por isso torna-se importante estudar as vulnerabilidades em SCD centralizados.

Diante disso, a pesquisa teve como objectivo geral elaborar um plano de gestão de riscos para o SCDM gerido pelo INTIC. Constata-se que o objectivo geral foi devidamente cumprido porque a pesquisa aborda um plano de gestão de riscos com a identificação, avaliação e controle dos riscos de segurança cibernética em SCD centralizados. Esta pesquisa teve cinco (4) objectivos específicos, nos quais verificou-se que:

- No primeiro, pretendeu-se explicar os conceitos relacionados à Segurança Cibernética e SCD e verificou-se que existem diversos conceitos relacionados a esses tópicos e fez-se uma delimitação, tratando somente de conceitos que envolvem a gestão de sistemas de certificação digital centralizados.
- No segundo, identificou-se as principais vulnerabilidades e o impacto dos riscos de segurança cibernética em SCD centralizados e verificou-se que esses sistemas utilizam diversos protocolos de comunicação que tornam-nos vulneráveis a ataques cibernéticos que podem causar danos leves ou graves e para a mitigação dos riscos não basta a utilização de uma técnica, podendo estas ser combinadas para a obtenção de resultados satisfatórios. Este objectivo foi parcialmente cumprido.
- No terceiro, descreveu-se a situação actual do INTIC como AC Raiz do Estado no que concerne aos procedimentos de segurança cibernética e constatou-se que os certificados que serão emitidos pela AC Raiz são auto-assinados e confiáveis sendo esta a primeira na hierarquia das ACs e existem alguns constrangimentos enfrentados

principalmente na conscientização da segurança cibernética em SCD nos funcionários do INTIC.

- No quarto e último, apresentou-se o plano de gestão de riscos das vulnerabilidades identificadas sob forma de uma matriz de gestão riscos e verificou-se que a utilização de ferramentas para análise de riscos torna o processo de avaliação mais eficiente e menos susceptível a erros.

No capítulo VII fez-se a análise e discussão de resultados com o objectivo de responder a pergunta de pesquisa levantada na introdução do trabalho e verificou-se que um plano de gestão de riscos é de extrema importância para as organizações e ferramentas de segurança cibernética auxiliam demasiadamente na sua elaboração. De salientar que o autor teve algumas dificuldades no desenvolvimento do trabalho, que foram:

- Foi identificada e devidamente analisada uma parte do universo das vulnerabilidades de SCD centralizados, contudo existem mais vulnerabilidades que podem ser identificadas.
- Não foram muito aprofundados os princípios de funcionamento dos ataques feitos em SCD centralizados isso porque a parte técnica requer a exploração de vários conceitos que fogem do escopo do trabalho.

6.2. Recomendações

SCD são utilizados em várias partes do mundo para reduzir o nível de ameaças em transacções electrónicas e automatizar o processo de assinaturas digitais, sendo que estes sistemas possuem diversas aplicações que lidam com documentos críticos para os seus utilizadores é necessário utiliza-los de forma segura e um plano de gestão de riscos objectiva minimizar as chances de perda de activos de informação em casos de ocorrência de ataques cibernéticos. O trabalho surgiu na tentativa de elaborar um plano de gestão dos riscos na gestão desses sistemas, porém foram identificadas algumas limitações. Dessa forma recomenda-se aos futuros investigadores o seguinte:

- A actualização continua do plano de gestão de riscos, pelo facto da constante evolução das TICs, pois novas vulnerabilidades e formas de exploração de SI são descobertos no dia-a-dia.

- O aprofundamento do funcionamento dos principais ataques feitos em SCD como forma de melhor compreender as técnicas que podem ser implementadas para a mitigação da sua ocorrência.
- Realização de avaliações sobre o nível de conscientização sobre segurança cibernética em SCD como forma de garantir que os gestores desses sistemas estejam sempre actualizados sobre as ameaças e ataques feitos nesses sistemas.
- Implementar um serviço de validação de assinaturas de documentos assinados por utilizadores, que valida documentos PDF assinados por utilizadores do SCDM.

Bibliografia

Referências Bibliográficas

[1]. Abdulla, M. (2020). Vulnerabilities in Public Key Cryptography. *International Journal of Psychosocial Rehabilitation*, *24*(5), 3881–3886. https://doi.org/10.37200/IJPR/V24I5/PR202096

[2] Alharthi, D. (2021). *Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis*. UNIVERSITY OF CALIFORNIA.

[3]. Ardigo, J. (2004). *Modelo de Infra-estrutura de Chaves Públicas como Organização Virtual para Processos de Avaliação Somativa à Distância*. Florianópolis.

[4]. Associação Brasileira De Normas Técnicas. ABNT ISO 3100. (2009). *Gestão de riscos princípios e diretrizes.* Rio de Janeiro.

[5]. Bereza, A. (2013). *AUDITORIA UNIFICADA EM MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA*. Florianópolis. UNIVERSIDADE FEDERAL DE SANTA CATARINA.

[6]. Bhattarai, P. (2020). *Summary on Public Key Infrastructure (PKI)*. https://doi.org/10.13140/RG.2.2.34199.70562

[7]. Casagrande, A. (2011). *CERTIFICAÇÃO DIGITAL*. Brasil

[8]. Cepik, M. (2018). *SEGURANÇA CIBERNÉTICA*.

[9]. Chaves Cepik, M. A., & Marcelino, H. M. (2021). Segurança cibernética em Moçambique: Conceitos, infraestrutura e desafios de implementação. *Carta Internacional*, *16*(3), e1130. https://doi.org/10.21530/ci.v16n3.2021.1130

[10]. Chilundo, D. (2018). Segurança Cibernética em Moçambique e seu enquadramento Legal. *I Conferência Nacional de Segurança Cibernética*.

[11]. Conselho, P. (2018*). METODOLOGIA DA SOLUÇÃO DOS PROBLEMAS*. UEM.

[12]. Cordeiro, N. (2011). *CERTIFICAÇÃO DIGITAL*. Belo Horizonte.

[13] Crashtest. (sem data). *GUIDE FOR PREVENTINGSSL/TLS VULNERABILITIES*. https://crashtest-security.com/

[14]. Crawley, K. (sem data). *Weak PKI Implementation is a Major Cyber Risk*. https://www.venafi.com/blog/weak-pki-implementation-major-cyber-risk

[15]. Dias, J. (2004). *Confiança no Documento Electrónico*. Brasil

[16]. ENTERPRISE RISK MANAGEMENT: TOOLS AND TECHNIQUES FOR EFFECTIVE IMPLEMENTATION. (2007). *Institute of Management Accountants*.

[17]. Ferreira, A. (2008). *Segurança da informação, conceitos e mecanismos*. Brasil

[18]. Frank, D., & Westervelt, R. (2021). *PKI Investments Help Organizations Improve Security and Modernize Business Processes, Study Finds*.

[19]. Gerhardt, T., & Silveira, D. (2009). *Métodos de pesquisa* (1.ª ed.). Porto Alegre. UFRGS.

[20]. *Gestão de Riscos de Empresas | LinkedIn*. (sem data). Obtido 10 de julho de 2022, de https://www.linkedin.com/pulse/gest%C3%A3o-de-riscos-empresas-luiz-cl%C3%A1udio-caffagni/?originalSubdomain=pt

[21]. Gil, A. (2002). *Como elaborar projetos de pesquisa* (4.ª ed.). São Paulo. Atlas.

[22]. *Global PKI and IoT Trends Study*. (2021). Obtido 27 de junho de 2022, de https://www.entrust.com/lp/en/global-pki-iot-trends-study

[23]. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

[24]. Lakatos, E. M., & Marconi, M. de A. (1995). *Metodologia do trabalho científico: Procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos*. São Paulo. Atlas.

[25]. Lakatos, E. M., & Marconi, M. de A. (2003). *Fundamentos de metodologia científica*. São Paulo. Atlas.

[26]. Lusa. (sem data). *Ataque de hackers deixa inoperacionais portais moçambicanos*. https://www.dw.com/pt-002/ataque-de-hackers-deixa-inoperacionais-portais-mo%C3%A7ambicanos/a-60854704

[27]. Mahendiran, A., & Appusamy, R. (2015). *Intrusion Detection and Prevention System: Technologies and Challenges*.

[28]. Mainka, C., Mladenov, V., & Rohlmann, S. (2021). Shadow Attacks: Hiding and Replacing Content in Signed PDFs. *Proceedings 2021 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, Virtual. https://doi.org/10.14722/ndss.2021.24117

[29]. Mainka, C., Mladenov, V., Rohlmann, S., & Schwenk, J. (2020). *Attacks bypassing the signature validation in PDF*.

[30]. Müller, J., Noss, D., Mainka, C., Mladenov, V., & Schwenk, J. (2021). *Processing Dangerous Paths—On Security and Privacy of the Portable Document Format*.

[31] *O que é um Provedor de Identidade?* | *Entrust*. (sem data). Obtido 7 de junho de 2022, de https://www.entrust.com/pt/resources/faq/what-is-an-identity-provider

[32]. *Okta vs ForgeRock Identity Platform vs Keycloak vs Gluu Comparison* | *SaaSworthy.com*. (sem data). Obtido 7 de junho de 2022, de https://www.saasworthy.com/compare/okta-vs-forgerock-identity-platform-vs-keycloak-vs-gluu?pIds=2940,5984,5998,6005

[33]. Oliveira, M. (2011). METODOLOGIA CIENTÍFICA: um manual para a realização de pesquisas em administração. *UFG*.

[34]. Oliveira, R. (2012). *Criptografia simétrica e assimétrica: Os principais algoritmos de cifragem*. Brasil

[35]. PDF, iText. (2021). *Attacks on PDF certification, and what you can do about them*. IText PDF; iTextpdf Software. https://itextpdf.com/blog/itext-news-technical-notes/attacks-pdf-certification-and-what-you-can-do-about-them

[36]. Purcell, A. (2018). *3 key ideas to help drive compliance in the cloud*.

[37]. Rashid, A. (2018). *Component of Information Technology*. https://www.researchgate.net/figure/Component-of-Information-Technology_fig1_329375249

[38]. Regulamento do Sistema de Certifição Digital de Moçambique (SCDM). (2019). *IMPRENSA NACIONAL DE MOÇAMBIQUE*.

[39]. RISK MANAGEMENT GUIDELINE: RISK THRESHOLDS. (2018). *National Treasure Republic of South Africa*.

[40]. Rohlmann, S., Mladenov, V., Mainka, C., & Schwenk, J. (2021). *Vulnerability Report: Attacks on PDF Certification*.

[41]. SABOONCHI, N. (2014). *Hardware Security Module Performance Optimization by Using a "Key Pool"*. KTH Royal Institute of Technology.

[42]. SailPoint. (sem data). *8 Types of Password Attacks*. SailPoint. Obtido 14 de julho de 2022, de https://www.sailpoint.com/identity-library/8-types-of-password-attacks/

[43]. Schardong, F., Athayde, L., & Custodio, R. (2021). PILOTO DE CERTIFICAÇÃO E IDENTIDADE ELETRÔNICA PARA MOÇAMBIQUE. *UFSC*.

[44]. Security Risk Assessment Tool (SRAT). (sem data). *Open Briefing*. Obtido 21 de junho de 2022, de https://www.openbriefing.org/resources/security-risk-assessment-tool/

[45]. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7ª. ed.). Boston. Pearson.

[46]. Stokes, P. (2019). *Malicious PDFs | Revealing the Techniques Behind the Attacks*. SentinelOne. https://www.sentinelone.com/blog/malicious-pdfs-revealing-techniques-behind-attacks/

[47]. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadores*. São Paulo. Pearson Prentice Hall.

[48]. Vasconcelos, A., Silva, M., & Netto, M. (2008). *ASSINATURA DIGITAL NO PROCESSO LEGISLATIVO DA CÂMARA DOS DEPUTADOS*. Brasília.

[49]. Vazão, L. (2020). *Implementação de sistema SIEM open-source em conformidade com o RGPD*.

[50]. Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Amsterdam Waltham, MA. Syngress.

[51]. Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4ª ed.). Boston, MA. Course Technology.

[52]. Zanella, L. (2013). *Metodologia de pesquisa* (2.ª ed.). Universidade Federal de Santa Catarina. UFSC.

Outras Bibliografias

[1]. *Apresentação – Instituto Nacional de Tecnologias de Informação e Comunicação*. (sem data). Obtido 8 de junho de 2022, de https://www.intic.gov.mz/?page_id=565

[2]. *ICP + ID de Moçambique*. (sem data). Obtido 9 de junho de 2022, de https://mz.labsec.ufsc.br/

[3]. *Instituto Nacional de Tecnologias de Informação e Comunicação*. (sem data). Obtido 10 de junho de 2022, de https://www.intic.gov.mz/

[4] INTIC. (2022). *Declaração de Práticas de Certificação e Políticas de Certificados da Autoridade Certificadora Raiz do Estado de Moçambique*.

[5]. Project Management Institute (Ed.). (2013). *A guide to the project management body of knowledge (PMBOK guide)* (Fifth edition). Project Management Institute, Inc.

[6] Moçambique. (2002). Decreto nº 90/2020 9 de Outubro. Boletim da República

[7] Moçambique. (2017). Decreto nº 60/2017 6 de Novembro. Boletim da República

[8] Moçambique. (2020). Decreto nº 60/2020 26 de Dezembro. Boletim da República

[9]. *Websites do governo moçambicano sofrem ataque cibernético*. (2022, Fevereiro de). https://pt.globalvoices.org/2022/02/28/websites-do-governo-mocambicano-sofrem-ataque-cibernetico/

Anexos

Anexo 1: Plano de Gestão de Riscos – Análise das Vulnerabilidades em SCD centralizados e das técnicas utilizadas na redução e mitigação de riscos de segurança cibernética

Tabela A1-1: Matriz de gestão de riscos

ID #	Ameaça	Vulnerabilidade	Risco inerente			Risco aceitável?	Estratégia do Risco
			Probabilidade	Impacto	Classificação do Risco		
1	Alteração do conteúdo em documentos PDF assinados por um determinado remetente sem invalidar a sua assinatura digital.	1. Utilização de aplicações PDF com versões susceptíveis a ataques *Shadow* no acto da assinatura de documentos digitais. 2. Não verificar o conteúdo do documento depois de efectuar a assinatura digital.	3	4	12	Não	Mitigar

2	Inserção de anotações maliciosas em documentos PDF assinados.	1. Habilitação da adição de anotações ou comentários em documentos PDF. 2. Utilização de aplicações PDF com versões susceptíveis a *Evil Annotation Attacks* e *Sneaky Signature Attacks*.	3	4	12	Não	Mitigar
3	Execução de *scripts* maliciosos em documentos PDF, que podem ser executados no servidor de hospedagem do SCDM ou nos dispositivos de utilizadores finais no momento da utilização dos documentos.	1. Obtenção de documentos utilizando fontes electrónicas não confiáveis. 2. Utilização de aplicações PDF com versões susceptíveis a ataques DoS, *Information disclosure, Data Manipulation* e *Code Execution Launch Action*.	3	5	15	Não	Mitigar
4	Inserção de conteúdos maliciosos em campos utilizados para a realização de assinaturas digitais de documentos electrónicos.	Utilização de tamanhos fixos de *bits* em campos utilizados para efectuar a assinatura de documentos electrónicos no SCDM através da implementação dum mecanismo de cálculo de *bits* necessários para armazenar a assinatura dos utilizadores.	2	4	8	Sim	Evitar

5	Obtenção de informações privadas de utilizadores do SCDM, como *passwords*, contas bancárias, entre outros e sobrecarga no processamento de informações.	1. Utilização de versões muito antigas de navegadores. 2. Utilização de certificados *wildcard* 3. Utilização de certificados TLS e SSL de autoridades certificadoras não confiáveis. 4. Utilização de chaves criptográficas relativamente fracas (como o RSA) 5. Utilização de versões de certificados TLS e SSL susceptíveis a ataques DDoS.	4	4	16	Não	Mitigar
6	Roubo da identidade electrónica de utilizadores por meio de autenticação.	1. Utilização de senhas fracas por utilizadores no provedor de identidade electrónica do SCDM. 2. Não utilização de autenticação multi-factor. 3. Acesso a páginas *web* não legitimas disponibilizando credenciais de autenticação.	3	5	15	Não	Evitar
7	Exclusão ou manipulação não autorizada de *logs* de eventos do SCDM.	Não utilização de ferramentas para gerir a conformidade, como monitorar, auditar e relatar acessos ao SCDM pelos administradores de segurança.	3	5	15	Não	Evitar

8	Ataques de engenharia social aos utilizadores com o intuito de obter as suas chaves, forjar assinaturas digitais e obter informações sigilosas sobre os dados de utilizadores do SCDM.	1. Divulgação por parte dos trabalhadores do local onde os dispositivos físicos do SCDM estão instalados, como HSMs e servidores. 2. Partilha do código fonte do SCDM a indivíduos não vinculados ao INTIC. 2. Fornecimento de informações pessoais e financeiras através de documentos enviados em *e-mails* ou por outros meios electrónicos com assinaturas electrónicas de entidades falsas fazendo-se passar por entidades legitimas. 3. Assinar documentos não legítimos. 4. Não utilização de VPNs em formas de trabalho hibridas (remotas e presenciais).	5	5	25	Não	Mitigar

Tabela 9: Continuação da matriz de gestão de riscos

	Medidas de mitigação	Risco residual			Risco aceitável?	Notas
		Probabilidade	Impacto	Classificação do Risco		
1	Para Mainka et al., (2021), as seguintes medidas podem ser tomadas: 1. No momento em que um PDF é assinado, todas as revisões posteriores do mesmo documento devem ser assinadas, sem uma única excepção. Esse comportamento tem uma desvantagem: não permite nenhum tipo de alteração no documento sem assinar essa alteração. Para afrouxar essa restrição, pode-se gerar um aviso ("O documento foi actualizado."). O utilizador interessado pode então visualizar e inspecionar manualmente essa revisão específica. Actualmente, muitos leitores PDF já exibem um aviso semelhante, mas não está definido com precisão em quais casos eles o exibem. 2. Utilização de versões de aplicações PDF recomendadas por Mainka et al., (2021).	3	4	12	Não	Existe uma percentagem de cidadãos que utilizam versões antigas de aplicações PDF e que não tem o habito de manter as suas aplicações sempre actualizadas, sendo assim estarão susceptíveis a ataques *Shadow*.

2	**Utilização da aplicação PDF-Detector:** Uma contramedida de curto prazo que esteja em conformidade, que pode detectar a sobreposição de conteúdo malicioso em documentos PDF analisando a posição de anotações e assinaturas no documento e estimando se elas se cruzam com algum conteúdo. Se tal intersecção for encontrada, um aviso pode ser lançado. Esta aplicação pode detectar ataques EAA e SSA. **Escolher o nível DocMDP (*Document Modification Detection and Prevention*) apropriado:** Como explicado no mesmo anexo nos ataques à certificação PDF, não é incomum ver assinaturas de certificação com DocMDP nível 2 ou 3 em situações em que elas não são apropriadas. Se o fluxo de trabalho não exige que os documentos sejam actualizados após a assinatura, basta definir o nível DocMDP como 1. O nível 1 do DocMDP neutraliza as explorações de EAA e SSA. Como se especifica no *website* iText, se é um utilizador de documentos PDF, exerça a devida diligência: ▪ Se o PDF já tiver uma assinatura de certificação, deve-se revisar cuidadosamente as configurações de permissão. Se os comentários forem permitidos nos documentos representam uma vulnerabilidade.	3	4	12	Não	Este risco é de difícil controle, devendo os utilizadores estar devidamente informados sobre os campos de adição de comentários em seus documentos PDF.

3	De acordo com a empresa SentinelOne (2019), alguns dos leitores e navegadores tem alguma forma de controle de *scripts* em *JavaScript*. No *Acrobat Reader* da *Adobe*, por exemplo, pode-se desabilitar o *Acrobat JavaScript* nas Preferências e gerir o acesso a URLs. Implementar um validador de conteúdo PDF, neste caso, ao realizar o carregamento do documento que deve ser assinado no *website* do SCDM, deve efectuar-se uma verificação do conteúdo.	3	4	12	Não	Este risco é de difícil controle pois os utilizadores possuem a liberdade de utilizar configurações ou preferências de acordo com a sua experiência e usabilidade em aplicações PDF. Os utilizadores não tem a cultura de efectuar verificações críticas de segurança.
4	Implementar um mecanismo de controle do tamanho da assinatura feita pelos utilizadores no SCDM, dessa forma evitando a inserção de conteúdo malicioso nos documentos.	2	2	4	Sim	A arquitectura actual do SCDM possui um tamanho fixo *bits* necessários para efectuar a assinatura de documentos PDF.

5	**Utilização de versões mais recentes do TLS (TLS 3.0)** A utilização da versões mais estáveis e actualizadas dos protocolos criptográficos TLS/SSL, pois incluem os aprimoramentos mais recentes para evitar vulnerabilidades conhecidas de versões anteriores. **Escolha de uma autoridade de certificação apropriada** Os registros de autorização de autoridades de certificação especificam quais ACs podem emitir certificados digitais para um domínio específico, eliminando a necessidade de certificados auto-assinados. O INTIC também pode utilizar ACs internas para redes proprietárias, embora elas só possam gerar certificados para usuários e servidores internos dentro da rede da organização. **Utilização de cifras fortes** O TLS oferece suporte a uma extensa lista de conjuntos de cifras que inclui cifras com diferentes níveis de segurança e força de criptografia. Como prática recomendada, a seleção do conjunto de cifras de uma organização deve envolver uma lista de conjuntos de cifras que abranja os algoritmos de criptografia mais apropriados. **Utilização de certificados *wildcard* apenas quando for necessário** Como os *wildcard*s tornam um único certificado válido para todos os subdomínios associados, eles violam o princípio de mesma origem e privilégio mínimo. Como vários sistemas de servidor geralmente compartilham um certificado *wildcard*, a chave privada do certificado deve	3	3	9	Sim	Dada a forte dependência de protocolos TLS/SSL no tráfego moderno de informações *web*, os ataques direccionados a esses protocolos são predominantes. Embora esse conjuntos de protocolos esteja em constante evolução para lidar com ameaças avançadas, a utilização de versões não actualizadas desses protocolos tem causado diversos ataques.

	existir em vários sistemas, aumentando a probabilidade de comprometimento. Desde que os atacantes valorizam muito a chave privada única, ela se torna o principal alvo para violações. Recomenda-se que, em vez de usar certificados *wildcard* em sistemas de produção, os desenvolvedores aproveitem certificados específicos de subdomínio de curta duração que são alternados regularmente para evitar ataques mal-intencionados.					
6	Segundo as informações listadas no *website* da empresa SailPoint (2021), a melhor maneira de evitar ataques de *password* é adoptar as melhores práticas a gestão de senhas. Aumentar a segurança de senha melhora significativamente sua capacidade de evitar uma violação de dados. Dentre as práticas recomendadas de *passwords* incluem: 1. Exigir *passwords* longas e complexas que são exclusivas para o utilização do PIE do SCDM. 2. Implementação de autenticação multi-factor sempre que possível. 3. Adoptar um gestor de senhas para simplificar a gestão de senhas e garantir o armazenamento seguro. 4. A equipe de TI também deve limitar o acesso a contas privilegiadas e adicionar camadas de segurança adicionais para essas contas. 5. Educar todos os seus funcionários e outras partes interessadas sobre a segurança de *passwords* também é um meio comprovado de prevenção.	1	4	4	Sim	O requisito autenticação é extremamente importante tratando-se do SCDM, pois este dá a possibilidade de utilizadores usufruírem dos recursos desse sistema. Tendo o acesso é possível emitir certificados confiáveis, contendo a chave pública da entidade para assinar documentos digitalmente e este facto pode causar enormes perdas dependendo da finalidade do documento assinado.

	A nível organizacional é necessário que uma política de controle de acessos seja estabelecida, documentada e contenham planos de revisão com base nos requisitos de segurança do INTIC.					
7	Utilização de ferramentas SIEM (*Security Incident and Event Management*) para de gestão de *logs* de eventos que ocorrem na utilização do SCDM pelo INTIC. De acordo com Granadillo et al. (2021) Sistemas de Gestão de Informações e Eventos de Segurança (SIEM) foram desenvolvidos em resposta para ajudar os administradores a projectar políticas de segurança e gerenciar eventos de diferentes fontes. Adicionar com frequência novos tipos de *logs* que criados durante a utilização do SCDM nas ferramentas SIEM.	2	2	9	Sim	O sistema deve ser capaz de responder a dados ou comandos corrompidos, inválidos ou maliciosos por meio de suas interfaces externas e internas, permanecendo disponível para uso primário.
8	Para Alharthi (2021), as contramedidas para ataques de engenharia social podem ser classificadas da seguinte forma: **a) Pessoas** Para proteger-se dos ataques de Engenharia Social a nível das pessoas deve-se (1) Educar seus funcionários periodicamente (2) Contratar pessoal técnico de TI conhecedor de ataques de segurança de engenharia social. **b) Dados**	3	4	12	Não	Estes ataques são geralmente causados pela falta de conhecimento de certos aspectos sobre segurança cibernética o que leva utilizadores de certos SI divulgarem aspectos críticos sobre a segurança da gerida pelos sistemas. No caso do

	Para defender esse activo, as organizações precisam (1) realizar backup e replicação de seus dados periodicamente, (2) determinar as informações mínimas que cada funcionário precisam para realizar suas tarefas e conceder apenas essas informações a esse funcionário e (3) criar políticas de segurança claras para identificar os limites de compartilhamento das informações para que os funcionários saibam o que compartilhar e com quem. **c) *Software* e *Hardware*** Para proteger os equipamentos do SCDM contra ataques de engenharia social, o INTIC precisa educar seus funcionários sobre (1) o processo de gestão de *hardware* e *software* da organização, (2) *e-mails* e contas de trabalho, (3) qualquer política de autenticação. **d) Rede** Além disso, a maioria das organizações hoje em dia permite VPN (*Virtual Private Network*) ou RDP (*Remote Desktop Protocol*) para permitir que seus funcionários acessem a rede local remotamente.					SCDM práticas como a divulgação do local de armazenamento dos dispositivos críticos e os meus de acesso a estes, como também a partilha de dados de utilizadores que são necessários para a autenticação destes.

Fonte: Elaborada pelo autor

1. Ataques *Shadow*

Conforme Mainka et al. (2020), a ideia dos *Shadow Attacks* é que os invasores criem um documento PDF com dois conteúdos diferentes: o conteúdo esperado pela autoridade que está revisando e assinando o PDF e o conteúdo oculto que será exibido após a assinatura do PDF. Os signatários do PDF recebem o documento, o revisam e o assinam. Os atacantes usam o documento assinado, modificam-no ligeiramente e enviam-no às vítimas.

De um modo geral, a ideia é permitir que os invasores escolham um PDF e usem os Signatários como um oráculo de assinatura. Após a assinatura, os invasores manipulam o PDF assinado novamente para impor uma alteração em seu conteúdo sem invalidar a assinatura.

Mainka et al. (2020) especificam o princípio de funcionamento e as contramedidas para este tipo de ataque, como detalhado abaixo:

Princípio de funcionamento

1) Os invasores criam o documento PDF1 = criarPDF() que contém o conteúdo da sombra invisível (por exemplo, um texto ou uma imagem).

2) Os signatários recebem o PDF1 (por exemplo, por e-mail) e criam um novo documento PDF2 assinando PDF1, ou seja, PDF2 = assinar(PDF1).

3) Os invasores recebem PDF2. Eles podem modificar o PDF2 novamente, por exemplo, os invasores criam PDF3 = manipular(PDF2). Os atacantes enviam PDF3 para as vítimas.

Figura 18: Ilustração de ataques *Shadow*

Fonte: Rohlmann et al. (2021)

2. Ataques à Certificação PDF

De acordo com os estudos feitos por Rohlmann et al. (2021), as certificações têm duas diferenças principais em relação às assinaturas. Primeiro, cada PDF pode ter apenas uma certificação e deve ser a primeira do documento. Em segundo lugar, as certificações definem permissões que permitem certas alterações no documento certificado. Conforme descrito na tabela abaixo, as certificações definem uma maneira mais flexível de lidar com actualizações incrementais, e as actualizações incrementais permitidas não levam a um aviso. O certificador escolhe entre três diferentes níveis de permissão (P) para permitir diferentes modificações.

- P1: Não são permitidas modificações no documento

- P2: É permitido o preenchimento de formulários e a assinatura digital do documento.
- P3: Além de P2, também são permitidas anotações.

Ainda para Rohlmann et al. (2021), os ataques EAA e SSA podem ser descritos conforme explicado abaixo.

a) *Evil Annotation Attacks*

A ideia do *Evil Annotation Attack* (EAA) é mostrar conteúdo arbitrário em um documento certificado abusando das anotações para esse fim. Como o documento certificado P3 permite adicionar anotações, o EAA quebra a integridade da certificação. De acordo com nosso modelo descritos pelos autores, o atacante possui um documento validamente certificado que permite a inserção de anotações. Para executar o ataque, o invasor modifica um documento certificado incluindo a anotação com o conteúdo malicioso em uma posição de escolha do invasor.

Figura 19: Evil Annotation Attack

Fonte: Rohlmann et al. (2021)

O preço por ação foi manipulado por uma anotação para mostrar o valor de $ 100.000.000. O visualizador de PDF exibe a notação. Em seguida oculta a anotação no documento.

b) *Sneaky Signature Attack*

O invasor modifica um documento certificado incluindo um campo de assinatura com o conteúdo malicioso em uma posição de escolha do invasor.

O invasor precisa então assinar o documento, mas não precisa possuir uma chave confiável. Um certificado auto-assinado para SSA é suficiente.

A única restrição é que o invasor precisa assinar o documento para inserir o campo de assinatura maliciosa. Essas informações de assinatura podem ser vistas abrindo o

documento PDF e mostrando informações detalhadas da validação da assinatura. Nesse caso, a vítima que abre o arquivo pode desconfiar e se recusar a aceitar o documento, mesmo que a certidão seja válida.

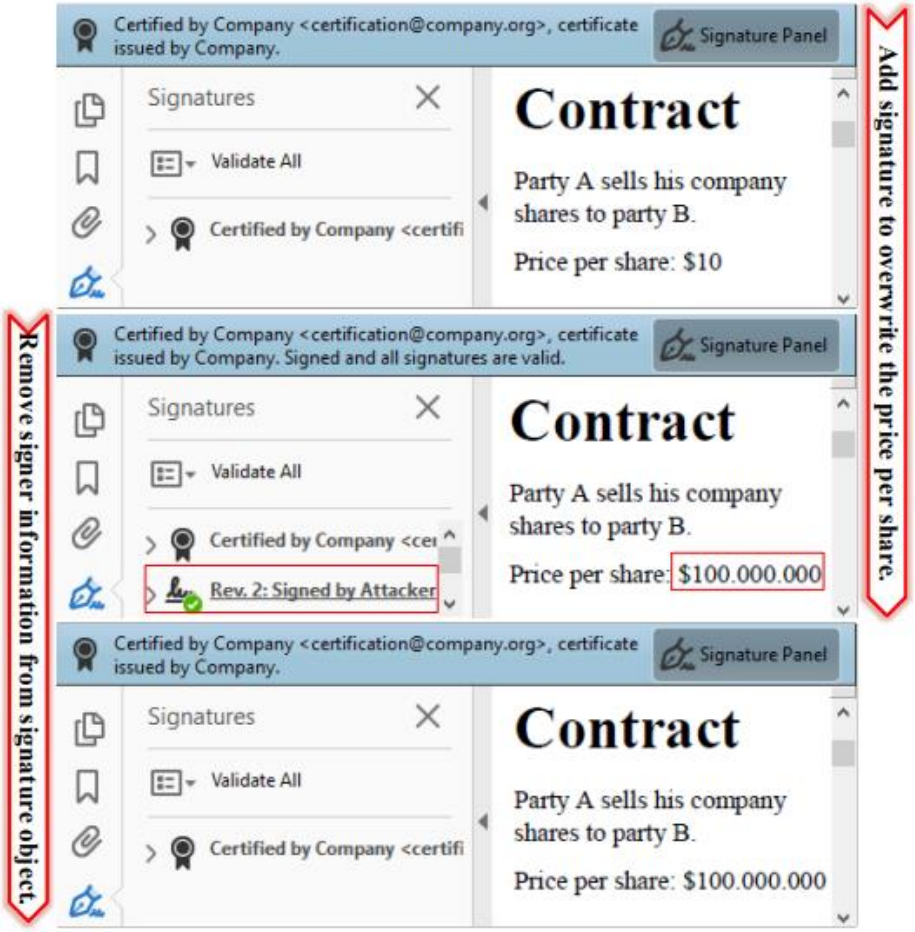

Figura 20: Sneaky Signature Attack

Fonte: Rohlmann et al. (2021)

O preço por acção foi manipulado usando o SSA que substitui o preço por U$ 100.000.000. Ao manipular o objeto de assinatura, as informações do assinante podem ser removidas.

3. Ataques de Engenharia Social

De acordo com Alharthi (2021), os ataques de engenharia social podem ser devidos em técnicos e não técnicos:

a) Ataques técnicos

- ***Phishing*:** dependem de mensagens cuidadosamente elaboradas para atrair as vítimas a abrir anexos ou clicar em hiperlinks incorporados. Neste ataque de segurança, a vítima é totalmente desconhecida do engenheiro social.
- ***Vishing* (*voice phishing*):** O *vishing* (*phishing* de voz) ocorre enganando as pessoas para que revelem informações confidenciais por meio de uma ligação telefônica.
- ***Baiting*:** acontece quando um meio de armazenamento infectado por *malware* é deixado em um local onde provavelmente será usado por vítimas direccionadas.
- ***Tailgating*:** visa acessar locais não autorizados obtendo ajuda de uma pessoa autorizada.
- ***Waterholing*:** significa comprometer um site que provavelmente será do interesse de uma vítima escolhida.
- ***Interesting Software e Popup Windows*:** são outras técnicas de engenharia social nas quais um engenheiro social convence a vítima a baixar e instalar um programa ou aplicativo útil, como um *software* para aumento de desempenho da CPU ou exibe uma janela pop-up que impede a vítima de prosseguir com a sessão, a menos que ele redigita seu nome de usuário e senha.

b) Ataques não técnicos

- ***Pretexting/Impersonation*:** ocorre quando um engenheiro social finge ser outra pessoa que é conhecida por uma pessoa-alvo.
- ***Dumpster Diving*:** acontece vasculhando o lixo de uma organização para encontrar itens descartados que incluem informações confidenciais.
- ***Shoulder Surfing* e *Spying*:** usam técnicas de observação direta para obter informações. Quando um engenheiro social tenta extrair informações confidenciais sobre a atividade recente de um usuário usando, por exemplo, óleos residuais em dispositivos de tela sensível ao toque para detectar a entrada do usuário.
- ***Hoaxing*:** uma tentativa de enganar o público a acreditar que algo falso é real.
- ***Authoritative Voice*:** é outro ataque SE, no qual um engenheiro social liga para o *help desk* do computador de uma empresa e finge ter acesso a um sistema de solução de problemas

- ***Support Staff and Technical Expert*:** são ataques físicos usados por engenheiros sociais actuando como equipe de suporte ou como equipe técnica. Por exemplo, um homem vestido como um membro da equipe de limpeza entra em uma área de trabalho, carregando equipamentos de limpeza e, em seguida, no processo de aparecer para limpar uma área de mesa, ele pode bisbilhotar e obter informações valiosas, como senhas ou arquivos confidenciais que um funcionário esqueceu de esconder, ou até mesmo fazer um telefonema se passando por um funcionário de sua mesa.

4. Ataques *Dangerous Paths*

De acordo com os estudos feitos por Müller et al. (2021), essa classe de ataques objectiva na execução de *scripts* maliciosos em documentos PDF nos dispositivos dos utilizadores finais. Segundo Müller et al. (2021), esses ataques são descritos conforme destacado abaixo:

a) *Denial-of-Service*

O objetivo dessa classe de ataques é construir um documento PDF especialmente criado que imponha aplicativos de processamento para consumir todos os recursos disponíveis (ou seja, tempo de computação ou memória) ou faça com que eles travem. Observe que, embora o impacto do DoS seja limitado para os usuários finais, ele pode levar a sérios danos aos negócios se o documento for processado em um servidor, por exemplo, por uma biblioteca que gera miniaturas de visualização de arquivos PDF carregados no armazenamento em nuvem.

- ***Infinite Loop*:** induzir um *loop* infinito faz com que a execução do programa fique travado.
- ***Deflate Bomb*:** A questão surge se bombas de compressão baseadas em documentos PDF maliciosos podem ser construídas, a fim de fazer com que os aplicativos de processamento aloquem toda a memória disponível.

b) *Information disclosure*

O objetivo dessa classe de ataques é rastrear o uso de um documento invocando silenciosamente uma conexão com o servidor do invasor assim que o arquivo for aberto ou expor dados do documento PDF.

c) *Data Manipulation*

Essa classe de ataque lida com os recursos de documentos maliciosos para modificar silenciosamente os dados do PDF, gravar em arquivos locais no sistema de arquivos do utilizador ou mostrar um conteúdo diferente com base no aplicativo utilizado para abrir o documento.

d) *Code Execution Launch Action*

O objetivo deste ataque é executar o código controlado pelo invasor. Isso pode ser feito lançando silenciosamente um arquivo executável, embutido no documento, para infectar o utilizador com *malware*.

5. Ataques direccionados ao Provedor de Identidade Electrónica.

Como explicado no anexo 3, o SCDM dispõe de um PIE, dessa forma é possível autenticar utilizadores ao sistema. Contudo a obtenção de credenciais de acesso ao sistema pode levar a obtenção de dados importantes dos utilizadores. Segundo o *website* SailPoint (2021) os principais ataques executados para roubo identidade electrónica de utilizadores são:

- ***Brute-Force*:** Um ataque de força bruta é um tipo de ataque de senha em que os hackers fazem inúmeras tentativas de acerto ou erro para obter acesso. É um ataque simples e geralmente envolve métodos automatizados, como *software*, para tentar várias variações de números de letras.
- ***Keylogger*:** é um *spyware* que registra a atividade de um usuário registrando os toques do teclado. Os invasores usam *keyloggers* para roubar uma variedade de dados confidenciais, de senhas a números de cartão de crédito. Em um ataque de senha, o *keylogger* registra não apenas o nome de usuário e a senha, mas também o site ou aplicativo onde essas credenciais são usadas, juntamente com outras informações confidenciais

- ***Dictionary*:** é baseado em uma lista de palavras e frases comumente usadas, bem como senhas usadas com frequência. Para evitar ter que quebrar uma longa lista de senhas possíveis, os invasores restringem a lista ao que é conhecido como palavras de dicionário.
- ***Credential Stuffing*:** é semelhante à força bruta, pois os invasores usam tentativa e erro para obter acesso. No entanto, em vez de adivinhar senhas, eles usam credenciais roubadas. O preenchimento de credenciais funciona com a suposição de que muitas pessoas reutilizam suas senhas para várias contas em várias plataformas.
- ***Man-In-The-Middle*:** um cenário MiTM envolve três partes: o usuário, o invasor e o terceiro com quem a pessoa está tentando se comunicar. Em um ataque de senha, os invasores normalmente se passam por terceiros legítimos, geralmente por meio de um e-mail de *phishing*.
- ***Traffic Interception*:** A interceptação de tráfego, uma variação do ataque MiTM, envolve os agentes de ameaças espionando o tráfego de rede para monitorar e capturar dados. Uma maneira comum de fazer isso é por meio de conexões Wi-Fi não seguras ou conexões que não usam criptografia, como HTTP.
- ***Password Spraying*:** Outra forma de ataque de força bruta, envolve a tentativa de um grande número de senhas comuns em um pequeno número de contas de usuário, ou mesmo em apenas uma conta. Os invasores fazem de tudo para evitar a detecção durante a pulverização de senhas. Normalmente, eles fazem algum reconhecimento primeiro para limitar o número de tentativas de *login* para evitar o bloqueio da conta.

6. Ataques direccionados aos protocolos SSL e TLS

De acordo com a pesquisa feita pela empresa CrashTest Security sobre as formas de prevenção dos ataques direccionados a protocolos SSL e TLS, são em seguida listados os principais ataques *Padding Oracle On Downgraded Legacy Encryption* (*Poodle*), *Browser Exploit Against* (*Beast*), *Compression Ratio Info-leak Made Easy* (*Crime*), *Reconnaissance and Exfiltration via Adaptive Compression* (*Breach*), *Factoring RSA Export Keys* (*Freak*), *Decrypting RSA with Obsolete and Weakened eNcryption* (*Drown*) *Cross-Protocol*, *Renegotiation.*

Anexo 2: Guião da Entrevista

1. Actualmente quais são os procedimentos, estratégias ou políticas de Segurança Cibernética utilizados pela instituição?
2. A instituição já implementou um Sistema de Certificação Digital antes?
3. Quais são os principais desafios enfrentados na implementação do Sistema de Certificação Digital de Moçambique?
4. Existem documentos contendo políticas ou procedimentos de segurança cibernética para o Sistema de Certificação Digital de Moçambique?
5. Se a resposta anterior tiver sido afirmativa. Quais são os documentos?
6. Existe algum método utilizado para avaliar o nível de conscientização sobre Segurança Cibernética aos funcionários da instituição?
7. Se a resposta anterior tiver sido afirmativa. De que forma a instituição avalia o nível de conscientização sobre segurança cibernética dos funcionários?
8. Como as equipes de segurança e liderança executiva se mantêm actualizadas sobre a evolução das tendências regulatórias de segurança cibernética?
9. Existe uma instituição terceira responsável pelo gestão de riscos de Segurança Cibernética do INTIC?
10. O que acha que torna um sistema vulnerável a ataques cibernéticos?

Respostas das perguntas

A entrevista foi dirigida ao Técnico de TIC no Engº. Helder Fernando.

1R: Actualmente existe uma segurança física no INTIC, para poder ter acesso a instituição deve ter permissão, através câmeras de vigilância CCTV faz-se a monitoria física da instituição. A nível lógico através da utilização de *firewalls* de análise de trafego, faz-se monitoria do que os usuários acessam utilizando a rede do INTIC. Utiliza-se um IDS (*Intrusion Detection System*).

Um dos objectivos a ser atingido pelo INTIC é a implementação de CSIRTs, o INTIC deverá estabelecer um CSIRT Nacional para regular CSIRTs sectoriais.

Ainda não há uma política de Segurança Cibernética Interna no INTIC, mas a sua implementação é urgente.

Para atingir esses objectivos deve-se realizar uma capacitação do pessoal.

2R: Desde 2018 o projecto iniciou mas houve problemas no antigo Sistema de Certificação Digital, não existia a capacidade de recursos humanos, dificuldade na retenção de quadros e o sistema não possuía muitas formas de utilização, sendo este baseava-se no uso de *Tokens* (Sistemas tradicionais) em que devia-se instalar o *software* no computador para poder usar enquanto que novo sistema existe a possibilidade do uso de *Tokens*, de *SmartCards* e telemóveis.

3R: Os maiores desafios são:

- Recursos humanos altamente qualificados;
- Retenção de quadros no INTIC;
- Inclusão de diferentes usuários para utilização do sistema (em que na identidade electrónica haverá múltiplos atributos para autenticação).

4R: Sim existem.

5R: O decreto do SCDM (documento utilizado para credibilizar o sistema) e o DPC (Declaração de Práticas de Certificação e Políticas de Certificados da Autoridade Certificadora Raiz do Estado de Moçambique) da AC Raiz.

6R: Não existe.

7. (Não tem resposta pois a questão 6 não foi afirmativa)

8R: Através de intercâmbios de Segurança Cibernéticas e grupos de trabalho, existe um grupo no *Whatsapp* em que as informações são disseminadas.

9R: Ainda não terceiriza serviços. O objectivo é que os próprios funcionários saibam o fazer por si só.

Anexo 3: Guião do Questionário

1. Já fez parte dum projecto de um projecto terminado de implementação dum Sistema de Certificação Digital

i. Sim

ii. Não

2. Possui conhecimentos dos procedimentos necessários para gestão de um Sistema de Certificação Digital?

i. Sim

ii. Talvez

iii. Não

3. Possui Conhecimento dos tipos de ataques feitos em Autoridades de Certificação?

i. Sim

ii. Não

4. Já participou no processo de recuperação ou defesa de um incidente cibernético?

i. Sim

ii. Não

5. Possui formação técnica na área da segurança de Sistemas de Certificação Digital?

i. Sim

ii. Não

Resultados do Questionário

Figura 21: Classificação em termos de participação de um projecto terminado dum SCD

Fonte: Elaborada pelo autor

Figura 22: Classificação em termos do conhecimento dos procedimentos necessários para a gestão de um SCD

Fonte: Elaborada pelo autor

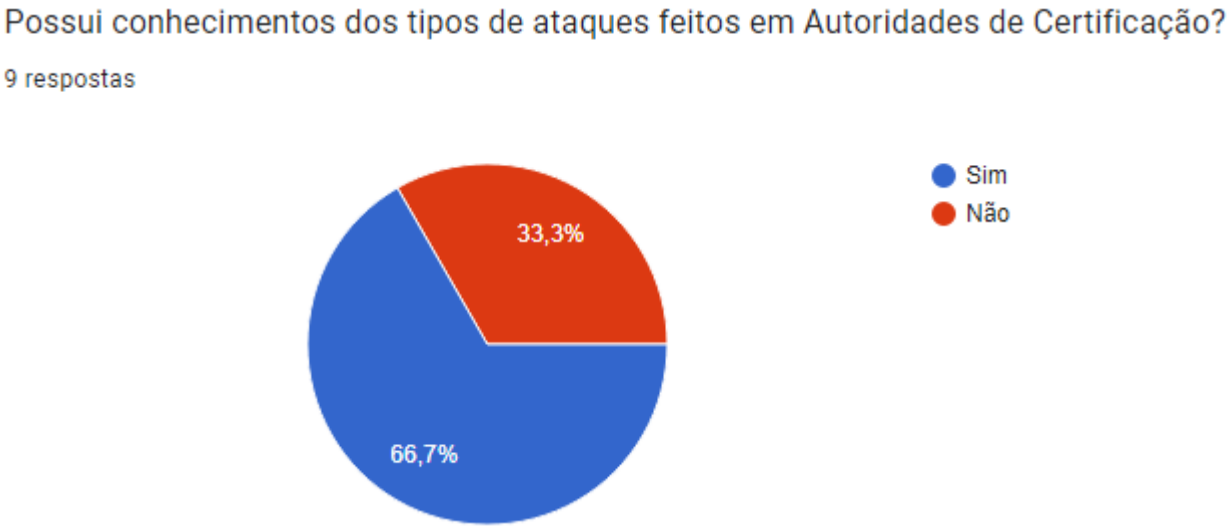

Figura 23-3: Classificação sobre o conhecimento dos tipos de ataques feitos ACs

Fonte: Elaborada pelo autor

Figura A3-4: Classificação sobre a participação de um processo de recuperação ou defesa de um incidente cibernético

Fonte: Elaborada pelo autor

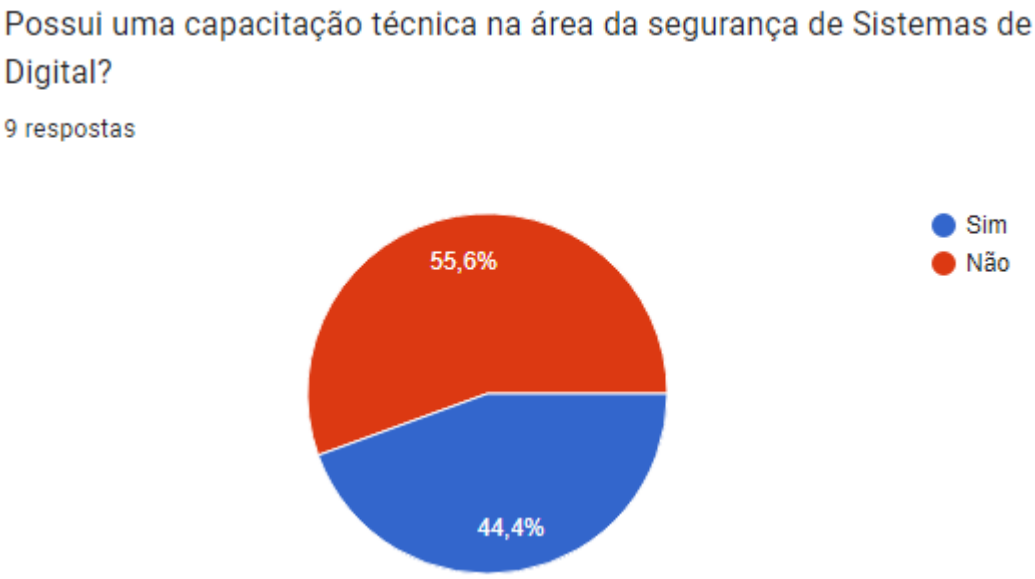

Figura 24: Classificação sobre a capacidade técnica na área de segurança em SCD

Fonte: Elaborada pelo autor

Anexo 4: Guião de Observação (Limite de Risco)

As questões abaixo foram obtidas na ferramenta de gestão de riscos SART (2017), com vista a auxiliar empresas na elaboração de planos de gestão de riscos nos projectos. As questões servem de guia para o cálculo da criticidade do projecto, da capacidade de resposta a crise e do limite do risco como definido no Capitulo IV sobre a Proposta de Solução.

1. Este projeto está fornecendo serviços que salvam vidas?
   a. Não
   b. Sim
2. Este projeto está a dar um contributo valioso para o programa da organização nesta área?
   a. Não
   b. Sim
3. Este projeto não é essencial para o trabalho contínuo da organização nesta área.
   a. Não
   b. Sim
4. Planos gerais de contingência estabelecidos em uma política de segurança global ou similar?
   a. Não
   b. Sim
5. Planos de contingência específicos estabelecidos em um plano de segurança para este projecto?
   a. Não
   b. Sim
6. Um gestor de segurança ou ponto focal de segurança.
   a. Não
   b. Sim
7. Apoio no país que pode ser chamado para ajudar em um incidente ou crise grave?
   a. Não
   b. Sim

8. Seguro de viagem médico e de resposta a crises?
    a. Não
    b. Sim
9. Um plano de gestão de crise?
    a. Não
    b. Sim
10. Uma equipe de gestão de crises?
    a. Não
    b. Sim
11. A equipe de gestão de crises concluiu pelo menos uma simulação de crise?
    a. Não
    b. Sim
12. Recursos financeiros reservados para uma crise ou facilmente acessíveis, se necessário.
    a. Não
    b. Sim

Criticidade do Projecto: Critico

Capacidade de Resposta a Crise: Moderada

Limite de Risco: 12

As respostas foram representadas em negrito. Os parâmetros identificados acima foram calculados tendo em conta as questões apresentadas acima.

Anexo 5: Protótipo do SCDM

Conforme publicado no *website* protótipo do SCDM, o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) em parceria com o Laboratório de Segurança em Computação (LabSEC) elaborou o projecto piloto de Infraestrutura de Certificação Digital e Identidade Electrónica com o objetivo não só de promover uma discussão sobre segurança da informação, mas também com o intuito de prover uma demonstração prática dos usos e benefícios de tais tecnologias.

Conforme Schardong et al. (2021), o Provedor de Identidade Electrónica de Moçambique PIE utilizado é o *Keycloak*, uma solução de código aberto e gratuita mantida pela *Red Hat*. Os dois serviços que disponibilizamos foram construídos em *Python* 3 e se conectam ao provedor de identidade através dos protocolos *OAuth* 2.0 e *OpenID Connect*, que são os padrões de facto utilizados internacionalmente para lidar com identidade electrónica.

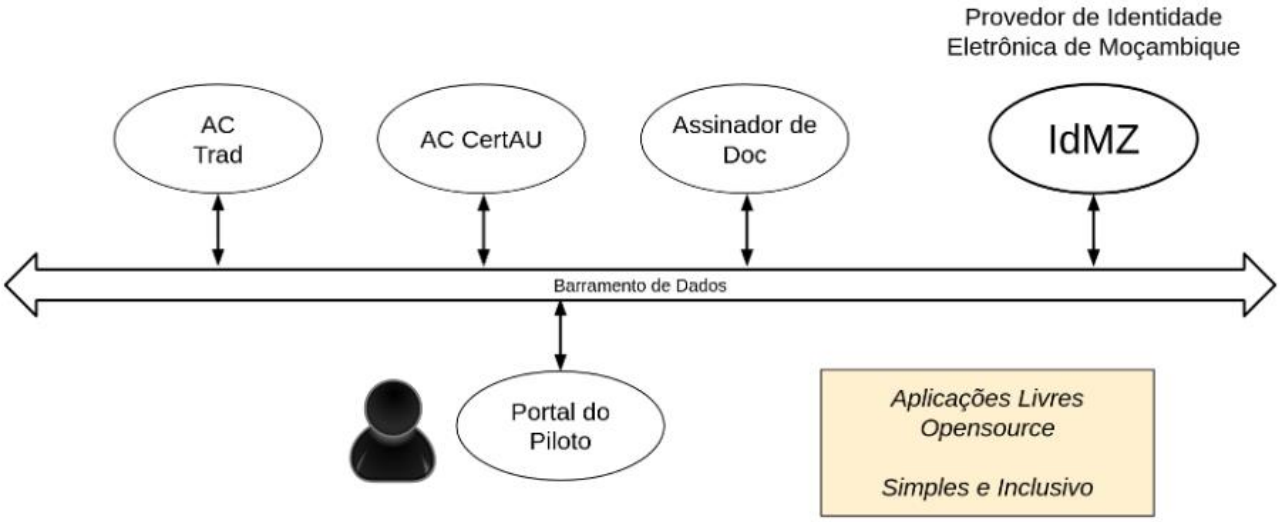

Figura 25: Arquitectura do protótipo do SCDM

Fonte: INTIC (2022)

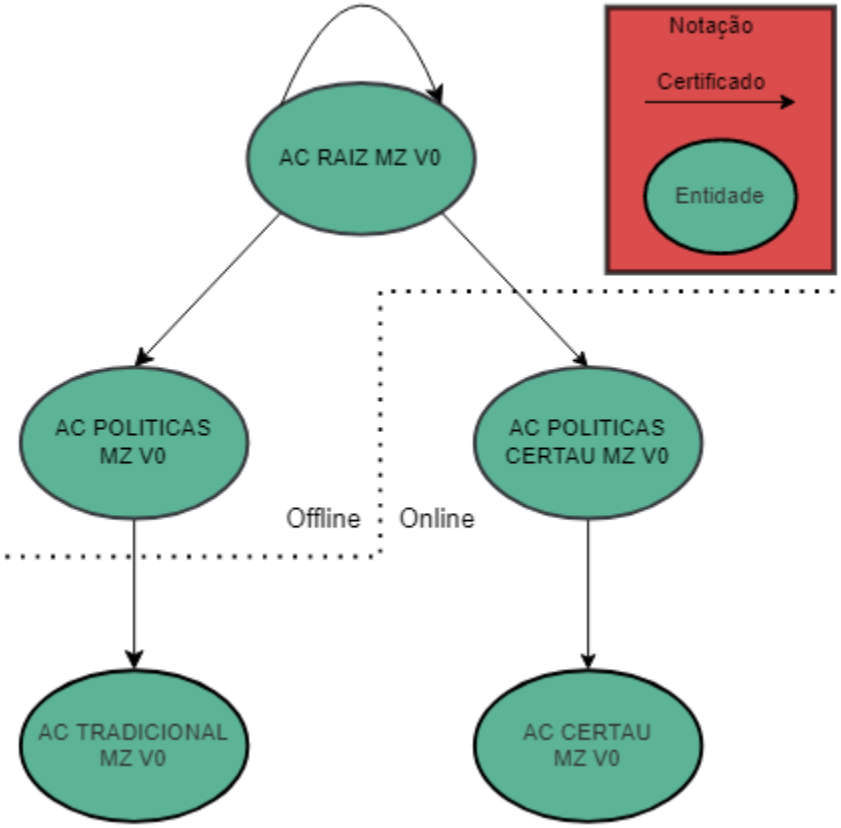

Figura 26: Cadeia de Certificados do protótipo do SCDM

Fonte: INTIC (2022)

Este protótipo conta com duas cadeias diferentes, uma tradicional que reflete como certificados são usados normalmente e uma cadeia que faz a emissão de certificados atrelados a apenas um documento, e portanto, chama-se este certificado de assinatura única (CertAU).

CertAU – de acordo com Schardong et al. (2021) são certificados com o formato X.509, esse certificado possui uma extensão não critica que contem *hash* (resumo criptográfico) do documento electrónico que é assinado utilizando esse certificado digital. Com esse certificado cria-se uma relação de unicidade pois cada certificado é capaz de assinar apenas um único documento. Nesse caso o *hash* do documento assinado e o *hash* do CertAU são diferentes, o que faz com a assinatura seja invalidada.

AC Tradicional – essencialmente o certificado é genérico, o usuário pode assinar um número ilimitado de documentos por um período de tempo definido. A desvantagem desse modelo é a segurança pois não se sabe se a AC ou a AR estão guardando os certificados

dos usuários finais, nesse caso deve existir uma confiança entre o usuário final e a AC (se a AC está ou não utilizando o certificado do usuário).

Figura 27: Aplicações do protótipo do SCDM

Fonte: INTIC (2022)

Ao acessar a página inicial do protótipo disponível em https://mz.labsec.ufsc.br/ são visualizadas as três aplicações acima, que segundo informações disponibilizadas no mesmo protótipo visam:

- **Criar uma Identidade Electrónica:** A criação de um identidade electrónica permite aos utilizadores usufruir dos serviços de (1) Assinatura digital de documentos e (2) Emissão de Certificados. Caso o utilizador já tenha criado a sua identidade electrónica no provedor de identidade mas não esteja autenticado, deverá fornecer seu e-mail e senha previamente cadastrados.
- **Assinatura Digital de documentos PDF:** Uma das possíveis aplicações dos certificados emitidos por uma ICP é a assinatura digital de documentos. No protótipo, uniu-se a assinatura digital de documentos em PDF com a proposta de ICP e identidade electrónica. A ICP é composta por duas Autoridades Certificadoras (ACs) que estão sempre online emitindo certificados, a AC Tradicional MZ V0 e a AC CertAU MZ V0. Enquanto a primeira é utilizada para emissão de certificados tradicionais para qualquer uso e de duração de 5 anos, a segunda emite certificados de duração de 30 anos e deve ser usada para propósitos específicos, como a assinatura digital de documentos. O sistema emite um certificado de assinatura única utilizando as informações provenientes da identidade electrónica do utilizador autenticado, assinará o seu documento com este

certificado e descartará a chave-privada. Pode-se verificar a assinatura digital com, por exemplo, o *Adobe Reader*. Entretanto, como a ICP será vista como desconhecida nos dispositivos dos utilizadores, o *Adobe Reader* não confiará na assinatura. O utilizador precisará adicionar nossa AC RAIZ MZ V0 como uma entidade confiável.

- **Emissão de certificados:** O certificado será criado dentro da ICP proposta neste protótipo pela AC Tradicional MZ V0 e será baixado pelo navegador no formato PKCS #12[11].

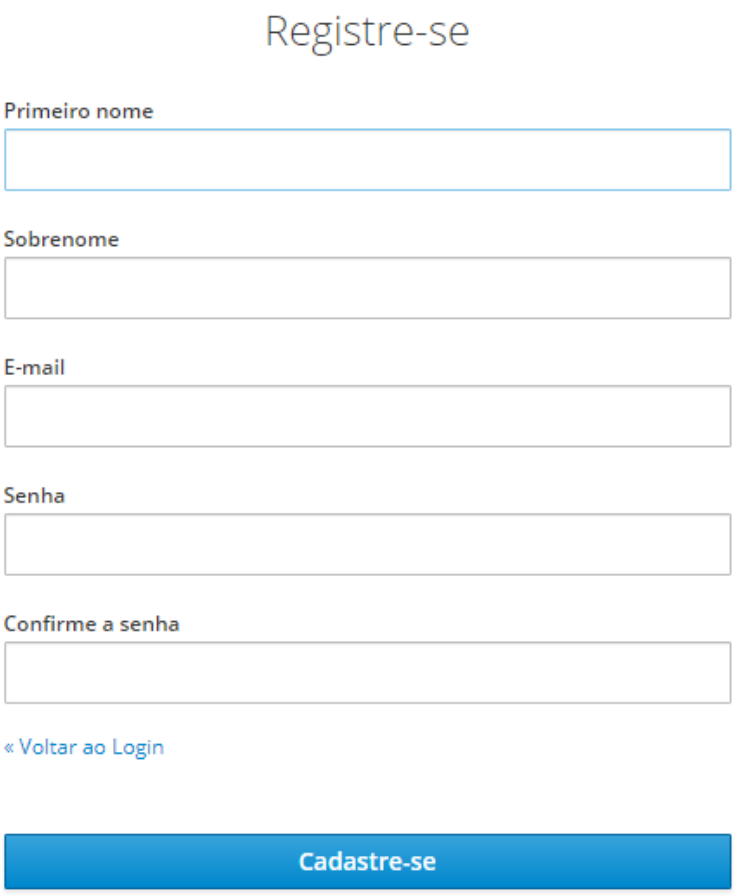

Figura 284: Formulário de registo de utilizadores

Fonte: INTIC (2022)

[11] Formato utilizado para armazenar objectos criptográficos num único ficheiro.