UNIVERSIDADE POLITÉCNICA APOLITÉCNICA

INSTITUTO SUPERIOR DE GESTÃO, CIÊNCIAS E TECNOLOGIAS

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

IMPLEMENTAÇÃO DE FERRAMENTAS & TÉCNICAS DE CIBERSEGURANÇA PARA GRANDES EMPRESAS DE CONSTRUÇÃO CIVIL EM MOÇAMBIQUE EM OBSERVÂNCIA COM A NORMA ISO 27001

CASO DE ESTUDO: MOTA-ENGIL MOÇAMBIQUE

(2018-2022)

FÁTIMA DANUZA HAMIDO

Maputo, Janeiro de 2024

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

Supervisor: Mestre Eng.º Ângelo Sumana

Maputo, Janeiro de 2024

DECLARAÇÃO DE HONRA

Declaro por minha honra que este trabalho é resultado da minha pesquisa pessoal e das orientações do meu tutor, feita segundo os parâmetros em vigor da Universidade Politécnica. O seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto e na Bibliografia.

Declaro também que este trabalho não foi apresentado em nenhuma Instituição para obtenção de qualquer Grau Académico.

Maputo, Janeiro de 2024

_____

(Fátima Danuza Hamido)

DEDICATÓRIA

Dedico este trabalho a minha mãe (Sara J. Hamido Pimentel), pai (Pedro Pimentel) e os meus dois irmãos (Pedro e Yumara) pelo apoio abnegado que me concederam para que o mesmo se tornasse uma realidade, mesmo tendo as suas obrigações não pouparam esforços prestando-me uma singela contribuição. Estendo a minha dedicatória em memoria da minha amiga Jeneth Margarida pela paciência e incentivos que concedeu de forma incansável.

AGRADECIMENTOS

Em primeiro lugar agradeço a Allah SWT, por ter estado do meu lado durante o meu percurso académico.

Ao meu supervisor, Mestre Engº Ângelo Sumana pela sua preciosa orientação e disponibilidade durante todo o decorrer da elaboração desta monografia.

A minha família, amigos e colegas por acreditarem em mim e incentivarem-me. Estendo os meus agradecimentos ao Engenheiro Abdul Júnior pelo seu empenho em ajudar-me no desenvolvimento desta pesquisa.

A Mota-Engil Moçambique, pelo apoio no fornecimento e aplicação da informação.

Por fim, agradeço a todas as pessoas que fizeram parte desta etapa decisiva da minha vida.

PARECER DO SUPERVISOR

Eu, Ângelo Mário Barros André Fernandes Sumana, da Universidade, declaro que supervisionei e acompanhei o trabalho final de curso, sob a forma de Monografia do estudante Fátima Danuza Hamido cujo tema é **Implementação de Ferramentas & Técnicas de Cibersegurança para grandes empresas de construção civil em Moçambique em observância com a norma ISO 27001** declaro que o trabalho é da autoria do Estudante e reúne todos requisitos pré-estabelecidos pela universidade Politécnica para trabalhos desta natureza, pelo que está pronto para defesa pública.

_____

Mestre Engº Ângelo Mário Barros André Fernandes Sumana

RESUMO

Numa era informatizada, as grandes empresas moçambicanas têm assistido a um aumento significativo na digitalização de dados de informação, levando ao aumento dos crimes cibernéticos.

Foi realizado um estudo na Mota-Engil Moçambique no qual se constatou a necessidade de formação e preparação para a implementação de estratégias de cibersegurança dentro das normas ISO 27001. O estudo introduziu a teoria da cibersegurança e a colecta de dados em situações de ameaça, propondo ferramentas e técnicas para implementação da segurança cibernética no contexto da empresa. Como métodos de pesquisa, foram utilizados os métodos descritivo e exploratório.

A proposta visa melhorar o controle e a precisão na criação de relatórios mensais e anuais, fortalecer a protecção da infra-estrutura, conscientizar os funcionários e realizar treinos contínuos, enquanto se investe no treino da equipe de TI e dos funcionários e na escolha de ferramentas robustas de segurança cibernética.

Palavras-chave: Cibersegurança, ISO, Cyber ataques, Ferramentas e Técnicas

ABSTRACT

In a computerized era, large Mozambican companies have seen a significant increase in the digitization of information data, leading to an increase in cybercrimes.

The study carried out at Mota-Engil Mozambique found the need for training and preparation for the implementation of cybersecurity strategies within ISO 27001 standards. The dynamic study of cybersecurity theory and data collection in threat situations, proposing tools and techniques for implement cybersecurity in the business context. Descriptive and exploratory methods were used as research methods.

The proposal aims to improve control and precision in the creation of monthly and annual reports, reinforce infrastructure protection, raise employee awareness and carry out ongoing training, while investing in the training of IT staff and employees and the choice of robust tools of cybersecurity.

Keywords: Cybersecurity, ISO, Cyber attacks, Tools and Techniques

LISTA DE FIGURAS

LISTA DE TABELAS

I. Lista de Siglas e Acrónimos

2FA – Autenticação de 2 factores

ACL - Lista de controle de acesso

AD – Active Directory

AP – Access point

AV - Antivírus

CBA – Autenticação baseada em certificado

CPU - Unidade Central de Processamento

Cyber - provém da cibernética, uma abordagem transdisciplinar para explorar sistemas regulatórios e intencionais.

DAC - Controle de acesso discricionário

Dark web - é o colectivo oculto de sites da Internet que só podem ser acessados com um navegador de Internet especializado.

DDoS - é o acrónimo para *Distributed Denial of Service* que, traduzido do inglês, significa algo aproximado a negação distribuída de serviço, termo que evidência a natureza coordenada destes tipos de ataques maliciosos.

DLP - Prevenção contra a perda de dados

FCM – Fiber Cloud Messaging

EU – União europeia

Gateway - é uma classe de dispositivos que atuam como intermediários de comunicação entre diferentes redes ou sistemas que envolvem protocolos, linguagens ou arquiteturas distintas.

Hackers - são pessoas que se dedicam intensamente a solucionar problemas e criar soluções que envolvem tecnologia, computação e informática.

ID - *Identity*

IDS - Sistema de Detecção de Intrusão

IEC – International Electrotechnical Commission

iOS - é um sistema operacional móvel da Apple Inc.

IPS - Sistema de Prevenção de Intrusão

ISO - *International Standards Organization*

Malware - é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas.

MFA – Autenticação multifactor

ME - Mota-Engil

MEMZ – Mota-Engil Moçambique

Microsoft Azure - é uma plataforma de computação em nuvem executada pela Microsoft, que oferece acesso, gerenciamento e desenvolvimento de aplicativos e serviços por meio de data *centers* globais.

NGIPS - Next-Generation Intrusion Prevention System

Ransomware - um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

PC – Personal computer

Phishing - que deve o seu nome à palavra inglesa "*fishing*" que significa "pescar", consiste em utilizar métodos tecnológicos que levam o utilizador a revelar dados pessoais e ou confidenciais, como, por exemplo, carregar num link malicioso.

PIN – Número de identificação pessoal

PKI - é um acrónimo para infra-estrutura de chave pública, que é a tecnologia por trás dos certificados digitais.

SD - *Secure Digital*

SGSI - Sistema de Gestão de Segurança da Informação

SQL - é o acrónimo para *Structured Query Language*, traduzido do inglês, significa linguagem de consulta estruturada, é uma linguagem de domínio específico desenvolvida

para gerenciar dados relacionais em um sistema de gerenciamento de banco de dados, ou para processamento de fluxo de dados em um sistema de gerenciamento de fluxo de dados.

SPA – *Stateful Protocol Analysis*

SSL - *Secure Sockets Layer*

SSO - Single Sign-On (é uma solução tecnológica que permite que esses aplicativos usem a mesma senha para todos os acessos de forma segura e transparente).

TCO – Custo total de propriedades

TI – Tecnologia da Informação

TLS - *Transport Layer Security*

TPM - Trusted Platform Module

VPN - Virtual Private Network

Índice

CAPÍTULO I – INTRODUÇÃO

1.1 Introdução

Nos últimos tempos vem-se observando que a segurança da informação tem ganho cada vez mais espaço em termos de prioridade, todos os dias vemos o desenvolvimento de novas técnicas e ferramentas com o objectivo de proteger os activos e informações de empresas contra uma ampla gama de ameaças, incluindo cyber ataques, perdas de dados e violações de privacidade.

Por outro lado, a escolha das ferramentas e técnicas de cibersegurança mais adequadas para uma grande empresa depende de uma série de factores, incluindo o tamanho e a complexidade da empresa, o sector em que ela actua, os riscos aos quais ela está exposta e ao orçamento disponível.

Segundo Kaspersky (2023) cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas electrónicos, redes e dados de contra-ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações electrónicas. O termo é aplicável a uma variedade de contextos, desde negócios até à computação móvel, e pode ser dividido em algumas categorias comuns.

Nesse contexto, adoptar uma abordagem sistemática e abrangente de implementação de ferramentas e técnicas de cibersegurança pode ajudar a proteger os activos de informação de uma empresa. Com o auxílio das normas e padrões ISO 27001, o pesquisador vai abordar a segurança da informação para grandes empresas de construção em Moçambique em conformidade com a norma atrás referida.

Em geral norma é um termo que advém do latim e significa “esquadro”. Uma norma é uma regra que deve ser respeitada e que permite ajustar determinadas condutas ou actividades. (Conceito 2019)

De acordo com a Devoteam Ciber Trust (2023) norma ISO 27001 é o padrão e a referência internacional para a gestão da segurança da informação, assim como a ISO 9001 é a referência internacional para a certificação de gestão em qualidade.

Com base em observações feitas constatou-se que nos últimos tempos grandes empresas em Moçambique têm sofrido ataques cibernéticos sistematicamente, isso traz muitos problemas no seio das empresas quer do lado financeiro quer social. As grandes empresas

de construção civil têm investido incansavelmente em estratégias de cibersegurança, mesmo assim, por vezes tem sido observado falhas na sua implementação. Ocasionalmente por quererem recursos para alocar na infra-estrutura de segurança, acabam por não cumprir com a norma ISO 27001.

O cumprimento da norma ISO 27001, garante confiabilidade e segurança tanto do lado dos utilizadores como do lado dos administradores dos sistema e segurança. O não cumprimento da norma ISO 27001 possibilita a permissibilidade de tentativas e reais ataques as infra-estruturas de informação e acabam por originar prejuízos tremendos podendo toda a informação ficar comprometida.

O comprometimento de dados e informação em uma infra-estrutura de rede de uma empresa pode gerar inacessibilidade de serviços cruciais para funcionamento da empresa, ou seja, os serviços podem ficar inoperacionais, o roubo ou criptografia dos dados, sequestro e mesmo depois de se pagar para a sua recuperação não se consegue obter acesso aos dados novamente.

1.2. Problema

A mudança nas relações humanas com a tecnologia, em particular no âmbito corporativo, traz não somente avanços e produtividade, é parte dessa mudança o surgimento de riscos e a necessidade de adaptação à nova realidade. Portanto, tem sido motivo de preocupação para os gestores de cibersegurança os mecanismos de controle de redes e dados internos sigilosos. Dispositivos mal configurados, e má adaptação do sector de tecnologia da informação em uma organização será entrada para intrusos mal-intencionados através de vírus, malwares e ransomwares (CUSTOIAS MENDONÇA; CUNHA, 2019)

Sendo a afirmação acima um ponto de partida, pode-se concluir que a ausência de informação sobre as boas praticas de cibersegurança levam aos cyber ataques que com o passar dos anos tornaram-se mais destrutivos, essas tentativas de roubar, danificar e ou destruir dados acabam por comprometer sites, servidores, pessoas físicas e podem culminar com a paralisação de actividades laborais, impactando negativamente as empresas e seus clientes.

Focando no caso de estudo na ME Moçambique, o pesquisador suspeita que a falta de formação e preparação para a implementação de estratégias dentro das normas ISO 27001, pode afectar a protecção dos dados. O pesquisador considera que a situação pode comprometer a segurança de dados e a infraestrutura da empresa devido à subestimação do que um cyber ataque pode causar, assim sendo, é importante garantir ferramentas e técnicas condizentes para a robustez e interceptação rápida de forma a se acautelar um cyber ataque. Dentro do contexto, o pesquisador pressupõe a elaboração da implementação de ferramentas e técnicas baseadas na norma ISO 27001, para posteriormente propor o seu uso na ME Moçambique.

1.3. Perguntas a investigar e Hipóteses a considerar

1.3.1. Formulação das Perguntas a investigar

- Quais são as ferramentas e técnicas de cibersegurança para grandes empresas de construção civil disponíveis na ME Moçambique?

- De que forma a implementação de ferramentas e técnicas de cibersegurança em observância com a norma ISO 27001 pode melhorar a segurança e protecção de dados de grandes empresas?

1.4. Justificativa

Tendo em conta que as grandes empresas moçambicanas de construção são um dos principais alvos dos cyber ataques devido ao grande volume de dados que manipulam. E que uma violação da segurança cibernética pode prejudicar gravemente a reputação de qualquer empresa junto aos seus clientes e parceiros, impactando nos seus lucros.

A escolha desta pesquisa assenta-se para além do interesse pessoal do investigador no tema e sua oportunidade de fazer parte na revisão das técnicas e ferramentas de cibersegurança em uma empresa onde esta inserida, na sua preocupação de que a observância da norma ISO 27001 irá garantir conformidade com os padrões internacionais e as leis locais de protecção de dados, tendo em conta a realidade moçambicana face a situação mundial.

1.5. Objectivos

1.5.1. Objectivo Geral

- Implementar ferramentas e técnicas de cibersegurança para grandes empresas de construção civil em Moçambique em observância da norma ISO 27001 tendo como caso de estudo a Mota-Engil Moçambique.

1.5.2. Objectivos Específicos

- Evidenciar os fundamentos teóricos sobre implementação de cibersegurança e a norma ISO 27001;
- Definir o procedimento de análise de ferramentas e técnicas de cibersegurança que compõem o processo de gerenciamento de segurança de dados;
- Analisar a implementação das medidas de cibersegurança;
- Desenhar um modelo de implementação e procedimento em observância da norma ISO 27001.

1.6. Delimitações do trabalho

A pesquisa será desenvolvida na cidade de Maputo, exclusivamente na empresa Mota-Engil Moçambique no departamento de sistemas de informação e comunicação. Em 2023, por se encontrar numa fase de revisão de estratégias de implementação de cibersegurança face aos cybers ataques estarem cada mais sofisticados.

Analisamos as técnicas existentes actualmente e as metodologias que podem ser implementadas em observância com a norma ISO 27001. De forma a se garantir maior protecção, segurança na infraestrutura de rede e segurança de dados.

1.6.1. Limitações do trabalho

- Umas grandes limitações deste trabalho é a falta de estudos sobre o tema no contexto moçambicano, sendo que os recursos para aprofundar as pesquisas são de difícil acesso;
- Para se poder aprofundar o estudo será importante realizar questionários físicos e digitais com recurso ao Google Docs, possivelmente poderá haver questões não respondidas devido ao facto das pessoas não estarem por vezes predispostas a colaborarem.

1.7. Capítulos Propostos

A pesquisa está dividida em seis capítulos, nomeadamente:

Primeiro capítulo: Introdução - é apresentado um enquadramento para este trabalho, indicado o seu objectivo e âmbito e descrita a sua estrutura.

Segundo capítulo: Revisão da Bibliográfica - neste capítulo pretende-se evidenciar uma revisão bibliográfica aprofundada, dos conceitos, sua evolução, princípios, técnicas e ferramentas de cibersegurança, que serão base para o estudo de caso.

Terceiro capítulo: Metodologia - são apresentados os métodos e técnicas utilizadas para análise e aplicadas para a materialização do trabalho prático.

Quarto capítulo: Caso de Estudo - consiste na análise dos dados, sendo feitas as interpretações e constatações sobre os dados, entrevistas e observações de campo recolhidos no decorrer da presente pesquisa.

Quinto capítulo: Apresentação e Analise dos Resultados: faz a apresentação da proposta realizada para a implementação do sistema de gestão de segurança da informação no INEM, com a definição do âmbito e alcance pretendido, a identificação e descrição das ferramentas necessárias ao processo de análise, avaliação e tratamento do risco.

Sexto capítulo: Conclusão - são traçadas conclusões e recomendações com base no estudo realizado.

Referencias. Bibliográficas - são enumerados livros, artigos técnicos, páginas de Web, entre outros, consultados para a realização deste trabalho.

CAPÍTULO II – REVISÃO BIBLIOGRÁFICA

Neste capítulo é abordado o conceito de cibersegurança evidenciado a sua magnitude como alavancar o desenvolvimento de segurança de dados de grandes empresas de construção civil em Moçambique, bem como, as ferramentas, técnicas, desafios e tendências em cibersegurança. São expostas as ameaças digitais e a importância da implementação com observância da norma ISO 27001 sua alocação como factor crítico de sucesso do seu desenvolvimento em grandes empresas de construção civil em Moçambique.

2.1. Conceito de Cibersegurança

De acordo com Gridinsoft (2023) a cibersegurança é definida como a defesa de redes, dados e informações contra o acesso não autorizado, adulteração ou sua destruição. Todas as redes, dados e conhecimento têm algo em comum; eles são o equivalente a dados armazenados em um banco. Um invasor pode acessar fisicamente o prédio e manipular os sistemas de segurança para entrar nos cofres do banco.

No entanto, cibersegurança é a prática de proteger sistemas críticos e informações confidenciais contra-ataques digitais. Também conhecida como segurança de tecnologia da informação (TI), as medidas de segurança cibernética são projectadas para combater ameaças contra sistemas e aplicações em rede, sejam essas ameaças originadas de dentro ou de fora de uma organização. (IBM 2022)

Na visão de Alves (2006, p. 15) a cibersegurança ou segurança da informação visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios.

Desta feita, a cibersegurança, ou segurança cibernética, é a arte de proteger redes, dispositivos e dados contra o acesso não autorizado ou uso criminoso, ou seja, ciberameaça, e a prática de garantir a confidencialidade, integridade e disponibilidade da informação no ciberespaço. (Faria 2022)

A cibersegurança concentra-se na protecção de dados contra invasores terceiros, como *spyware* ou acesso não autorizado. Oferece mecanismos de segurança e métodos de combate a *malware*.

2.1.1. Evolução da Ciberameaça

As organizações estão a adoptar cada vez mais soluções diversificadas de segurança para detectar e bloquear um único tipo de ataque cibernético, como *ransomware*, negação de serviço distribuída (DDoS), *phishing* de credenciais e injecção de SQL. No entanto, os cibercriminosos utilizam cada vez mais técnicas e combinam diferentes tipos de ataques em campanhas coordenadas, tornando-os mais eficazes contra-recursos de TI limitados e campanhas concentrando-se num único tipo de cibersegurança.

2.1.1.1. Cronologia de Cibersegurança

Antes do pesquisador aprofundar com os temas subsequentes é importante contextualizar com os principais marcos que ocorreram ao longo do tempo que levam aos estudos que serão expostos nos pontos que se seguem.

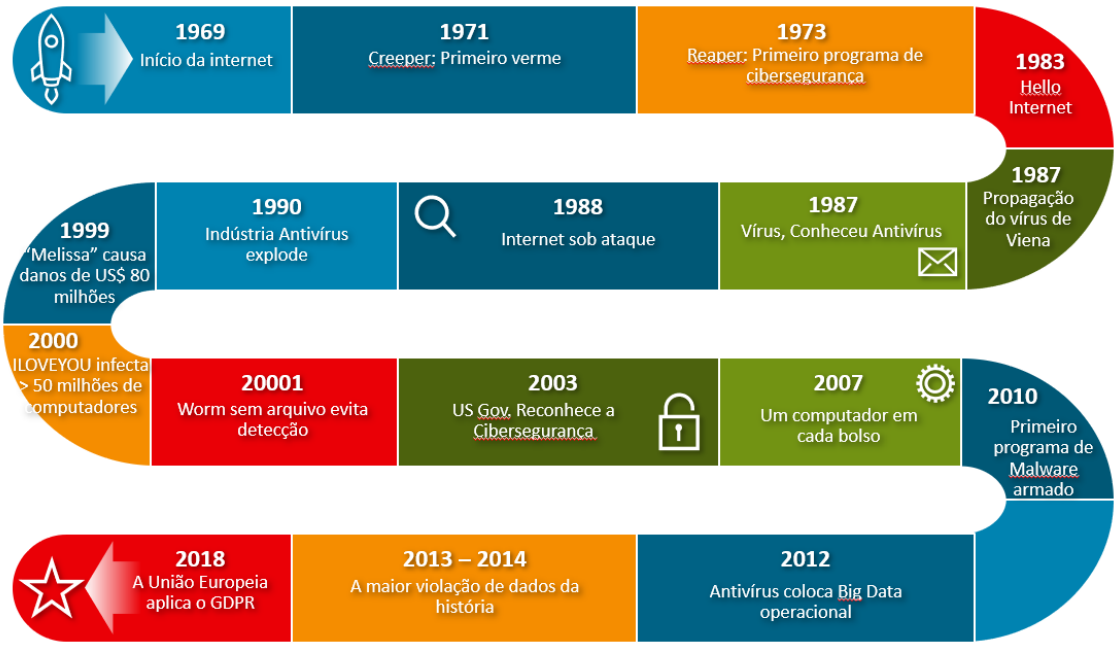

Fig. 2. 1 Principais eventos do marco cronologia de cibersegurança - (Fonte: Future of tech, 2023)

2.1.2. Princípios da Cibersegurança

Segundo Fernandes (2013), a protecção da informação é vital, sendo caracterizada pela trilogia CID, ou seja, Confidencialidade, Integridade e Disponibilidade, conforme a figura 2.2. abaixo ilustra:

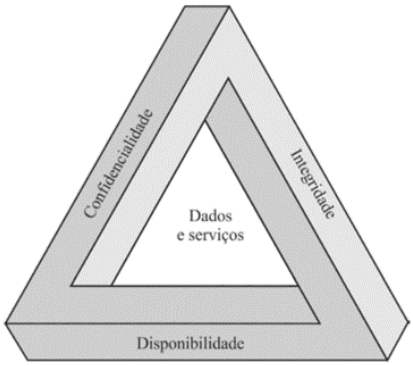

Fig. 2. 2 Trilogia de Princípios de Cibersegurança - (Fonte: Silva, 2023)

a. **Confidencialidade** – é acessível para usuários autorizados sempre que solicitarem e fica protegido o acesso por usuários não autorizados. A confidencialidade é a garantia de que os dados sejam conectados por quem realmente tem acesso.
b. **Integridade** - É a garantia de que a mensagem não foi alterada durante a transmissão, ou seja, é a garantia da exactidão e envio da informação completa;
c. **Disponibilidade** - É a precaução de que um sistema estará sempre disponível para usuários autorizados a qualquer momento para solicitações. Medidas mais frequentes de tempo de disponibilidade:
    - Tempo de utilização: representa a quantidade de tempo total que um sistema, aplicativo e dados ficam disponíveis. O tempo de utilização (ou *uptime*) é medido normalmente em unidades de segundos, minutos e horas, dentro de determinado mês.
    - Tempo de paralisação: apresenta a quantidade de tempo total que um sistema, aplicativo e dados não ficam acessíveis. O tempo de paralisação (ou *downtime*) também é medido em unidades de segundos, minutos e horas para um mês.

- Disponibilidade é calculada com o percentual de tempo durante o qual o sistema está disponível.

Além da trilogia, existem outros princípios de segurança que podem acrescentar outros aspectos a cibersegurança, tendo eles como: (Silva, 2023)

- **Legalidade** – Garantia de que a informação foi produzida em conformidade com a lei;
- **Autenticidade** - garante que o processo de comunicação entre os remetentes sejam exactamente como a mensagem ou informação enviada sem sofrer qualquer alteração no seu percurso ou envio.

A cibersegurança visa controlar os factores humanos, que são motivos frequentes de violações de dados em grandes empresas. Para evitar e combater estes problemas, os utilizadores devem compreender como evitá-los e combatê-los. As soluções são complexas, tornando a cibersegurança um campo crucial na protecção de redes informáticas e dados armazenados.

2.2. Ferramentas e Técnicas de Cibersegurança

2.2.1. Ferramentas de Cibersegurança

Nesta secção vai-se descrever as ferramentas específicas de cibersegurança utilizadas na construção civil, como *firewalls*, antivírus, detecção de intrusões, VPNs, entre outras, destacando como essas ferramentas contribuem para a segurança digital.

2.2.1.1. Antivírus e Antimalware

Para Lima (2022) Antivírus - é um tipo de programa de software que ajuda a proteger o sistema do computador contra vírus. Ele detecta os vírus no sistema do computador e os destrói. Basicamente, protege o sistema do computador de um *malware* específico. É usado para protecção contra algumas ameaças tradicionais e simples que podem danificar o sistema do computador. É usado principalmente em computadores pessoais para fins de segurança.

Desta feita, *Antimalware* é um antigo método de detecção de *malware* baseado em assinatura pode ser eficaz, mas os programas *antimalware* modernos podem detectar *malware* usando métodos que procuram comportamentos maliciosos. Esses métodos incluem impressões digitais de criminosos, que podem ser uma forma eficaz de identificar ameaças desconhecidas. A análise heurística é uma tecnologia de segurança cibernética nova e eficaz que pode detectar *malware* em arquivos e iniciar registos antes que ele tenha a chance de infectar o computador. (Gridinsoft 2023)

Antivírus e *antimalware* são softwares feitos para detectar, proteger contra e remover *malware*. Antivírus protege de vírus de uma forma antiquada, e *antimalware* abrange a todos os tipos de softwares maliciosos, incluindo vírus. Os antivírus e *antimalware* encontram-se em uma categoria mais abrangente chamada de cibersegurança.

2.2.1.2. Firewall

Segundo Fortinet (2023) uma firewall é uma solução de segurança de rede que protege a mesma contra tráfego indesejado. As *firewalls* bloqueiam o *malwar*e de entrada com base em um conjunto de regras pré-programadas. Essas regras também podem impedir que os usuários na rede conectem determinados sites e programas.

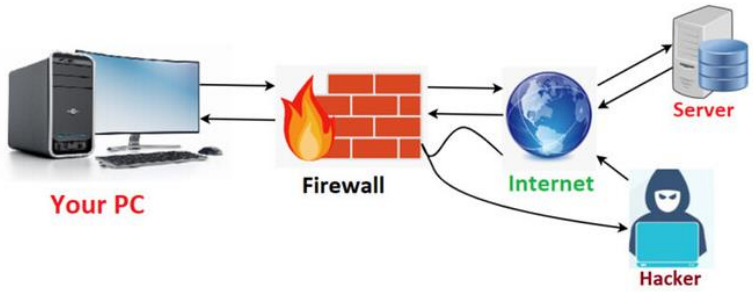

Fig. 2. 3 Ilustração de firewall com barreira de protecção entre internet e o host - (Fonte: Ismail, 2022)

2.2.1.2.1. Papel de Firewall em uma empresa de construção civil em Moçambique

De acordo com Cisco (2023) *Firewalls* são os principais equipamentos usados para segurança de perímetro de rede. A função de uma firewall é permitir ou negar o tráfego que tenta passar por ele com base em regras específicas predefinidas. Todos os *firewalls* desempenham a função de examinar o tráfego de rede e efectuar esse tráfego com base no conjunto de regras, porém os métodos que empregam podem ser diferentes. Existem três tipos diferentes de tecnologias de firewall:

a. Filtragem de Pacotes

A *firewall* de filtragem de pacotes simplesmente inspecciona o tráfego de entrada na camada de transporte do modelo de referência *Open System Interconnection* (OSI). A *firewall* de filtragem de pacotes analisa pacotes TCP ou UDP e compara-os a um conjunto de regras estabelecidas chamada lista de controle de acesso (ACL). A filtragem de pacotes inspecciona o pacote apenas para os seguintes elementos:

- Endereço de IP de origem;
- Porta de origem;
- Endereço de IP destino;
- Porta de destino;
- Protocolo.

b. Proxy

Uma firewall proxy, também conhecida como servidor proxy, actua em nome de *hosts* em segmentos de rede protegidos, garantindo que não haja conexões com o mundo externo. Eles são executados nas camadas superiores do modelo de referência OSI e são projectados para armazenar em cache informações comumente usadas para agilizar o tempo de resposta. No entanto, eles suportam apenas aplicativos e protocolos específicos, e a sua principal desvantagem é que eles são executados em sistemas operacionais, tornando os dispositivos tão seguros quanto o sistema operacional em que estão sendo executados.

c. Inspecção de estados

A inspecção de estado, também chamada de filtragem de pacotes com estado, é uma combinação de filtragem de pacotes e serviços de proxy. Essa tecnologia é a mais segura e oferece maior funcionalidade porque as conexões não são aplicadas apenas a uma ACL, mas também registadas em uma tabela de estados. Depois que uma conexão é estabelecida, todos os dados da sessão são comparados com a tabela de estados. Se os dados da sessão não corresponderem às informações da tabela de estado dessa conexão, a conexão será interrompida.

2.2.1.2. Sistemas de Detecção e Prevenção de Intrusão (IDPS)

A detecção de intrusão (IDS) é um software que automatiza o processo de detecção. A primeira geração de sistemas IDS apenas desempenhava a sua função sem contramedidas. Como resultado, os fornecedores de IDS introduziram o IPS (Sistema de Prevenção de Intrusões) para diferenciar os seus produtos dos anteriores. (Martins 2012).

2.2.1.3. VPN

Na visão de Fortinet (2023) uma VPN, ou seja, uma rede privada virtual, mascara seu endereço de protocolo de Internet (IP), criando uma conexão privada a partir de uma conexão WiFi pública. Uma VPN é uma das melhores ferramentas de privacidade e anonimato para um usuário conectado a qualquer serviço público de Internet porque estabelece conexões seguras e criptografadas.

2.2.1.3.1. Benefícios de uma conexão VPN em grande empresa de construção civil

Uma VPN protege seus dados online e impede o acesso externo, de modo a evitar que hackers e cibercriminosos descriptografem dados não criptográficos que podem ser conectados por qualquer pessoa. (Kaspersky 2023)

- Criptografia segura: Para ler os dados, você precisa de uma chave de criptografia. Sem uma, levaria milhões de anos para um computador decifrar o código no caso de um ataque de força bruta. Com a ajuda de uma VPN, suas actividades online ficam ocultas mesmo em redes públicas.
- Disfarçando seu paradeiro: Os servidores VPN actuam como *proxies* da Internet, mas a sua localização real não pode ser determinada. A maioria das VPNs não regista o comportamento do usuário, fazendo com que os possíveis registos de comportamento do usuário permaneçam ocultos.
- Acesso a conteúdo regional: O conteúdo da Web nem sempre é acessível de qualquer local, pois os serviços e sites normalmente usam servidores locais para determinar sua localização. O VPN *Spoofing* permite que os usuários alterem a sua localização mudando para um servidor de outro país.
- Transferência segura de dados: O trabalho remoto requer acesso seguro aos activos da empresa, normalmente através de conexões VPN, que se conectam a servidores privados e usam métodos de criptografia para reduzir os riscos de perda de dados.

2.2.1.3.2. Aplicabilidade de VPN em grandes empresas de construção civil

Abaixo seguem-se algumas das aplicações mais frequentes em grandes empresas de construção civil.

a. SSL VPN

Uma VPN é um serviço que estabelece uma conexão segura e criptografada entre uma Internet pública e uma rede corporativa ou institucional. As VPNs SSL permitem que os usuários possam aceder à rede de uma organização, aplicativos cliente-servidor, aplicativos utilitários e directórios de rede internos sem software especializado. Todo o tráfego entre um navegador da web e um dispositivo VPN SSL é criptografado usando SSL ou segurança da camada de transporte (TLS). Os usuários não precisam decidir qual protocolo usar. (Fortinet 2023)

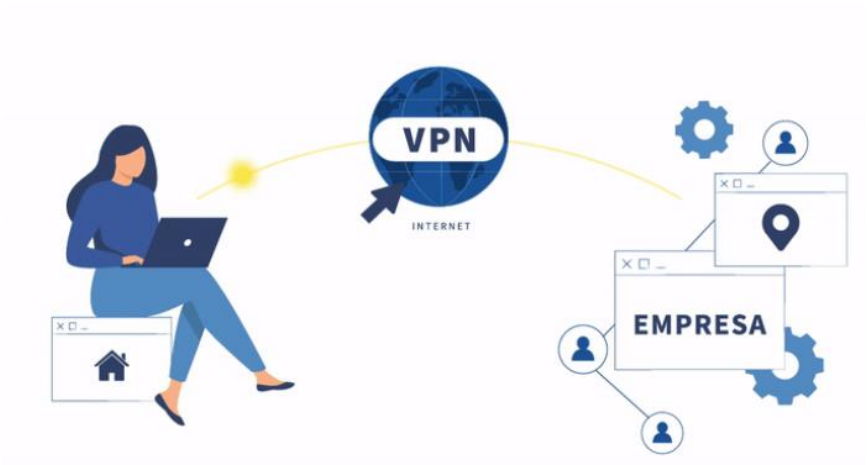

Fig. 2. 4 Cenário de aplicação do usuário - (Fonte: Avato, 2021)

b. VPN empresarial

As VPNs corporativas protegem usuários e dispositivos, fornecem conexões web seguras, de acesso remoto criptografado das transmissões de dados, mas podem causar atrasos e problemas de latência. As VPNs ponto a ponto melhoram a comunicação e reduzem a latência. Os serviços e aplicações em nuvem aumentam os riscos de cibersegurança, uma vez que a transmissão ou armazenamento não criptografado pode levar a violações de dados. Tanto as VPNs quanto as VPNs ponto a ponto são essenciais para a segurança corporativa e a produtividade dos funcionários.

c. VPN site a site

Uma VPN site-to-site conecta múltiplas redes, permitindo que as organizações compartilhem recursos como servidores de e-mail e instalações de armazenamento de dados em vários locais, permitindo acesso a todos os usuários como se os servidores estivessem no escritório físico.

2.2.1. Técnicas de Cibersegurança

Explora as técnicas utilizadas para proteger contra ameaças, incluindo criptografia, monitoramento de rede, autenticação multifactorial, e treinamento de conscientização de segurança para os colaboradores.

2.2.2.1. Criptografia

Segundo Amazon (2023) Criptografia é a prática de proteger informações por meio do uso de algoritmos codificados, *hashes* e assinaturas. As informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação electrónica trocada entre duas ou mais partes) ou em uso (durante a computação de dados).

2.2.2.1.1. Técnicas de criptografia mais comuns encontradas em empresas de construção civil

Os dois métodos mais comuns são a criptografia simétrica e assimétrica. Os nomes referem-se para verificar se a mesma chave é usada ou não para criptografia e descriptografia: (Kaspersky 2020)

Chaves de criptografia simétrica: também conhecidas como criptografia de chave privada. A chave usada para codificar é a mesma usada para decodificar, sendo a melhor opção para usuários individuais e sistemas fechados. Caso contrário, a chave deve ser enviada ao destinatário. Isso aumenta o risco de comprometimento se for interceptada por um terceiro, como um hacker. Esse método é mais rápido do que o método assimétrico.

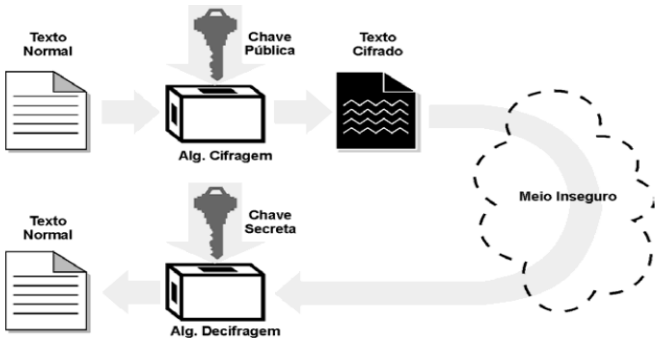

Fig. 2. 5 Ilustração de um processo de criptografia por chave secreta - (Fonte: Ishikawa 2003)

Chaves de criptografia assimétrica: esse tipo usa duas chaves diferentes, uma pública e uma privada, que são vinculadas matematicamente. Essencialmente, as chaves são apenas grandes números que foram emparelhados um ao outro, mas não são idênticos, daí o termo assimétrico. A chave privada é mantida em segredo pelo usuário, e a chave pública também é compartilhada entre destinatários autorizados ou disponibilizada ao público em geral.

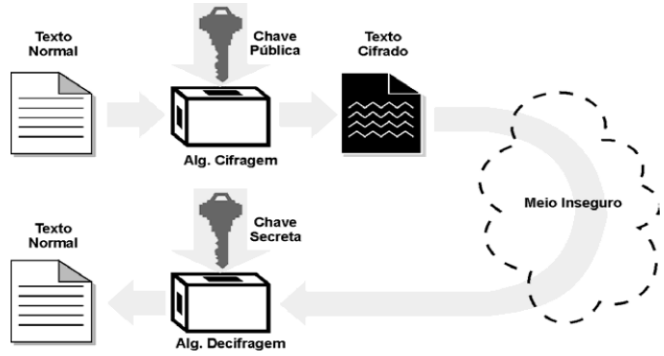

Fig. 2. 6 Ilustração de um processo de criptografia por chave pública – (Fonte: Ishikawa 2003)

2.2.2.2. Controle de Acesso na realidade de uma empresa de construção civil

Segundo Oliveira (2019) o controle de acesso pode ser definido como um mecanismo para proteger dados confidenciais contra acesso não autorizado, sujeitos, mediado como o acesso a um recurso é concedido ou negado de acordo com certos critérios.

As decisões de controle de acesso devem ser aplicadas por políticas de segurança que descrevam sob quais condições em que um *user* pode executar um conjunto de operações em um recurso disponibilizadas pelo gestor ou administrador dos sistemas.

a. Modelos de Controle de Acesso

Nesta seção é apresentada uma descrição sucinta de alguns dos mais importantes controles de acesso a modelos na literatura.

- **Controle de acesso discricionário (DAC)**

O controle de acesso discricionário (DAC) - baseia-se na ideia de que o proprietário dos dados deve determinar quem tem acesso a eles. O DAC permite que os dados sejam copiados livremente de objecto para objecto, portanto, mesmo que o acesso aos dados originais seja negado, o acesso a uma cópia pode ser obtido. (Sandhu 1996)

- **Matriz de controle de acesso**

Segundo Oliveira (2019) a matriz de controle de acesso é um controle de acesso discricionário introduzido por Butler W. Lampson que define o conjunto de direitos de acesso de cada sujeito a cada objecto dentro de um sistema operacional.

- **Lista de controle acesso**

A lista de controle de acesso (ACL) é um controle de acesso orientado a recursos e a implementação mais comum de políticas DAC. Conforme ilustrado na Figura 1, uma lista de controle de acesso corresponde a uma coluna da matriz de controle de acesso. Portanto, cada coluna representa uma lista de assuntos e seus direitos de acesso para um objecto específico. Cada entrada na lista é uma dupla (sujeito, conjunto de direitos).

Em sistemas baseados em ACL é fácil conceder ou negar acesso a um usuário específico ou a um conjunto de usuários, bem como para determinar quais usuários têm acesso a um determinado objecto.

Sob outra perspectiva, as ACLs não fornecem facilmente uma revisão de todos os privilégios associados a um usuário em um sistema informático, uma vez que é necessária a consulta de todas as listas de controlo de acessos. Como consequência de que as ACLs não são adequadas para sistemas grandes e dinâmicos com um grande número de assuntos e objectos onde é necessária uma descrição de política complexa. (Oliveira 2019)

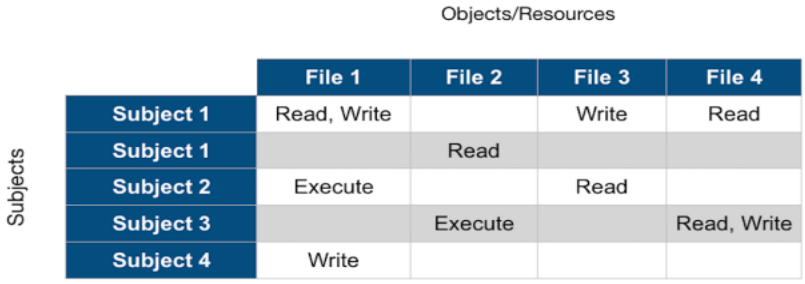

Fig. 2. 7 Exemplo de matriz de controle de acesso – (Fonte: Oliveira, 2019)

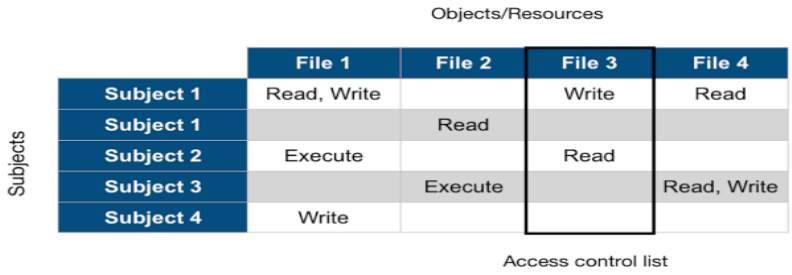

Fig. 2. 8 ACL representa as colunas da lista de controle de acesso – (Fonte: Oliveira, 2019)

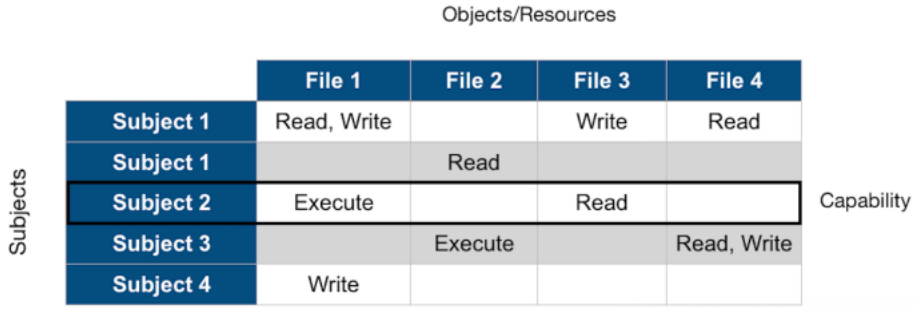

Fig. 2. 9 ACL representa as colunas da lista de controle de acesso – (Fonte: Oliveira, 2019)

2.2.2.3. Detecção de Intrusões

Os sistemas de detecção de intrusão (IDS) desempenham um papel importante na segurança da rede de computadores, que se concentra no tráfego monitorado tentando inspeccionar o tráfego em busca de anomalias ou comunicações indesejáveis para manter a rede como um lugar seguro. Existem dois métodos principais para detectar invasões em redes de computadores; baseado na rede assinaturas de intrusão e com base na detecção de anomalias na rede. Neste trabalho adoptamos uma abordagem baseada em assinaturas. (Salgueiro e Abreu 2010)

Metodologias de detecção de intrusão

As metodologias de detecção de intrusão são classificadas em três categorias principais:

a. Detecção Baseada em Assinatura (SD) - é a procura de rede de bytes ou sequências de pacotes conhecidos como maliciosos, com vantagem chave de serem desenvolvidas e entendidas quando se sabe o comportamento da rede. IDS baseado em assinaturas podem comunicar eventos gerados e co-relacionamento, testes são executados rápidos em sistemas modernos, o que permite remover outras assinaturas. (Leobons 2023)

b. Detecção Baseada em Anomalias (AD) - utilização de técnicas de identidade estabelece uma base com anomalias, e o desviar desta forma é considerado anomalia, mas o incidente com frequência de dois desvios gera preocupação.

c. Análise de Protocolo com Estado (SPA) - alguns fornecedores usam o termo "inspecção profunda de pacotes" para se referir à realização de algum tipo de análise de protocolo com estado, muitas vezes combinada com um recurso de firewall que pode bloquear comunicações consideradas maliciosas. (Wu 2020)

- Esta publicação usa o termo "análise de protocolo com estado" porque é apropriado para analisar actividades baseadas em rede e em *host*, enquanto "inspecção profunda de pacotes" é um termo apropriado apenas para actividades baseadas em rede.
- Além disso, historicamente não houve consenso na comunidade de segurança quanto ao significado de "inspecção profunda de pacotes".

2.2.2.4. Análise de Vulnerabilidades

Segundo Bugs (2020) vulnerabilidade é definida como uma falha no projecto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Os pilares da fase de prevenção são os seguintes e são executados por meio de uma política bem documentada: (TrendMicro 2023)

- Defina o que proteger;
- Determinar responsabilidades organizacionais;
- Estabelecer procedimentos de implementação:
- Aplicação de detalhes:
- Crie um programa de conscientização de segurança educando todos os funcionários:
- Estabeleça o controle de acesso para gerenciar como os funcionários acedem e usam os recursos organizacionais.

2.2.2.5. Segurança de Redes

De acordo com VMWare (2023) a segurança de rede é o conjunto de estratégias, processos e tecnologias desenvolvidos para proteger a rede de uma empresa contra danos e acesso não autorizado. Ameaças típicas contra dados e infraestrutura de rede incluem hackers, *malware* e vírus. Todos eles podem tentar *logar*, modificar ou invadir uma rede. Uma das principais prioridades da segurança de rede é controlar o acesso e impedir que essas ameaças invadam e se propaguem por toda a rede.

Tipos de segurança de redes

A segurança da rede envolve controles de protecção específicos que são adicionados a uma rede. Esses controles evoluíram ao longo dos anos e continuarão a crescer à medida que aprendemos mais sobre como defender uma rede e os atacantes aprendem novas maneiras de atacar. Para garantir que você tenha os melhores controles adicionados para protecção, é necessário primeiro entender o cenário de ameaças e as vulnerabilidades da rede. Também é importante entender quais tipos de controles estão disponíveis para que você possa aplicar os fornecedores, soluções e configurações correctos à sua rede. (Trend Micro 2023)

Os tipos de segurança de rede segundo a Cisco (2023) nomeadamente:

- Segurança de e-mail - Os *gateways* de e-mail são os principais vectores de ameaça de uma violação de segurança. Os invasores usam informações pessoais e tácticas de engenharia social para criar campanhas de *phishing* sofisticadas, com o objectivo de enganar destinatários e enviá-los para sites de *malware*. Um

aplicativo de segurança de e-mail bloqueia a entrada de ataques e controla mensagens de saída para impedir a perda de dados confidenciais.

- Análise de comportamento - Para detectar um comportamento anormal da rede, você deve saber como é o comportamento normal. As ferramentas de análise comportamental distinguem automaticamente as actividades que se desviam da norma. A equipe de segurança pode identificar melhor os indicadores de comprometimento que apresentam um possível problema e remediar rapidamente as ameaças.
- Prevenção contra perda de dados - As empresas devem garantir que a equipe não envie informações confidenciais para fora da rede. As tecnologias de prevenção contra perda de dados, ou DLP, podem impedir as pessoas de enviar, encaminhar ou, até mesmo, imprimir informações importantes de modo não seguro.
- Sistemas de prevenção contra invasão - Um sistema de prevenção contra invasão (IPS) analisa o tráfego da rede para bloquear activamente os ataques. Os dispositivos Cisco Next-Generation IPS (NGIPS) fazem isso correlacionando grandes quantidades de inteligência de ameaças global, não apenas para bloquear actividades mal-intencionadas, mas também para acompanhar a progressão de arquivos e *malware* suspeitos na rede, a fim de impedir a disseminação de ataques e reinfecções.
- Segurança de dispositivo móvel - Os criminosos cibernéticos estão visando cada vez mais os dispositivos e aplicativos móveis. Nos próximos 3 anos, 90% das empresas de TI devem ter aplicativos corporativos em dispositivos móveis pessoais. É claro, você precisa controlar quais dispositivos podem conectar a rede. Você também precisará configurar as conexões para manter a privacidade do tráfego de rede.
- Segurança das informações e gerenciamento de eventos - Os produtos SIEM colectam informações que a equipe de segurança precisam para identificar e responder a ameaças. Eles vêm em diversas formas, incluindo dispositivos físicos e virtuais, além de software do servidor.
- VPN - Uma rede virtual privada criptografa a conexão de um *endpoint* para uma rede, geralmente pela Internet. Normalmente, uma VPN de acesso remoto usa IPsec ou o protocolo SSL (*Secure Sockets Layer*) para autenticar a comunicação entre o dispositivo e a rede.

- Segurança da web - Uma solução de segurança da Web controlará o uso da Web da equipe, bloqueará ameaças baseadas na Web e negará acesso a sites mal-intencionados. Ela protegerá o *gateway* da Web no local ou na nuvem. "Segurança da Web" também se refere às etapas que você executa para proteger o próprio site.

2.2.2.5. MFA

A autenticação multifactor (MFA) é um processo de login de conta com várias etapas que obriga o usuário a inserir informações que vão além de uma simples senha. Por exemplo, juntamente com a senha, os usuários podem ser solicitados a inserir um código que foi enviado para o e-mail deles, responder a uma pergunta secreta ou verificar uma impressão digital. Em caso de comprometimento de uma senha do sistema, uma segunda forma de autenticação pode ajudar a impedir o acesso não autorizado à conta. (Amazon 2023)

Opções de autenticação sem senha para o Microsoft Entra ID

Os recursos de MFA protegem as organizações, mas os usuários muitas vezes têm dificuldade em memorizar senhas. Usar métodos de Auto autenticação é mais conveniente porque a senha é facilmente substituída.

Cada organização tem necessidades diferentes de autenticação. O Microsoft *Azure* e o *Azure* Governamental oferecem as seguintes quatro opções de autenticação sem senha que se integram ao Microsoft Entra ID:

a. Windows *Hello* para Empresas;
b. Microsoft Authenticator;
c. Chaves de segurança do Fido2;
d. Autenticação baseada em certificado.

Windows Hello para Empresas

O Windows *Hello* para Empresas é ideal para operadores de informações com seu PC Windows, com biométricas e PIN conectados ao usuário e infraestrutura de chave pública (PKI) e suporte interno para *logon* único (SSO).

As etapas a seguir mostram como o processo de entrada funciona com o Microsoft Entra ID:

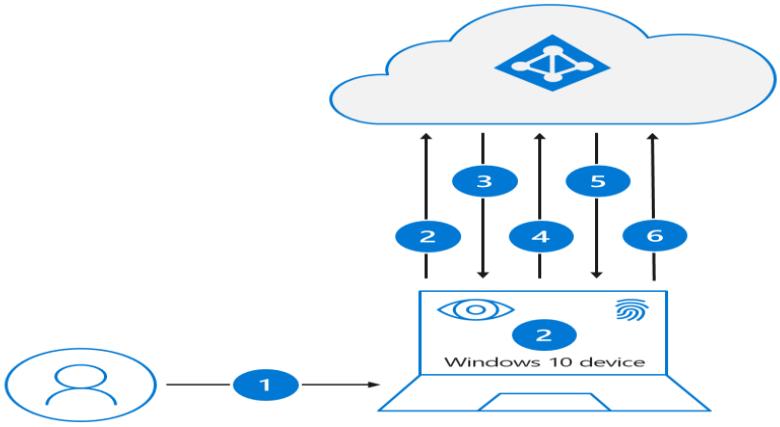

Fig. 2. 10 Etapas de processo de entrada na Microsoft – (Fonte: Microsoft, 2023)

1. Um usuário entra no Windows usando um gesto biométrico ou PIN. O gesto desbloqueia a chave privada do Windows *Hello* para Empresas e é enviado ao provedor de suporte de segurança de autenticação de nuvem, chamado de provedor de AP de nuvem.
2. O provedor de AP de nuvem solicita um *nonce* (número arbitrário aleatório que pode ser usado apenas uma vez) do Microsoft Entra ID.
3. O Microsoft Entra ID retorna um *nonce* que é válido por 5 minutos.
4. O provedor de AP de nuvem assina o *nonce* usando a chave privada do usuário e retorna o *nonce* assinado ao Microsoft Entra ID.
5. O Microsoft Entra ID valida o *nonce* assinado usando a chave pública registada com segurança do usuário na assinatura de *nonce*. O Microsoft Entra ID valida a assinatura e, em seguida, valida o *nonce* assinado retornado. Quando o *nonce* é validado, o Microsoft Entra ID cria um PRT (*token* de actualização principal) com a chave de sessão criptografada para a chave de transporte do dispositivo e a retorna para o provedor de AP de nuvem.

6. O provedor de AP de nuvem recebe o PRT criptografado com a chave da sessão. O provedor de AP de nuvem usa a chave de transporte privada do dispositivo para descriptografar a chave de sessão e protegê-la usando o TPM (*Trusted Platform Module*) do dispositivo.
7. O provedor de AP de nuvem retorna uma resposta de autenticação bem-sucedida ao Windows. O usuário então consegue comunicar com o Windows, bem como aplicativos locais e na nuvem sem a necessidade de autenticar novamente (SSO).

a. Microsoft Authenticator

O autenticador permite que o telefone se torne um método de autenticação sem senha, fornecendo uma opção conveniente de autenticação multifactorial, além de uma senha.

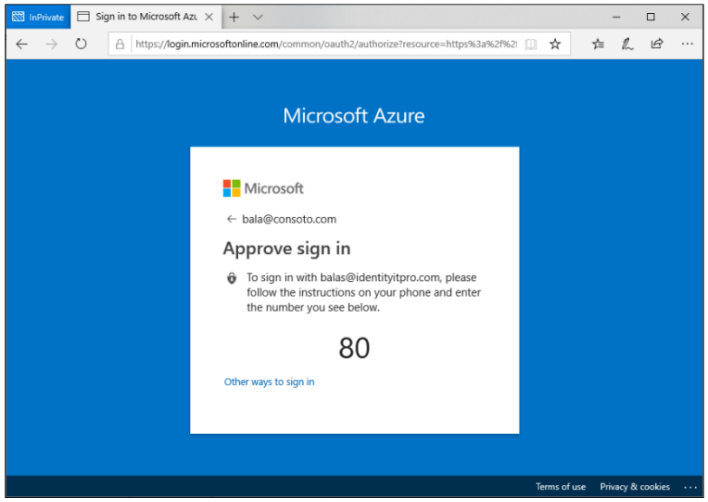

Fig. 2. 11 Microsoft Authenticator – (Fonte: Microsoft, 2023)

No entanto, segundo Micrsoft (2023) o aplicativo *Authenticator* transforma qualquer iOS ou Android em uma credencial forte e sem senha. Para o utilizador poder aceder ao e-mail através de uma plataforma ou navegador, os usuários recebem uma notificação no telemóvel de confirmação do número previamente registado no momento da configuração e faz-se a correspondência do número que vem no ecrã e depois utilizam um gesto biométrico (toque ou rosto) ou PIN para confirmar.

Por outro lado, a autenticação sem senha com o aplicativo *Authenticator* segue o mesmo padrão básico do Windows Hello para empresas. Isso é um pouco mais complicado, pois

o usuário precisa ser identificado para que o Microsoft Entra ID possa encontrar a versão do aplicativo Microsoft Authenticator.

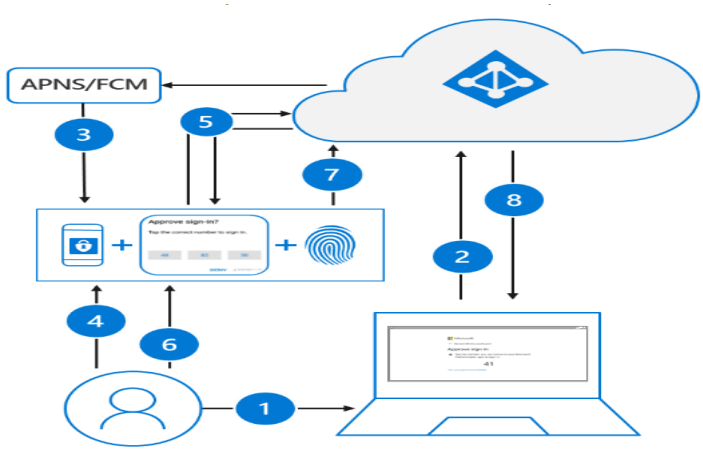

Fig. 2. 12 Processo autenticação da na Micrsoft e telemóvel (Fonte: Microsoft, 2023)

1. O usuário insere o nome de usuário.
2. O Microsoft Entra ID detecta que o usuário tem uma credencial forte e inicia o fluxo de credencial forte.
3. Uma notificação é enviada para o aplicativo via *Apple Push Notification Service* (APNS) em dispositivos iOS ou *Firebase Cloud Messaging* (FCM) em dispositivos Android.
4. O usuário recebe a notificação por *push* e abre o aplicativo.
5. O aplicativo chama o Microsoft Entra ID e recebe um desafio de prova de presença e um *nonce*.
6. O usuário conclui o desafio ao inserir seu dado biométrico ou PIN para desbloquear a chave privada.
7. O *nonce* é assinado com a chave privada e enviado de volta ao Microsoft Entra ID.
8. O Microsoft Entra ID executa a validação de chave pública/privada e retorna um *token*.

b. Autenticação baseada em certificado

A autenticação baseada em certificado (CBA) do Microsoft Entra permite que os usuários se autentiquem directamente com certificados X.509 para aplicativos e acesso ao navegador, fornecendo autenticação resistente a *phishing* e segurança PKI.

Fig. 2. 13 Autenticação baseada em certificado (Fonte: Microsoft, 2023)

Principais benefícios do uso da CBA do Microsoft Entra

Benefícios	Descrição
Óptima experiência do usuário	- Os usuários que precisam da autenticação baseada em certificado agora podem se autenticar directamente no Microsoft Entra e não precisam investir no AD FS federado. - A interface do usuário do portal permite que os usuários configurem facilmente como mapear campos de certificado para um atributo de objecto de usuário para pesquisar o usuário no locatário (associações de nome de usuário do certificado) - A interface do usuário do portal para configurar políticas de autenticação ajuda a determinar quais certificados são de factor único versus multifator.
Fácil de implantar e administrar	- A CBA Microsoft Entra é um recurso gratuito e você não precisa de nenhuma edição paga do Microsoft Entra ID para usá-lo. - Não há necessidade de implantações locais ou configurações de rede complexas. - Autentique-se directamente no Microsoft Entra ID.
	- As senhas locais não precisam ser armazenadas na nuvem de forma alguma.

Seguro	- Protege suas contas de usuário trabalhando perfeitamente com políticas de acesso condicional do Microsoft Entra ID, incluindo autenticação multifator resistente a *phishing* (MFA que requer uma edição licenciada) e bloqueio de autenticação herdada. - Suporte de autenticação forte, onde os usuários podem definir políticas de autenticação por meio dos campos de certificado, como emissor ou OID de política (identificadores de objecto), para determinar quais certificados se qualificam como factor único versus multifator. - O recurso funciona perfeitamente com recursos de Acesso Condicional e capacidade de força de autenticação para impor a MFA para ajudar a proteger seus usuários.

Tabela. 2. 1 Principais benefícios do uso da CBA do Microsoft Entra - (Fonte: Microsoft 2023)

Normas ISO 27001

As normas ou padrões internacionais garantem que os produtos e serviços que você utiliza diariamente sejam seguros, confiáveis e de alta qualidade. Eles também orientam as empresas na adopção de práticas sustentáveis e éticas, ajudando a criar um futuro onde as suas compras não apenas tenham um desempenho excelente, mas também protejam nosso planeta. Em essência, os padrões combinam perfeitamente qualidade com consciência, melhorando suas experiências e escolhas cotidianas.

As normas são a sabedoria destilada de pessoas com experiência na sua matéria e que conhecem as necessidades das organizações que representam – pessoas como fabricantes, vendedores, compradores, clientes, associações comerciais, utilizadores ou reguladores. (ISO 2023)

As normas ISO cobrem uma ampla gama de indústrias e sectores, incluindo tecnologia, manufactura, saúde e muito mais. Estas normas são desenvolvidas através de um processo baseado em consenso que envolve especialistas de indústrias e países relevantes.

2.3.1. ISO: Organização Internacional de Padronização

ISO é uma organização internacional independente e não governamental. Reúne especialistas globais para chegar a acordo sobre as melhores formas de fazer as coisas, desde a produção de produtos até à gestão de processos. A nossa missão é tornar a vida mais fácil, mais segura e melhor para todos, em qualquer lugar.

2.3.2. A NORMA ISO/IEC 27000 E SUA INTERLIGAÇÃO COM OUTRAS NORMAS

2.3.2.1. Família ISO/IEC 27000

A ISO e a IEC desenvolveram a ISO/IEC 27000 para ajudar as organizações a manter actividades de informação seguras, incluindo informações financeiras, de propriedade intelectual, dados de funcionários e informações confidenciais. Estas normas fornecem directrizes para a introdução, implementação e manutenção do SGSI, fornecendo uma base comum para práticas de segurança organizacional e estabelecendo confiança nas relações Intra e interorganizacionais. Eles também descrevem os requisitos para sistemas de gestão de segurança da informação.

Em síntese, a família de normas ISO/IEC 27000, inclui normas para: (Correia 2016)

a. Definir os requisitos para um SGSI;
b. Prestar apoio directo, orientação e / ou interpretação detalhada para o processo global de estabelecer, implementar, manter e melhorar um SGSI;
c. Fornecedoras de orientações sectoriais e específicas para SGSI; e
d. Endereçar directrizes para realizar auditoria e avaliação de conformidade para SGSI.

A lista de normas da família ISO/IEC 27000, é a seguinte (ISO/IEC 27000:2014, p.3):

- ISO/IEC 27000, Sistemas de gerenciamento de segurança visão geral e vocabulário;
- ISO/IEC 27001: Sistemas de gerenciamento de segurança da informação requisitos;
- ISO/IEC 27002: Código de prática para controles de segurança da informação;

- ISO/IEC 27003: Orientação para implementação de sistema de gestão de segurança da informação;
- ISO/IEC 27004: Medição de gerenciamento de segurança da informação;
- ISO/IEC 27005: Gestão de riscos de segurança da informação;
- ISO/IEC 27006: Requisitos para organismos que realizam auditoria e certificação de sistemas de gestão de segurança da informação;
- ISO/IEC 27007: Directrizes para auditoria de sistemas de gestão de segurança da informação;
- ISO/IEC TR 27008: Directrizes para auditores sobre controles de segurança da informação.
- ISO/IEC 27010: Gestão da segurança da informação para comunicações intersectoriais e interorganizacionais;
- ISO/IEC 27011: Directrizes de gerenciamento de segurança da informação para organizações de telecomunicações baseadas na ISO/IEC 27002;
- ISO/IEC 27013: Orientação sobre a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1
- ISO/IEC 27014: Governança da segurança da informação;
- ISO/IEC TR 27015: Directrizes de gestão de segurança da informação para serviços financeiros;
- ISO/IEC TR 27016: Gestão da segurança da informação economia organizacional;
- ISO 27799:2008: Informática em saúde gestão da segurança da informação na saúde usando ISO/IEC 27002
- ISO/IEC 27034:2011: Tecnologia da informação Técnicas de segurança de aplicativos.

A cibersegurança e a protecção da privacidade são vitais para empresas e organizações actualmente. A família de normas ISO/IEC 27000 mantém-as seguras.

Segundo ISO (2023) a ISO/IEC 27001 é a norma mais conhecida do mundo para sistemas de gestão de segurança da informação (SGSI) e seus requisitos. As suas boas práticas adicionais em protecção de dados e resiliência cibernética são cobertas por mais de uma dúzia de normas da família ISO/IEC 27000. Juntos, eles permitem que organizações de todos os sectores e tamanhos gerenciem a segurança de activos como informações

financeiras, propriedade intelectual, dados de funcionários e informações confiadas por terceiros.

A estrutura actualmente desenhada para padronização de normas seguem-se abaixo: (Correia 2016)

- Seleccionar controlos dentro do processo de implementação de um sistema de gestão de segurança da informação com base na ISO/IEC 27001;
- Implementar controlos de cibersegurança geralmente aceite;
- Desenvolver suas próprias directrizes de gestão de cibersegurança.

ISO/IEC 27002, a norma ISO/IEC 27001, é um guia de prática de controlos de segurança, integrados na gestão da segurança da informação em uma organização.

ISO/IEC 27003:2010 *Information technology-security techiques-information security management system implementation* aborda o processo de especificação e desenho de um SGSI, desde concepção através dos planos de implementação, orientando como planear um SGSI e o final plano de implementação.

Segundo Correia (2016) a norma ISO/IEC 27004:2009 *Information technology-security techniques-Measurement* fornece um guia com orientações sobre o desenvolvimento e a utilização de métricas e medição, com a finalidade de avaliar a eficácia de um sistema de gestão de cibersegurança já implementado com os controlos ou grupos de controlos especificados na norma ISO\IEC 27001:213

A norma ISO/IEC 27005:2011 – *Information security risk management* contém as directrizes para a gestão de riscos de cibersegurança. Esta norma suporta os conceitos gerais especificados na norma ISO/IEC 27001:2013 e está desenhada para ajudar na implementação de um sistema de gestão de cibersegurança com base na gestão risco.

De certo modo, este trabalho concerne na apresentação do estudo da norma 27001, por razão não se aprofundou a pesquisa em relação as outras normas.

Integração da norma ISO/IEC 27001

A norma ISO/IEC 27001 especifica os requisitos referentes a um sistema de gestão de segurança da informação, de forma a permitir que as organizações avaliem os seus riscos

e implementem os procedimentos necessários para a preservação da confidencialidade, integridade e disponibilidade da informação. Tem como principal objectivo impedir que a informação seja utilizada por terceiros não desejados ou perdida de forma irremediável. (Correia 2016)

Não obstante da interligação existente entre a norma e outras séries 27000, existe um alinhamento explicito com a norma ISO 3100:2013 gestão de risco – princípios e linhas de orientação, onde inclui, os requisitos para a avaliação e tratamento de riscos de cibersegurança à medida das necessidades da organização. Os requisitos definidos na norma ISO/IEC "são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do seu tipo, dimensão ou natureza." (NP ISO/IEC 27001:2013, p.6)

A estrutura global da norma ISO/IEC 27001 pode ser apresentada na seguinte forma:

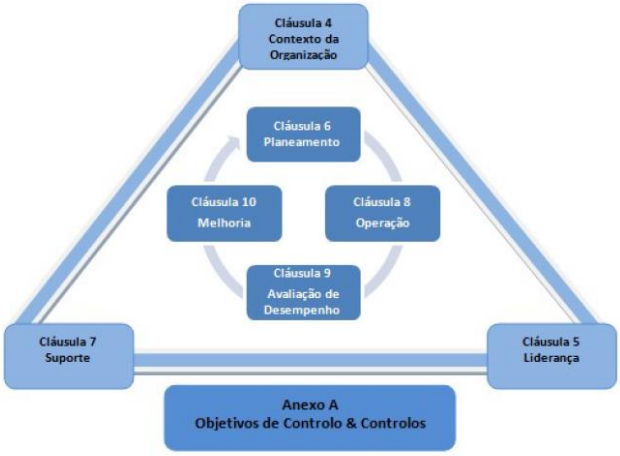

Fig. 2. 14 Estrutura global da norma ISO/IEC27001 - (Fonte: (Correia, 2016)

Benefícios da aplicabilidade da norma ISO/IEC 27001

ISO/IEC 27001 é universal em todos os tipos de organizações, mas tem flexibilidade na especificação de requisitos para a implementação de controlos de segurança.

A certificação ISO/IEC 27001 é possível, mas não obrigatória, para que as organizações se beneficiem das melhores práticas. Reconhecem cada vez mais o valor da implementação de normas internacionais para o sucesso dos projectos.

Independentemente das organizações se certificarem ou não, a adopção das práticas de gestão documentadas na norma, representa um conjunto de benefícios, nomeadamente: (Correia 2016)

1. Demonstra um compromisso dos executivos da organização para com a segurança da informação, pois uma das grandes preocupações da actualidade é efectivamente a confiança no tratamento adequado da informação sensível da sua organização.
2. Dotar a organização de ferramentas que demonstre o cumprimento ao Regulamento EU 2016/679 no tratamento e circulação de dados pessoais.
3. Aumenta a fiabilidade e a segurança da informação e dos sistemas, em termos de confidencialidade, disponibilidade e integridade.
4. Garante a realização de investimentos mais eficientes e orientados ao risco, ao invés de investimentos apenas baseados em tendências.
5. Incrementa os níveis de sensibilidade, participação e motivação dos colaboradores da organização para com a segurança da informação.
6. Identifica e endereça de forma continuada oportunidades para melhorias, sendo um processo em melhoria contínua.
7. Aumenta a confiança e satisfação dos clientes, utentes, parceiros, entidades reguladoras e judiciárias, providenciando um elevado compromisso com a protecção da informação, o que representa um nível considerável de conforto para quem interage com entidades que processam e arquivam dados pessoais.
8. A implementação dos controlos provenientes da norma e da análise de risco, melhora o desempenho operacional das organizações, potencia a realização de mais negócios e poder negocial.

O estudo exploratório de Silva (2021) sobre "Benefícios e factores condicionadores da obtenção de certificação em gestão da segurança de sistemas de informação" destaca a importância da obtenção de certificações através de normas de Gestão de Segurança da Informação como promotor e evidência dos esforços das organizações na protecção dos seus sistemas de informação.

Capítulo III – METODOLOGIA

Após a conclusão da revisão bibliográfica, de forma a alcançar os objectivos da investigação propostos no primeiro capítulo, foram aplicadas metodologias de investigação para técnicas e instrumento de colecta de dados e analise dos mesmos no período em que se procedeu a pesquisa, de modo a permitirem dar resposta às questões inicialmente formuladas na presente pesquisa.

Para Ferreira e Oliveira (2014), os métodos de investigação consistem num conjunto de procedimentos lógicos de investigação empírica que envolvem a selecção de técnicas de recolha e tratamento da informação adequada bem como o controlo da sua utilização.

3.1. Classificação quanto abordagem

Mediante a complexidade do tema enunciado e a abordagem holística feita, foi necessário recorrer a dois métodos em termos de abordagens. Tendo primeiramente, utilizado o método qualitativo, que se baseou pela recolha de documentação.

3.2. Classificação quanto a natureza

No que diz respeito a natureza foi utilizada a metodologia de pesquisa aplicada, por buscar resolver os problemas reais de forma prática. Tem como objectivos claros, envolver as partes interessadas relevantes, com métodos adequados e gera resultados com o impacto e uteis.

3.3. Classificação quanto ao tipo de pesquisa

Quanto aos objectivos da indagação, pretende-se seguir uma pesquisa explicativa, visando deste modo identificar os factores que determinam ou contribuem para a ocorrência da implementação com base nas normas ISO 27001.

O tipo de metodologia que melhor se enquadra neste trabalho são a descritiva e exploratória. A pesquisa descritiva porque vai auxiliar nas técnicas padronizadas de colectas de dados, com questionários e observações sistemáticas. A pesquisa exploratória tem como objectivo permitir maior proximidade entre o pesquisador e o tema da pesquisa, por ser pouco conhecido.

O tipo de abordagem de pesquisa, pode ser classificada como descritiva a fim de apresentar um estudo detalhado, com a colecta de dados, análise e interpretação dos mesmos. Não há a interacção ou envolvimento do pesquisador no assunto analisado. (Alves 2009)

Segundo Gil (20008) Pesquisa Exploratória: proporcionar uma maior familiaridade com o problema (explicitar). Pode envolver levantamento bibliográfico, entrevistas com pessoas experientes no problema pesquisado. Geralmente, assume a forma de pesquisa bibliográfica e estudo de caso.

3.4. Técnicas e Instrumento de Colecta de Dados

Para este trabalho o pesquisador centrou-se em investigação qualitativa, e recorreu ao uso das seguintes técnicas de recolha de informação em análise documental, entrevistas e observação.

De forma a dar sustentabilidade à investigação, desenvolveu-se uma pesquisa bibliográfica e documental a várias bibliotecas, artigos entre outros repositórios científicos *on-line*. O primeiro método originou na recolha dos dados por análise documental.

Por conseguinte, as entrevistas permitiram possibilitar uma resposta aberta, de forma a conduzir a repostas livres, suportando a orientação do entrevistador. No que concerne às entrevistas estas decorreram entre 10 e 30 de Junho de 2023, tendo como total três entrevistas semiestruturadas do tipo intensivas, assim sendo, centrou-se apenas em um individuo.

3.5. Análise de Dados

Foi utilizado uma abordagem qualitativa, de modo a destacar a recolha da documentação como método principal. Divido a enfase na compreensão aprofundada do tema, explorando detalhes e nuances por meio de análise textual e contextual.

A metodologia de pesquisa aplicada foi empregue, em foco na resolução prática de problemas reais. A pesquisa visa envolver partes interessadas relevantes e gerar resultados impactantes e úteis. Isso implica uma orientação pragmática para a aplicação dos resultados da pesquisa na prática.

A pesquisa é de natureza explicativa, com o objectivo de identificar os factores que contribuem para a implementação com base nas normas ISO 27001.

A combinação de métodos qualitativos e técnicas de colecta de dados variadas, como análise documental e entrevistas, oferece uma perspectiva ampla e profunda do tema estudado.

A pesquisa demonstra um compromisso com a compreensão detalhada e contextualizada do problema em questão, visando fornecer insights significativos para a prática e a implementação das normas ISO 27001.

Essa análise fornece uma visão abrangente da abordagem metodológica adoptada na pesquisa, destacando suas características, objectivos e técnicas de colecta de dados utilizadas.

CAPÍTULO IV – ESTUDO DE CASO

Neste capítulo é apresentado o estudo de caso, identificado na Mota-Engil Moçambique, no departamento de sistemas de informação e comunicação, baseado na análise à infra-estrutura e sistemas de cibersegurança.

O estudo de caso é um estudo empírico que investiga um fenómeno actual dentro do seu contexto de realidade, quando as fronteiras entre o fenómeno e o contexto não são claramente definidas e no qual são utilizadas várias fontes de evidencia. (Gil, 2008)

4.1. Características da infra-estrutura de cibersegurança da MEMZ

A MEMZ faz parte do grupo ME fundado em 1946, é hoje uma multinacional com actividade centrada na construção e gestão de infra-estruturas segmentada pelas áreas de Engenharia e Construção, Ambiente e Serviços, Concessões e Transportes, Energia e Mineração.

No entanto, a MEMZ encontra-se dividida em vários departamentos de acordo com as necessidades existentes na instituição, dentre eles uns autónomos e outros apoiam-se uns aos outros. Nesta direcção, a gestão de segurança de infra-estrutura da rede é da MEMZ e é desempenhada pelo departamento SIC.

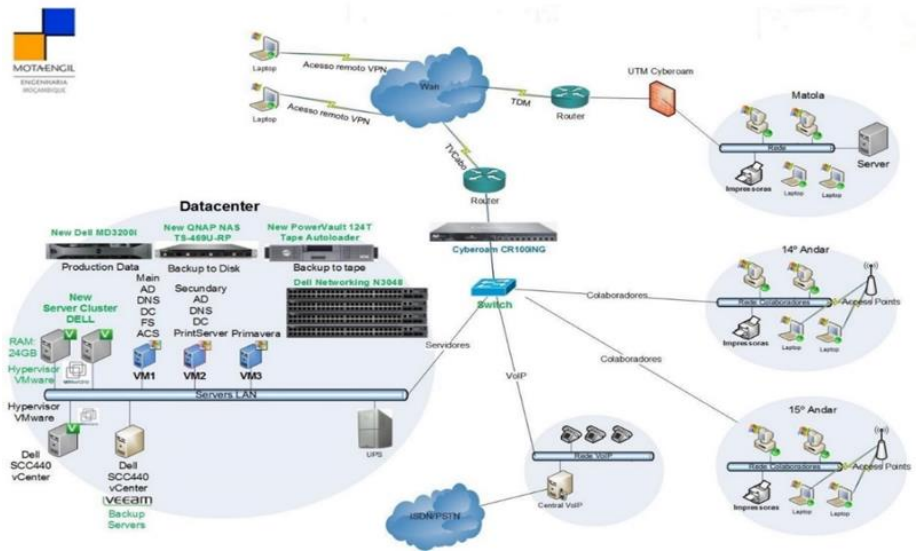

Fig. 4. 1 Representação lógica da estrutura de rede Mota-Engil Moçambique - (Fonte: Mota-Engil, 2017)

4.2. Ferramentas de cibersegurança existentes da MEMZ

Uma vez que os *hackeres* têm insistentemente procurado mecanismos de derrubar barreiras ou padrões estabelecidos de cibersegurança, a ME Moçambique também tem por seu lado tido em conta o estabelecimento de mecanismos para fortificar a segurança para não ser surpreendidos com cyber ataques. Estando para o efeito de acordo com os padrões de segurança estabelecidos internacionalmente para uma empresa. A Mota-Engil Moçambique segue os seguintes padrões de segurança:

a. Antivírus e *antimalware*

São aplicados para proteger os dispositivos finais contra softwares mal-intencionados, com este intuito a ME Moçambique optou pelo uso de Trend Micro, que oferece tecnologias de cibersegurança para empresas e usuários domésticos, com análise comportamental e inteligência de ameaças.

Este antivírus conta com as seguintes vantagens é excelente para protecção anti-*phishing*, a extensão do navegador funciona bem para detecção online e oferece digitalização *dark web*. Em relação as desvantagens do envio do spam para utilizador com muitas ofertas complementares quando o utilizador abre o aplicativo pela primeira vez, o seu desempenho em testes independentes não é eficaz e sem opções de licenciamento para vários dispositivos.

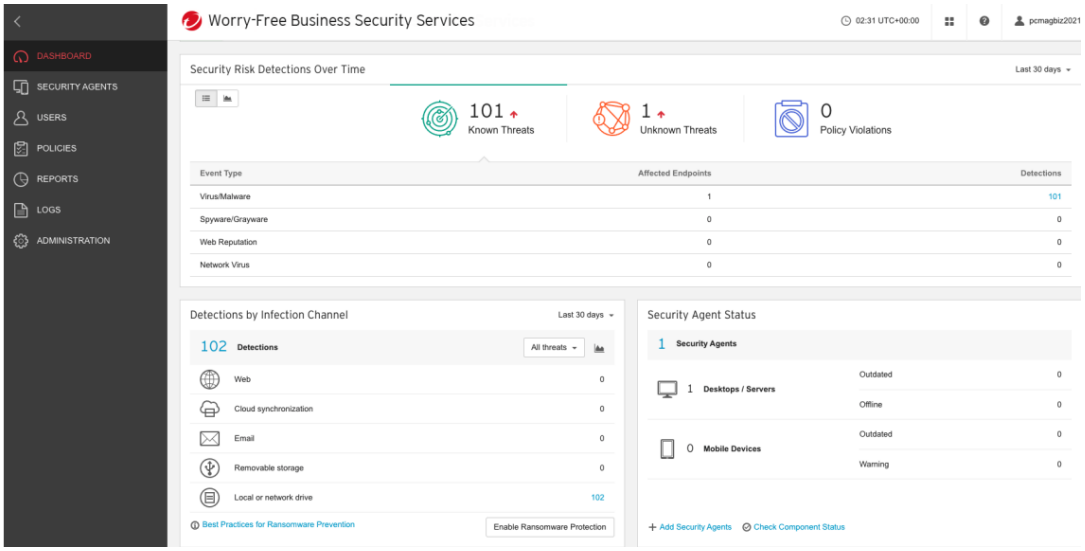

Fig. 4. 2 Interface de consola de antivírus – (Fonte: Brame 2022)

b. Firewall

Para bloquear o acesso não autorizado à rede. Inclui um sistema de *firewall* baseado em *host* que é implementado para impedir o acesso não autorizado ao dispositivo final. Abaixo seguem outras aplicabilidades da *firewall* na empresa:

- Sistemas de *firewall* dedicados - Usados para fornecer mais recursos avançados de *firewall* que podem filtrar grandes quantidades de tráfego com mais granularidade.
- Redes privadas virtuais (VPN) - Usadas para fornecer acesso seguro para funcionários remotos.

Neste contexto, a MEMZ implementou a cyberoam CR100NG, que é da série cyberoam NG de dispositivos de gerenciamento unificado de ameaças, são dispositivos de segurança de rede de última geração que incluem recursos de segurança UTM junto com o desempenho necessário para redes futuras.

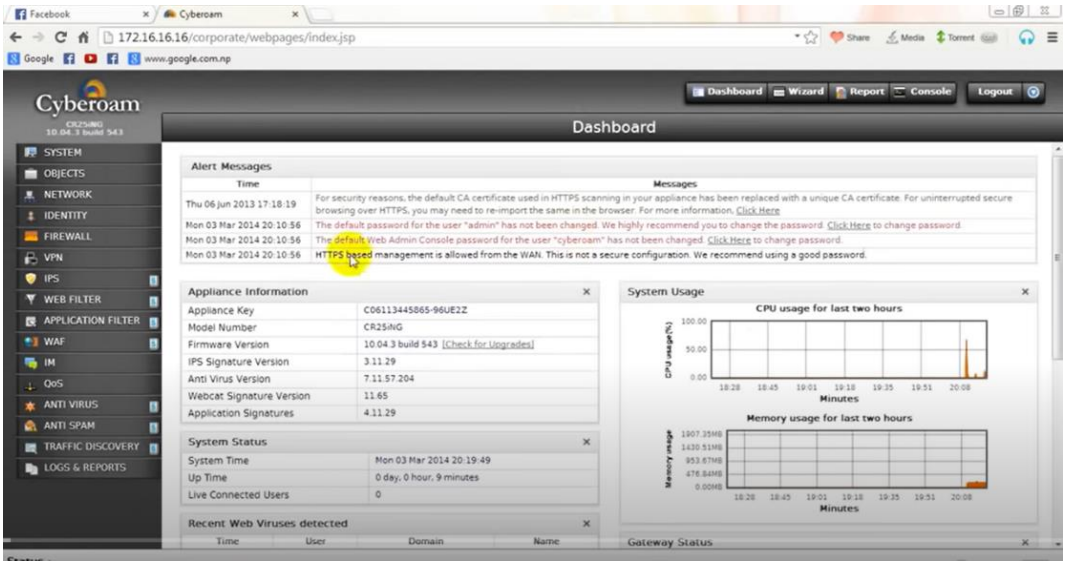

Fig. 4. 3 Painel de cyberoam - (Fonte: Autora 2023)

Adicionalmente, a cyberoam tem como vantagem que é simples de configurar e monitorar, o painel de configuração é excelente e fácil compreensão e tem um recurso específico de busca e que só pode alcançar com este dispositivo, que é o bloqueio de VPN IPSEC. Por outro lado, tem como desvantagem a SSL VPN não transmite confiabilidade, os utilizadores que não tem permissões por vezes solicitam senhas Admin na firewall para fazer login de forma a solucionar os problemas em canais sociais não criptografados.

c. Listas de controle de acesso (ACL)

Usadas para filtrar ainda mais o acesso e o encaminhamento de tráfego.

d. Sistemas de prevenção de invasão (IPS)

Usados para identificar ameaçam como ataques de dia zero ou de zero horas.

4.3. Técnicas e procedimentos de cibersegurança existentes da MEMZ

SIC possui políticas e procedimentos que devem ser seguidos por todos membros do departamento de manutenção da infra-estrutura, nomeadamente:

- Todos equipamentos novos que se pretenda ligar à rede necessitam de ter o seu *Mac-address* registado.
- As tomadas de rede são registadas para poderem activadas e utilizadas.
- Um equipamento de rede só pode estar registado em uma tomada.
- Os servidos que acedem aos serviços externos não podem ter um dispositivo intermédio que se liga a rede interna.
- Não é permitido a criar de pontos de acesso wireless com ligação à rede MEMZ.

Assim sendo, foi elaborada uma análise da estrutura de segurança de dados da MEMZ e observou-se uma necessidade de uma melhoria continua de alguns aspectos estabelecidos no sistema de gestão de segurança da informação (SGSI), para reforçar as práticas de cibersegurança tornando-as mais eficazes na protecção dos activos de informação e fortalecer a postura de segurança da organização.

Capítulo V – APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Neste capítulo, foi prevista a apresentação da proposta, análise e discussão dos resultados do trabalho, designadamente, os resultados obtidos através da análise de conteúdo das entrevistas e da recolha documental. As análises aqui expostas foram alvo, de uma organização prévia, de modo a utilizar diferentes meios de tratamento que já foram expostos no capítulo anterior. Adicionadas todas as respostas dos três entrevistados por pergunta, ou seja, analisado cada resposta a cada pergunta, foram construídos quadros com as menções mais importantes das respostas dos entrevistados, para posterior comparação de ideias.

5. 1. Proposta de Implementação de Ferramentas e Técnicas de Cibersegurança em Observância da Norma ISO 27001

Desenvolveu-se a proposta com a finalidade de demonstrar e auxiliar em configuração, reparações e manutenções de infra-estrutura de segurança da MEMZ. Tal como todos projectos, este também teve fases de implementação pré-analisadas em entrevistas com os gestores de rede.

No contexto desta monografia, por se tratar de uma empresa de construção civil, constatou-se uma necessidade de comunicação remota por ligação de internet entre as obras e a sua sede em Maputo.

Antes de se avançar com a proposta procedeu-se primeiro a uma pesquisa que assessorou como base as necessidades ajustadas na instituição, sendo estas segmentadas por 4 fases de implementação dentro da norma ISO 27001, a primeira onde fez-se um levantamento dos requisitos para dar seguimento ao esboço de uma estrutura de rede de segurança, que levou a segunda fase da escolha das ferramentas e técnicas, postas as duas fases acima seguiu-se a terceira com a sua implementação mediante as estratégias expostas nas etapas anteriores e acabando com a quarta fase de monitorização e actualização.

5.1.1. Esboço de estrutura de segurança de rede da ME Moçambique

Para começar esta etapa fez-se primeiramente uma avaliação de riscos com o objectivo de apoiar a identificação dos activos críticos, potenciais ameaças e vulnerabilidades da infra-estrutura. Posteriormente a selecção de tecnologias avançadas com base nas escolhas, como de sistemas de detecção e prevenção de intrusões (IDS/IPS), soluções de análise de comportamento, antivírus avançados e *firewalls* de última geração. E conseguinte projectou-se um esboçou de estrutura segurança de rede actualizada à resposta aos incidentes, suportada nos padrões ISO 27001.

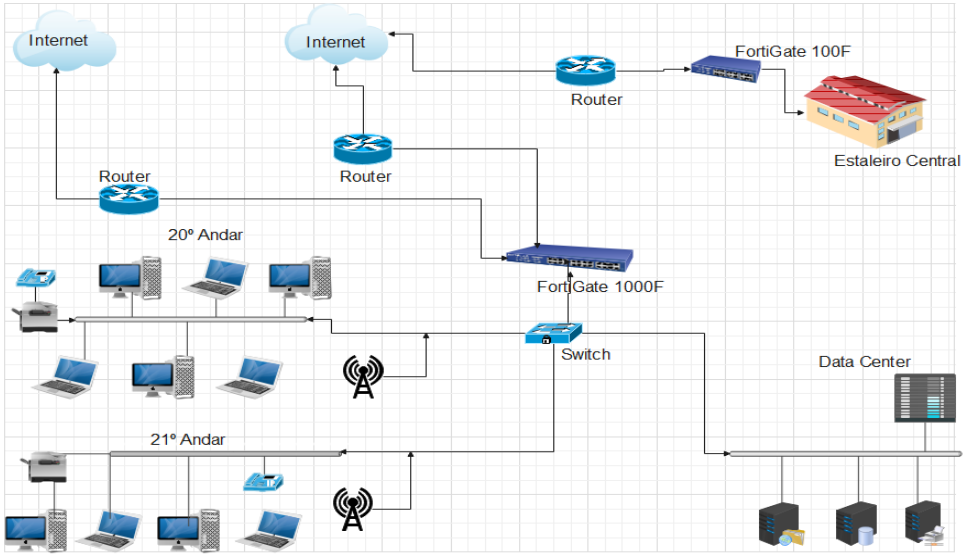

Fig. 5. 1 Estrutura de rede da Mota-Engil Moçambique – (Fonte: própria autora 2023)

Dando seguimento ao ponto anterior e de acordo com a informação recolhida, seguiu-se a etapa da selecção das ferramentas e técnicas que possam corresponder as exigências da segurança dos dados da MEMZ dentro dos padrões de orçamento.

Ao escolher as ferramentas de cibersegurança, foram considerados vários factores para garantir uma protecção eficaz. Aqui estão alguns aspectos importantes a serem considerados, compatibilidade com o ambiente, integração, fácil gestão, o desempenho do sistema e capacidade de lidar com as exigências da ME Moçambique, actualização e suporte regular e essenciais para manter a defesa de protecção, conformidade constante das ferramentas nos padrões de requisitos específicos da área de actuação da empresa, analisou-se a escalabilidade para acompanhar o crescimento da organização e aumento da demanda de segurança de dados.

Por ser uma empresa de construção, a maior dos colaboradores trabalha remotamente, ou seja, nas obras e acaba por existir uma necessidade de ligação remota a sede através da internet de forma segura, isto significa por SSL VPN que tem um protocolo de segurança que fornece comunicação segura e criptografada dos dados transmitidos para permitir que os usuários remotos acessem aos recursos de rede corporativa.

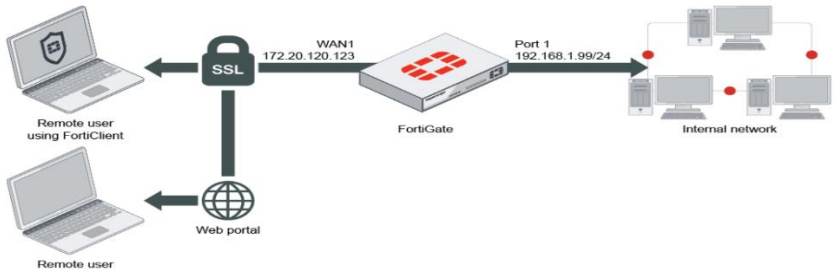

Fig. 5. 2 SSL VPN Fortigate - (Fonte: Fortinet, 2023)

Após escolher as ferramentas de controle de acesso que se enquadram no cenário acima apresentado, escolheu-se de seguida as técnicas para poderem acompanhar as ferramentas expostas, entretanto, o controle de acesso auxilia na protecção de dados sensíveis e recursos contra acessos não autorizados, por reduzir o risco de violações de segurança e fuga de informação. Tratando-se de uma empresa grande que possui vários departamentos existem informações que são especificas para cada departamento e não para todos, assim sendo os gestores de segurança de dados determinam o tipo e privilégio que cada utilizador (colaborador) deve ter acesso de acordo com as suas necessidades, para essas situações o controle de acesso adequado é o DAC.

IDS desempenha um papel crucial na identificação proactiva de actividades maliciosas ou suspeitas na rede, por ajudar a proteger os sistemas contra possíveis ameaças e garantir a segurança contínua dos ambientes de TI. Por possuir soluções de análise comportamental que monitoram o funcionamento normal do sistema e identifica actividades suspeitas, ajudando na detecção precoce de ameaças.

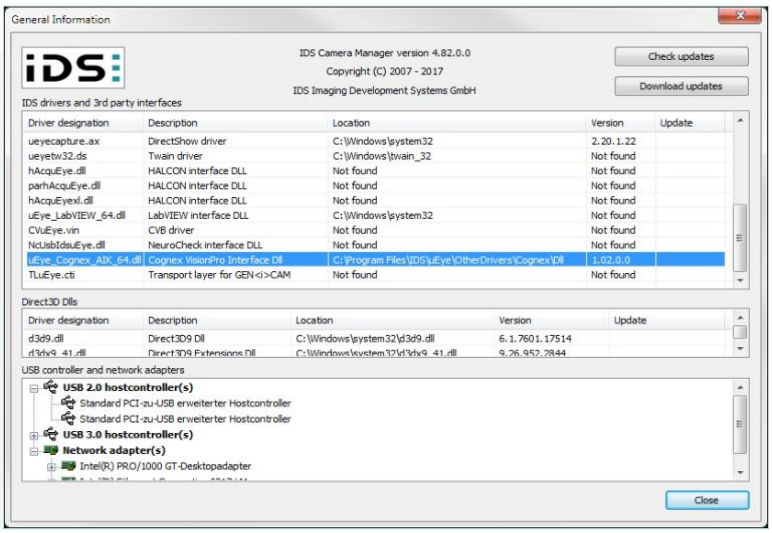

Fig. 5. 3 Sistema de detenção a Intrusão - (Fonte: IDS Camera Manager, 20)

No apoio a segurança de rede ao e-mail pode optou-se por *Microsoft Authenticator* um aplicativo de dois factores (2FA), disponibiliza uma camada adicional de segurança ao processo de login.

As políticas de segurança para o caso da MEMZ, foram desenvolvidas de forma cuidada e especifica. Inclui-se políticas para controle de acesso, uso de dispositivo moveis entre outros. Tendo medidas de avaliação de fornecedores o que permite avaliar a segurança de fornecedores e parceiros. Assegurar-se de que eles atendam a padrões de segurança adequados.

5.1.2.1. Identificação do âmbito e alcance das medidas de cibersegurança

Tendo em conta a proposta de implementação das ferramentas e técnicas de cibersegurança, é importante ter em conta a disposição. No âmbito do esboço ou arquitectura da estrutura de rede anterior, os requisitos e prioridades da informação da MEMZ. Como resultado desta fase pretende-se fazer a elaboração de um documento com identificação do seu âmbito que servirá de apoio na tomada de decisões no decorrer do processo de implementação.

Obteve-se a compreensão dos seguintes resultados identificados:

i. Implementar políticas de segurança de informação que vão de acordo com os objectivos estratégicos da instituição e sua visão.

ii. Manter uma relação integrada entre os requisitos institucionais e a norma ISO/IEC 27001e os outros standards existentes, como ISO 9001:2015 e ISO 14000 e a política de gestão de risco ISO/IEC 31000.
iii. Execução de confidencialidade dos dados de informação da empresa, de acordo com a Lei da protecção de dados empresariais. Lei do acesso a documentos administrativos.
iv. Ter como base a implementação dos requisitos da ISO/IEC 27001 no auxílio da gestão do SIC, para melhoramento de processos associados a cibersegurança.
v. Actualizar arquitectura do SIC de modo que seja capaz de responder com eficácia as eventuais vulnerabilidades.
vi. Introduzir e aplicar cultura de segurança de informação obliqua em toda ME Moçambique.
vii. Definir recursos que garantam a protecção da informação e continuidade na melhoria nos processos.
viii. Adoptar processos de gestão de risco da infra-estrutura SIC.

5.1.3. Implementação ajustada com as necessidades

As implementações das medidas de segurança foram ajustadas com base nas necessidades especificas da ME. A ME Moçambique possui uma imagem padrão do sistema operativo Windows que foi customizada consoante as necessidades de uma empresa de construção civil, depois da aplicação da imagem instalou-se o antivírus em conformidade.

5.1.3.1. Ferramentas de cibersegurança para Mota-Engil Moçambique

a. Requisitos para Antivírus Mota-Engil Moçambique

Tendo em conta a dimensão da empresa, os requisitos para escolha de um antivírus também devem ser exigentes, tais como:

- Protecção múltipla – é abrangente e engloba desktop;
- Protecção em vários níveis – para cada ponto de rede deve existir protecção em vários níveis, ou seja, protecção de arquivos, e-mail e páginas web, controle de portas entre outro tipo de protecção;

- Distribuição automatizada – automática do software sem a necessidade da instalação individualizada em cada *host*, de modo a conectar-se a rede que instalação do sistema de protecção;
- Suporte personalizado – em casos necessidade, o departamento SIC deve contar com apoio de técnicos preparados e especializado para poderem responder qualquer eventualidade de forma rápida e eficaz.

b. Requisitos para Firewall Mota-Engil Moçambique

Em virtude dos requisitos de firewall para auxiliar na segurança de dados da Mota-Engil, existem vários aspectos que se analisou para se ter em consideração, tais como:

- Capacidade e Desempenho – É feita certificação da firewall com capacidade suficiente para ajudar com o tráfego de uma empresa de grande porte, considerando o número de usuários, dispositivos e volume de tráfego.
- Recursos de Segurança - Uma firewall oferece vários recursos de segurança, como inspecção profunda de pacotes, prevenção de invasões (IPS), detecção de *malware*, VPN (rede privada virtual) e filtragem de conteúdo.
- Facilidade de Gerenciamento - Deve ser fácil de configurar, monitorar e gerenciar. Uma interface de gerenciamento intuitiva e recursos de relatórios sólidos são importantes para simplificar a administração.
- Compatibilidade com Políticas de Segurança – Deve garantir que a implementação das políticas de segurança específicas da empresa, incluindo controle de acesso, restrições de aplicativos e políticas de prevenção de ameaças.
- Escalabilidade – Recomenda-se que o dimensionamento da infra-estrutura de acordo as necessidades de crescimento da empresa para garantir que sua solução de segurança possa acompanhar o desenvolvimento da infra-estrutura da empresa.
- Suporte Técnico e Actualizações - Avaliar a qualidade do suporte técnico oferecido pelo fornecedor da firewall. Além disso, verifique a frequência e a facilidade de acesso a actualizações de segurança e *patches*.
- Conformidade com Regulamentações - Certificar-se de que a firewall atenda às regulamentações específicas do sector empresarial em concordância com o país, para garantir conformidade com normas de segurança e privacidade de dados.

- Integração com Outras Soluções de Segurança - Ao verificar a capacidade da firewall de integrar-se a outras soluções de segurança, como sistemas de detecção de ameaças, antivírus e sistemas de gerenciamento de identidade.
- Monitoramento em Tempo Real - Capacidade de monitorar em tempo real o tráfego de rede e receber alertas imediatos em caso de actividade suspeita é fundamental para responder prontamente a ameaças.
- Custo Total de Propriedade (TCO) - Considerar não apenas o custo inicial da firewall, mas também os custos contínuos, como licenciamento, manutenção e suporte.

Para se tomar uma decisão, é aconselhável realizar uma avaliação detalhada das necessidades específicas da empresa e buscar a orientação de profissionais de segurança da informação. No entanto, existem várias soluções de firewall no mercado que atendem aos requisitos de uma empresa de grande porte na indústria da construção em Moçambique. Aqui estão alguns *firewalls* amplamente reconhecidos:

- Fortinet FortiGate – São conhecidos pela combinação de segurança, desempenho e funcionalidades abrangentes, incluindo firewall, VPN, prevenção de intrusões e mais.
- Palo Alto Networks PA Series - São reconhecidos por sua abordagem inovadora de segurança, incluindo inspecção de aplicativos e ameaças, prevenção de ameaças avançadas e capacidades de VPN.
- Check Point Security Gateway – É conhecida por fornecer soluções abrangentes de segurança de rede. Seus *gateways* de segurança oferecem recursos como firewall, VPN, prevenção de ameaças e gerenciamento centralizado.
- Sophos XG Firewall - Oferece *firewalls* com recursos de segurança avançados, incluindo protecção contra ameaças avançadas, controle de aplicativos e filtragem da web.
- Juniper Networks SRX Series - Oferecem uma combinação de *firewall*, VPN e prevenção de ameaças. Eles são conhecidos por sua escalabilidade e desempenho.
- WatchGuard Firebox - Incluem recursos de segurança abrangentes, como firewall de próxima geração, prevenção de ameaças e VPN.

Para se escolher uma firewall ideal depende das necessidades específicas da empresa, do orçamento disponibilizado pela empresa e de outros factores exclusivos. Entretanto, recomendou-se entrar em contacto com os fornecedores locais para obter informações mais detalhadas, realizar testes de desempenho, se for possível consultar outros especialistas em segurança de rede para uma avaliação personalizada.

5.1.2.2. Técnicas de cibersegurança para a Mota-Engil Moçambique dentro da Norma ISO 27001

A empresa tem de investir em formação e conscientização por forma a instruir os colaboradores com programas de treinamento e a divulgar boas praticas de segurança, de modo a reduzir o risco de ameaças internas. Seguem-se algumas directrizes para a criação de programas de treinamento eficazes e promoção de boas práticas de segurança:

a. Gestão de riscos de cibersegurança na Mota-Engil

Primeiramente deve-se compreender o que advém da palavra risco como a probabilidade de ameaça ou perigo e gestão de administrar, ou seja, administração de possíveis perdas.

A gestão de risco não é só apenas de prejuízos, mas também ligada ao reconhecimento de oportunidades, e se identificados correctamente, pode distinguir uma empresa das outras.

Ao planear o sistema de gestão de cibersegurança, a organização deve considerar os requisitos que determinam os riscos e oportunidades que precisam ser abordados:

- Garantir que o sistema de gestão da segurança da informação possa alcançar o resultado pretendido;
- Prevenir ou reduzir efeitos indesejados;
- Alcançar a melhoria contínua.

A organização deve planear:

- Ações para enfrentar esses riscos e oportunidades;
- Como fazer a integração e implementação de acções em seu sistema de gestão de cibersegurança e os processos de avaliação da eficácia dessas acções.

A gestão de riscos eficiente para a empresa, por facilitar na tomada de decisões com dados considerando problemas futuros. Ele gera potencial para o aproveitamento das oscilações do mercado, obter grande crescimento e a elaboração de planos para redução de danos e perdas.

Fig. 5. 4 Etapas de gestão de risco na norma ISO 31.000- (Fonte: Riskex, 2017)

Primeiro estabeleceu-se o contexto e execução do um processo de avaliação de risco. Se forem fornecidas informações suficientes, a tarefa estará concluída e o tratamento do risco poderá prosseguir. Se forem fornecidas informações insuficientes, outra iteração revisa o contexto, potencialmente em partes do escopo. Para a norma ISO 27001:2013 o planeamento do sistema de gestão de cibersegurança da organização deve determinar os riscos e as oportunidades tem de ser dirigidas por forma a assegurar que a cibersegurança possa atingir os resultados pretendidos, evitar ou reduzir os efeitos indesejados e atingir a melhoria continua.

b. Processos de gestão de ricos de cibersegurança

Avaliação de risco é um processo de identificação de vulnerabilidade das quais uma empresa fica exposta, depois de serem elaboradas estratégias e soluções para conter e prevenir os riscos. É importante salientar quais devem ser consideradas as prioridades sendo elas diferentes de modo a serem classificadas de acordo com o grau de gravidade.

No decorrer do processo de avaliação de riscos, o gestor de segurança analisa a organização de modo que permita:

- Identificar processos e ocorrências que possam causar danos à empresa.
- Determinar a probabilidade de cada perigo e também a gravidade das consequências.
- Definir quais passos que a organização de forma a impedir que esses riscos possam ocorrer, ou para controlá-los.

Após a sucessão dos procedimentos expostos o gestor de segurança deve considerar ser capaz de reconhecer ameaças internas específicas, como negligência acidental ou intenções maliciosas.

De acordo com a norma NP ISO 31000:2013 recomenda-se que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objectivo é integrar um processo para gerir o risco na administração de estratégia e planeamento, gestão, processos de reporte, políticas, valores e cultura.

c. Desenvolvimento de técnicas no departamento SIC da Mota-Engil Moçambique

Os programas de treinamento para defesa contra cyber ataques são fundamentais para preparar os colaboradores e proteger a organização contra ameaças online. Abaixo encontram-se alguns tópicos essenciais que podem ser incluídos em um programa de treinamento para cyber ataques:

É mandatário que o treinamento seja contínuo e adaptado às mudanças nas ameaças cibernéticas. Ao incluir exercícios práticos e simulações de ataques pode ser especialmente útil para fortalecer as habilidades práticas dos colaboradores.

5.1.4 Monitorização e actualização

Nesta última fase, foram estabelecidos os processos para monitorização continua da segurança de modo a identificar os padrões de comportamento anómalos e potenciais ameaças em tempo real. Configurações de sistemas de alertas para enviar notificações das possíveis violações aos gestores de segurança. Forçar realizações de actualizações conforme as necessidades.

Testagem e simulações de *cyber* ataques essas realizações de testes frequentes de vulnerabilidade, permitem ajustar as medidas de cibersegurança com base nos resultados.

Revisão e actualização contínua a manter a revisão de forma regular e actualizar os sistemas e suas políticas de segurança recentes, optar por procedimentos e tecnologias que possam acompanhar a evolução do cenário de ameaças. Fazer o acompanhamento dos resultados para se basear nas medidas a implementar.

Auditorias e Conformidade a realização de auditorias internas e externas regularmente é importante para garantir a conformidade com as normas e regulamentações de segurança. E ajuda a encontrar aspectos a serem melhorados.

Esta fase é crucial para tomadas de decisões futuras, porque é através dos resultados obtidos e do histórico gerado aqui que é feita a melhoria e adaptações de segurança. É importante salientar que a cibersegurança é um esforço contínuo. Ao integrar as práticas acima citadas na instituição, desta forma o gestor de cibersegurança pode melhorar significativamente a postura de segurança a reduzir os riscos associados.

Análises dos resultados

5.1. Análise à questão n.º 1

No quadro n.º 1, é apresentada a argumentação relativa à Questão n.º 1 – O que é cibersegurança e quais são os desafios que a empresa Mota-Engil Moçambique com a segurança de informação?

Entrevistado	Ideias Chave
1	Cibersegurança é o conjunto de métodos e práticas aplicadas no processo de protecção lógica e física de recursos informáticos desde dados até sistemas. Tendo como objecto de analise a ME Moçambique os grandes desafios com a segurança de informação são a implementação de mais recursos para ´educação´ e testagem de seus colaboradores quando ao uso recursos digitais assim como a padronização e manutenção da documentação das soluções de cyber segurança adoptadas.
2	A cibersegurança diz respeito à prática de proteger sistemas, redes e programas contra-ataques digitais, roubo de dados e danos à integridade da informação. Os desafios que a Mota-Engil Moçambique enfrenta em relação à segurança da informação incluem ameaças como ataques de *malware*, *phishing*, *hacking*, espionagem cibernética e outros eventos que visam comprometer a confidencialidade, integridade e disponibilidade dos dados da empresa.
3	- A cibersegurança envolve a protecção de sistemas, redes e dados contra ameaças digitais, com a Mota-Engil Moçambique a apostar na segurança da informação devido a informação corporativa e operacional sensível. - Nosso principal desafio é gerenciar a crescente sofisticação das ameaças cibernéticas, garantir a segurança em projectos estratégicos e gerenciar de forma eficiente o acesso automatizado, e estamos constantemente adaptando nossas estratégias para enfrentar esses desafios.

Tabela. 5. 1 **Respostas análise à questão n.º 1**

Análise da questão n.º 1

Ao fazer se analisar os resultados da Questão n.º 1 revela que a cibersegurança é conceito protecção aos dados de informação. Entretanto existe uma estrutura que sustenta toda a segurança de informação, constituída por antivírus, *firewall*, VPN e técnicas expostas no capítulo 2. No último século, a cibersegurança é uma grande preocupação da empresa que teve o seu desenvolvimento exponencial, por estar interligado com aspecto vivencia da empresa com a digitalização de dados. No âmbito de uma análise introspectiva, na época actual, a ME Moçambique e a cibersegurança são realidades inseparáveis.

Deve-se ao facto de existirem repercussões ao nível de cibersegurança e aproximação do estado tecnológico com as grandes empresas de construção civil em Moçambique. Os crimes praticados no mundo real também são praticados no mundo digital, está tipologia torna-se mais complexa, desenvolvida tecnologicamente e sofisticada.

5.1.2. Análise à questão n.º 2

No quadro n.º 2, é apresentada a argumentação relativa à Questão n.º 2 – O que é e como é possível garantir a cibersegurança das infra-estruturas críticas como Mota-Engil Moçambique?

Entrevistado	Ideias Chave
1	Continuado ou repetindo o ponto exposto anteriormente posso dizer que a garantia da cibersegurança das infra-estruturas críticas na instituição assentara na formação cíclica dos diferentes colaboradores, adopção de soluções padronizadas e da revisão da documentação sobre a infra-estruturas e procedimentos tendo em conta ISOs e Normas internacionais no geral, claro que tendo em conta o que já foi estabelecido pela administração da empresa.
	As infra-estruturas críticas, como as da Mota-Engil Moçambique, englobam sectores essenciais para o funcionamento da empresa. Garantir a cibersegurança nesse contexto requer medidas como o desenvolvimento de políticas de segurança robustas, implementação

2	de *firewalls*, antivírus, controlo de acesso, criptografia, formação de funcionários em práticas seguras, monitorização contínua e a aplicação de patches de segurança.
3	- A cibersegurança na Mota-Engil Moçambique envolve a protecção de sistemas essenciais para o funcionamento contínuo do projecto, incluindo a salvaguarda de redes, servidores e dados vitais para garantir a integridade e fiabilidade. - As de infra-estruturas críticas necessita uma abordagem multifacetada, incluindo sistemas de intrusões, *firewalls*, rigorosos acessos gestão, regular vulnerabilidades e contínuo treinamento.

Tabela. 5. 2 **Respostas da análise da questão 2**

Análise da questão n.º 2

Apos analisar os resultados adquiridos na Questão nº.2 na óptica dos entrevistados, pode se garantir a cibersegurança eficaz nas infra-estruturas críticas da ME Moçambique, com uma estratégia integrada que possa combinar com formação, conformidade com padrões, medidas técnicas avançadas e monitoramento contínuo. Além disso, a sensibilização e a participação activa dos colaboradores são aspectos fundamentais em todas as abordagens.

5.1.3. Análise à questão n.º 3

No quadro n.º 3, é apresentada a argumentação relativa à Questão n.º 3 – Qual é o espectro da ameaça da cibersegurança da Mota-Engil Moçambique?

Entrevistado	Ideias Chave
1	A ME Moçambique ainda se beneficia de estar inserida em um país em vias de desenvolvimento, ou seja, o parque empresarial não constitui interesse de grupos *hackes* internacionais e ataques de efeitos cascata, porem o mesmo não pode ser dito a sua Matriz

	(empresa mãe) e algumas homologas em outras regiões do globo. Geralmente os ataques de tipo passivo associado a criação de *bots* são os mais comuns devido principalmente a falta de atenção de colaboradores sobre as boas praticas no uso da internet.
2	O espectro da ameaça de cibersegurança na Mota-Engil Moçambique pode incluir uma variedade de ameaças, desde ataques direccionados a sistemas específicos até ameaças mais amplas, como *ransomware*, ataques de negação de serviço (DDoS), roubo de propriedade intelectual e espionagem industrial. A avaliação precisa do espectro de ameaças é crucial para implementar medidas de segurança adequadas.
3	A ME Moçambique como as demais grandes empresas moçambicanas dentro do espectro das seguintes ameaças ataques de *malware*, *phishing*, ataques de navegação de serviço (DDoS), vazamento de dados, ataques a dispositivos conectados (IoT) e falhas de segurança interna.

Tabela. 5. 3 **Respostas da análise da questão 3**

Análise da questão n.º 3

De acordo com a combinação das respostas expõe-se uma visão abrangente das possíveis ameaças, abordando aspectos geográficos, comportamentais e uma variedade de vectores de ataque. Para proteger efectivamente contra essas ameaças, a empresa pode considerar estratégias abrangentes que envolvam conscientização dos colaboradores, medidas técnicas avançadas e uma abordagem proactiva para identificar e mitigar riscos potenciais.

5.1.4. Análise à questão n.º 4

No quadro n.º 4 é apresentada a argumentação relativa à Questão n.º 4 – Qual é o impacto de cyber ataques nas actividades da ME Moçambique?

Entrevistado	Ideias Chave
1	Como qualquer organização os ataques trazem a ME Moçambique a paragem forçada de trabalhos e serviços e o bloqueio de recursos e ferramentas de trabalho, o que culmina com perdas financeiras e prestígio.
2	Os impactos dos ciberataques nas actividades da Mota-Engil Moçambique podem ser significativos. Isso inclui a interrupção das operações, perda de dados sensíveis, danos à reputação da empresa, custos financeiros associados à recuperação e possíveis implicações legais. A extensão do impacto depende da natureza e gravidade do ataque.
3	Tendo como ponto de vista os impactos de um cyber ataque que a ME Moçambique é significativa e variada, como: perda de dados sensíveis, interrupção das operações, danos à reputação, custos financeiros, roubo de recursos financeiros, conformidade e penalidades, tempo de inactividade e ameaças futuras.

Tabela. 5. 4 **Respostas da análise da questão 4**

Análise da questão n.º 4

É do entender geral dos entrevistados a seriedade dos potencias impactos de cyber ataques na MEMZ, tendo como: paragem forçadas das actividades laborais e perdas financeiras, essa compreensão é crucial para a implementação de medidas de prevenção e de resposta eficazes para mitigar esses impactos e proteger as operações da empresa.

5.1.5. Análise à questão n.º 5

No quadro n.º 5, é apresentada a argumentação relativa à Questão n.º 5 – Que alterações ou ajustes são necessários para os gestores de segurança da ME Moçambique possam garantir maior eficácia de actuação no desempenho?

Entrevistado	Ideias Chave
1	Desenho e implementação de uma solução unificada de técnicas, procedimento e ferramentas de segurança tendo em conta questões logísticas, financeiras e humanas.
2	Para garantir maior eficácia na segurança cibernética da Mota-Engil Moçambique, os gestores de segurança devem considerar: -Avaliação contínua de riscos: Identificar e avaliar regularmente as vulnerabilidades e ameaças potenciais. -Políticas e procedimentos: Desenvolver e implementar políticas de segurança claras e procedimentos operacionais padrão para garantir o cumprimento de práticas seguras. -Conscientização e treinamento: Educar os funcionários sobre práticas seguras, reconhecimento de ameaças e procedimentos de resposta a incidentes.
3	De modo que haja eficácia na actuação dos gestores de segurança ME Moçambique, é fundamental adoptar uma abordagem abrangente que inclua políticas, práticas e tecnologias de segurança cibernética. Pode melhorar significativamente a postura da empresa, reduzindo os riscos e protegendo os activos digitais contra ameaças potenciais.

Tabela. 5. 5 **Respostas da análise da questão 5**

Análise da questão n.º 5

Segundo os entrevistados, sugere-se que os gestores de segurança da MEMZ devem considerar abordagens integradas e abrangentes que envolvam não apenas tecnologias,

mas também políticas, práticas e treinamento para garantir uma segurança cibernética eficaz. Essas recomendações abordam tanto os aspectos técnicos quanto os humanos da segurança, reconhecendo a importância da colaboração entre diferentes áreas para fortalecer a postura de segurança da organização.

Capítulo VI – CONSIDERAÇÕES FINAIS

6.1. Conclusões

Está pesquisa teve como principal objectivo desenvolver uma proposta de ferramentas e técnicas de cibersegurança em observância com a Norma ISO 27001 ajustada as necessidades e realidade encontrada na Mota-Engil Moçambique feitas com base num estudo desenvolvido ao longo dos anos 2018 e 2022. No contexto desta monografia, por se tratar de uma empresa de construção civil, constatou-se uma necessidade de comunicação remota por ligação de internet entre as obras e a sua sede em Maputo.

Primeiramente foi feita uma introdução do cibersegurança e levantamento das ferramentas e técnicas existentes na empresa e constatou-se que alguma delas não estão de acordo com as normas ISO 27001, que auxilia as organizações de manterem-se seguras, dentro de boas práticas adicionais em protecção de dados e resiliência cibernética. A aplicação de normas ISO 27001, trazem diversos benefícios às empresas de modo a demonstrar um compromisso dos executivos da organização, confiança no tratamento adequado da informação sensível, garante a realização de investimentos mais eficientes e orientados ao risco, entre outros.

Nesta direcção, a pesquisa foi acompanhada por metodologias quantitativas e qualitativas que auxiliaram a conduzir e suportar dentro das funções chaves da cibersegurança, juntamente de uma natureza básica, alicerçada com abordagens descritivas e exploratórias.

Por outro lado, a proposta de implementação de ferramentas e técnicas de segurança cibernética no escritório ou na infra-estrutura de rede da MEMZ envolve a identificação dos requisitos e prioridades de informação da organização. Este processo resulta na criação de um documento que apoia a tomada de decisões durante o processo de implementação. Os principais resultados incluem a implementação de políticas de segurança da informação, a manutenção de uma relação integrada entre os requisitos institucionais e as normas ISO/IEC 27001, a garantia da confidencialidade dos dados da empresa, a implementação dos requisitos da ISO/IEC 27001 na gestão do SIC, a implementação de uma cultura de segurança da informação, a definição de recursos para protecção da informação. e adopção de processos de gestão de riscos.

Assim sendo, o pesquisador concluiu através das análises de cyber ataques que a implementação da proposta exposta permitirá a elaboração de relatórios de activos mensais e anuais com maior controle e precisão, robustez a na protecção da infra-estrutura, sensibilização dos colaboradores de forma a serem mais cautelosos com as actividades e treinamento continuo, juntamente com simulações de ameaças para solidificar e preparar em casos reais de ameaças.

6.2. Recomendações

- Devido a importância do tema, recomenda-se que é necessário que sejam feitos investimentos na formação da equipa do TI e dos colaboradores, escolha de ferramentas e técnicas de cibersegurança robustas capazes de responder as demandas actuais.
- Recomenda-se pesquisas constantes de ferramentas e técnicas de cibersegurança por se tratar de áreas tecnológicas que estão sempre em evolução.

Referências Bibliografias

BARATA, R., (2023) Procedimentos de resposta a incidentes de cibersegurança no GRA, Escola superior de tecnologia e gestão do instituto politécnico de bragança, Bragança

BRAME, D., (2022) Trend Micro Worry-Free Services Advancecd Review https://www.pcmag.com/reviews/trend-micro-worry-free-business-security-services (Consultado em Novembro de 2023)

CABRAL, T., (2023) Cibersegurança: Uma Guerra Constante Ameaças em Evolução https://athenasecurity.com.br/2023/09/06/ciberseguranca-guerra-constante-contra-ameacas-evolucao/ (Consultado em 14 de Setembro de 2023)

CONCEITO (2019) Conceito de Norma https://conceito.de/norma (Consultado em 14 de Setembro de 2023)

CORREIA, C., (2016) Plano de implementação da norma ISO/IEC 27001 no INEM, Instituto nacional de emergência médica, I. P, Lisboa

COTINO, L., SÁNCHEZ, M., (2021) Guia de cibersegurança para cidades inteligentes.

DEVOTEAM CIBER TRUST (2023) O que é a norma ISO 27001? https://www.27001.pt/ (Consultado em 14 de Setembro de 2023)

FARIA, Nelson., (2022), Estratégias de Cibersegurança, Universidade do Minho, Braga.

FERNANDES, N., (2013) Segurança da informação. Cuiabá-MT

FERREIRA, P., & OLIVEIRA, E. R. de. (2014). Métodos de Investigação: da Interrogação à descoberta científica. (S. Vida Económica - Editorial, Ed.). Porto.

GIL, A., (2008). Como elaborar projectos de pesquisa. 4. ed. São Paulo: Atlas.

Gridinsoft (2023) O que é Cibersegurança? Princípios de Segurança do Computador Obtido: https://pt.gridinsoft.com/cybersecurity (Consultado em 24 de Outubro de 2023)

https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-da ciberseguranca-200930/ (Consultado em 14 de Setembro de 2023)

IBM (2023) What is cibersecurity? Obtido: https://www.ibm.com/topics/cibersecurity (Consultado em 13 de setembro de 2023)

IDS, (2016) Bilderfassung in Cognex VisionPro, https://de.ids-imaging.com/techtipp-details/app-note-acquire-images-cognex-quickbuild.html (Consultado em 09 de Dezembro de 2023)

ISHIKAWA, E., (2003) Um modelo computacional o funcionamento da assinatura digital no sistema de informatização processual, Universidade federal de santa catarina program de pós-graduação em engenharia de produção, Florianópolis,

ISO (2022) ISO/IEC 27001 Information security management systems. Obtido: https://www.iso.org/standard/27001 (Consultado em 13 de setembro de 2023)

ISO, (2013) Information technology Security techniques Information security management systemas requirements

ISO, (2005) Information technology security techniques Information security management systems requirements, Ed. 2005-11

JÚNIOR, Abdul., (2021) Implementação de uma base de dados distribuída para monitoria de entrega de encomendas internacionais, Instituto Superior Politécnico de Tete, Tete.

JÚNIOR, D., (2011) Proposta de interface para ensino de funcionamento interno de um firewall, Pontifica universidade católica de são Paulo, São Paulo

Kaspersky (2023) O que é cibersegurança? Obtido: https://www.kaspersky.com.br/resource-center/definitions/what-is-ciber-security (Consultado em13 de Setembro de 2023)

LIMA, A., (2022) Diferença entre antivírus e antimalware https://acervolima.com/diferenca-entre-antivirus-e-antimalware/ (Consultado em 24 de Outubro de 2023)

LIMA, M., (2022) Um sistema de detecção e prevenção contra intrusão em ambientes da internet das coisas baseado em processamento de eventos complexos, Universidade federal de Pernambuco centro de informático programa de pós-graduação em ciência da computação, Recife

MARTINS, D., (2012) Uma estratégia para sistemas de detecção e prevenção de intrusão baseada em software livre, Universidade federal do ceará departamento de computação curso de ciência da computação, Ceará

MEDEIROS, T., (2008), Proposta de uma metodologia para geração de dados para avaliação das ferramentas de detecção de intrusão, Universidade federal do rio grande sul instituto de informática, curso de especialização em tecnologias gerências e segurança de redes de computadores, Porto

MICROSOFT (2023) Autenticação multifator no Microsft Entra https://www.microsoft.com/pt-br/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication (Consultado em 24 de Novembro de 2023)

NETTO, V., (2022) Metodologia para aplicação conjunta de frameworks de segurança, Universidade federal fluminense instituto de computação, Niterói

NOGUEIRA, M., (2023) Afinal, o que é cibersegurança? Obtido: https://horizontes.sbc.org.br/index.php/2023/07/afinal-o-que-e-ciberseguranca/ (Consultado em 13 de setembro de 2023)

OLIVEIRA, R., (2019), Mecanismos de controlo de acesso para uma plataforma de IoT, Access control mechanisms for na IoT Platform, Departamento de electrónicas telecomunicações e informática, Aveiro

PATRÍCIO, D. et al. Detecção de intrusão, Académica do curso de ciência da computação departamento de ciência da computação, universidade do extremo sul catarinense.

SANDHU, R., SAMARATI, P., (1996) Authentication Access control and audit

SANTOS, P., (2016) Segurança Informática: A importância para a segurança interna, Lisboa

SERENO, J., (2015) Tendências de implementação e segurança nas redes wireless organizacionais, Instituto politécnico de Setúbal, Escola superior de ciências empresarias, Setúbal

SILVA, O., (2021) A pesquisa bibliográfica nos estudos científicos de natureza, Rio de Janeiro

YOSHIZAWA, D., (2027) Implementação de uma infraestrutura de redes de computadores na empresa FEAD, Universidade tecnológica federal do paraná departamento académico de electrónica, Especialização em configuração e gerenciamento de servidores e equipamentos de rede, Curitiba

7. ANEXOS

Questionário de Apoio para entrevistar os gestores de infra-estrutura de rede da Mota-Engil

Questão n.º 1 – "O que é cibersegurança e quais são os desafios que a empresa Mota-Engil Moçambique com a segurança de informação?"

Questão n.º 2 – "O que é e como é possível garantir a cibersegurança das infra-estruturas críticas como Mota-Engil Moçambique?"

Questão n.º 3 – "Qual é o espectro da ameaça da cibersegurança da Mota-Engil Moçambique?"

Questão n.º 4 – "Qual é o impacto de cyber ataques nas actividades da ME Moçambique?"

Questão n.º 5 – Que alterações ou ajustes são necessários para os gestores de segurança da ME Moçambique possam garantir maior eficácia de actuação no desempenho?