Universidade de Évora - Escola de Ciências e Tecnologia

Mestrado em Engenharia Informática

Dissertação

Projeto de Melhoria da Segurança da Infraestrutura de TI e Capacitação Técnica para Autoridade Tributária de Moçambique

Joao Manuel Uamba

Orientador(es) | Salvador Abreu

Pedro Patinho

Évora 2024

Universidade de Évora - Escola de Ciências e Tecnologia

Mestrado em Engenharia Informática

Dissertação

Projeto de Melhoria da Segurança da Infraestrutura de TI e Capacitação Técnica para Autoridade Tributária de Moçambique

Joao Manuel Uamba

Orientador(es) | Salvador Abreu

Pedro Patinho

Évora 2024

A dissertação foi objeto de apreciação e discussão pública pelo seguinte júri nomeado pelo Diretor da Escola de Ciências e Tecnologia:

Presidente	|	Teresa Gonçalves (Universidade de Évora)
Vogais	|	Lígia Maria Ferreira (Universidade de Évora) (Arguente) Pedro Patinho (Universidade de Évora) (Orientador)

Évora 2024

Projeto de Melhoria da Segurança da Infraestrutura de TI e Capacitação Técnica para Autoridade Tributária de Moçambique

João Manuel Uamba

Trabalho de dissertação apresentado à Universidade de Évora como requisito para obtenção do grau de Mestrado no Curso de Mestrado em Engenharia Informática.

Orientadores:

Salvador Abreu

Pedro Patinho

Évora 2023

AGRADECIMENTOS

Este trabalho foi desenvolvido numa fase de muitos desafios na minha vida profissional o que fazia com que muitas tarefas fossem adiadas ou prolongadas para além do período programado. Para chegar ao fim foi necessário a contribuição de várias pessoas às quais gostaria neste momento de endereçar o meu profundo agradecimento.

Endereço agradecimento especial a minha amada esposa, Belmira Uamba, pelo suporte nos momentos difíceis e compreensão nas horas de solidão enquanto eu me dedicava ao trabalho.

Aos meus colegas de profissão pelo encorajamento e cobertura nas várias vezes em que estive ausente para investigar e pelo contributo no refinamento da redação, o meu muito obrigado.

RESUMO

Esta pesquisa é desenvolvida em resposta à manifesta necessidade de reforçar a segurança da infraestrutura de tecnologias da informação na Autoridade Tributária de Moçambique, configurando-se num instrumento de base para implementação prática. Não obstante os esforços empreendidos, as informações inerentes à situação das tecnologias de informação e comunicação revelam lacunas na implementação de medidas para uma efetiva gestão do risco e alinhamento da tecnologia com o negócio da instituição. Para reversão do cenário apresentam-se medidas de segurança (confidencialidade, integridade e disponibilidade da informação, formação e outros) baseadas nas boas práticas internacionalmente testadas e aprovadas para infraestruturas críticas, considerando o plano estratégico institucional e a realidade económica do país. Pese embora o otimismo em relação aos resultados alcançados, o trabalho tem potencial de servir de base para estudos complementares que se julguem de mais valia para uma resposta holística aos problemas de TI na organização.

Palavras-chave: informática; segurança; infraestrutura; tecnologia; informação.

ABSTRACT

PROJECT FOR IT INFRASTRUCTURE SECURITY IMPROVEMENT AND TECHNICAL TRAINING FOR THE MOZAMBIQUE REVENUE AUTHORITY

This research is developed in response to the clear need to reinforce the security of the information technology infrastructure in the Mozambique Revenue Authority, becoming a basic instrument for practical implementation. Despite the efforts undertaken, the information inherent to the situation of information and communication technologies reveals gaps in the implementation of measures for effective risk management and alignment of technology with the business. To reverse the scenario, security measures are presented (confidentiality, integrity and availability of information, training and others) based on internationally tested and approved good practices for critical infrastructures, considering the institutional strategic plan and the country's economic reality. For all the optimism regarding the results achieved, the work has the potential to serve as a basis for additional studies that could be considered of added value for a holistic response to IT problems in the organization.

Keywords*: computing; security; infrastructure; technology; information.*

ÍNDICE

LISTA DE SIGLAS E ABREVIATURAS

AT	Autoridade Tributária de Moçambique
ATAF	Fórum Africano das Administrações Fiscais Africanas
CSIRT	*Computer Security Incident Response Team* (Equipa de Resposta a Incidentes de Segurança)
ENSC	Estratégia Nacional de Segurança Cibernética
GovNet	Rede Electrónica do Governo
INAGE	Instituto Nacional de Governo Electrónico
INCM	Instituto Nacional das Comunicações de Moçambique
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
OMA	Organização Mundial das Alfândegas
PESI	Plano Estratégico para a Sociedade de Informação
PNSC	Política Nacional de Segurança Cibernética
SADC	*Southern African Development Community* (Comunidade de Desenvolvimento da África Austral)
SDWAN	*Software defined wide area network* (Rede de longa distância definida por software)
TI	Tecnologia de Informação
TIC	Tecnologias de Informação e Comunicação
UTICT	Unidade Técnica de Implementação da Política de Informática

1 INTRODUÇÃO

A revolução no sector das tecnologias veio trazer mudanças inquestionáveis na vida das pessoas e das organizações, forçando a transformações das mentes e cultura para um melhor proveito das potencialidades que as mesmas trazem para o cotidiano. Hoje é inimaginável desenvolver qualquer atividade sem recurso às tecnologias, ainda que no mais básico elas estão sempre presentes. Um dos ramos da tecnologia que em muito impulsiona esta revolução é sem dúvida a área das tecnologias de informação, que vem criando novas tendências e disrupções no seio das organizações e da sociedade criando novas formas de ser e estar que ao mesmo tempo desafiam a todos a mudanças profundas e irreversíveis. Segundo Atieh (2021), mais do que nunca as organizações tornaram-se mais dependentes da informática e das telecomunicações para o seu funcionamento. Esta revolução tem influenciado todos os sectores da sociedade, governos, organizações público-privadas a se reinventarem e criar novas formas de maximizar as suas atividades, desde comerciais às recreativas com geração de conexões e quantidades de dados jamais imagináveis. Este crescimento da tecnologia desde cedo vem dividindo opiniões sobre os benefícios versus os males que podem advir da adoção das tecnologias de informação, sobretudo quando se fala do uso abusivo assim como consequências inerentes aos malfeitores que se fazem desta para alcançar objetivos ilícitos prejudicando aos demais. Ainda assim, os benefícios mostram-se imensuráveis, de tal forma que os serviços digitais públicos e privados vieram para ficar.

Como referido por Oliveira (2022) todas as gerações são relevantes para o mercado, mas a Geração Z ou geração digital é naturalmente mais conectada e isso certamente não só impacta, mas também influencia os diversos setores, já que vivemos em um mundo cada vez mais integrado virtualmente. Esta geração demanda que as tecnologias de informação estejam presentes em todos os locais onde se dirigem e que literalmente tudo seja provido por meios digitais, aumentando assim a convicção de que a adoção do digital é essencial para a subsistência das organizações. Visto que nem tudo é "um mar de rosas" os riscos devem ser devidamente endereçados para que se evite o comprometimento ou perda dos ativos das organizações, com particular destaque para os governos que estão cada vez mais a envidar esforços para que as suas infraestruturas de tecnologias de informação sejam robustas o suficiente no que refere a confidencialidade, integridade e disponibilidade protegendo assim as suas economias, a sociedade e a soberania no geral.

A Autoridade Tributária de Moçambique (AT), um órgão de suma importância na prestação de serviços público, críticos e estratégicos do governo moçambicano, pressionada com esta nova realidade adicionou à sua carteira um projeto amplo de modernização da infraestrutura tecnológica com o objetivo maior de se colocar na vanguarda no que respeita à satisfação do cidadão por meio de serviços seguros e de qualidade. Os desafios são enormes, tendo em conta a conjuntura nacional assim como internacional que tornam o setor das finanças públicas e seus utentes apetecíveis para ataques. Portanto, o presente trabalho procura contribuir com soluções que concorram para a melhoria da segurança na componente da infraestrutura de TI tendo a formação do capital humano como um dos fatores críticos de sucesso. Esta é uma forma de dar resposta às diversas inconformidades de segurança que são relatadas e que inquietam a sociedade moçambicana que se beneficia dos serviços da AT assim como aos membros das organizações nacionais e internacionais onde a instituição está filiada.

1.1 Problematização

Moçambique é um país em vias de desenvolvimento e como tal depende de apoio externo para o orçamento do estado. Este apoio é efetuado por parceiros internacionais que muitas vezes ditam onde e como os valores devem ser aplicados. O governo tem vários desafios prioritários, que vão desde investimentos, segurança até sociais como a saúde, a educação e o transporte. Atualmente o governo depara-se com uma urgência em dar resposta às necessidades de fortalecimento da segurança da informação que se vislumbra onerosa. É nesse contexto que se levanta a seguinte questão:

Como é que a AT pode se robustecer em matérias de segurança de TI para fazer face à crescente onda de ataques cibernéticos que ameaçam as infraestruturas críticas do governo, concretamente as instituições ligadas às finanças públicas num período de contenção de recursos financeiros?

1.2 Justificativa

A nova conjuntura exige que os serviços providos pelas instituições da administração pública sejam disponibilizados por via eletrónica e estas instituições trabalham no sentido de adequar os seus serviços de forma que sejam providos por estes canais. Esta filosofia está a ser seguida pela Autoridade Tributária de Moçambique como um movimento de todo o governo moçambicano. Todavia apesar de existirem iniciativas a serem levadas a cabo sente-se que muito ainda há que possa ser feito para dinamizar este processo. O mais recente ataque cibernético à rede eletrónica

do governo de moçambique e ao mais antigo provedor de serviços de Internet, ambos registados e tornados públicos no ano 2022, veio colocar em causa a resiliência dos sistemas em uso, um cenário que se torna deveras preocupante pelo facto do país encontrar-se em combates contra o terrorismo que eclodiu na região norte, sendo de prever que as ações nefastas perpetradas por via militar tarde ou cedo possam evoluir para uma guerra cibernética passando os malfeitores a fazer ofensivas com inestimáveis prejuízos ao estado e a soberania do país.

1.3 Objetivos

O presente trabalho pretende propor soluções e boas práticas a serem implementadas na infraestrutura de TI da Autoridade Tributária de Moçambique que concorram para o aumento da disponibilidade de serviços, integridade e confidencialidade na comunicação de dados quer dentro da instituição assim como na comunicação de e para o exterior.

Para tal são listados os seguintes objetivos específicos:

- Avaliar o nível de segurança na infraestrutura de tecnologia de informação e identificar as oportunidades de melhoria;
- Identificar as soluções de segurança de redes de comunicação de dados que melhor se adequam para a proteção dos ativos da instituição;
- Identificar uma estratégia de formação do quadro técnico e dos utilizadores a todos os níveis em matérias de segurança da informação.

2 METODOLOGIA

Em sua essência este trabalho compreende a apresentação de uma base sólida a partir da qual se possa aplicar na prática para a resolução do problema levantado que é verificado em uma organização concreta, no caso a Autoridade Tributária de Moçambique, no que concerne a necessidade de melhorar a segurança da sua infraestrutura de TI.

A primeira fase do trabalho consistiu em uma pesquisa bibliográfica e observação direta, fruto do trabalho que o autor desenvolve, levada a cabo durante o período de leccionamento a fim de apresentar o estudo do caso. De acordo com Gil (2002) esse levantamento bibliográfico preliminar pode ser entendido como um estudo exploratório. O mesmo teve a finalidade de proporcionar a familiaridade do autor com a área de estudo bem como a sua delimitação.

A fase seguinte compreendeu a revisão bibliográfica com base em livros e trabalhos científicos disponíveis. Parte do material foi disponibilizado e usado durante o curso com mais destaque ao da disciplina de Segurança em sistemas informáticos. Para um melhor enquadramento recorreu-se a revisão documental com a consulta da base legal e normativa aplicada ao sector de TICs na República de Moçambique. Toda a bibliografia e documentação usada para o trabalho foi anteriormente recolhida e selecionada em função da pertinência dos conteúdos para o tema em desenvolvimento.

2.1 Caracterização da Organização em Estudo

A AT é um órgão do estado criado pela Lei n.º 1/2006. A presente lei define como propósito da instituição a cobrança de impostos internos e do comércio externo, sendo, portanto, uma instituição crítica que se rege pela legislação para as instituições públicas e financeiras. A instituição providencia serviços através dos quais o cidadão pode cumprir com suas obrigações fiscais nomeadamente declarar as suas atividades e pagar o imposto; e serviços voltados para administração pública como por exemplo a canalização dos valores coletados aos cofres do estado, neste caso a conta única do tesouro, através da qual é realizada a despesa pública. A AT conta atualmente com um universo de 4000 funcionários, fruto da fusão de duas instituições extintas nomeadamente a Direção Nacional de Impostos e Auditoria (DNIA) que era responsável pela coleta de impostos internos e as Alfândegas de Moçambique que se responsabiliza pela coleta de impostos externos. A unificação da infraestrutura de TI veio a ser finalizada em 2014, isto é, 8

anos depois. Em 2015 é criado o plano estratégico que incorpora as TICs como um dos fatores estratégicos para tornar a AT numa referência internacional na arrecadação de receita. No apêndice A é apresentada uma ilustração sobre a presença da AT no território moçambicano assim como a topologia de ligação entre as principais unidades. Na ilustração é compreensível que os serviços são centralizados na capital do país, Maputo e todas as comunicações fluem de cada província para a capital e vice-versa. Na sua estrutura orgânica a instituição conta com uma direção de tecnologias de informação e comunicação (DTIC) cuja missão é velar por todas as matérias ligadas às TICs dentro da organização. Esta direção contempla 4 divisões centrais, nomeadamente, divisão de infraestrutura tecnológica, divisão de sistemas aplicacionais, divisão de segurança da informação e sistemas e a divisão do centro de dados. Esta direção está representada nas três regiões do país (sul, centro e norte) através de repartições regionais que prestam o suporte técnico às 11 províncias do país. O apêndice B do presente trabalho, apresenta a estrutura orgânica da DTIC com a ilustração dos sectores assim como a distribuição dos profissionais de TICs, num total de 31 técnicos.

2.2 Opções para Coleta e Tratamento dos Dados

A recolha dos dados acorreu entre os dias 1 a 5 de Setembro de 2023 com recurso à entrevistas e inquéritos aos colaboradores no sector das TICs. As entrevistas foram direcionadas ao diretor das TICs e ao chefe da divisão da segurança da informação e os inquéritos por questionário aos técnicos da área. Esta abordagem visava responder a cada objetivo específico do trabalho. Com as entrevistas pretendia-se a radiografia ao alto nível da situação atual e uma perspetiva futurista da organização. Por sua vez, os inquéritos viriam ajudar a ter uma visão técnica sobre a segurança da informação e as necessidades de formação. Para acomodar estes dois objetivos técnicos foram usados dois formulários de inquérito, um que visava a todos os profissionais de TI (formulário geral) e um direcionado exclusivamente aos profissionais das redes e comunicações – alvo principal no que respeita à segurança da infraestrutura de TI.

Optou-se pela criação de questionário de inquérito geral destinado a todos os profissionais de TICs pelos seguintes motivos:

- ✓ Há um número reduzido e insuficiente de quadros de TI (31 profissionais para um universo de 4000 funcionários e 10 províncias). Observou-se que os chefes das divisões e repartições também realizam trabalhos técnicos;

- ✓ Na divisão de segurança da informação, para além do chefe (entrevistado) existe apenas um técnico e o mesmo foi alocado recentemente;
- ✓ O nível de domínio das matérias sobre a segurança da informação entre os técnicos das províncias e da sede é muito desproporcional;
- ✓ O estudo não visava inquirir os utilizadores, portanto, pretendia-se ter a sensibilidade dos técnicos em relação ao nível de preparação dos utilizadores em matérias de segurança da informação.

Como referido foram realizadas duas entrevistas e no caso estruturadas. A opção de criar dois formulários deveu-se ao fato de se pretender dialogar com o diretor das TICs aspetos mais voltados à governança da segurança da informação. Já com o chefe da divisão de segurança pretendia-se debruçar sobre a gestão da segurança da informação. Os guiões da entrevista assim como os questionários de inquérito podem ser visitados do apêndice C à F.

Os inquéritos foram realizados recorrendo às plataformas eletrónicas devido às vantagens e a facilidade de acesso aos visados tendo em conta a dispersão geográfica dos mesmos. Os formulários foram criados no *Google Forms* e os links foram partilhados por correio eletrónico e pelo *whatsApp*.

É de salientar a realização de visitas ao Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) e Instituto Nacional de Governo Eletrónico (INAGE) no âmbito da apresentação da execução do plano de implementação das equipas de resposta a incidentes de segurança (CSIRT) nacional e do governo, respetivamente. Durante as visitas o autor teve a oportunidade de tomar notas de diferentes aspetos relevantes no seu diário de observações. Estas notas tiveram uma contribuição significativa para o processo de recolha de dados assim como na consideração de mais elementos de pesquisa importantes para o enriquecimento do trabalho.

A fase final compreendeu a análise dos dados e apresentação dos resultados da pesquisa. Para a análise dos dados seguiu-se o método combinado, isto é, analisou-se parte dos dados de forma quantitativa e outros de forma qualitativa. A partir dos resultados foi possível tecer as conclusões do trabalho e melhor elaborar as recomendações para a organização.

3 REVISÃO DA LITERATURA

3.1 Quadro regulatório das TICs em Moçambique

O Instituto Nacional de Tecnologia de Informação e Comunicação (INTIC) é um órgão do estado criado através do Decreto n.º 9/2011, segundo o qual, a competência inicial desta instituição era regular o sector das TICs bem como implementar e operacionalizar todos os sistemas do governo no âmbito da implementação da rede do governo eletrónico. O mesmo decreto extinguiu a Unidade Técnica de Implementação da Política de Informática (UTICT) que operava desde 2002, criada pelo Decreto n.º 50/2002, que simplesmente era um órgão técnico que devia prestar apoio à então Comissão para a Política de Informática na realização das suas funções. A extinção da UTICT e criação do INTIC visava melhorar a prestação de serviços públicos e da governação.

Segundo o Decreto n.º 60/2017, na necessidade de dinamizar ainda mais o sector de TICs face às novas realidades e novos desafios do governo são atualizadas as atribuições do INTIC, passando as suas competências a cingir-se na regulação, supervisão e fiscalização do sector das TICs no país. Para a segunda componente, isto é, implementação e operacionalização é criado pelo Decreto n.º 61/2017, o Instituto Nacional de Governo Eletrónico (INAGE) cuja atribuição é elaborar e implementar soluções tecnológicas transversais para a administração pública e prestação de serviços de governação eletrónica (GovNet). A partir deste momento pode se dizer que o país assiste uma aceleração no que compreende as TICs pois de um lado tem-se uma entidade que vela pela regulamentação e fiscalização do sector a nível nacional podendo de entre outras auditar qualquer sistema de informação e TICs público assim como privado, enquanto o INAGE se dedica a operacionalização e interligação das infraestruturas do governo.

3.1.1 Regulamento do domínio ".mz"

Em Moçambique todos os nomes de domínio são registados tendo como raiz ".mz" tanto para pessoas singulares assim como coletivas, públicas ou privadas. O Decreto n.º 82/2020 determina os termos e condições aplicáveis à gestão, reserva e registo de nomes sob o domínio de Internet ".mz", isto é, no espaço da Internet cuja gestão é da responsabilidade de Moçambique, bem como o estabelecimento de direitos e deveres inerentes ao licenciamento dos agentes de registo. Esta lei remete à entidade reguladora, para o caso o INTIC, a definição e publicação das políticas de gestão de dados pessoais.

3.1.2 Lei das telecomunicações

Estabelecida pela Lei n.º 4/2016, aplicável às pessoas singulares e coletivas licenciadas para o estabelecimento, gestão e exploração de redes e serviços de telecomunicações definindo as bases gerais por forma a manter o mercado liberalizado num ambiente de concorrência e de convergência de redes e serviços.

Esta lei remete ao regulador do sector, o Instituto Nacional das Comunicações de Moçambique (INCM), as funções de regulação, supervisão e fiscalização. Por se tratar de um imperativo a lei reserva um capítulo (VIII) para debruçar sobre os deveres que os operadores devem seguir para assegurar qualidade dos serviços e proteção do consumidor, obrigando adoção de medidas necessárias para garantir a segurança e a integridade do funcionamento das redes e serviços e assegurar, sempre que possível, alternativas para a sua disponibilidade em situações de emergência e de casos fortuitos ou de força maior.

3.1.3 Lei das Transações Eletrónicas

É a partir da aprovação da Lei n.º 3/2017, de 9 de janeiro, que versa sobre as transações eletrónicas que se assiste a uma nova abordagem no que se refere ao quadro legal e regulatório atual sobre as TICs em Moçambique. Esta lei normatiza o quadro jurídico para todas as transações eletrónicas, incluindo o comércio eletrónico e o governo eletrónico e extingue todas as demais legislações sectoriais e ou contrárias que inclui alguns artigos da já mencionada Política de informática. Segundo o art. 2º da Lei n.º 3/2017, ela é uma lei de referência e aplica-se a pessoas singulares, coletivas, públicas ou privadas que apliquem tecnologias de informação e comunicação nas suas atividades.

Nesta lei podemos encontrar as diretrizes para a gestão do espaço de Internet tutelado pelo governo de Moçambique (domínio ".mz") bem como as normas para o registo de nomes de domínios. Ao governo está reservado o subdomínio ".gov.mz" abaixo do qual são registadas as instituições do governo e devem ser trocadas as informações deste, estando vedado o uso de qualquer outro subdomínio. O instrumento define as balizas para a troca de mensagens de dados e comunicações eletrónicas estabelecendo os requisitos para, de entre outras, a escrita, transmissão, receção e conservação que estas devem obedecer. A lei trata ainda de aspetos inerentes à certificação digital e criptografia, proteção de dados eletrónicos pessoais que devem ser confidenciais e usados apenas para os objetivos especificados antes da sua recolha.

3.1.4 Lei sobre a Sociedade da Informação

O governo de moçambique criou a Política para a sociedade de informação através da Resolução n.º 17/2018 do Conselho de Ministros no qual é presente um quadro de princípios que concorrem para permitir que as TICs se assumam como uma alavanca para o desenvolvimento económico e social do país objetivando no seu final a modernização do aparelho do Estado e da prestação de serviços ao cidadão.

O plano estratégico vem ser aprovado pela Resolução n.º 52/2019, que estabelece as prioridades de desenvolvimento da sociedade da informação para um horizonte temporal 2019-2028 do qual constam de entre várias, 4 iniciativas sobre a alçada da Autoridade Tributária de Moçambique: Sistema de Pagamento de Impostos (e-Tributação), Portal do Contribuinte, Central de Atendimento ao Contribuinte e o Sistema de Gestão de Máquinas Fiscais.

Segundo a política para a Sociedade da Informação, o desenvolvimento da sociedade de informação alavancada pela utilização de tecnologias de informação e comunicação tem inúmeras vantagens e simultaneamente riscos que devem ser acautelados.

3.1.5 Política de Segurança Cibernética

No cumprimento da estratégia do governo aliado à necessidade de cumprir os acordos regionais nomeadamente recomendações emanadas na 14ª sessão ordinária da Cimeira dos chefes de Estado e de Governo da União Africana e a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, Moçambique aprova através da Resolução n.º 69/2021, a política da segurança cibernética e a estratégia da sua implementação, que de entre outras reconhece a importância da Infraestrutura de Informação Crítica (IIC), identifica os riscos que ela corre e define a forma de mitigação. Segundo este documento entende-se:

> **Espaço cibernético** ao ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação; e por
>
> **Segurança cibernética** ao conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no espaço cibernético, e das pessoas que nele interagem. Portanto a segurança cibernética inclui todas as medidas legais,

> tecnológicas e processos que visam proteger pessoas, coletivas e singulares e bens com destaque para as infraestruturas críticas de informação no espaço cibernético. (art. 2º, Resolução n.º 69/2021).

A resolução indica que a altura da elaboração e aprovação da política já era preocupante a situação do país em matérias de segurança cibernética onde predominavam os abusos e assédios no espaço cibernético, crimes financeiros, ciberterrorismo e outros crimes informáticos que levaram a que a União Internacional de Telecomunicações (UIT) no seu relatório de 2018, colocasse o país entre os com o pior nível de Segurança Cibernética, nas posições 132 (do total de 175 países) e 26 (de 42 países) para a classificação global e regional respetivamente. Em 2020 a mesma entidade publicou o Relatório do índice global de Segurança Cibernética em que se regista uma ligeira melhoria passando o país para a posição 123, do total de 194 países, no índice global e posição 23, de um conjunto de 44 países, para índice regional, fruto de algumas ações levadas a cabo com o objetivo de fomentar a consciencialização sobre os compromissos das nações em relação à segurança cibernética.

O documento da Política e Estratégia Nacional da Segurança Cibernética enumera 6 pilares sobre os quais se sustenta: I. Liderança e Coordenação; II. Proteção de Infraestruturas Críticas de Informação; III. Proteção de Ativos de Informação; IV. Quadro Legal e Regulatório; V. Desenvolvimento de Capacidade, Pesquisa e Inovação e VI. Cultura de Segurança Cibernética e Consciencialização. Elenca como um dos fatores críticos de sucesso o capital humano e diz: "a implementação eficiente da segurança cibernética requer recursos humanos altamente qualificados em todos os sectores da sociedade. A capacidade das instituições do sector público e privado de obter e reter recursos humanos qualificados é, portanto, importante para manter e garantir uma forte abordagem de proteção contra ameaças cibernéticas, especialmente com operadores de infraestruturas críticas, assim sendo é extremamente importante que o governo invista na formação do capital humano".

3.2 Infraestrutura de Tecnologias da Informação

Segundo Stair e Reynolds (2018) infraestrutura de TI é a coleção de todo o hardware, software, bases de dados, redes e procedimentos que são configurados para a coleta, manipulação, armazenamento e possibilitam o processamento de dados em informação, e que, portanto, formam a fundação para um sistema de informação baseada em computador. O objetivo principal de se ter

uma infraestrutura de TI é poder proporcionar aos utilizadores os serviços e soluções de tecnologias de informação necessários para o dia-a-dia das pessoas assim como das organizações.

Segundo a IBM (2021) existem duas principais formas de infraestrutura de TI, a infraestrutura tradicional e a infraestrutura em nuvem. A principal diferença está na forma como os recursos são disponibilizados e acedidos sendo que a infraestrutura tradicional é implementada no local para uso da corporação, isto é, uso privado enquanto que infraestruturas em nuvem são disponibilizadas por provedores de serviços a partir de diferentes pontos e os clientes acedem aos recursos computacionais via Internet. Os típicos componentes de hardware e software de uma infraestrutura de TI tradicional incluem instalações, centros de dados, servidores, hardware de rede, computadores de mesa e as soluções de software de aplicativos corporativos.

Infraestrutura crítica de tecnologias de informação

Em função do nível de dependência da organização assim como da sociedade em relação aos serviços e soluções tecnológicas para as suas operações diárias e estratégias, a infraestrutura que os suporta pode desempenhar diferentes níveis de importância chegando a ser um fator crítico para as mesmas organizações. No presente trabalho iremos abordar a proteção de infraestrutura crítica por se tratar de uma componente estratégica e fundamental para o governo. Cada país ou grupo de países tem uma definição particular de infraestrutura crítica sendo que no global nenhuma contradiz a outra. Para o caso em alusão iremos trazer duas que são mais próximas do caso de estudo, uma referente a Moçambique e outra sobre a União Africana.

A convenção da União Africana sobre a cibersegurança e proteção de dados pessoais, define infraestruturas críticas de TIC como aquelas que são essenciais aos serviços vitais da segurança pública, estabilidade económica, segurança nacional, estabilidade internacional, bem como para a manutenção e a restauração do ciberespaço.

Na sua política de segurança cibernética, Moçambique define infraestrutura crítica de TI como um subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

Outras definições podiam ser mencionadas como a da União Europeia e outros grupos, mas fica evidente das já apresentadas o quão importante e fundamental é a infraestrutura de TI para as

organizações e sociedade e isto demanda que sejam tomadas medidas concretas e suficientes para operacionalização das mesmas.

3.3 Segurança de Infraestrutura de TI

A tecnologia, quando devidamente configurada e conectada em rede, pode melhorar os processos de *back-office*, aumentar a eficiência e simplificar a comunicação (Atieh, 2021).

Como temos vindo a referir a massiva adoção das TICs fazem emergir novas preocupações referentes à segurança da informação e dos ativos envolvidos neste ecossistema com destaque para os ambientes corporativos onde o impacto é maior. As triangulações, nas quais uma organização A acede às informações de C, por intermédio de sua comunicação com a organização B, é apenas um desses problemas que devem ser tratados. A complexidade de conexões e heterogeneidade do ambiente também devem ser consideradas (Nakamura & Geus, 2007).

A segurança da infraestrutura de TI é o eixo central da estratégia geral de segurança de qualquer organização, pois está no coração de suas operações de tecnologia e pode ser considerada como o plano mestre de segurança da organização, que sustenta as estratégias, táticas e tudo mais que é produzido ao seu redor (Atieh, 2021).

Segundo Andrés, Kenyon e Birkholz (2004) quando se fala de segurança de infraestruturas a nível da rede podemos verificar que aqui se concentram as maiores vulnerabilidades da corporação o que justifica existirem mais métodos para proteção desta camada se compararmos com outras componentes. Não obstante, é importante olhar com o mesmo nível de atenção a outras componentes da infraestrutura de TI para que a segurança seja efetiva. Os escritores Goodrich e Tamassia (2014) realçam a importância de se assegurar as infraestruturas físicas, isto é, colocação de barreiras que limitem o acesso aos recursos computacionais a serem protegidos. Estas barreiras podem ser através do uso de gabinetes técnicos e portas com fechaduras, colocação de computadores críticos em salas ou compartimentos sem janelas ou envolvidos por paredes reforçadas, uso de sistemas de alertas, entre outros. Enquanto isso, Albugmi, Madini, Robert e Gary (2016) alertam para a necessidade de proteção de dados que são trafegados entre o utilizador final e um provedor de serviços por meio de mecanismos de proteção da rede e encriptação de dados. Este recurso é fundamental quando se migra para o uso de serviços baseados na nuvem. Tratando-se de um mundo em que todos estão conectados a todos, deve-se igualmente

salvaguardar que a comunicação entre os provedores assim como serviços que disponibilizam interfaces de programação de aplicações (API) estejam protegidos.

3.3.1 Princípios da segurança da informação

Quando se fala de segurança da informação deve-se ter em vista as medidas a serem tomadas para garantir que seja tirado o maior benefício das tecnologias tendo controlados os riscos que dele advém, como sejam perda de dados, disrupção de serviços, crimes cibernéticos dentre outros males que advêm da adoção das tecnologias de informação. Para cada estado no ciclo de vida da informação existem medidas ou tecnologias de segurança apropriadas, todavia seja qual for o caso, a literatura específica os princípios que determinam que uma informação está segura.

Stallings e Brown (2015) apresentam e explicam os três objetivos chave que são o coração no campo da segurança da informação, a confidencialidade, integridade e disponibilidade apelidos de tríade CIA, em inglês *CIA triad*.

Confidencialidade – para os autores a confidencialidade nos remete a dois conceitos. O primeiro refere-se à confidencialidade dos dados, que assegura que os dados privados e confidenciais não são disponibilizados ou divulgados a indivíduos não autorizados. O segundo termo a que a confidencialidade nos remete é Privacidade. Este assegura que os indivíduos controlam ou têm influência sobre as informações que podem ser coletadas e armazenadas e por quem ou para quem as mesmas podem ser disponibilizadas.

Integridade – este termo segundo Stallings e Brown (2015) nos remetem a dois conceitos. Integridade dos dados que refere a garantia de que as informações e os programas são alterados somente de forma especificada e autorizada. Por outro lado, a integridade dos sistemas garante que os mesmos realizam as funções predefinidas, livre de manipulações inadvertidas ou não autorizadas.

Disponibilidade – assegura que os sistemas funcionam prontamente e que os serviços não são negados aos utilizadores legítimos.

Ainda segundo Stallings e Brown (2015) a tríade CIA completa aquilo que são os alicerces para a segurança da informação, contudo há que considerar dois objetivos que em muitas literaturas são adicionados como sendo suplementares para os princípios da segurança da informação, sendo estes a autenticidade e a contabilidade. Segundos os autores estes podem ser interpretados como:

Autenticidade – refere-se à propriedade de se ser genuíno e poder ser verificado e confiável, sendo a confiança relativa à validade da transmissão, a mensagem ou originador da mensagem. Isto significa verificar se os utilizadores são quem dizem ser e se cada entrada recebida no sistema vem de uma fonte confiável.

Não-repudio – este objetivo de segurança introduz o requisito para que as ações de uma entidade sejam rastreadas de forma exclusiva e sem repúdio a essa entidade. Portanto os sistemas devem manter os registos de suas atividades para permitir análise forense posterior para rastrear violações de segurança ou auxiliar em disputas jurídicas ou de outra natureza. Este requisito tem uma grande relevância pois constata-se e é evidente que sistemas verdadeiramente seguros ainda não são uma meta alcançável.

3.3.2 Ataques à segurança da Informação

De forma simples, um ataque é a exploração de uma vulnerabilidade em sistemas de tecnologias de informação. Assim, para uma efetiva proteção das infraestruturas de TI é fundamental perceber no contexto real as motivações que levam os indivíduos a perpetrar um ataque, perceber os diferentes tipos de ataques e os vetores usados.

3.3.2.1 Motivações para Ataques

Segundo a EC-Council (2021) a motivação para um ataque é originada pela noção de que os sistemas contêm ou processam algo valioso. Os atacantes usam várias ferramentas e técnicas para explorar as vulnerabilidades em sistemas de computadores ou nos controles implementados para suprir as suas motivações. Este mesmo órgão lista 6 das principais motivações:

- ✓ Disrupção da continuidade de negócios das vítimas;
- ✓ Roubo de informação e manipulação de dados;
- ✓ Criar caos e medo ao causar disrupção em infraestruturas críticas;
- ✓ Criar perdas financeiras nos alvos;
- ✓ Destruir a reputação das vítimas.

3.3.2.2 Tipos de ataques

Ainda segundo a EC-Council (2021), os ataques podem ter a seguinte classificação quanto ao seu tipo:

- ✓ Ataques passivos - que não objetivam distorção ou nenhuma interferência apenas monitoram o tráfego na rede e os fluxos de dados no alvo;
- ✓ Ataques ativos – compõem este grupo os que criam distorção/interferência nos dados ou criam disrupção das comunicações ou serviços entre os sistemas para ultrapassar barreiras e atingir os ativos segurados;
- ✓ Ataques de proximidade - acontece quando o atacante está fisicamente nas proximidades com os sistemas ou rede do alvo de forma a coletar, modificar ou criar disrupção no acesso às informações;
- ✓ Ataques internos - envolve o uso de privilégios de acesso para violar as regras ou intencionalmente causar ameaças à informação ou aos sistemas de informação das organizações;
- ✓ Ataques de distribuição/distribuidor – é um tipo de ataque não muito abordado na literatura, que ocorre quando o atacante interfere com o hardware ou software antes da sua instalação, seja na origem ou em trânsito ao destinatário. Podemos incluir o ataque a cadeia de suprimentos em inglês *supply chain attack* que ocorre com alteração do *software* pelo distribuidor oficial ou um *hacker* antes da entrega ao cliente com o objetivo criar futuros distúrbios ao cliente.

3.3.2.3 Vetores de Ataques

Para perpetrar os seus intentos os malfeitores usam diferentes vetores de ataques. Uma definição simples de vetor de ataque é trazida por Goodrich e Tamassia (2014) e refere vetor de ataque como o meio que o atacante usa para ganhar acesso ou injetar um código (*payload*) em um sistema. Neste trabalho iremos apresentar alguns dos mais comuns vetores de ataques resultantes da compilação de alguns mencionados nas diferentes literaturas consultadas:

- ✓ *Cloud computing threats* (Ameaças de computação em nuvem) - num serviço demandado na cloud pode verificar-se uma falha/imperfeição em um cliente e dessa falha outros clientes serem afetados;
- ✓ Ameaças persistentes avançadas, em inglês *Advanced persistent threats* (ATP) - os atacantes focalizam-se em ganhar acesso prolongados à rede e roubar informações dos computadores das vítimas sem que estas tenham noção do mesmo;

- ✓ Vírus e vermes (*vírus and worms*) - são as ameaças que mais prevalecem na rede de computadores. Através destes é possível introduzir e disseminar código malicioso em vários ativos da organização;
- ✓ Ransomware - restringe o acesso a informações e ficheiros da organização e demanda um resgate para restituir os danos;
- ✓ Ameaças a dispositivos móveis (*Mobile Threats*) - a grande adesão a dispositivos móveis para assuntos pessoais assim como negócio e ainda com baixo controle de segurança levou a que aumentassem os ataques a estes dispositivos;
- ✓ Botnet - uma grande rede de sistemas comprometidos que é usado por um invasor para perpetrar vários ataques a redes;
- ✓ Ataque interno (Insider attack) - um ataque perpetrado na corporação, seja na rede ou em apenas um computador, levado a cabo por alguém com acesso autorizado;
- ✓ Phishing - consiste em enviar um falso email fingindo ser originário de onde se diz ser ou de um site legítimo com a intenção de obter informações pessoais ou credenciais;
- ✓ Ameaças para aplicativos baseados na Web (*Web application threats*) - atacantes vitimizam aplicações web para roubar credenciais, construir sites de phishing ou adquirir informações privadas para ameaçar/comprometer a performance do *website* e comprometer a sua segurança;
- ✓ IoT therats - As imperfeições/falhas nestes dispositivos permitem que atacantes ganhem acesso remoto aos mesmos e façam diversos ataques, tornando-se eles mesmos em ameaças para a organização.

3.4 Tecnologias de Segurança de Dados

Para Kistler (n.d.) quando se fala de tecnologias de segurança deve entender-se como as ferramentas e métodos que implementam os protocolos de segurança em uma infraestrutura de TI. Portanto, para que se tenha um sistema de segurança devidamente robusto é necessário combinar diferentes componentes que operem juntos para a proteção dos ativos. Seja qual for o modelo ou o tipo de segurança implementado deve-se sempre ter em vista que a tecnologia de segurança deve assegurar quatro elementos principais: prevenção, dissuasão, deteção e resposta.

Panetta (2016) cita em um artigo publicado na página da Gartner aquelas que considera serem as 10 tecnologias a se ter em conta quando se objetiva a segurança da informação. Desta lista

podemos destacar as que mais impactam a segurança de infraestrutura de TI e melhor se adequam ao caso em estudo: deteção e resposta de *endpoint*, análise comportamental de usuários e entidades, teste de segurança para DevOps, centro de operações de segurança orientado por inteligência e tecnologia de engano.

De Stallings e Brown (2015) podemos listar as seguintes tecnologias de segurança: controle de acesso, Encriptação de dados, Resiliência de dados e backups, Destruição dos dados e Retenção de dados.

3.4.1 Controle de acesso

Este é o mecanismo usado para garantir que somente utilizadores autenticados e autorizados tenham acesso aos recursos. Para Stallings e Brown (2015) o controle de acesso pode ser visto como o elemento central da segurança pois cobre os seus principais objetivos que são de evitar que indivíduos não autorizados tenham acesso aos recursos, prevenir que os utilizadores legítimos não façam o uso inapropriada de recursos e dar acesso aos utilizadores legítimos com base nas políticas da organização.

Quando se fala de autenticação quer se referir à existência de mecanismos de verificação da validade das credenciais do utilizador ou outra entidade enquanto que autorização se refere a atribuição de níveis de privilégios ou direitos a cada entidade durante o acesso a um dado recurso. Para além dos dois elementos mencionados, o terceiro tem a ver com a auditoria. A auditoria está ligada à coleção de informações sobre a utilização de dado recurso. Com base em análises dos registos dos sistemas é possível comprovar se os controles implementados estão de acordo com a política e procedimentos, bem como detetar violações e propor alterações quer nos controles assim como nas políticas.

Várias técnicas vêm sendo recomendadas para aprimorar o controle de acesso como sendo o uso de múltiplos fatores de autenticação, controle de acesso baseado em tarefas em inglês *role-based access control* (RBAC), adoção de princípio de privilégios mínimos, modo a prova de falhas – permite que aos utilizadores recém-criados sejam atribuídos privilégios mínimos.

3.4.2 Deteção e Resposta de Endpoint

A solução de deteção e resposta de *endpoint* permite aos administradores de segurança detetar potenciais brechas de segurança e reagir com flexibilidade. Estas ferramentas coletam eventos dos

dispositivos do utilizador, em inglês designados de *endpoints,* e da rede onde se encontram. A informação coletada é continuamente analisada usando os indicadores de comprometimento conhecidos e técnicas de aprendizado de máquinas, em inglês *machine-learning*, para identificação precoce das violações de segurança.

3.4.3 Análise Comportamental de Utilizadores e Entidades

A análise comportamental de utilizadores e entidades (UEBA do inglês: *User and Entity Behavior Analytics*) fornece análise centrada no utilizador juntamente com informações sobre redes, *endpoints* e aplicativos. A correlação dessas análises oferece deteção de ameaças mais eficaz e precisa.

3.4.4 Teste de Segurança para DevOps

Para Baldwin (2023), o *DevOps Security* abrange os controles relacionados à engenharia de segurança e operações nos processos de desenvolvimento e operações (*DevOps)*, incluindo a implantação de verificações de segurança críticas (como teste de segurança de aplicativo estático, gerenciamento de vulnerabilidades) antes da fase de implantação para garantir a segurança em todo o processo de DevOps. Inclui também tópicos comuns, como modelagem de ameaças e segurança de fornecimento de software.

3.4.5 Centro de Operações de Segurança Orientadas por Inteligência

A Wikipedia (2021) refere a centro de operações de segurança em inglês *Security Operations Center* (SOC) como um termo genérico que descreve parte ou a totalidade de uma plataforma cujo objetivo é prestar serviços de deteção e reação a incidentes de segurança, podendo incluir seis operações a serem executadas a saber: identificação de eventos de segurança, coleta, armazenamento, análise, reação e observação.

Para Panetta (2016) os SOCs devem ser projetados para atender o novo paradigma de deteção e resposta, estando no centro a componente inteligência que habilita a que os SOCs ofereçam uma arquitetura adaptável e componentes sensíveis ao contexto.

3.4.6 Tecnologia de Engano

Esta é uma tecnologia que procura replicar para o mundo da segurança cibernética uma das estratégias bastante usadas e bem-sucedidas das forças armadas para superar o inimigo. A equipa de segurança cria vulnerabilidades, sistemas, conjuntos de dados e *cookies* falsos que imitam os ativos de tecnologia legítimos em uma infraestrutura de uma organização para atrair e também

servir de armadilhas aos invasores. Qualquer tentativa de acesso a esses recursos indicará às equipas de segurança que um ataque está em curso, pois, utilizadores legítimos não têm visibilidade ou precisam aceder aos sistemas falsos. As notificações destes ataques são enviadas instantaneamente para um servidor central que regista a "isca" afetada e os vetores de ataque usados pelo malfeitor.

3.4.7 Encriptação de Dados

Encriptação é a técnica através da qual os dados são transformados para um modo tal que não possa ser lido por indivíduos não autorizados. Esta é uma medida importante pois garante a confidencialidade da informação mesmo para casos de dados que são roubados por malfeitores, como em ataques de *ransomware*. A criptografia, ou seja, a ciência que se dedica à construção e análise de protocolos que impedem a terceiros de terem acesso às informações privadas, funciona com um par de chaves, sendo uma para encriptar os dados transformando-os em cifras e a outra para a desencriptação que recupera a informação original. Nos casos em que se usa a mesma chave tanto para encriptação assim como para desencriptação chamamos criptografia simétrica de contrário chamamos criptografia assimétrica.

Segundo Goodrich e Tamassia (2014) um modelo de encriptação deve tornar extremamente difícil para qualquer um obter a informação original sem o conhecimento da chave para decriptação. os arquitetos de segurança devem optar por algoritmos de encriptação públicos (*open design*) pois esta opção permite que o sistema seja examinado por múltiplas entidades que lidam com a rápida descoberta e correção de vulnerabilidades decorrentes de erros de desenho. Portanto a segurança nestes modelos resume-se apenas em garantir que as chaves criptográficas estejam seguras.

3.4.8 Resiliência de Dados e Backups

Um dos objetivos da segurança da informação é garantir a recuperação após desastre e isso pressupõe a existência de um plano de contingência que garanta tal recuperação. Uma das técnicas recomendadas nos planos de contingência é a realização de cópias de segurança ou em inglês *backups* dos dados. Para Fernandes e DeAbreu (2014) as cópias de segurança ou *backups* seja da informação, software, imagens de sistemas e ficheiros de configuração devem ser feitas e testadas regularmente de acordo com uma política estabelecida para *backups*.

Entretanto, a resiliência de dados e backups refere-se à realização de cópias duplicadas ou múltiplas cópias dos dados críticos que possam ser usadas para efeitos de restauração ou

recuperação se a cópia primária for perdida ou corrompida seja acidentalmente ou propositadamente. A política de *backups* da organização deve indicar quais outras medidas devem acompanhar a criação de multiplicidade de cópias de dados de forma a não só tornar a recuperação possível, mas também a não criar vulnerabilidade dos dados. Duas medidas devem ser consideradas a priori: a encriptação de dados de *backup* e alojamento em lugares diferentes e seguros. De contrário, tornar-se-á perigoso ter várias cópias de dados em texto claro e de nada adiantará ter várias cópias se estiverem fisicamente localizadas no mesmo lugar.

3.4.9 Retenção e Destruição dos Dados

Para cada organização os dados terão um determinado valor durante algum período de tempo em função do seu ramo de atuação ou negócio, que seria diferente se os mesmos dados fossem detidos por outra organização.

Portanto é importante armazenar ou arquivar os dados necessário para longos períodos que sejam usados para questões de *compliance* ou certos requisitos de negócio de forma segura, assim como uma destruição segura daqueles que tenham perdido a sua utilidade para a organização usando algoritmos e técnicas comprovadas de tal forma que não possam ser recuperados e usados para fins errados.

A utilização destas técnicas deve ser também considerada quando a organização faz o descarte de ativos sejam eles dispositivos de utilizadores assim como equipamentos de processamento, de comunicação ou armazenamento que tenham atingido o fim da vida útil ou por qualquer outro motivo. No caso deste processo ser terceirizado é imprescindível a apresentação do certificado de destruição definitiva da informação.

A Iron Mountein (n.d.) no seu artigo sobre *Melhores práticas para a destruição de dados*, menciona que a literatura fala de diferentes técnicas de destruição de dados e destaca as três técnicas que se podem considerar como as mais indicadas para organizações que lidam com informações críticas.

Sobre gravação – envolve a gravação de novos dados sobre os antigos, tornando estes completamente ilegíveis. Esta técnica é suficiente para a maioria das situações, entretanto, para aplicativos de alta segurança podem ser necessárias várias limpezas para se atingir o nível ótimo de garantia de que os dados antigos foram destruídos.

Desmagnetização – esta técnica usa ímanes de alta potência para interromper o campo magnético do meio de armazenamento magnético como discos rígidos, fita magnética ou disquetes, limpando-o de forma rápida e eficaz. Não obstante tem a desvantagem de tornar o disco rígido inoperante.

Destruição física – é recomendada para casos em que o meio não será mais usado. Pode ser feita de várias maneiras incluindo trituração, perfuração, fusão ou qualquer outro método que torne o meio de armazenamento físico inutilizável. Alguns cuidados devem ser observados pois não é fácil de auditar e é propenso a erros humanos ou manipulação.

3.5 Boas Práticas para Segurança de Redes

A International Organization for Standardization (ISO, 2022) recomenda que sejam criados controles que assegurem a proteção da informação assim como dos serviços na rede. Neste exercício devem ser considerados as seguintes práticas:

- ✓ Definir o tipo e o nível de classificação da informação que a rede pode suportar;
- ✓ Definir as responsabilidades e procedimentos para a gestão dos equipamentos e dos dispositivos de rede;
- ✓ Manter atualizada a documentação incluindo os diagramas de rede e ficheiros de configuração;
- ✓ Definir os controles para a salvaguarda da integridade e confidencialidade dos dados que atravessem redes públicas, de terceiros ou rede sem fio para proteção das aplicações e sistemas conectados;
- ✓ Definir os controles que garantam a disponibilidade dos serviços de rede e dos computadores ligados à rede;
- ✓ Estabelecer os mecanismos apropriados para registo e monitoria que permitam a rápida deteção de ações que possam impactar na segurança da informação;
- ✓ Estabelecer uma permanente coordenação das atividades de gestão da rede para otimização do serviço prestado à organização e garantir que os controles são aplicados de forma efetiva ao longo da infraestrutura de processamento da informação;
- ✓ Autenticar os sistemas na rede;
- ✓ Restrição e filtragem de conexões dos sistemas para a rede;
- ✓ Fortalecimento das configurações dos dispositivos de rede;
- ✓ Separação do canal de administração da rede de outros tipos de tráfego de rede;

- ✓ Estabelecimento de mecanismos para isolamento temporário de segmentos de rede críticos em caso de deteção de ataque;
- ✓ Desabilitar os protocolos de rede vulneráveis e os que não estejam em uso;
- ✓ Assegurar a aplicação de controles apropriados para o uso de redes virtualizadas. Inclui-se aqui as redes definidas por *software,* em inglês *software-defined network* (SDN).

3.6 Governança de Tecnologia e Segurança da Informação

Como referido por DosSantos e Baruque (2010) quanto maior é a dependência da organização com relação a TI, maior é o risco para o negócio. Isso justifica o facto de ser de extrema importância fazer-se o alinhamento da TI aos objetivos estratégicos da organização para que os investimentos na tecnologia se tornem em fator agregador de valor para as organizações. Isso é alcançado através do estabelecimento de um modelo de governança que focalize os aspetos corporativos como um todo e os particularmente ligados à TI.

O ponto de partida da governança de uma organização é o estabelecimento da governança corporativa que deve ser vista como um sistema através do qual as entidades são dirigidas e controladas. Portanto a proposta é que para as instituições onde a cultura de governança já esteja estabelecida sejam também acrescidas tanto a governança de TI assim como a governança da segurança da informação, devido a relação de complementaridade entre elas como ilustrado na figura 1. Segundo Manoel (2014) enquanto a governança da tecnologia da informação visa um processo pelo qual decisões são tomadas sobre os investimentos em TI, o que envolve: como as decisões estratégicas são tomadas, quem toma as decisões, quem é responsabilizado pela função de gestão e operação da TI e como os resultados são medidos e monitorados, o escopo da governança da segurança da informação abrange a confidencialidade, integridade e disponibilidade da informação.

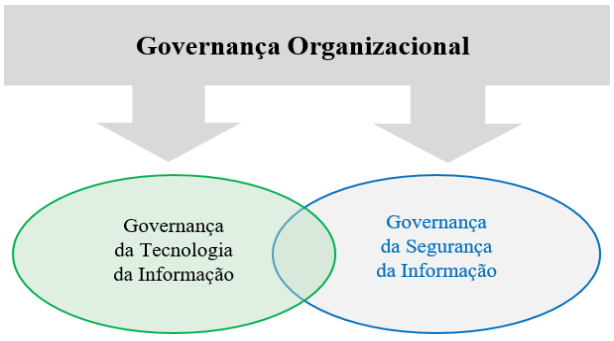


Figura 1. *Relação entre governança de TI e Governança de SI*. Fonte: ABNT NBR ISO/IEC 27014:2013

3.6.1 Governança da Tecnologia da Informação

A governança da TI é da responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e os objetivos da organização. (Fernandes & DeAbreu, 2014, p.13).

Um dos grandes problemas com que as organizações e mais concretamente os decisores de TI se debatem hoje é a multiplicidade de soluções tecnológicas existentes fruto mesmo dos avanços desta indústria. Esta multiplicidade de soluções tecnológicas vem dificultar muito quando chega a hora de fazer a decisão sobre os caminhos de investimento a seguir levando muitas vezes a que as empresas tomem decisões erradas e no fim a TI seja vista não como o veículo de otimização de processos e redução de custos, mas como um empecilho. Portanto existem *frameworks* que auxiliam as organizações a implantar de forma assertiva a governança de TI. Na tabela 1 são apresentadas as *frameworks* mais comuns juntamente com algumas normas e boas práticas disponíveis no mercado que contribuem para que no final se alcance a tão almejada eficácia bem como eficiência de TI.

Segundo DosSantos e Baruque (2010) as boas práticas representam um caminho rápido para alcançar ótimos resultados, uma vez que elas tratam de conhecimentos testados e aprovados por várias organizações em todo o mundo. A adoção das boas práticas não é obrigatória e pode ser global ou parcial, isto é, da forma que melhor satisfaça os interesses da organização, salvaguardando o alinhamento estratégico com o negócio.

Para Fernandes e DeAbreu (2014) podemos destacar os seguintes componentes típicos da governança de TI: otimização do risco, *Compliance*, avaliação independente, gestão da mudança organizacional em matérias de TI, alinhamento estratégico, entrega de valor, gestão de desempenho, comunicação e gestão de recursos.

Tabela 1. *Frameworks*, normas e boas práticas

Modelo	Escopo do modelo
ISO/IEC 38500	Norma sobre Governança Corporativa de TI
CobiT	Modelo abrangente aplicável para a governança e gestão da TI em ambiente corporativo
ITIL	Serviços de TI, segurança da informação, gestão da infraestrutura, gestão de ativos e aplicativos, etc.
ISO/IEC 20000	Norma que aborda os requisitos e melhores práticas para a gestão de serviços de TI
ISO/IEC 27014	Norma sobre Governança da Segurança da Informação
ISO/IEC 27001 e ISO/IEC 27002	Requisito e código de prática para a gestão da segurança da informação
PRINCE2	Metodologia de gestão de projetos
PMBOK	Base de conhecimento em gestão de projetos
SCRUM	Método ágil para a gestão de projetos
BSC - Balanced Scorecard	Metodologia de planeamento e gestão estratatégica

Da pesquisa realizada verificou-se que os dois modelos mais conhecidos são o ITIL e o CobiT, sendo que em termos de implementação, o ITIL é o *framework* que mais foi adotado. Comparando estes dois modelos constata-se que apesar de apresentarem certas semelhanças e poderem ser implementados de forma isolada o seu foco é ligeiramente diferente.

Segundo a WalkMe Team (2023) o CobiT é um *framework* que apresenta uma visão de alto nível da organização, das metas de negócio, da tecnologia de informação e da própria gestão da informação. Neste contexto desenvolve processos e sistemas para áreas que incluem: controle de processos e maturidade de TI; gestão de recursos de TI, incluindo aplicativos, informações, infraestrutura e pessoas; adesão aos requisitos de negócio e governança; gestão estratégica, entrega de valor, riscos, recursos e desempenho. Enquanto que a ITIL é um *framework* que se concentra na gestão, entrega e manutenção de serviços de TI, tendo como processos principais a estratégia, desenho, transição, operação e melhoria contínua de serviços.

Portanto, a WalkMe Team (2023) sugere a implementação combinada das potencialidades do CobiT, mais inclinada para a governança de TI – indicar o caminho e definir as regras, e da ITIL mais relacionado com a gestão da TI, ou seja, com aspetos operacionais.

Considerações para implementação da Governança de TI

Segundo DosSantos e Baruque (2010) há muito que se considerar quando se pretende implementar a governança de TI em uma organização. Dado que a implementação de governança de TI não faz parte do escopo do trabalho é ilustrado na figura 2 o que os autores consideram como sendo os passos mínimos para construção de processos visando a governança de TI:

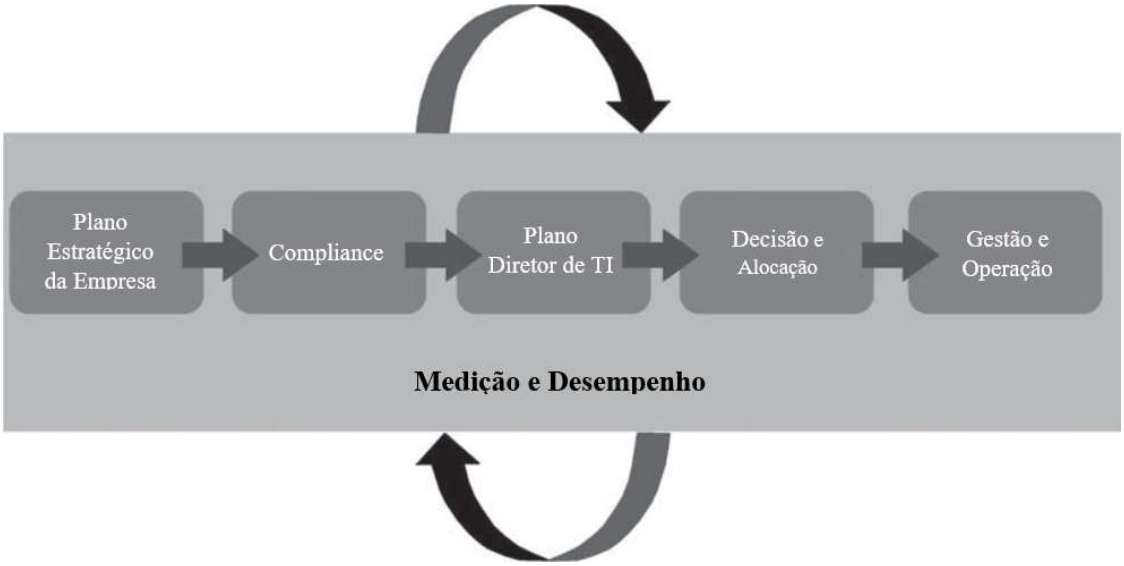


Figura 2. *Etapas do modelo de Governança*. Fonte: (DosSantos & Baruque, 2010)

1º Passo: Elaboração do plano estratégico da empresa

Definição da estratégia da empresa tendo em conta a sua visão e missão como forma de atingir aquelas que são as suas metas.

2º Passo: Examinar as questões de conformidade regulatória

Ter claras as leis (técnicas, ambientais, laborais) que regulam a área de atuação da organização e a frequência de alterações das mesmas.

3º Passo: Elaborar o plano diretor de tecnologias de informação (PDTI)

Incorpora as diretrizes para a área de TI em alinhamento com o negócio para curto, médio e longo prazo, geralmente um ano, dois a três anos e cinco a seis anos, respetivamente.

4º Passo: Tomar decisões e fazer as alocações

O foco é a eficácia estratégica, ou seja, escolher o que deve ser feito de acordo com o PDTI que pode incluir iniciar e cancelar projetos, obter e alocar recursos, estabelecimento de diretrizes para a gestão operacional da TI.

5º Passo: Garantir o controle e o gestão da operação

Nesta fase deve se ter como meta a utilização eficiente de recursos e a continuidade dos serviços tendo em vista os requisitos e as dinâmicas da organização.

Fora o que já foi considerado, um aspeto importante e determinante para o sucesso na implementação da governança de TI tem a ver com a definição clara de papéis e responsabilidades dentro da organização. Não se encontrou na literatura uma abordagem apontada como certa ou errada sobre como deve ser tratado este assunto. Segundo Fernandes e DeAbreu (2014) a prática mostra que algumas empresas criam departamentos ou indicam alguns profissionais responsáveis pela implementação da governança de TI que podem ter autonomia na decisão ou estar subordinada ao CIO da empresa; outras criam programas para a implementação da governança de TI após o qual estes são extinguidos e uma última abordagem que passa por abdicar de ter equipas internas e usar a consultoria externa tendo o CIO como o líder da mudança.

3.6.2 Governança da Segurança da Informação

As informações devem ser protegidas pelo seu valor, pelo impacto da sua ausência, pelo impacto resultante de seu uso por terceiros, pela importância da existência da informação para a geração do conhecimento, pela relação de dependência entre todos os processos de negócio da organização (Manoel, 2014).

Segundo a Associação Brasileira de Normas Técnicas (ABNT, 2013) os objetivos da governança da segurança da informação são:

- ✓ Estabelecer segurança da informação abrangente e integrada em toda a organização.
  Este objetivo pressupõe a existência de um único conjunto de medidas de segurança que abarque todas as prioridades da organização no que respeita à segurança física e lógica e onde a responsabilidade e a responsabilização estejam estabelecidas em toda a extensão da organização inclusive na relação com entidades externas;
- ✓ Tomada de decisões usando uma abordagem baseada no risco.
  A organização deve estabelecer um mecanismo de gestão de risco que considere os riscos da informação, tendo em consideração os impactos financeiros, operacionais e relativos à reputação, derivados da violação e não conformidade com as leis. É na base dessa avaliação de risco que será determinada a quantidade de segurança que se deve considerar e os recursos necessários para a sua efetivação;
- ✓ Definir a direção das aquisições.

É fundamental para a garantia da segurança que se faça uma avaliação do impacto ao se empreender novas atividades, incluindo, mas não se limitando a, investimentos, compras, fusões, adoção de nova tecnologia, acordos de terceirização e contratos com fornecedores externos. Portanto a segurança da informação deve estar integrada aos processos existentes na organização, incluindo gestão de projetos, aquisições, realização de despesas financeiras, entre outros;

- ✓ Assegurar a conformidade com os requisitos internos e externos.

  A governança da segurança da informação deve garantir que as políticas de segurança da informação e as práticas estejam em conformidade com as partes envolvidas. As auditorias independentes podem ser chamadas para verificar ou validar se a legislação e regulamentos assim como requisitos ou cláusulas contratuais estejam a ser observados;
- ✓ Promoção de cultura positiva de segurança da informação.

  É fundamental que na organização se desenvolva uma cultura em que todos entendam os objetivos, as responsabilidades da implementação da segurança da informação. Portanto as pessoas devem se sentir inclusas nos processos inerentes à construção das políticas e sejam formadas para saber melhor lidar com as práticas e regras por elas emanadas no exercício das suas atividades ou funções;
- ✓ Assegurar que o desempenho da segurança atenda aos requisitos atuais e futuros da organização.

  A governança deve assegurar que a abordagem adotada para a proteção da informação seja adequada ao propósito de apoiar a organização e que acompanhe as dinâmicas desta. Portanto, a medição de desempenho das medidas, as auditorias e a identificação de oportunidades de melhoria devem acontecer numa base regular para manter o alinhamento e serviço à estratégia da organização.

3.6.2.1 Governança de SI vs Gestão de SI

Tornou-se normal encontrar situações em que se confunde a governança com a gestão da segurança devido sobretudo à falta de cultura de governança e/ou do desconhecimento em relação à governança da segurança da informação. É importante reter que a realização de backups, monitoria dos serviços de TI, verificação das *firewalls*, portanto a maioria dos trabalhos diários de um departamento de TI tem a ver com gestão de segurança. A tabela 2 apresenta um resumo da ilustração do que são atribuições de governança versus gestão da SI.

Tabela 2. Diferenças entre governança e Gestão da SI

Governança	Gestão
Fiscalização	Implementação
Confere os poderes de decisão	Toma as decisões necessárias
Aprova as políticas	Implementa as políticas
Planeamento estratégico	Planeamento de projetos
Alocação de Recursos	Utilização dos recursos

Para Manoel (2014) uma implementação bem-sucedida de governança de segurança da informação irá propiciar:

- ✓ Visibilidade da alta direção sobre a situação da segurança da informação;
- ✓ Uma abordagem ágil para tomada de decisões sobre os riscos da informação;
- ✓ Investimentos eficientes e eficazes em segurança da informação;
- ✓ Conformidade com requisitos externos.

3.6.2.2 Aspetos a considerar na implementação da GSI

Antes de qualquer ação é preciso vender a ideia de governança para alta direção de forma que esta possa entender e concordar com a sua implementação. Para West (2023) é importante uma estratégia de diálogo com a alta direção para convencê-los a investir na segurança da informação. Este realça que o uso de dicionário técnico não ajuda, antes pelo contrário o que a alta direção deve perceber é como o investimento em segurança se alinha com suas áreas de responsabilidade. Portanto, os líderes máximos da organização vão querer perceber como a segurança da informação impacta a sua forma de conduzir os negócios e cria vantagens estratégicas. Enquanto isso, um gestor financeiro ficaria satisfeito em saber que a noção de que a organização usa padrões de segurança bem estabelecidos possibilitaria atrair clientes e parceiros com impacto na reputação e receitas.

Outro aspeto que deve ser enfatizado é a necessidade de incorporar a segurança em todo ciclo de desenvolvimento de aplicações e na infraestrutura de TI que é sobre a qual se assenta todo o negócio da organização, isto é, as pessoas devem perceber que elas precisam de proteger a informação como parte da sua rotina diária.

Após obter a aprovação e suporte da máxima direção, podem seguir os passos para a implementação da governança de segurança da informação. Segundo Manoel (2014) existem elementos que devem ser cautelosamente levados em conta:

a) É importante a indicação de uma figura que será responsável pela governança da segurança da informação, muitas vezes designada de CISO do termo inglês *Chief Information Security Officer*. Este é um cargo de extrema importância e requer que seja ocupado por alguém de confiança e com boas habilidades técnicas assim como de comunicação para lidar com todas as áreas da organização;
b) A organização deve ter um plano estratégico de segurança da informação que seja abrangente. Para este fim deve-se partir dos requisitos de segurança da informação que podem ser facilmente obtidos por meio de realização de entrevistas à direção de topo para ter a realidade atual e a visão do futuro.
c) Recomenda-se a criação de um comité de segurança da informação que terá a função de tomar decisões estratégicas, elaborar as diretrizes que serão seguidas por todos, mostrar apoio às decisões e posicionar-se em relação aos aspetos que demandam a deliberação da alta direção. Este comité deve preferencialmente ter o envolvimento de representantes das áreas dos diferentes sectores da organização como por exemplo área jurídica, comunicação e marketing, planificação, finanças e recursos humanos.

3.6.2.3 Boas práticas para governança de SI

São apresentadas algumas das boas práticas de governança de SI partilhadas por alguns autores segundo os quais já se provou serem de mais valia para uma efetiva governança e proteção da informação institucional:

- ✓ A organização deve desenvolver uma política de segurança da informação que abranja todas as áreas com maior incidência para as áreas críticas;
- ✓ As atividades de segurança da informação devem ser regidas com base nos requisitos relevantes, incluindo leis, regulamentos e políticas organizacionais;
- ✓ Os gestores seniores devem estar ativamente envolvidos no estabelecimento da governança da segurança da informação;

- ✓ Os gestores de segurança da informação devem monitorar continuamente o desempenho do programa de segurança pelo qual são responsáveis, usando ferramentas e informações disponíveis;
- ✓ As responsabilidades da segurança da informação devem ser atribuídas e executadas por indivíduos adequadamente treinados. Estes devem ser responsabilizados por suas ações ou falta de ações;
- ✓ As informações descobertas por meio do monitoramento devem ser usadas como entrada nas decisões de gestão sobre prioridades e alocação de fundos para efetuar a melhoria da segurança e do desempenho geral da organização. Planos, estratégias e práticas devem ser atualizados, contínuos e baseados em métricas de desempenho e seus resultados;
- ✓ As prioridades da segurança da informação devem ser comunicadas às partes interessadas em todos os níveis dentro da organização para garantir uma implementação bem-sucedida;
- ✓ Os funcionários da organização, incluindo todos os níveis de gestão, devem ser treinados e consciencializados de suas funções e responsabilidades.

4 RECOLHA E ANÁLISE DE DADOS

Como mencionado na seção sobre a metodologia foram conduzidas duas entrevistas estruturadas: uma destinada ao diretor do departamento de tecnologia de informação e comunicação e outra para o Chefe da divisão de segurança da informação e sistemas. As questões foram partilhadas antecipadamente por meio do *Google forms* e as entrevistas foram conduzidas presencialmente. Foram realizados dois inquéritos recorrendo à mesma plataforma, sendo um destinado a todos os profissionais de TI designado inquérito geral e outro exclusivo para os técnicos de redes e comunicações que acabam sendo os únicos técnicos a desenvolver alguma tarefa respeitante à segurança de infraestrutura de TI. O inquérito geral foi respondido por 17 profissionais dos 31 esperados. Já o inquérito aos técnicos de redes foi atendido pelos quatro colaboradores do sector.

A análise dos dados será apresentada em três subseções em alinhamento com os objetivos constantes da primeira seção do trabalho.

4.1 Radiografia geral da segurança da informação na instituição

Conforme referido na introdução a AT tem muitos desafios no que respeita à segurança da informação e espera resolvê-los com a ajuda de um plano de modernização da infraestrutura tecnológica. Na revisão da literatura as questões financeiras e do envolvimento da alta gestão foram apontadas como sendo cruciais para uma boa e efetiva governança da segurança e consequente otimização de risco de TI para um melhor serviço de TI ao negócio da organização.

Para aferir como estes aspetos estão a ser endereçados foram realizadas as seguintes questões basilares:

1 - A instituição terá adotado algum *framework* de governança?

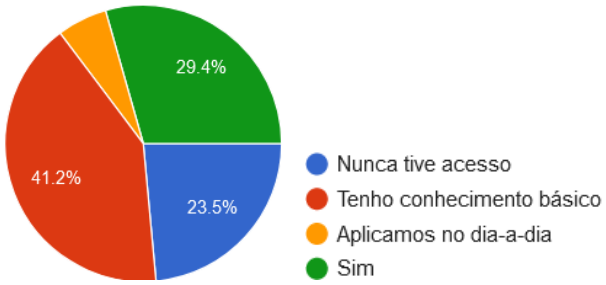
2 - A organização possui política de segurança aprovada e divulgada?

3 - Que controles já foram implementados e quais ainda esperam implementar?

4 - A organização usa encriptação de dados no armazenamento e/ou transmissão?

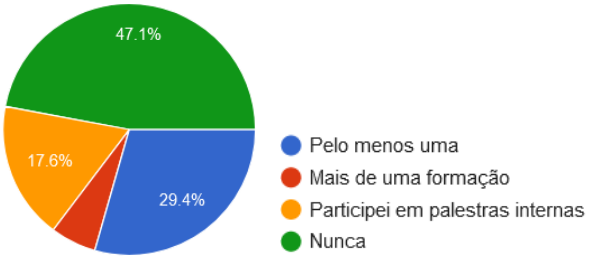
As questões que se seguem foram retiradas do formulário do inquérito geral (Apêndice E) para aferir o nível de conhecimento em matérias ligadas a segurança da informação:

Tem conhecimento sobre a política de segurança da organização? – Geral

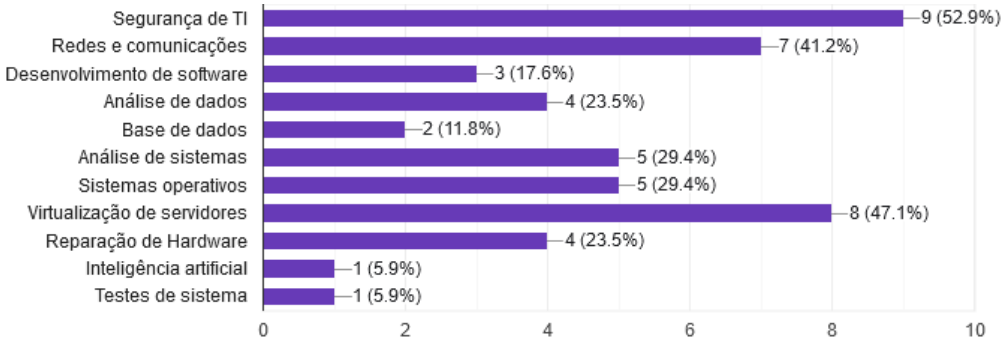


Como avalia a organização em termos de segurança da informação após o início da modernização tecnológica (ano de 2015)? – Geral

Já se beneficiou de alguma formação sobre segurança da informação? – Geral

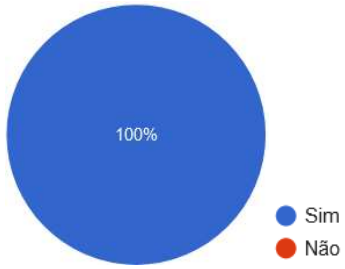


De que áreas tem interesse a nível das TICs? (Máximo duas) - Geral

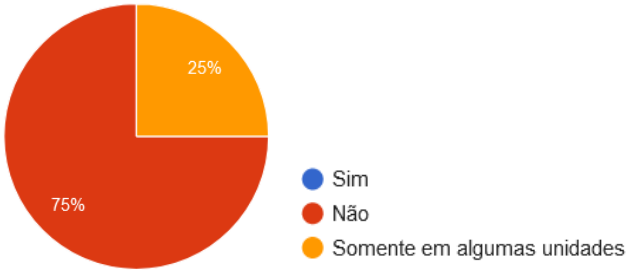


A terminar seguem as questões retiradas do inquérito aos técnicos de redes e comunicações para aferir o grau de observância das boas práticas para segurança de infraestrutura de TI:

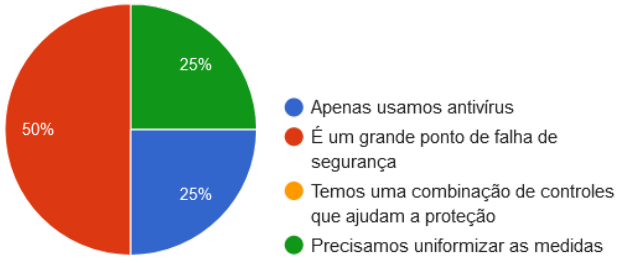
Na sua opinião estão implementados mecanismos de controle de perímetro adequados para proteção do tráfego de e para fora da instituição? – Técnicos de Redes



Os gabinetes para equipamentos de rede estão protegidos em todas as unidades orgânicas? – Técnicos de Redes



Acha que as medidas de segurança dos *endpoints* é efetiva? – Técnicos de Redes



Os resultados permitiram tirar as seguintes leituras:

Em resposta à primeira questão base, a direção de TICs afirmou não ter adotado nenhuma *framework* de governança, pese embora para alguns processos sigam as recomendações da ITIL. Na sequência da entrevista, em resposta à questão sobre a formação em matérias ligadas à governança, a direção afirma não ter formação suficiente sobre a matéria. De acordo com a revisão da literatura, o ITIL é uma *framework* com boa aplicação na gestão de TI sendo complementada por outras *frameworks* com maior direcionamento à implementação de processos de governança de segurança.

Relativamente à segunda questão, a direção afirma que a organização tem uma política de segurança, todavia desatualizada. Como referido na seção sobre a revisão da literatura, a política da segurança da informação é basilar pois é a partir dela que se desenrolam todos outros aspetos inerentes à aplicação dos controles de segurança e ela deve ser flexível às mudanças da organização.

As últimas duas questões de base permitiram saber que alguns controles recomendados pelas boas práticas já se encontram implementados. Para a questão foram listados 14 controles (ver apêndice D) dos quais 10 encontram-se implementados, todavia na maioria dos casos a implementação não é efetiva, isto é, não responde à exigência, desviando-se deste modo do plasmado na literatura. Não se usa encriptação de dados tanto em armazenamento assim como na comunicação, com exceção do tráfego transmitido via redes virtuais privadas (VPN). Compulsando a revisão da literatura pode afirmar-se que a não encriptação dos dados viola o pilar da confidencialidade o que se configura num risco de segurança grave.

Em relação aos dois inquéritos tem-se:

- ✓ Um número considerável de técnicos (76%) tem conhecimento sobre a política de segurança, contudo grande parte destes (41%) apenas detém conhecimento básico;
- ✓ 53% dos técnicos afirma que os projetos de modernização tecnológica estão a trazer melhorias para a segurança da informação, mas que há ainda espaço para melhoria;
- ✓ 47% dos técnicos afirma nunca ter beneficiado de formação em matérias de segurança da informação;

- ✓ 53% dos técnicos de informática demonstra interesse em matérias relacionadas com a área de segurança da informação;
- ✓ Os técnicos de redes são unânimes em afirmar que existem mecanismos de controle do perímetro;
- ✓ 75% dos técnicos de redes afirmam que os gabinetes de equipamento de rede não estão protegidos;
- ✓ 25% dos técnicos de redes afirma existir uma proteção básica para os *endpoints* proporcionada através de antivírus.

4.2 Avaliação da Implementação de Controles de Segurança de Redes

Na revisão da literatura referiu-se a importância da implementação de controles adequados para a proteção da rede. Alguns autores advogam ser nesta componente de infraestrutura onde maior investimento é despendido quando se trata de proteger os dados da organização. Outra grande preocupação tem a ver com a adoção de tecnologias que garantam continuidade de serviços e boa performance na comunicação de dados entre unidades geograficamente separadas onde geralmente recorre-se a serviços contratados a terceiros.

Um conjunto de questões foram apresentadas e respondidas para aferir o enquadramento ou a pertinência de implementar as boas práticas emanadas pela literatura no que compreende a melhoria da segurança da rede e das comunicações na AT.

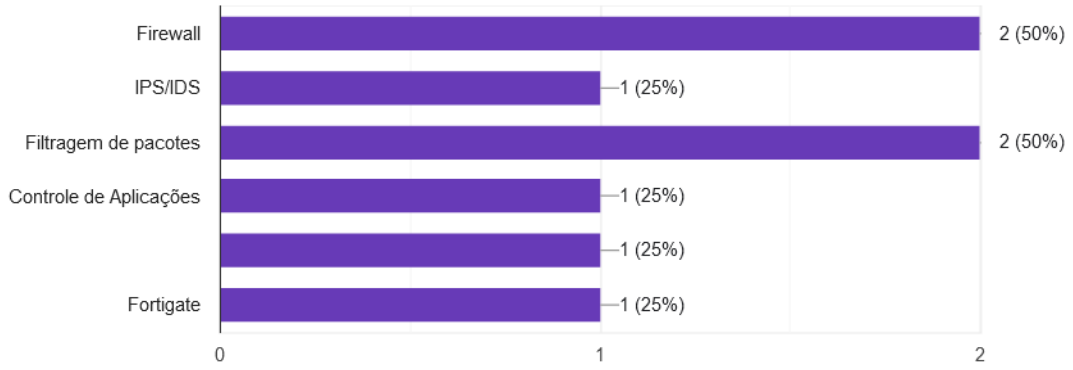
Como no ponto anterior iniciamos com as questões base:

1 - Quais são as principais vulnerabilidades com que se deparam e qual o tratamento dado?

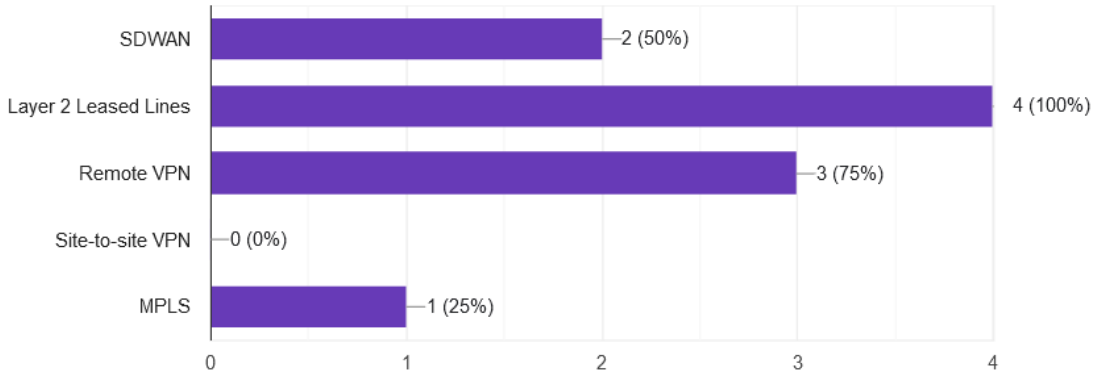
2 – Existe uma política de redundância de ativos críticos?

As outras questões foram colocadas via inquérito à equipa de redes cujos resultados passamos a apresentar:

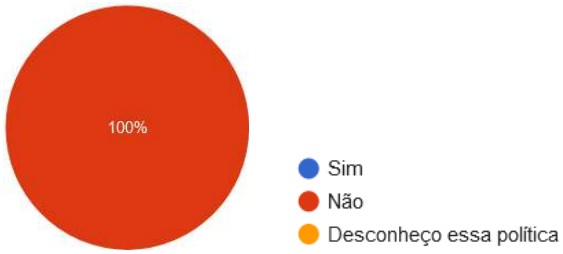
Que controles para o perímetro foram implementados? – Técnicos de Redes



Quais são as tecnologias usadas na rede alargada (WAN) para a conexão entre as unidades da AT? – Técnicos de Redes



A atualização das versões do hardware assim como software responde às políticas da organização. – Técnicos de Redes



Os resultados ajudaram a compreender o seguinte:

Em resposta às questões de base, a equipa de gestão de segurança informou que a análise de vulnerabilidades não é rotineira, contudo indica que a maior fragilidade está com os serviços disponibilizados via Internet como por exemplo o serviço de correio eletrónico, sistema de

pagamento de imposto via banco, consulta online do número de identificação tributário, entre outros. Razão pela qual a organização está a empreender maior esforço na melhoria da segurança da rede e das comunicações, o que de certa forma alinha-se com a literatura quando afirma ser na rede onde recaem as maiores preocupações.

Com relação à redundância de ativos, esta é feita apenas a nível do equipamento alocado ao centro de dados. Há ainda por considerar alguns pontos críticos como os centros de derivação sitos nas capitais provinciais pois é a partir destes pontos onde são derivadas as ligações das comunicações para todas as unidades orgânicas a nível de cada província.

Quanto ao inquérito pode-se constar que:

- ✓ A gestão julga importante a implementação de outros controles recomendados na revisão da literatura;
- ✓ Há deficiência no controle do perímetro da rede. Faltam controlos e os implementados não são efetivos. A ver pelas respostas nenhum dos controlos implementados teve confirmação de todos os técnicos sendo a pontuação individual máxima 50% para dois dos quatro controlos apresentados;
- ✓ A maior parte das ligações de longa distância para comunicação entre as unidades remotas e o centro de dados são por via de linhas alugadas de camada 2 (*layer 2 leased lines*). Pese embora seguras estas deixam a desejar quando se trata de otimização de custos operacionais (geralmente são mais caras) e aplicação da qualidade de serviços (QoS);
- ✓ Há interesse na migração para tecnologias atuais. Este alinha-se com as recomendações referidas na literatura como sendo fundamental para o alinhamento tecnológico.

4.3 Formação de Quadros em Matérias de Segurança da Informação

Como visto no capítulo 2 as pessoas são o elemento principal para provimento de serviços de TI de qualidade incluindo a garantia de segurança da informação. A formação das pessoas interessadas deve ser abrangente o suficiente para que a segurança esteja presente em todo o ciclo de vida da informação e em todos os setores da instituição onde se faça uso da tecnologia.

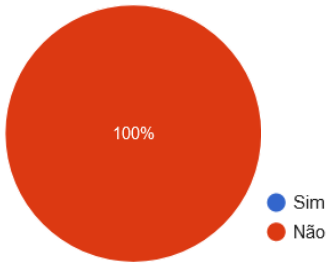
Neste caso, serviram como perguntas de base as seguintes:

1 - O investimento é suficiente para que as TICs estejam em altura de contribuir no seu máximo para a eficiência da instituição?

2 - Existe uma política de formação de quadros em matérias de segurança da informação que incorpore as pessoas de todos os níveis e sectores da organização?

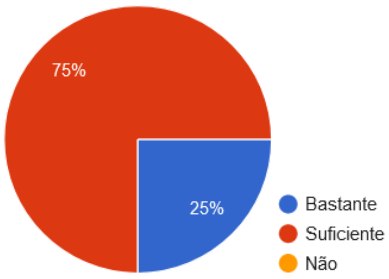
Outras questões foram colocadas por meio dos formulários de inquérito a nível de gestão assim como aos técnicos:

Já participou de alguma formação em governança de TICs ou governança de segurança da informação? – Direção de TICs

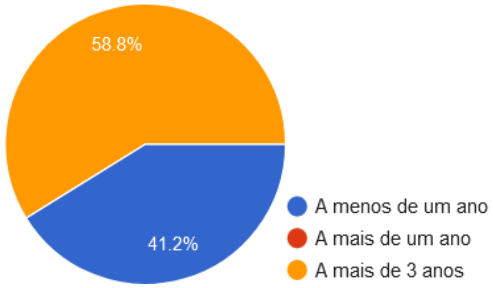


Tem se beneficiado de formações em matérias sobre segurança da informação? – Técnicos de Redes.

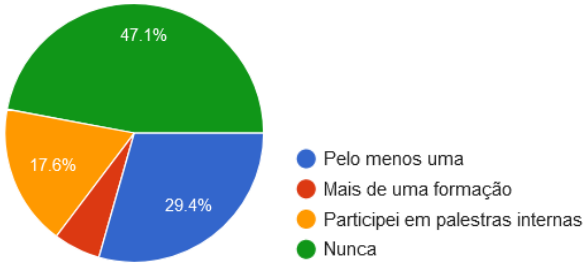
Tem conhecimento sobre o que é infraestrutura crítica de TI? – Técnicos de redes



Quando é que se beneficiou da última formação? - Inquérito Geral



Já se beneficiou de alguma formação sobre segurança da informação? – Inquérito Geral



Em sua opinião, acha que os utilizadores conhecem os cuidados básicos da segurança da informação? - Inquérito Geral

Com estas questões foi possível ter o seguinte alinhamento.

De acordo com a direção de TICs, os investimentos na área não são suficientes e estão aquém de responder às necessidades. Isto choca com os especialistas na matéria. Na seção 3 foi referido ser importante ter uma formação adequada, proporcional aos investimentos feitos em TI, que por sua vez devem estar dimensionados a altura do valor que os ativos representam para a organização. A

instituição ressente-se da falta de uma estratégia de formação de quadros específica para as matérias relativas à segurança da informação.

Estes resultados informaram o seguinte:

- ✓ Não se tem registo de frequência em formações que estivessem ligadas à governança da segurança da informação. Como mencionado na revisão da literatura esta deve ser primordial para garantir melhor preparo dos profissionais de TI e maior alinhamento da segurança da informação com o negócio;
- ✓ Cerca de 59% do total de técnicos de TI não se beneficiaram de formação sobre segurança da informação nos últimos 3 anos. Esta pode ser vista como uma oportunidade de melhoria;
- ✓ 47 % dos técnicos nunca beneficiou de uma única formação sobre a segurança da informação. Isto contrasta a recomendação de tornar as formações o mais abrangente possível;
- ✓ Pelo menos 18% dos técnicos já participaram de palestras internas sobre segurança da informação. Atesta o que a literatura diz sobre as palestras serem um mecanismo importante para consciencializar e formar as pessoas;
- ✓ O facto de 53% dos inquiridos ter manifestado interesse em matérias relacionadas com segurança da informação representa um sinal positivo. A literatura aponta este cenário como sendo propício para se lograr sucesso no processo de mudança cultural da organização;
- ✓ 71% dos técnicos afirmam que os utilizadores não têm conhecimento dos cuidados básicos sobre segurança da informação. Há necessidade de trabalhar mais para melhorar o nível de treinamento dos utilizadores nestas matérias.

5 RECOMENDAÇÕES

A radiografia geral da situação das TICs na Autoridade Tributária de Moçambique e em particular, o pulsar da segurança da informação, possibilita o cruzamento dos dados compilados com as sugestões aprovadas por vários autores consultados na revisão da literatura e formular sugestões que se espera resolvam os problemas atuais e futuros da instituição no que tange a segurança da informação.

A abordagem das boas práticas para a segurança da infraestrutura de TI foi feita tendo em conta as necessidades e a realidade da AT sem, contudo, ignorar as exigências fundamentais para a segurança das infraestruturas críticas da informação. A avaliação dos mecanismos a adotar foi com base na situação técnico-financeira da organização para produção de sugestões e recomendações que sejam sustentáveis a curto, médio e longo prazo. Na sequência procurou-se destacar algumas medidas e/ou tecnologias julgadas prioritárias para responder aos requisitos de segurança prementes que se espera comecem a produzir os resultados desejados em curto tempo, sendo fundamental que se avance o mais breve possível na consolidação da proteção do perímetro da rede de dados como forma de impedir que os ataques externos tenham sucesso, o que sem dúvidas traria enormes prejuízos à reputação da instituição.

Assim como na literatura, foi notável que na AT o baixo investimento na segurança da infraestrutura de TI tem impacto direto no nível de segurança dos ativos da organização e na formação dos profissionais que devem garantir a segurança, contudo não é um fator determinante para a falta de consciencialização sobre a segurança da informação a nível dos utilizadores. Entende-se haver ações sem custos ou possíveis de realizar com orçamento reduzido que quando devidamente planificadas podem trazer bons resultados. Neste aspeto a estratégia de formação enumera a troca de experiência com outras entidades público-privadas assim como a preparação dos recursos humanos mais qualificados em matérias de segurança da informação para a realização de treinamentos dos utilizadores e difusão de conteúdos úteis como caminhos a seguir para alcance de altos índices de consciencialização dos colaboradores em matérias sobre a segurança da informação.

No entanto, a segurança da informação deve ser vista como um conjunto de ações a serem planificadas e devidamente programas, esperando-se que a AT considere criar um plano a curto e

médio prazo liderado pela gestão máxima com engajamento de todas as equipas objetivando a proteção da infraestrutura de TI como um ativo importante e de suporte aos negócios da organização. A atualização da política de segurança da AT deve ser encarada como outra prioridade e esta deve abarcar a proteção das pessoas e todos ativos da organização elencando todos os aspetos relevantes inerentes à segurança física e lógica. Portanto, as equipas que fazem a gestão da TI precisam melhorar as técnicas de comunicação para fazer perceber e convencer aos decisores sobre a necessidade de estabelecer na organização a governança da TI e a governança da segurança da informação como elementos fundamentais para o desenvolvimento do negócio com suporte numa infraestrutura de TI mais segura.

5.1 Estratégia de Formação

A coleta dos dados permitiu fundamentar a necessidade de uma estratégia para a formação dos colaboradores em matérias de segurança da informação para que se possa aumentar as habilidades técnicas e o preparo dos utilizadores para melhor lidar com as questões ligadas à segurança da informação. Dessa forma é apresentada a estratégia de formação que leva em conta alguns pressupostos, nomeadamente:

- ✓ Existe na organização interesse comprovado em matérias de segurança da informação;
- ✓ A nível técnico e de gestão de TICs há uma elevada consciência sobre a importância de dominar as matérias ligados a segurança da informação;
- ✓ Há exiguidade de fundos para estabelecimento e cumprimento dos planos de formação de forma contínua, isto é, a médio ou longo prazos;
- ✓ Há abertura para parcerias em formações técnicas com outras instituições do governo como sejam o INTIC, INAGE e INCM;
- ✓ O INTIC e o INAGE têm parcerias internas assim como internacionais para formação de quadros em matérias de segurança da informação e estão abertos a incorporar técnicos de outras instituições públicas, seja na modalidade de partilha de custos, assim como bonificação.

Nestes termos a proposta de formação incluiria duas abordagens, sendo uma para os técnicos de informática e outra para os utilizadores e a alta direção da instituição. Seja qual for a abordagem é preciso desenhar programas de consciencialização, educação e treinamentos sobre matérias relativas à segurança da informação. Como recomendado na ISO (2022) estes programas devem

estar alinhados com a política de segurança da informação da organização, os procedimentos relevantes e devem acontecer numa base periódica.

5.1.1 Formação técnica

Como já referido na revisão da literatura, a capacitação dos técnicos de segurança é fundamental para a gestão da segurança da informação. Uma das caraterísticas desta área é a constante transformação movida tanto por necessidades de negócio assim como pela evolução tecnológica que suscita competências técnicas para gerir e acompanhar a mudança. Portanto é desejável que a AT tenha um plano muito bem elaborado que inclua as pessoas certas a serem formadas e as matérias nas quais devem ser formadas.

Roadmap de formações técnicas

É importante que a instituição tenha uma agenda de formações sobre governança e sobre gestão de segurança da informação para curto e médio prazo que esteja alinhado com os objetivos da organização. O *roadmap* das formações técnicas tem que ser elaborado tendo em conta a obtenção das seguintes competências:

- ✓ A direção e os gestores deverão levar a cabo ações para implementação de governança de segurança da informação;
- ✓ Os técnicos de segurança precisam dominar componentes de defesa dos ativos de TI da organização assim como conhecer as técnicas ofensivas, ou seja, de ataque (Ver Anexo);
- ✓ Os técnicos da AT devem conhecer as técnicas de análise de vulnerabilidade a fim de detetar os pontos de falha e efetuar os testes de penetração numa base rotineira para medir a eficácia dos controles implementados;
- ✓ Parte dos profissionais de segurança serão capacitados para formação dos utilizadores e pessoas interessadas.

Identificação dos técnicos chave

Para este âmbito, os técnicos chave são aqueles que estarão na linha da frente na proteção dos ativos da organização. Na identificação deste grupo dever-se-á englobar técnicos dos diferentes subsetores de TI, todavia a prioridade deverá ser para os técnicos que vão lidar com a segurança da infraestrutura de TI pois é urgente assegurar esta componente tecnológica. O esforço inicial

deve contemplar os técnicos afetos na sede da instituição e nos três centros regionais (sul, centro e norte) para criação de uniformidade em termos de domínio das matérias e tornar eficaz o processo de implementação dos controles. Dada a exiguidade de técnicos nesta área deve-se equacionar a contratação de novos funcionários qualificados para as tarefas de segurança da infraestrutura de TI.

Metodologia de formação

As formações em sala de aulas ministradas por profissionais qualificados têm um bom resultado e devem sempre ser consideradas principalmente para a fase inicial como forma de criar bases de conhecimento sólidos no seio dos profissionais. Não obstante, a AT deve apostar em outras modalidades de formação como os programas de treinamento à distância via plataformas digitais sejam elas pagas ou livres com uma efetiva avaliação e monitoria dos formandos; formações *on-the-job* ministradas tanto por técnicos da AT com mais experiência ou consultores externos; promoção da interação entre os técnicos dos subsectores da direção de TICs para troca de experiências em relação às políticas específicas (setoriais).

O plano de formação de profissionais de TI deverá garantir a contínua atualização dos quadros usando modelos de interação que os permitam estar em contacto permanente com as novas tendências de mercado, nomeadamente:

- ✓ Promover o cadastro dos profissionais de TI em canais eletrónicos que debatam/exponham matérias sobre a segurança da informação;
- ✓ Priorizar a participação deste grupo em conferências e seminários nacionais e internacionais por forma a mantê-los em contacto com outras realidades e promover a inovação;
- ✓ Incentivar os técnicos a desenvolver/atualizar as políticas específicas (setoriais) e os materiais para a formação de utilizadores e disseminação de informações sobre segurança da informação.

5.1.2 Formação de utilizadores

Para este grupo dever-se-á criar um plano consistente de disseminação de matérias de segurança da informação a nível central, regional e local por meio de palestras e formações internas. Esta disseminação deve ter como público alvo os utilizadores, membros da alta direção e pessoas

interessadas, podendo acontecer de forma conjunta ou isolada dependendo da situação ou da especificidade das matérias.

Objetivos

O plano de capacitação dos utilizadores deve ter foco nos seguintes objetivos:

- ✓ Consciencialização das pessoas em relação a necessidade de proteger a informação;
- ✓ Treinamento das pessoas interessadas (*stakeholders*) nas boas práticas e procedimentos para o uso correto e cuidado dos recursos tecnológicos da instituição assim como pessoais;
- ✓ Obter o suporte da alta gestão para os investimentos em segurança da informação.

Ações a desenvolver

Para o cumprimento dos objetivos traçados dever-se-á priorizar encontros presenciais e ao mesmo tempo potenciar a disseminação de informação sobre a segurança da informação e das boas práticas através dos canais eletrónicos assim como físicos existentes. A lista de ações deverá incluir:

- ✓ Realização de palestras sobre matérias relativas à segurança da informação. Estas podem ser conduzidas pelos técnicos e gestores de TI da organização assim como profissionais de fora da organização a serem contratados ou convidados no âmbito de parcerias e iniciativas do governo;
- ✓ Divulgação de mensagens e vídeos curtos sobre a matéria de segurança da informação por via do correio eletrónico e página oficial da instituição;
- ✓ Criação de uma coluna na revista oficial para veicular matérias ligadas a segurança da informação;
- ✓ Expandir a divulgação de mensagens curtas (neste momento dominante a nível central) nos papéis de parede para todos os dispositivos de utilizador final. Fixação de panfletos em locais estratégicos e de fácil visibilidade em todas as unidades da AT.

Será necessário criar um programa de treinamento de base ou inicial a ser ministrado sempre que forem admitidos novos funcionários ou observar-se a transferência de funcionários para posições ou sectores onde os requisitos de segurança sejam diferentes dos da proveniência.

A organização deve adotar um mecanismo de testes de conhecimentos a ser submetido a todos os colaboradores numa base rotineira. Estes testes devem versar sobre aspetos práticos do dia-a-dia e a atitudes tomadas quando em presença de ataque ou suspeita de tentativa de ataque. Os resultados dos testes devem ser divulgados para conhecimento geral sem revelar os nomes dos que porventura tenham procedido mal. Os mesmos serão usados para direcionar as formações no sentido de reforçar os aspetos que se julgarem menos estabelecidos ou omissos.

Conteúdos a abordar

Estas ações de consciencialização e treinamento devem abordar de forma clara e com uma linguagem de fácil compreensão os aspetos contidos na política de segurança da informação especialmente as que dizem respeito aos deveres dos utilizadores; os procedimentos no uso dos ativos de TI da organização; cuidados com relação troca ou partilha da informação quer de forma verbal, eletrónica ou por meios físicos; e todas as matérias ligadas à segurança física que possam impactar na segurança da informação.

À lista devem ser acrescidas às matérias ligadas a legislação específica e aos aspetos que resultem da análise dos incidentes que a organização faça ou que receba de outras entidades e que suscitam a necessidade de realização de formação para a sua mitigação.

6 CONCLUSÃO E TRABALHOS FUTUROS

A metodologia seguida no presente trabalho permitiu a produção de informação qualitativa e quantitativa que possibilita ter uma leitura a escala nacional de como a AT se posiciona em relação à segurança da infraestrutura de TI e formação dos técnicos de TI. Foi possível identificar os pontos fortes como sejam a implementação de alguns controles de segurança, existência de uma política de segurança da informação e parcerias com outras instituições públicas melhor posicionadas em matérias de segurança da informação, bem como os pontos fracos, com destaque para falta de cultura de governança para a área de TI especialmente para a governança da segurança da informação, a falta de técnicos devidamente formados e a baixa consciencialização sobre a segurança da informação. Os entrevistados mostraram-se abertos e colaborativos o que permitiu desenhar a situação real, listar e descrever as dificuldades bem como conhecer a visão futura no que toca a segurança da infraestrutura de TI e com isso mapear os segmentos onde há oportunidades para serem explorados sendo a prioridade para a segurança da rede de dados.

Foi possível confirmar que apesar da AT encontrar-se num bom caminho com o projeto de modernização da infraestrutura tecnológica em curso, ainda se depara com desafios para a efetiva materialização dos mecanismos de segurança e adoção das boas práticas para a segurança da infraestrutura de TI, devido sobretudo, aos baixos investimentos na área das TICs e às fragilidades na gestão dos recursos existentes. Entende-se que a exiguidade de fundos pode ser compensada através da otimização dos processos de gestão financeira por forma a evitar desperdícios e melhorar a eficácia e a eficiência. Portanto, uma melhor planificação para a área de TI, direcionando os investimentos para soluções que sejam sustentáveis a médio e longo prazos e impactantes no sentido de promover a digitalização e simplificação dos processos, evitando a duplicação de esforços, ajudará a alcançar ganhos que incidam na redução dos custos operacionais e consequentemente possibilitar investimentos para área de segurança na infraestrutura de TI, que neste momento encontra-se bastante penalizada no que se refere a alocação de fundos.

Pese embora o otimismo nos resultados obtidos, olhando para as soluções propostas à questão levantada e aos desafios da organização é de concordar que há ainda muito a ser explorado e aprofundado para alavancar este sector crucial a níveis superiores. Grande parte dos problemas de segurança da informação na AT, quer seja na infraestrutura de TI assim como na formação de quadros nas matérias relacionadas, podem ser melhor endereçadas partindo de uma governança

bem estabelecida. Assim, assumindo que para o cumprimento da sua missão a instituição tem as TICs como um fator estratégico, julga-se que trabalhos complementares ao presente podem ser considerados para que a Autoridade Tributária se posicione como uma instituição de excelência na prestação de serviços públicos e que no futuro alcance o patamar de uma instituição de referência internacional na arrecadação de receitas, conforme refere a visão da organização.

Propostas para futuros trabalhos:

Implementação da governança da segurança da informação

Para uma efetiva materialização das medidas já implementadas no âmbito do projeto de modernização da infraestrutura tecnológica em curso na AT e das propostas no presente trabalho é importante que seja feito um estudo para a implementação de um modelo de governança da segurança da informação na AT. Conforme apurou-se, a instituição tem neste momento projetos estruturantes implementados em parceria com outros órgãos públicos assim como empresas privadas sendo a gestão dos serviços feita à margem da direção das TICs. Apesar de ser este o sector legalmente estabelecido na AT para velar sobre todas as matérias ligadas às TICs, não tem sobre si a gestão/controlo de todos os projetos e iniciativas, não podendo, portanto, garantir a efetiva implementação e harmonização das políticas de segurança.

Interoperabilidade dos sistemas da AT

É de sugerir um estudo para promover os mecanismos de comunicação segura entre os sistemas da AT que atualmente funcionam de forma isolada. As infraestruturas de TI criadas para cada sistema dão suporte aos serviços que são oferecidos aos mesmos grupos de interessados, usando diferentes pontos e políticas de acesso, o que vem propiciar a duplicação de bases de dados e/ou dispersão de informações complementares. Uma vez estabelecidas as plataformas eletrónicas de comunicação e partilha da informação entre os sistemas poder-se-á abandonar a execução de cópias da informação via discos externos de um ambiente para o outro, bem como a introdução manual de mesmos dados nos diferentes sistemas, geralmente feita pelos funcionários da AT o que tem levado a erros e inconsistência dos dados. Esta solução deverá definir e incorporar os mecanismos para a partilha de qualquer informação de forma eletrónica com outras instituições públicas assim como privadas com destaque para as instituições financeiras, defesa e segurança, ligadas aos processos de comércio interno e externo.

REFERÊNCIAS

Albugmi, A., Alassafi, M., Walters, R., & Wills, G. (2016). *Data security in cloud computing*. Recuperado de https://eprints.soton.ac.uk/401802/1/paper_2final.pdf

Andrés, S., kenyon, B., & Birkholz, E. (2004). *Security Sage's guide to hardening the network infrastructure*. Rockland, US: Syngress.

Associação Brasileira de Normas Técnicas. (2013). Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação. (ABNT NBR ISO/IEC 27014:2013).

Atieh, A. (2021). *Assuring the optimum security level for network, phisical and cloud infrastructure*. Recuperado de https://www.scienceopen.com/hosted-document?doi=10.14293/S2199-1006.1.SOR-.PPZTVGD.v1

Baldwin, B. (2023). *Controle de segurança: segurança de DevOps.* Recuperado de https://learn.microsoft.com/pt-br/security/benchmark/azure/mcsb-devops-security [Acedido em 04 de Agosto de 2023]

Decreto n.º 50/2002, de 26 de dezembro. (2002). Cria a Unidade Técnica de Implementação da Política de Informática-UT1CT. Boletim da República, 1ª Série - N.º 52.

Decreto n.º 60/2017, de 6 de novembro. (2017). Redefine o âmbito das atribuições do instituto nacional de tecnologias de informação e comunicação. Boletim da República, 1ª Série - N.º 173.

Decreto n.º 61/2017, de 6 de novembro. (2017). Cria o instituto nacional de governo eletrónico. Boletim da República, 1ª Série - N.º 173.

Decreto n.º 82/2020, de 10 de setembro. (2020). Aprova o regulamento do uso do domínico "mz" Moçambique. Boletim da República, 1ª Série - N.º 174.

Decreto n.º 9/2011, de 4 de maio. (2011). Cria o Instituto Nacional de Tecnologias de Informação e Comunicação, abreviadamente designado por INTIC, e extingue a UTICT, criada pelo Decreto n.º 50/2002, de 26 de dezembro. Boletim da República, 1ª Série - N.º 18.

DosSantos, L., & Baruque, L. (2010). *Governança em tecnologia de Informação.* Rio de Janeiro, Brasil: Fábio Rapello Alencar.

EC-Council (2021). *Network Defense Essentials*. New Mexico, USA: EC-Council. Recuperado de https://codered.eccouncil.org/

Fernandes, A., & DeAbreu, V. (2014). *Implementando a governança de TI*. Rio de Janeiro, Brasil: BRASPORT Livros e Multimídia Lda.

Gil, A. (2002). *Como elaborar projetos de pesquisa* (4a ed.). São Paulo, Brasil: Editora Atlas.

Goodrich, M., & Tamassia, R. (2014). *Introduction to Computer Security*. Londres, UK: Pearson Editora.

IBM (2021). *Why IT infrastructure is important*. Recuperado de https://www.ibm.com/topics/infrastructure

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022). ISO

Iron Mountein. (n.d.). *Best practices for data destruction*. Consultado a 12 de Agosto de 2023. https://www.ironmountain.com/resources/whitepapers/b/best-practices-for-data-destruction

Kistler, K. (n.d.). *4 Security technology trends dominating the industry.* Consultado a 2 de Agosto de 2023. https://butterflymx.com/blog/security-technology/

Lei n.º 1/2006, de 22 de março. (2006). Cria a Autoridade Tributária de Moçambique. Boletim da República, 1ª Série - N.º 12.

Lei n.º 3/2017, de 9 de janeiro. (2017). Lei de transações eletrónicas. Boletim da República, 1ª Série - N.º 5.

Lei n.º 4/2016, de 3 de junho. (2016). Altera a Lei n.º 8/2004. Lei das Telecomunicações. Boletim da República, 1ª Série - N.º 66.

Manoel, S. (2014). *Governança da segurança da informação: como criar oportunidades para o seu negócio*. Rio de Janeiro, Brasil: BRASPORT Livros e Multimídia Lda.

Nakamura, E., & Geus, P. (2007). *Segurança de redes em ambientes coorporativos*. São Paulo, Brasil: Novatec Editora Lda.

Oliveira, A. (2022). *Quem é a geração Z? Quais as características mais marcantes?* Consultado a 15 de Agosto de 2023. https://mindminers.com/blog/quem-e-a-geracao-z-caracteristicas/

Panetta, K. (2016). *Gartner's top 10 technologies for information security.* Consultado a 2 de Agosto de 2023. https://www.gartner.com/smarterwithgartner/gartners-top-10-technologies-for-information-security

Resolução n.º 17/2018, de 21 de junho. (2018). Aprova a política para a sociedade da informação de Moçambique. Boletim da República, 1ª Série - N.º 122.

Resolução n.º 52/2019, de 16 de outubro. (2019). Aprova o Plano Estratégico para a Sociedade de Informação 2019-2028 e o respetivo Plano Operacional. Boletim da República, 1ª Série - N.º 199.

Resolução n.º 69/2021 de 31 de dezembro. (2021). Aprova a política de segurança cibernética e estratégia da sua implementação. Boletim da República, 1ª Série - N.º 253.

Stair, R., & Reynolds, G. (2018). *Principles of information systems* (13a ed.). Boston, US: Cengage Learning

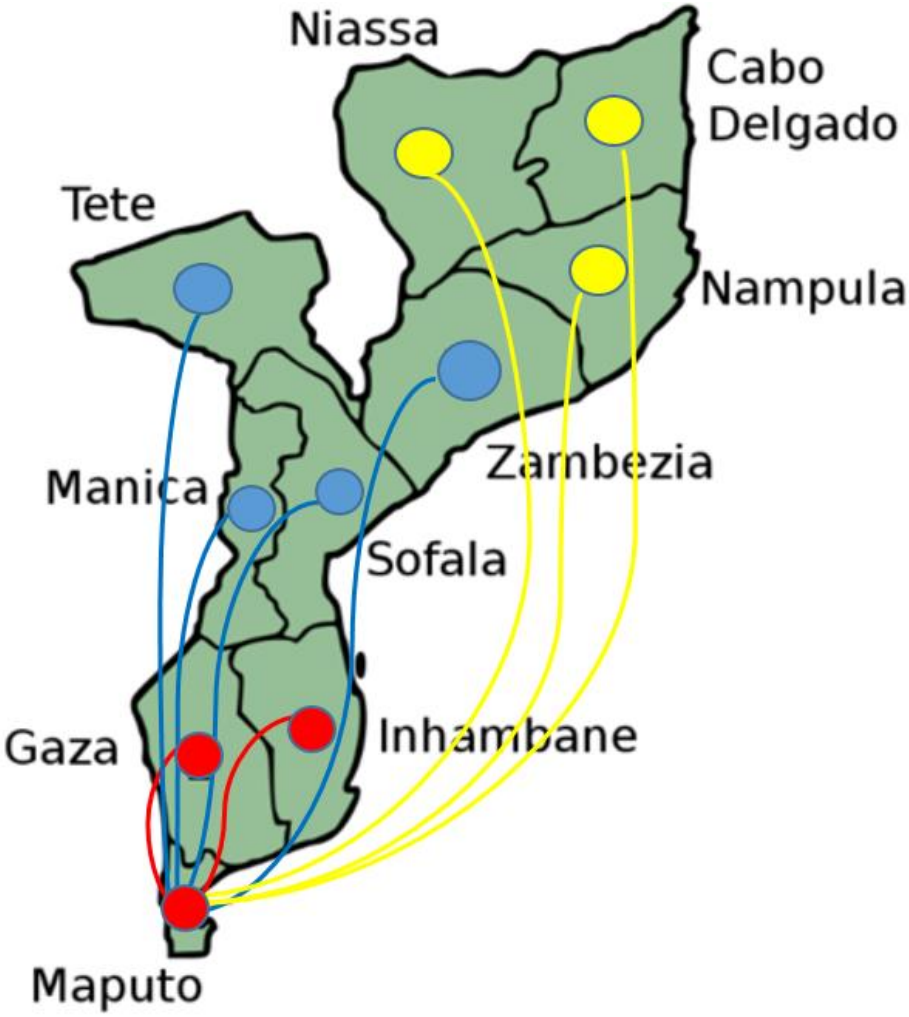
Stallings, W., & Brown, L. (2015). *Computer security principles and practice* (3a ed.). US: Pearson.

WalkMe Team. (2023). *COBIT vs. ITIL vs. other IT frameworks: which is the best?*. Consultado a 09 de Agosto de 2023. https://www.walkme.com/blog/cobit-vs-itil-vs-other-it-frameworks/

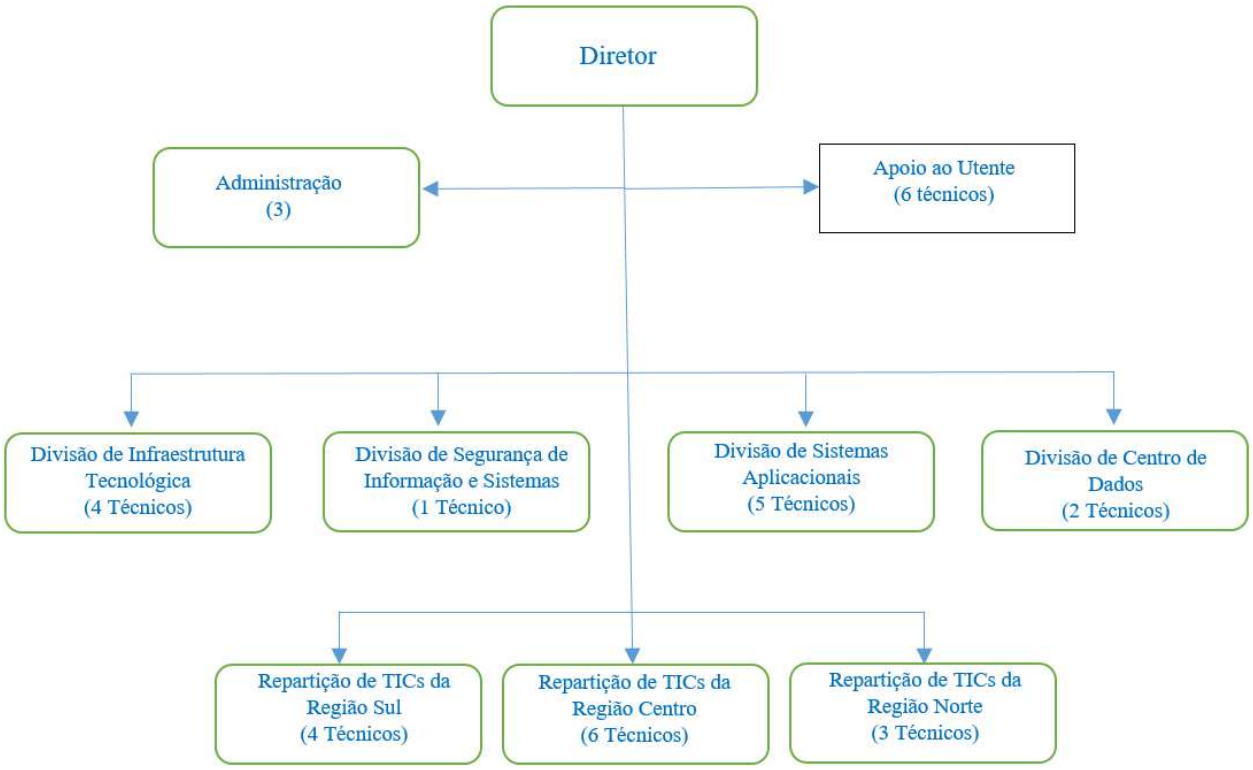
West, B. (2023). *Information security governance*. Consultado a 10 de Agosto de 2023. https://www.paloaltonetworks.com/blog/prisma-cloud/information-security-governance/

Wikipedia. (2021). *Centro de operações de segurança.* Consultado a 4 de Agosto de 2023. https://pt.wikipedia.org/wiki/Centro_de_opera%C3%A7%C3%B5es_de_seguran%C3%A7a#:~:text=Um%20centro%20de%20opera%C3%A7%C3%B5es%20de%20seguran%C3%A7a%20%28em%20ingl%C3%AAs,de%20detec%C3%A7%C3%A3o%20e%20rea%C3%A7%C3%A3o%20a%20incidentes%20de%20seguran%C3%A7a

Apêndice A – Presença da AT no território Moçambicano e disposição das linhas alugadas de comunicação.



Apêndice B – Estrutura orgânica da direção de tecnologias de informação e comunicação.



Apêndice C – Guião de entrevista ao Diretor de TICs da AT

A quantos anos é funcionário da AT?

Já participou de alguma formação em governança de TICs ou governança de segurança da informação?

A instituição terá adotado algum *framework* de governança? Se sim, qual?

Qual é o nível de importância que as TICs ocupam no negócio da Organização? (Baixo, moderado, importante, extremamente importante)

Como é feita a gestão do risco das TICs na organização?
Como avalia a segurança da infraestrutura de TI da AT?

A organização possui política de segurança aprovada e divulgada?
Se sim, na sua opinião ela está alinhada aos objetivos estratégicos da instituição?

Como é que a direção máxima da organização encara a segurança da informação, isto é, tem clara noção da sua importância e apoia a adoção das medidas de segurança?

Qual é a sua opinião em relação ao investimento que a organização faz na área das TICs? Acha o investimento suficiente para que as TICs estejam em altura de contribuir no seu máximo para a eficiência da instituição?

Existe uma política de formação de quadros em matérias de segurança da informação que incorpore as pessoas de todos os níveis e sectores da organização?

Tendo em conta as novas ameaças à segurança das infraestruturas críticas, estará a equipa técnica devidamente treinada?
A AT encontra-se no processo de modernização tecnológica. Na sua opinião, quais são os maiores desafios para a segurança da infraestrutura de TI que gostava de ver resolvidos?

Apêndice D – Guião de entrevista ao Chefe da Divisão de Segurança da AT

A quantos anos é funcionário da AT?
A organização possui política de segurança da informação?
Se tiver respondido sim à pergunta anterior, como avalia o nível de entendimento e cumprimento das políticas de segurança por parte dos utilizadores das TICs?

Acha que as políticas são suficientes para cobrir os riscos da TI para o negócio da instituição?
É feita análise de vulnerabilidades à infraestrutura de TI? Se sim, a análise é regular?

Quais são as principais vulnerabilidades com que se deparam e qual o tratamento dado?
Dos controles abaixo listados identifique os que já estão implementados. (Políticas de controlo de acesso, políticas de password, scan do perímetro, política de backups, política de gestão de alterações, política de atualização de software, antivírus e/ou *endpoint security*, *IDS/IPS*, *firewall*, segmentação da rede, criptografia de dados, política de destruição da informação, auditoria informática, testes de penetração, segurança de redes, outros)
Que controles estão por implementar?

A organização possui um SOC?
Acha pertinente ter um SOC dentro da organização?

Existe ou existem entidades externas públicas ou privadas às quais são ou podem ser submetidos os incidentes que necessitem de tratamento de outro nível? Se sim, pode indicar as com as quais têm parcerias?

Existem áreas críticas do negócio/segurança identificadas? Se sim, elas estão demarcadas nas plantas do(s) edifício(s)?

Quais são os fatores de risco para a segurança da informação que requerem atenção redobrada? As medidas de controle são efetivas para os mesmos?

Como é feita a consciencialização/formação dos utilizadores em matérias de segurança da informação? Existe algum mecanismo de teste para aferir o nível de consciencialização?

A organização usa encriptação de dados no armazenamento e/ou transmissão?
Existe uma política de redundância de ativos críticos?
Em caso de desastre, a organização possui um plano de recuperação?

Apêndice E – Formulário de Inquérito aos profissionais de TICs da AT

Inquérito para os Técnicos de TI - Geral

Este inquérito tem como
objetivo a recolha da informação para a realização de um trabalho de mestrado em Engenharia Informática. A população alvo são
os técnicos e profissionais do sector das TICs da Autoridade Tributária.

Os dados fornecidos são
tratados como confidenciais e anónimos e servirão exclusivamente para fins de investigação cientifica. Peço que siga as instruções e seja preciso nas respostas.
jmuamba1@gmail.com

Desde já agradeço pela ajuda!

* Indicates required question

1. 1 - A quantos anos é funcionário da AT?

Primeira Parte

2. 2 - Acha que a instituição tem uma estratégia de formação que se adequa as necessidades dos técnicos de TI? *

Mark only one oval.

- ( ) Sim
- ( ) A estratégia de formação não reflete as necessidades
- ( ) Não há estratégia

3. 3 - Quando é que se beneficiou da última formação? *

Mark only one oval.

- ( ) A menos de um ano
- ( ) A mais de um ano
- ( ) A mais de 3 anos

4. 4 - As formações de que tem beneficiado ajudam na melhoria da execução das suas atividades? *

Mark only one oval.

- ( ) Sim
- ( ) Não tem impacto considerável
- ( ) As formações têm sido para áreas que não são de TI

5. 5 - Já se beneficiou de alguma formação sobre segurança da informação? *

Mark only one oval.

- ( ) Pelo menos uma
- ( ) Mais de uma formação
- ( ) Participei em palestras internas
- ( ) Nunca

6. 6 - Tem conhecimento sobre a politica de segurança da organização? *

Mark only one oval.

- ◯ Nunca tive acesso
- ◯ Tenho conhecimento básico
- ◯ Aplicamos no dia-a-dia
- ◯ Sim

Segunda Parte

7. 7 - De que áreas tem interesse a nível das TICs? (Máximo duas) *

Tick all that apply.

- ☐ Segurança de TI
- ☐ Redes e comunicações
- ☐ Desenvolvimento de software
- ☐ Análise de dados
- ☐ Base de dados
- ☐ Análise de sistemas
- ☐ Sistemas operativos
- ☐ Virtualização de servidores
- ☐ Reparação de Hardware
- ☐ Other:

8. 8 - Como avalia a organização em termos de segurança da informação após início da modernização tecnológica (ano de 2015)? *

Mark only one oval.

- ◯ Ainda deixa a desejar
- ◯ Melhorou bastante porem há muito que fazer
- ◯ Não noto diferença

9. 9 - Em sua opinião, acha que os utilizadores conhecem os cuidados básicos da segurança de informação? *

Mark only one oval.

- ◯ Muitos não tem noção dos riscos das TICs
- ◯ Alguns sabem, mas ignoram as recomendações
- ◯ Os utilizadores são zelosos na observação das medidas de segurança

Apêndice F – Formulário de Inquérito aos Técnicos de Redes da AT

Inquérito aos Técnicos de Network

Este inquérito tem como
objetivo a recolha da informação para a realização de um trabalho de mestrado em Engenharia Informática a efetuar na Autoridade Tributária. A população alvo são os técnicos e profissionais do sector das TICs.

Os dados fornecidos são
tratados como confidenciais e anónimos e servirão exclusivamente para fins de investigação cientifica. Peço que siga as instruções e seja preciso nas respostas.

Desde já agradeço pela ajuda!

* Indicates required question

1. 1 - A quantos anos é funcionário da AT?

Primeira Parte

2. 2 - Tem se beneficiado de formações em matérias sobre segurança de informação? *

Mark only one oval.

- ◯ Sim e de forma regular
- ◯ Sim, porém, não são regulares
- ◯ Não tenho recebido

3. 3 - Tem conhecimento sobre o que é infraestrutura crítica de TI? *

   Mark only one oval.

   - ◯ Bastante
   - ◯ Suficiente
   - ◯ Não

4. 4 - Na sua opinião estão implementados mecanismos de controle de perímetro adequados para proteção do tráfego de e para fora da instituição? *

   Mark only one oval.

   - ◯ Sim
   - ◯ Não

5. 5 - Se sim, quais?

   Tick all that apply.

   - ☐ Firewall
   - ☐ IPS/IDS
   - ☐ Filtragem de pacotes
   - ☐ Controle de Aplicações
   - ☐ Other: _____

Segunda Parte

6. 6 - Quais as tecnologias usadas na rede alargada (WAN) para a conexão entre as unidades da AT? *

   Tick all that apply.

   - ☐ SDWAN
   - ☐ Layer 2 Leased Lines
   - ☐ Remote VPN
   - ☐ Site-to-site VPN
   - ☐ MPLS

7. 7 - Os gabinetes para equipamentos de rede estão protegidos em todas as unidades orgânicas? *

   Mark only one oval.

   - ◯ Sim
   - ◯ Não
   - ◯ Somente em algumas unidades

8. 8 - A atualização das versões do hardware assim como software responde às politicas da organização. *

   Mark only one oval.

   - ◯ Sim
   - ◯ Não
   - ◯ Desconheço essa política

9. 9 - Acha que as medidas de segurança dos *endpoints* é efetiva? *

Mark only one oval.

- ( ) Apenas usamos antivírus
- ( ) É um grande ponto de falha de segurança
- ( ) Temos uma combinação de controles que ajudam a proteção
- ( ) Precisamos uniformizar as medidas

Anexo - Tabela periódica da Segurança da Informação – Paul Bird

Fonte: *https://www.opservices.com.br/glossario-da-cyber-security/*