UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA – PÓS LABORAL

RELATÓRIO DE ESTÁGIO PROFISSIONAL

Segurança Cibernética: Shadow IT e suas implicações nas organizações

Caso de estudo: Meridian 32

Autor:

Valério Vasco Macumbuia

Supervisor da Faculdade:

Engº. Délcio Chadreca

Supervisor da Instituição:

Engº. Frederico Muianga

Maputo, 08 de Dezembro de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA – PÓS LABORAL

RELATÓRIO DE ESTÁGIO PROFISSIONAL

Segurança Cibernética: Shadow IT e suas implicações nas organizações

Caso de estudo: Meridian 32

Autor:

Valério Vasco Macumbuia

Supervisor da Faculdade:

Engº. Délcio Chadreca

Supervisor da Instituição:

Engº. Frederico Muianga

Maputo, 08 de Dezembro de 2023

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

LICENCIATURA EM ENGENHARIA INFORMÁTICA – PÓS LABORAL

TERMO DE ENTREGA DE ENTREGA DO RELATÓRIO

Declaro que o estudante Valério Vasco Macumbuia entregou no dia 05/12/2023 as 3 cópias do relatório do seu Estágio Profissional com a referência: **2023EIEPN3**, intitulado: Segurança Cibernética: Shadow IT e suas implicações nas organizações. Caso de estudo: Meridian 32

Maputo, ____ de _____ de 2023

O Chefe da Secretaria

_____

Dedicatórias

Dedico este trabalho aos meus pais, pelo apoio imensurável durante a minha jornada académica.

Agradecimentos

Em primeiro lugar quero agradecer a Deus pelo dom da vida e por permitir que eu chegasse tão longe na minha vida académica.

Agradecer aos meus pais, Vasco Macumbuia e Isabel David, pelo amor, educação, apoio, ensinamentos e por sempre criarem condições para mim e aos meus irmãos para que alcancemos os nossos sonhos.

Agradecer aos meus irmãos, Ivis Macumbuia e Hortência Macumbuia, pelos conselhos e por me apoiarem durante a minha jornada académica.

Agradecer a minha noiva, Joice Matsope, pelo apoio moral e incentivo nos momentos mais difíceis durante a minha jornada académica.

Ao meu supervisor da Faculdade de Engenharia, Engº Délcio Chadreca, os meus agradecimentos pela orientação durante a execução do relatório de estágio.

Agradeço ao meu supervisor da ALTEL Engº. Frederico Muianga pela paciência, apoio e os ensinamentos durante o estágio.

RESUMO

O crescimento das tecnologias de informação e comunicações (TIC) trouxeram dinamismo na execução de processos e celirdade na troca de informação, aumentando desta forma a produtividade no sector empresarial. Não obstante os seus benefícios, o seu crescimento é também acompanhado pelo crescimento de ataques cibernéticos. Posto isto, a implementação das TICs deve ser feita sob a gestão dos responsávies de TI de forma a garantir a segurança cibernétnica e a redução da probibildidade de ocorrência dos ataques cibernéticos. A utilização de TICs sem o conhecimento e apoio dos responsáveis de TI é conhecida como *Shadow IT* e acontece na maioria das vezes sem nenhuma intenção de prejudicar a segurança da informação, porém, pode constituir riscos para a segurança da informação, podendo resultar em custos altos para a organização e em danos irreparáveis. O presente relatório procurou propor medidas de mitigação para os riscos do *Shadow IT,* sendo que para tal recorreu-se a avaliação de risco baseada na norma ISO/IEC 27001, que é o principal padrão no que tange a segurança da informação. Para materialização do mesmo, recorreram-se aos inquéritos dirigidos aos utilizadores da organização e a entrevista dirigida ao responsável de TI da organização, suportada por uma revisão bibliográfica. Os priniciapis resultados do inquérito e da entrevista mostraram que os utilizadores do grupo Meridian 32 já utilizaram alguma aplicação, dispositivo ou serviço, sem o consentimento do TI para poder realizar alguma tarefa da organização e os resultados da avaliação de risco mostraram que existem riscos na utilização do *Shadow IT* para o grupo Meridian 32. Para os riscos identificados foram apresentadas medidas de mitigação, tendo mais uma vez como base a norma de segurança da informação ISO/IEC 27001. Ademais as medidas apresentadas, recomendou-se a implementação de políticas e programa de treinamento/conscientização sobre a segurança da informação.

Palavras-chave: Informação, ISO/IEC 27001, medidas de mitigação, risco, segurança cibernética*, Shadow IT*.

ABSTRACT

The growth of information and communications technologies (ICT) has brought dynamism to the execution of processes and speed to the exchange of information, thereby increasing productivity in the business sector. Despite its benefits, its growth is also accompanied by an increase in cyber-attacks. Post that, ICTs must be implemented under the management of IT managers to guarantee cyber security and reduce the likelihood of cyber-attacks. The use of ICTs without the knowledge and support of those responsible for IT is known as Shadow IT and most of the time happens without any intention of damaging information security, but it can constitute risks to information security and can result in high costs for the organization and irreparable damage. This report sought to propose mitigation measures for Shadow IT risks, using a risk assessment based on the ISO/IEC 27001 standard, which is the main standard for information security. To perform this, we used surveys of the organization's users and an interview with the organization's IT manager, supported by a literature review. The main results of the survey and interview showed that the users of the grupo Meridian 32 have already used an application, device or service without the consent of IT in order to carry out an organizational task and the results of the risk assessment showed that there are risks in the use of Shadow IT for the grupo Meridian 32. Mitigation measures were presented for the risks identified, once again based on the ISO/IEC 27001 information security standard. In addition to the measures presented, it was recommended that policies and a training/awareness program on information security be implemented.

Keywords: cyber security, information, ISO/IEC 27001, mitigation measures, risk, Shadow IT.

ÍNDICE

1. capítulo i – Introdução 1
1.1. Contextualização 1
1.2. Descrição do problema 2
1.3. Justificativa 2
1.4. Objectivos 3
1.4.1. Geral 3
1.4.2. Específicos 3
1.5. Metodologia 3
1.5.1. Classificação da metodologia de pesquisa 3
1.5.2. Colecta de Dados 4
1.6. Estrutura do Trabalho 6
2. capítulo ii – Revisão de Literatura 7
2.1. Informação 7
2.2.1. Classificação da Informação 8
2.2. Segurança da informação 9
2.2.1. Segurança Cibernética 9
2.2.2 Princípios da segurança da Informação 9
2.2.3. Vulnerabilidades 11
2.2.4. Ameaças 11
2.2.5. Controlos de segurança cibernética 12
2.2.6. ISO/IEC 27001 12
2.3. Caraterização do Shadow IT 14
2.3.1. Conceito de Shadow IT 14
2.3.2. Tipos de *Shadow IT* 15
2.3.3. Factores de influência para o uso de *Shadow IT* 16

2.3.4. Riscos do *Shadow IT* 18
2.3.5. Benefícios do *Shadow IT* 19
2.3.6. Medidas de mitigação dos riscos do uso de *Shadow IT* 20
3. Capítulo iii - Caso de estudo: grupo Meridian 32 23
3.1. Apresentação da Altel 23
3.1.1. Serviços e soluções oferecidas pela Altel 23
3.1.2. Política de qualidade 24
3.2. Apresentação do grupo Meridian 32 25
3.2.1. Política integrada da qualidade e do ambiente 27
3.3. Situação actual do grupo Meridian 32 28
3.3.1. Infra-estrutura de TI 28
3.3.2. Acesso a rede 28
3.3.3. Segurança física 29
3.3.4. Segurança Lógica 29
3.4. descrição das actividades desenvolvidas 30
4. capítulo iv - análise e discussão dos resultados 33
4.1. Identificaçaõ e avaliação de riscos dos shadow it 33
4.1.1. Identificação de riscos 33
4.1.2. Proprietário do risco 35
4.1.3. Análise do risco 35
4.1.4. Cálculo do nível de risco 38
4.1.5. Avaliação de risco 39
4.2. Apresentação dos resultados do inquérito 40
4.2.1. Utilização das redes sociais 40
4.2.2. Utilização de dispositivos electrónico pessoais 41
4.2.3. Utilização de web apps 41

4.2.4. Desenvolvimento de software/ planilha excel 42
4.3. Discussão de resultados 42
4.4. Proposta de medidas de mitigação 44
5. capítulo v – Conclusões e recomendações 46
5.1. Conlclusões 46
5.2. Recomendações 46
Bibliografia 48
Anexos 1
Anexo 1 – Guião de entrevista ao gestor de TI do Grupo Meridian32 ..... A1
Anexo 2 – Cátologo de vulnerabilidades e ameaças A2
Anexo 3 – Inquérito sobre a utilização do *Shadow IT* A6
Anexo 4 – Plano de actividades do estágio profissional A9

Lista de abreviatura e acrónimos

BYOD – Bring Your own Device

CCTV - Closed-circuit television

CIA - *Confidentiality, Integrity, and Availability*

EDR - Endpoint Detection and Response

ERP - Enterprise resource planning

HDD - Hard disk drive

IEC - International Electrotechnical Commission

IoT – Internet of Things

ISO – International Organization for Standardization

IT – Information Technology

NAS - Network Attached Storage

SaaS - Software as a Service

SaaS – Software as a service

TIC – Tecnologias de informação e comunicação

VPN - Virtual Private Network

WPA - Wi-Fi Protected Access

Índice de Tabelas e figuras

Tabela 1: Tabela de activos 28

Tabela 2: Activos do grupo Meridian 32 34

Tabela 3: Identificação dos riscos 35

Tabela 4: Avaliação de probabilidade 36

Tabela 5: Avaliação de impacto 37

Tabela 6: Análise de risco 38

Tabela 7: Nível de risco 38

Tabela 8: Metodologia para classificação de risco 39

Tabela 9: Resultados da avalição de riscos 40

Tabela 10: Proposta de medidas de mitigação 45

Figura 1: Relação entre pessoas, processos e tecnologias 7

Figura 2: Tríade CIA 9

Figura 3: Requisitos da ISO/IEC 27001:2022 13

Figura 4: diagrama da rede. 32

Figura 5: Resultados do inquérito - utilização de redes sociais 40

Figura 6: Resultados do inquérito - utilização de dispositivos electrónicos pessoais 41

Figura 7: Resultados do inquérito - utilização de web apps 41

Figura 8: Resultados do inquérito - desenvolvimento de planilha ou software 42

Glossário de Termos

Active Directory – Refere-se à um serviço de directório desenvolvido pela Microsoft para redes de domínio do Windows.

Backdoors – é uma porta no sistema não documentada que permite ao utilizador entrar no sistema.

Consumerização – prática onde os dispositivos como latptops e smartphones são usados tanto para o uso pessoal como corporativo.

Firewall – é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Hardware – componente física do computador.

Home Office – também chamado de trabalho remoto é uma prática que permite que uma pessoa tenha a possibilidade de trabalhar de qualquer lugar.

ISO/IEC – refere-se à uma organização mundial responsável pelos padrões de normatização de procedimentos.

Malware – é qualquer programa ou código malicioso seja prejudicial para os sistemas de TI.

Política – refere-se à um documento que estabelece directrizes que se aplicam numa organização e que ajudam a mesma alcançar os seus objectivos.

Software – Sequência de instruções escritas para serem interpretadas por um computador com o objectivo de executar tarefas específicas.

Switch – refere-se à um dispositivo composto por várias portas de comunicação que conecta os elementos de uma rede para transmissão de dados, vídeo ou voz.D

1. CAPÍTULO I – INTRODUÇÃO

1.1. CONTEXTUALIZAÇÃO

A transformação digital, o surgimento e o crescimento de dispositivos móveis revolucionaram a indústria das tecnologias, permitindo que os utilizadores tenham acesso a informação de forma simples e fácil, em diferentes dispositivos.

Estes acontecimentos fizeram com que os utilizadores estivessem mais familiarizados com as tecnologias e ganhassem mais domínio das mesmas. Por este contacto quase constante com as tecnologias, é comum os utilizadores desejarem usar estas tecnologias dentro do ambiente de trabalho, de forma a tornar as suas tarefas mais produtivas.

A prática de utilizar softwares, hardwares ou outro tipo de tecnologia dentro do ambiente corporativo com objectivo de aumentar os resultados dos entregáveis, sem aprovação do departamento de TI é conhecida como *Shadow IT*.

Esta prática apesar de trazer algumas vantagens tanto para o utilizador como para as organizações, aumenta a probabilidade da ocorrência de um ataque de segurança cibernético pelo facto da sua utilização não ser do conhecimento do departamento de TI, razão pela qual o departamento não tem como definir medidas de protecção.

O *Shadow IT* não é uma prática nova nas organizações, mas devido o surgimento de riscos de segurança cibernética resultados desta prática e devido o crescimento de tendências como trabalho remoto, consumerização do TI, *BYOD,* entre outros, esta prática tem ganhado muita atenção por partes das empresas, que buscam formas de reduzir os riscos desta prática.

A utilização do *Shadow IT* esta várias vezes ligada à alguns factores como limitação nas tecnologias (hadwares ou softwares) fornecidas pelo departamento de TI, morosidade no processo de aprovação e implementação de uma nova solução de IT, entre outros. Conhecer estes factores é importante para a definição de medidas de segurança de cibernéticas que ajudarão na redução dos riscos contra o *Shadow IT.*

1.2. DESCRIÇÃO DO PROBLEMA

Cada vez mais funcionários utilizam seus dispositivos e serviços pessoais como smartphones, serviços de email, gestores de tarefas e serviços de armazenamento na nuvem, para realização de tarefas corporativas, tendência esta influenciada pelo *BYOD*, consumerização, *home office*, entre outros.

Apesar de algumas vantagens que o uso de *Shadow IT* pode trazer, como produtividade ou redução de investimentos por parte da organização, a utilização de tecnologias sem conhecimento/aprovação do TI pode constituir um risco para segurança cibernética, pois sem conhecimento da utilização de certos dispositivos ou de certos softwares para tarefas corporativas, não tem como proteger-se dos possíveis riscos que possam advir desta prática.

Nestes termos, motiva-se a formulação da seguinte pergunta de pesquisa: Quais são os riscos do uso de *shadow IT* na segurança cibernética nas organizações?

1.3. JUSTIFICATIVA

A utilização de *Shadow IT* tem crescido exponencialmente, crescimento este influenciado pela adopção dos serviços em nuvem, expensão do trabalho remoto, a consumerização do TI e o *BYOD.*

O seu crescimento deve-se também ao facto do *Shadow IT* ser de fácil implementação e utilização, sendo na sua maioria distribuído de forma gratuita. Várias organizações têm adoptado a utilização do *Shadow IT* devido aos seus vários benefícios.

Entretanto, apesar dos seus vários benefícios, o *Shadow IT* constitui alguns riscos para a segurança da informação, como por exemplo, o risco do vazamento de informação causado pelo facto de dados serem acedidos ou armazenados em dispositivos e aplicações de *Shadow IT* não seguras.

Este trabalho servirá como meio um meio para despertar às organizações sobre as implicações que podem advir da utilização do *Shadow IT* se a sua implementação não for feita forma controlada e monitorada, ou seja, sem observar as medidas de segurança cibernética necessárias, aumentando o risco de um ataque cibernético.

Este trabalho irá apresentar medidas de segurança cibernética que podem ser adoptadas de forma a mitigar os riscos da utilização do *Shadow IT*.

Escolheu-se o grupo Merdian 32 como caso de estudo por se tratar de um local de fácil acesso em relação à obtenção de dados e em relação à deslocação pois permitirá uma mobilidade acelere e menos dispendiosa no que concerne aos fundos para realização do trabalho.

1.4. OBJECTIVOS

1.4.1. Geral

Analisar o uso de *Shadow IT* e suas implicações na segurança cibernética no grupo Meridian 32.

1.4.2. Específicos

- Descrever o uso de *Shadow IT* nas organizações;
- Identificar os riscos associados ao uso do *Shadow IT* nas organizações;
- Propor medidas de mitigação de riscos associado ao uso de *Shadow IT.*

1.5. METODOLOGIA

1.5.1. Classificação da metodologia de pesquisa

Classificação quanto ao objectivo

Segundo Gil (2002), uma pesquisa quanto aos objectivos pode ser exploratória, descritiva ou explicativa. O presente trabalho classifica-se como uma pesquisa descritiva, pois visa descrever o *Shadow IT* e os factores que influenciem a sua utilização dentro de uma organização, recorrendo desta forma ao caso de estudo.

Classificação quanto à natureza

Segundo Leão (2019), a pesquisa aplicada também chamada de pesquisa prática tem como finalidade propor soluções para um problema existente. O presente trabalho classifica-se como uma pesquisa aplicada, pois o trabalho visa propor medidas para reduzir os riscos associados a utilização do *Shadow IT*.

Classificação quanto à abordagem

Relativamente a abordagem, uma pesquisa pode ser classificada como uma pesquisa quantitativa ou pesquisa qualitativa. O presente trabalho classifica-se como uma pesquisa mista, pois o pesquisador para descrever o *Shadow IT* e as suas implicações para segurança cibernética, recorrem a evidências qualitativas e quantitativas, baseadas em inquéritos e entrevistas.

Classificação quanto ao procedimento

Relativamente aos procedimentos, o presente trabalho pode ser classificado como:

- **Pesquisa bibliográfica:** Conforme Gil (2002), a pesquisa bibliográfica é desenvolvida segundo conteúdo que existe na sua maioria em livros e artigos científicos. Todos os trabalhos científicos iniciam com uma pesquisa bibliográfica, dando ao pesquisador a oportunidade de saber o que já se estudou sobre o assunto.
- **Pesquisa documental:** Segundo Gil (2002), a pesquisa documental utiliza materiais que ainda não receberam algum tratamento analítico como cartas, diários, regulamentos, ofícios, etc.
- **Pesquisa participante:** Caracteriza-se pela interacção entre os pesquisadores e membros das situações investigadas. (Gil, 2002)
- **Estudo de caso:** segundo Prodanov & De Freitas (2013), o estudo de caso é um tipo de pesquisa que visa colectar e analisar informações sobre um grupo, comunidade ou organização com objectivo de estudar um determinado fenómeno. Para o presente trabalho escolheu-se o grupo Meridian 32 como estudo de caso para análise do *Shadow IT*.

1.5.2. Colecta de Dados

No presente trabalho recorreu-se aos seguintes instrumentos de colecta de dados:

Pesquisa bibliográfica

Para o presente trabalho foram consultados livros e artigos científicos disponíveis nos repositórios académicos como, Google académico, Researchgate, IEEE Xplore e Semantic Scholar.

A pesquisa bibliográfica foi realizada com o auxílio do Zotero, que é uma ferramenta gratuita para gestão de referências, que permite que os utilizadores busquem conteúdo em repositórios de dados e em outras fontes da internet e organiza os dados colectados para produzir citações e referências bibliográficas.

Pesquisa documental

Foram consultados documentos disponibilizados pelo grupo Meridian 32. Estes documentos são na sua maioria procedimentos, políticas e instruções de trabalho.

Questionário

De forma a recolher dados sobre o *Shadow IT* e os factores de influência para o seu uso dentro da organização Meridian32, foi elaborado um inquérito aos utilizadores finais e um questionário dirigido ao responsável pelo departamento TI.

Estes questionários foram elaborados e partilhados com o auxílio do *Microsoft Forms*, que é uma aplicação gratuita da Microsoft usada para elaboração de questionários, pesquisas, etc. Os questionários poderão ser consultados na secção dos anexos.

Para além dos questionários, foram colhidas outras informações com base nas experiências colhidas durante o período de estágio, de forma a complementar os resultados obtidos dos questionários, das pesquisas documentais e bibliográficas.

1.6. ESTRUTURA DO TRABALHO

O presente trabalho está organizado em 7 capítulos, nomeadamente:

Capítulo 1 – Introdução: Consiste da parte introdutória do trabalho, sendo constituída pela contextualização do tema, descrição do problema, justificativa, objectivos e metodologia usada.

Capítulo 2 – Revisão de literatura: Neste capítulo apresenta-se tópicos importantes para a realização do presente trabalho.

Capítulo 3 – Caso de Estudo: Neste capítulo abordam-se conceitos relativos a utilização do *Shadow IT* e as suas implicações para a segurança cibernética no grupo Meridian 32. Adicionalmente abordam-se as actividades desenvolvidas no decorrer do estágio profissional.

Capítulo 4 – Análise e discussão de resultados: Neste capítulo apresentam-se os resultados do inquérito, faz-se avaliação dos resultados da entrevista e da análise do risco e propõe-se a solução para o problema estudado no presente.

Capítulo 7 – Conclusão e recomendações: Neste capítulo avalia-se o cumprimento dos objectivos do trabalho e propõe-se recomendações para trabalhos posteriores.

Bibliografia: Consiste das fontes usadas durante a realização do presente trabalho, quer tenham sido citadas ou não.

Anexo: Procede-se a apresentação de elementos adicionais que facilitem a compreensão do trabalho.

2. CAPÍTULO II – REVISÃO DE LITERATURA

2.1. INFORMAÇÃO

A informação pode ser definida de diferentes formas, dependendo da área ou contexto. Em informática, a informação é comumente definida como sendo um conjunto de dados processados em um computador, gerando resultados.

Conforme (Messias, 2005), a informação movimenta a economia global, sendo considerada o a fonte de renda e poder de uma sociedade. O uso racional da informação, permite que as organizações resolvem os seus problemas e tomem decisões.

Da afirmação acima, pode-se perceber que o desenvolvimento de qualquer organização, está directamente ligado à informação que esta possui, como também a forma que a organização gere esta informação.

Para Laureano (2012), a informação agrega um valor altamente significativo, por esta estar integrada com processos, pessoais e tecnologias,. A figura 1, demonstra o relacionamento dos processos, tecnologias e pessoas.

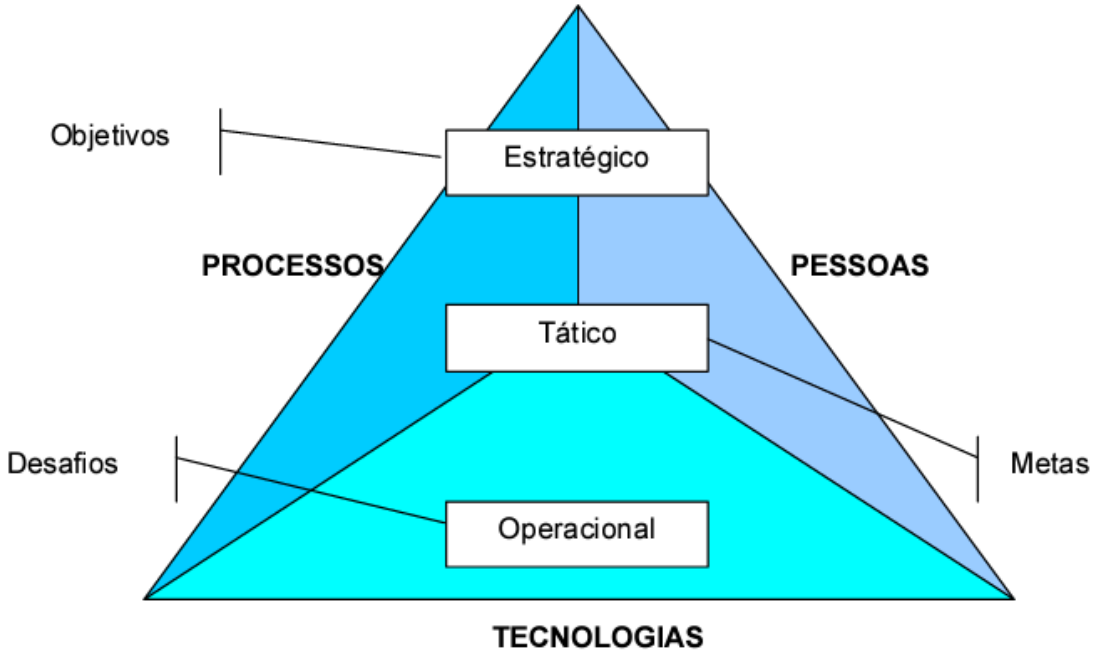

Figura 1: Relação entre pessoas, processos e tecnologias

Fonte: LAUREANO (2012)

Segundo Fontes (2017), a informação é um activo importante para qualquer organização, por isso esta deve ser protegida independentemente do seu formato, que pode ser físico ou digital.

Por ser um activo intangível e abstracto, a informação pode facilmente sair da empresa, seja através de um meio magnético, papel ou através de um funcionário. Estas características tornam a informação um activo vulnerável, por isso esta requer muita atenção e cuidados. (Ferreira, 2003)

2.2.1. Classificação da Informação

Segundo Laureano (2012), há uma necessidade de classificar a informação em níveis de prioridade, de forma assegurar o nível adequado de protecção para a informação e garantir que a esta não seja acedida por pessoas não autorizadas. O autor classifica a informação em quatros classes, dependo do valor que esta apresenta para a organização. As classes são:

- **Pública**: a informação fica disponível para qualquer pessoa, ou seja, funcionários, terceirizados, fornecedores, clientes e público em geral, sem que isso provoque impactos no negócio.
- **Interna**: a informação é acedida somente por colaboradores da organização, não sendo desejável que ela seja acedida por pessoas que não pertençam a organização. Entretanto, caso haja vazamento e a informação fique disponível para o público, o prejuízo será pequeno pois o foco deste tipo de informação é a protecção da integridade.
- **Confidencial**: a informação é acessível apenas para um grupo de pessoas. O vazamento deste tipo de informação pode implicar grandes prejuízos como perdas financeiras, de imagem, de concorrência no mercado, etc.
- **Secreta**: a informação é acessível apenas para pessoas autorizadas. São informações mais importantes que as informações confidencias por isso devem receber um grau de protecção ainda mais elevado.

2.2. SEGURANÇA DA INFORMAÇÃO

De acordo com Sêmola (2003), a segurança da informação é definida como sendo “uma Área de conhecimento dedicada à protecão de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

A segurança da informação protege todos os dados que estejam em armazenamento, processamento ou transmissão através da implementação de políticas, treinamento e conscientização e tecnologias. (Whitman & Mattord, 2021)

Para Alves (2006), a segurança de informação tem como objectivo proteger a informação de forma a segurar a continuidade de negócio, diminuindo os danos e aumentando o retorno dos investimentos.

Das definições acima, percebe-se que o objectivo principal da segurança da informação é criar uma estrutura adequada para protecção da informação, sendo necessário que a organização defina um grupo responsável pela implementação segurança de informação.

2.2.1. Segurança Cibernética

A segurança cibernética tem sido tema de debate, a medida que muitas empresas transitam para o mundo digital e o número de ataques de segurança de informação vai crescendo.

2.2.2 Princípios da segurança da Informação

De acordo com o padrão ISO/IEC 17799:2005, as propriedades básicas da segurança da informação são: confidencialidade, integridade e disponibilidade. Estas propriedades são conhecidas como tríade CIA, demonstrados na figura 2.

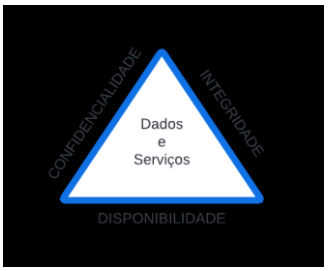

Figura 2: Tríade CIA

Fonte adaptado de Whitman & Mattord (2021)

Confidencialidade

Uma propriedade que quando presente garante que a informação somente seja acedida por pessoas autorizadas, evitando desta forma que a informação seja divulgada sem autorização prévia do proprietário. (Ferreira, 2003)

Integridade

Garante que a informação não sofrerá nenhuma modificação durante o trajecto entre a pessoa que envia e a pessoa que recebe a informação, garantindo assim a sua real veracidade após chegar ao destino. (Peixoto, 2006)

Disponibilidade

Garante que a informação está sempre disponível para pessoas ou sistemas devidamente autorizados. A informação disponível deve ser de fácil acesso e deve confiável. (Ferreira, 2008)

De acordo com alguns autores, a tríade CIA não é suficiente para garantir a segurança da informação, sendo necessário a existência de outras propriedades. Sêmola (2014) acrescenta à CIA, os seguintes atributos:

Legalidade

Garante que a informação está em conformidade com a lei, cláusulas contratuais, procedimentos, políticas e legislações nacionais ou internacionais.

Autenticidade

Propriedade que garante que a informação ou o utilizador da mesma é autêntico, ou seja, garante que a informação foi enviada pelo real remetente e que a mensagem não foi modificada após o seu envio.

Não Repúdio

Propriedade que garante a não negação da recepção, envio ou modificação da informação.

Auditoria

Propriedade que permite rastrear todos os passos de um utilizador em um sistema, identificando o local e o horário. A auditoria permite identificar violações de segurança.

2.2.3. Vulnerabilidades

Pela definição de Santos & Soares (2018), vulnerabilidade é uma falha ou fraqueza de um activo que quando explorado por uma ameaça, pode causar impacto para a organização.

Para Ferreira (2003), as vulnerabilidades podem ser classificas em três categorias:

- **Tecnológicas**: todas as actividades que envolvem tecnologia, como por exemplo, computadores, rede de computadores, smartphones, etc.
- **Físicas**: representam o ambiente físico onde encontram os activos de hardware.
- **Humanas**: envolvem o factor humano, podendo ser considerada a mais difícil de analisar porque tratar de questões relacionadas à aspectos emocionais e socioculturais que podem variar de pessoa para pessoa.

2.2.4. Ameaças

Conforme Peixoto (2006), a ameaça de segurança é qualquer acção capaz de causar danos à confidencialidade, integridade e disponibilidade da informação. As ameaças resultam das vulnerabilidades existentes.

De acordo com Sêmola (2003), as ameaças da segurança da informação podem ser classificadas nas seguintes categorias:

- **Naturais**: fenómenos da natureza. Como por exemplo, raios que danificam equipamentos, chuvas, umidades, terramotos, etc.
- **Involuntárias**: são aquelas que ocorrem por causa do desconhecimento, erros ou acidentes.

Voluntárias: são acções propositais, resultantes de acções como, por exemplo, acções de crackers, espiões, disseminadores de vírus de computador, etc.

2.2.5. Controlos de segurança cibernética

Dependendo da importância e da sensibilidade da informação para a organização, esta deve ser protegida através de controlos de segurança para evitar que a mesma fique disponível para pessoas não autorizadas. (Fontes, 2017)

Controlos preventivo – são os que melhoram representam custo-benefício, seu objectivo é evitar que os incidentes de seguranças aconteçam.

Controlos detectivos – têm como objectivo principal detectar um incidente de segurança que não foi impedido pelo controlo preventivo.

Controlos correctivos – são medidas tomadas quando há um incidente de segurança e têm objectivo de corrigir um determinado problema e minimizar o impacto do mesmo.

2.2.6. ISO/IEC 27001

Sendo a informação um activo importante para as organizações, nos últimos anos foram criadas várias normas que estabelecem um conjunto de boas práticas com objectivo de proteger a confidencialidade, integridade e disponibilidade da informação.

ISO/IEC 27001 é uma norma internacional publicada pela organização internacional de normalização (ISO) em parceria com a comissão electrónica internacional (IEC). Faz parte da série ISO/IEC 27000, que é um conjunto de normas criadas para abordar a segurança da informação, sendo que a ISO/IEC 27001 é considerada a principal norma no que tange a segurança da informação. (Kosutic, 2023)

A ISO/IEC 27001 conta com três versões, sendo que a primeira versão foi lançada em 2005 (ISO/IEC 27001:2005), a segunda versão em 2013 (ISO/IEC 27001:2013) e última versão foi lançada em 2022 (ISO/IEC 27001:2022).

De acordo com Konzen (2013), a norma ISO/IEC 27001 especifica os requisitos para o estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhoria de um sistema de gestão de segurança da informação.

A ISO/IEC 27001 é composta por duas partes distintas, onde na primeira parte (vide gráfico 3) são definidos os requisitos da norma e na segunda parte, denominada como

anexo A, são definidos um conjunto de controlos que ajudam na redução de risco. (Kosutic, 2023)

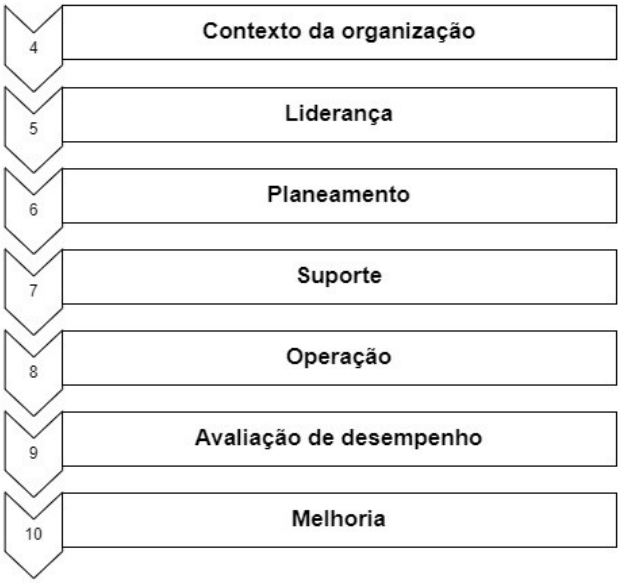

Figura 3: Requisitos da ISO/IEC 27001:2022

Fonte: adaptado de (Kosutic, 2023)

Ainda de acordo com o mesmo autor, o anexo A da ISO/IEC 27001:2022 é composto por 93 controlos organizados em quatro secções, nomeadamente:

- **Secção A.5 (controles organizacionais)** – defina regras a serem adoptadas, bem como o comportamento esperado dos utilizadores, dispositivos, software e sistemas. Por exemplo, política de controle de acesso, política BYOD, política, de gestão do *Shadow IT,* etc.
- **Secção A.6 (controles de pessoas)** – fornecem conhecimento, edução, habilidades ou experiência de modo que as pessoas executem as suas actividades de forma segura. Por exemplo, treinamento para utilização segura Do *Shadow IT.*
- **Secção A.7 (controles físicos)** – definem dispositivos físicos utilizados para segurança da informação. Por exemplo, câmeras *CCTV*, sistemas de alarme, fechaduras, etc.
- **Secção A. 8 (controles tecnológicos)** – definem softwares e hardwares para garantir a segurança em um sistema de informação. Por exemplo: backup, firewall, antivírus, etc.

2.3. CARATERIZAÇÃO DO SHADOW IT

2.3.1. Conceito de Shadow IT

Silic et al. (2016), define o *Shadow IT* como sendo uma prática que envolve a criação, modificação ou utilização de qualquer sistema sem qualquer conhecimento prévio, aprovação ou apoio do departamento de TI.

Para Klotz et al. (2019), o *Shadow IT* pode ser definido como a criação ou utilização de software, hardware ou serviços de TI por parte dos utilizadores de uma organização sem o conhecimento ou alinhamento da gestão de TI.

Dos conceitos apresentados acima pelos autores, ambos concordam que o *Shadow IT* ocorre sem o conhecimento ou aprovação do departamento de TI.

De acordo com Haag & Eckhardt (2014), a utilização do *Shadow IT* é voluntária e viola as políticas da organização como forma de resposta às restrições impostas pelo departamento de TI com o objectivo de melhorar o desempenho no trabalho, mas não de prejudicar a organização.

Entretanto, em muitos casos os utilizadores utilizam o *Shadow IT* de forma inconsciente, sem saber que o seu uso pode trazer riscos para a organização, e isto acontece devido a inexistência de políticas de TI e pela falta de conscientização em relação a segurança de informação.

Silic et al., (2016), acrescenta que outro motivo que leva os utilizadores a seguirem as práticas de *Shadow IT* é a falta de ferramentas, processos ou procedimentos suficientes para ajudá-los a serem mais eficientes ou produtivos na organização.

Em outras palavras, o *Shadow TI,* revela a capacidade do departamento de TI de uma organização em satisfazer as necessidades dos utilizadores no que diz respeito as tecnologias de informação.

Exemplos de utilização *Shadow IT* incluem:

- Utilização de serviços em nuvem para gerir tarefas, agendas de trabalho, etc.;
- Utilização de email pessoal para troca de informação confidencial da organização;

- Instalação de aplicações nos dispositivos da organização, sem autorização do departamento de TI;
- Utilização de *SaaS*, que é um serviço que permite a utilização de software sem a necessidade de instalar, sendo necessário que haja apenas uma conexão de internet.

Outros exemplos de Shadow IT incluem a utilização de macros do Excel/Access criadas pelos utilizadores para proporcionar melhores resultados em termos de produtividade e utilização de aplicações de terceiros como o Trello. (Silic et al., 2016)

2.3.2. Tipos de *Shadow IT*

Conforme Haber (2023) , o *Shadow IT* pode ser classificado em 6 grupos, nomeadamente:

1. **Dispositivos *Shadow IoT*** - Referem-se a todos dispositivos *Shadow IoT* como smartwatches, termos estáticos sem fio, cameras, impressoras sem fio, Smart TVs, entre outros. Estes dispositivos possuem recursos avançados e quando conectados à rede corporativa podem dar espaço a potencias de ameaças;
2. **Aplicações *SaaS*** - Referem-se as aplicações de nuvem, onde geralmente a sua implementação não segue o processo normal seguido pelas aplicações implementadas pelo departamento de TI da organização e por isso o seu uso representa riscos no ponto de vista do que são as melhores de práticas de segurança;
3. **Máquinas virtuais** - Referem-se as máquinas virtuais que não são disponibilizadas pelo departamento de TI, mas sim por provedores de soluções e na sua maioria são disponibilizadas de forma gratuita, permitindo aos utilizadores a realização de testes de softwares, demonstração de aplicações, etc.;
4. **Sub-rede** - Referem-se as sub-redes roteáveis que são desconhecidas pela organização, que resultam do crescimento das organizações e expansão das suas redes;
5. **Dispositivos de rede** - Representam a forma mais antiga do *Shadow IT* e pode ser encontrada em muitas organizações, pela facilidade de adicionar estes dispositivos a rede, seja através de uma tomada ou uma rede WiFi. Estes dispositivos podem variar de smartphones, pontos de acessos WiFi,

Computadores, etc. Cada dispositivo não gerido representa um risco, devido a falta de monitoramento de vulnerabilidades ou de acessos inapropriados;

6. **Aplicações locais** - referem-se a todas aplicações instaladas nas estações de trabalho ou sem servidores, sem aprovação do TI. Dependendo da aplicação, estas podem representar um risco inaceitável, principalmente se as aplicações não forem geridas pelo departamento de TI.

2.3.3. Factores de influência para o uso de *Shadow IT*

A utilização do *Shadow IT* é motivada várias vezes por factores que podem variar desde factores técnicos até factores humanos.

Haag & Eckhardt (2014), argumentam que a frustração devido às restrições dos sistemas de TI é um dos factores que pode levar com que os utilizadores procurem meios alternativos para ultrapassar os obstáculos técnicos com a intenção de obter o resultado desejado.

Klotz et al. (2019), apresentam alguns factores que podem levar os colaboradores a utilizarem o *Shadow IT,* nomeadamente:

Acessibilidade técnica – ocorre quando a acessibilidade da TI aumenta resultado da diminuição na complexidade da TI e no aumento das ofertas tecnológicas no mercado. A medida que as soluções de TI se tornam simples, a sua implementação nas organizações também se torna mais simples. As aplicações WEB, os serviços de nuvem e os dispositivos móveis tem um papel importante neste factor, pois, facilitam a implementação e o acesso às soluções de TI.

Competência do utilizador – cada vez mais utilizadores nas organizações ganham conhecimento a até mesmo domínio sobre tecnologias de TI, permitindo que estes criem e acedam as soluções de TI de forma fácil.

Falta de alinhamento entre o departamento de TI e outros departamentos – a falta de conhecimento da regra do negócio pelo departamento de TI, faz com que algumas necessidades do utilizador não sejam atendidas, o que acaba motivando o uso de *Shadow IT*.

Deficiência nos sistemas de TI – As limitações dos sistemas podem ser superadas pela utilização do *Shadow IT*.

Motivação dos funcionários - os utilizadores de S*hadow IT* têm maior motivação para alcançar os objectivos em relação aos utilizadores que não usam *Shadow IT*. O aumento do desempenho individual a nível pessoal ou profissional também são factores de motivação para utilização do S*hadow IT*.

Lentidão do departamento de TI – respostas lentas às solicitações, influenciadas pelo processo de priorização desvantajoso das solicitações, representam a falta de agilidade por parte do departamento de TI, promovendo deste modo o surgimento do *Shadow IT* nas organizações.

Incerteza do ambiente de negócio – condições de incertezas aumentam a probabilidade do desenvolvimento e implementação do *Shadow IT*, incluindo a necessidade de reagir a condições de mercado voláteis com alta flexibilidade. A incerteza no ambiente de negócios pode ser causada pelo aumento da concorrência, pela necessidade de diversificar o portfólio de produtos ou por necessidades estratégicas.

Falta de competência ou escassez de recursos no departamento de TI – Um dos factores de motivação menos comum para o *Shadow* IT é falta de *know-how* de TI ou a falta de recursos no departamento de TI.

Perda de controlo – outro factor menos comum é a perda de controlo das organizações. Por exemplo, a implementação de um sistema *ERP* pode levar a uma perda de controle sobre os processos de negócio. Portanto, a implementação do *Shadow IT* pode fornecer aos funcionários uma oportunidade de “de recuperar algum controle”.

Haber (2023), acrescenta outros factores que podem influenciar os utilizadores a aderirem soluções do *Shadow IT*. Estes factores incluem:

Adopção de nuvem - A *Shadow IT* cresceu nos últimos anos com a adopção de aplicações e serviços baseados em nuvem, isso porque a sua instalação, configuração e uso podem ignorar os controlos internos;

Eficiência dos funcionários - um dos principais factores pelos quais funcionários utilizam o *Shadow IT*, é a busca pela eficiência nas suas tarefas, razão pela qual alguns se sentem motivados a contornar as políticas de segurança da empresa.

2.3.4. Riscos do *Shadow IT*

Para Haber (2023), a utilização do *Shadow TI* pode criar riscos no que diz respeito a segurança de informação. O autor destaca os principais riscos que podem ser encontrados no uso do *Shadow IT:*

- **Introdução de *Malware*** - O *Shadow IT* expande a superfície de ataque da organização, pois uma vez que os dispositivos e aplicações do *Shadow IT* são ocultos, as soluções de segurança cibernética implementadas na organização não abrangem o *Shadow IT*, aumentado desta forma a chance de um ataque cibernético;
- **Criação de *backdoors*** - Por definição, *o Shadow IT* está fora da visão da segurança cibernética, o que em outras palavras significa que quaisquer configurações incorrectas ou vulnerabilidades introduzidas permanecerão indetectadas, abrindo espaço para actuação de agentes maliciosos;
- **Incompatibilidade com os sistemas usados na organizaçã**o - O uso do *Shadow IT* nas estações de trabalho pode apresentar problemas devido a incompatibilidade do *Shadow IT* com os sistemas usados pela organização;
- **Custos** - O *Shadow IT* pode apresentar custos resultados de uma possível violação de dados, do tempo de inactividade ou da falta de escalabilidade da *Shadow IT*;
- **Perda ou roubo de dados** - Uma vez que o departamento de TI não tem controlo das contas pessoais de email e armazenamento, não existem tarefas de backup criadas para estes tipos de contas, o que dificulta a recuperação de dados em caso de um desastre, violação de dados ou ataques cibernéticos.

Klotz et al. (2019), acrescenta a existência de outros riscos que podem advir da utilização do *Shadow IT,* nomeadamente:

Falta de privacidade de dados – devido a gestão oculta do *Shadow IT*, medidas típicas de avaliação e prevenção de riscos não podem ser realizadas, o que pode gerar

problemas de conformidade, além disso, a privacidade de dados não pode ser garantida, principalmente em softwares como *SaaS* ou para aplicativos em nuvem;

Falta de consciência – os funcionários geralmente não têm consciência das políticas em vigor na organização, como também não tem consciência das possíveis consequências da utilização do *Shadow IT*;

Falta de integração e inconsistência de dados – o *Shadow IT* geralmente carece de integração com os sistemas oficiais, não é padronizado e pode ser baseado em arquitecturas não confiáveis. Além disso, as soluções *Shadow IT* podem levar a inconsistências de dados levando a perda de credibilidade dos dados;

Perda de sinergia e criação de ineficiência - a diversificação do cenário de TI aumenta com uma diminuição simultânea da padronização. Consequentemente, as sinergias não podem ser realizadas, existem redundâncias e a automação é prejudicada. Em resumo, as ineficiências ocorrem devido ao uso de *Shadow IT* que leva a custos mais altos, desperdício de recursos ou conflitos de recursos com sistemas e projectos oficiais;

Perda de controlo – Devido a gestão oculta do *Shadow IT*, surgem lacunas na transparência, assim sendo, o *Shadow IT* não pode ser formalmente controlado. Portanto, a *Shadow IT* prejudica a governança de TI, as intenções da gestão e os objectivos estratégicos;

Falta continuidade - uma instância de *Shadow IT* é frequentemente implementada por um ou poucos funcionários, o que leva a uma alta dependência de tais funcionários para continuidade de negócio. Reforçado pela falta de documentação e suporte potencialmente baixo ou inexistente, existe o risco de interrupções do sistema, levando a interrupções nos serviços.

2.3.5. Benefícios do *Shadow IT*

De acordo com Klotz et al. (2019), apesar dos riscos encontrados na *Shadow IT*, a sua utilização também apresenta vários benefícios, nomeadamente:

Ganho de produtividade – A *Shadow IT* permite que as organizações se beneficiem de um aumento na produtividade, eficiência e eficácia, influenciado pelo aumento de

produtividade entre os funcionários, pois a *Shadow IT* leva a um melhor desempenho individual.

Os utilizadores têm maior desempenho com soluções autodesenvolvidas do que com soluções desenvolvidas por outros.

Aumento da inovação – A *Shadow IT* pode ser uma fonte de criatividade e inovação como uma manifestação da criatividade dos utilizadores e inovação pessoal.

Aprimoramento da agilidade e aumento da flexibilidade – Um outro benefício da *Shadow IT* é agilidade, que pode ser visto, por exemplo, na redução do tempo de implementação.

A *Shadow IT* permite também maior flexibilidade devido à sua adaptabilidade, especialmente em comparação com soluções grandes e rígidas como *ERP*.

Melhoria da satisfação do utilizador/cliente – A *Shadow IT* pode melhorar a satisfação do utilizador, uma vez que esta pode fornecer uma funcionalidade específica ou pelo facto do utilizador estar mais familiarizado.

Aprimoramento da colaboração – Certos tipos de *Shadow IT* permitem uma comunicação melhor e mais rápida, como no caso de compartilhamento de conhecimento.

2.3.6. Medidas de mitigação dos riscos do uso de *Shadow IT*

Nos capítulos anteriores foram apresentados os benefícios e os riscos que podem advir da utilização da *Shadow IT,* contudo apesar da existência dos riscos, medidas de segurança podem ser implementadas de forma a tirar o maior proveito dos benefícios da *Shadow IT.*

Klotz et al. (2019), defende que para processos críticos ou negócios altamente regulamentados, pode ser mais razoável que a *Shadow IT* seja estritamente proibida.

Entretanto, considerando os benefícios da Shadow IT, uma proibição completa não parece ser razoável. Tal medida também impactaria negativamente a motivação dos funcionários e o comportamento de inovação. Portanto, parece ser mais promissor permitir *Shadow IT*, mas a sua implementação deve ser controlada. (Klotz et al., 2019)

Em todos os casos, a decisão de permitir ou proibir a utilização da *Shadow IT* dentro da organização deve ter como base a avaliação de risco que permitirá a organização ter uma visão do impacto e da probabilidade de ocorrência dos riscos de *Shadow IT* dentro da organização.

No que diz respeito a medidas de segurança cibernéticas, estas podem ser baseadas em cincos estratégias, nomeadamente:

- **Defender**: consiste em impedir a ocorrência do risco, criando medidas de protecção contra ameaças e removendo vulnerabilidade de activos;
- **Transferir**: consiste em transferir o risco para terceiros, como seguradoras ou provedores de serviços;
- **Mitigar**: consiste em tentar reduzir ao máximo o impacto do risco através do planeamento e preparação;
- **Aceitar**: consiste em não tomar nenhuma acção em relação a um risco, tendo como base que o custo de protecção de um activo não pode ser maior que o valor do mesmo activo;
- **Eliminar/evitar**: consiste em terminar/eliminar actividades que apresentam riscos incontroláveis.

Haber (2023), apresenta algumas medidas de segurança que podem ser implementadas para gestão de gestão do risco da *Shadow IT*, nomeadamente:

Estabelecer uma política de gestão de *Shadow IT*: Deve-se estabelecer uma política a ser aplicada a todas operações no que diz que respeito a gestão do *Shadow IT*, independentemente de o funcionário estar a trabalhar localmente ou remotamente.

Reconhecer a existência do *Shadow IT*: Deve-se reconhecer a existência do *Shadow IT* e deve-se garantir que a *Shadow IT* seja implementada sob a gestão de TI.

Apoiar uma política de portas abertas: O departamento de TI deve estar aberto as novas ideias, conselhos, fornecer ajuda aos utilizadores e não ser resistente a mudanças, uma vez que a *Shadow IT* tende a surgir como resposta aos obstáculos da TI tradicional.

Adoptar uma política para identificar a *Shadow IT*: Devem-se utilizar técnicas para detectar a *Shadow IT* e classificar seu risco para os negócios.

Equilibrar a segurança com as solicitações: Deve-se procurar um equilíbrio entre as necessidades dos funcionários e a segurança da informação, devendo se adoptar um modelo seguro para implementação de necessidades.

Klotz et al. (2019), apresenta também algumas medidas de segurança que podem ser aplicadas para a gestão do risco da *Shadow IT*, complementando as medidas apresentadas anteriormente. Estas medidas são:

Treinamento e conscientização - Os treinamentos de segurança ajudam os utilizadores a entenderem os riscos associados ao *Shadow IT* e que atitudes estes devem adoptar para mitigar ou evitar riscos.

Resolução de lacunas – a utilização da *Shadow IT* pode ser reduzida se as lacunas existentes nos sistemas de TI forem colmatadas para satisfazer as necessidades dos utilizadores.

Monitorização e identificação - A monitorização técnica pode ser uma medida para aplicar políticas ao *Shadow IT* e ajudar a identificar instâncias encobertas da *Shadow IT.*

Outras possibilidades de identificar a *Shadow IT* incluem avaliações da arquitectura de TI, a avaliação dos pedidos de assistência técnica, inquéritos aos funcionários e a análise do software instalado nos dispositivos dos utilizadores.

3. CAPÍTULO III - CASO DE ESTUDO: GRUPO MERIDIAN 32

O estágio foi realizado na ALTEL que é uma empresa que faz parte de uma organização denominada Grupo Meridian32 (caso de estudo). A ALTEL é responsável pela gestão de TI de todos empresas do Grupo Meridian 32. Esta gestão inclui gestão de redes, administração de sistemas, segurança de informação e outros serviços de TI.

3.1. APRESENTAÇÃO DA ALTEL

Altel Soluções Globais de Comunicação é uma empresa moçambicana de telecomunicações e tecnologias de informação, fundada em 2003. Localizada no Edifício TVSD – Avenida Vladimir Lenineº 3071, 5º Andar Maputo, Moçambique, conta com vários parceiros de renome como Alcatel Lucent, APC, AXIS, Cisco, HP, McAfee, Microsoft, vmware e outros.

A Altel tem mais de 20 funcionários, e conta em seu corpo técnico com especialistas em Switching, redes, sistemas de comunicação de voz e dados, sistemas de radiotransmissão, segurança lógica, segurança electrónica, centro de dados, CCTV, videoconferência e outras soluções de tecnologia de informação.

3.1.1. Serviços e soluções oferecidas pela Altel

Altel é uma empresa IT focada em inovação, automação e segurança da informação com uma ampla gama de campos especializados através de colaboradores e parceiros certificados.

Tem como principais serviços e soluções:

- **Soluções de engenharia de dados**: inclui gestão de meta dados, *Datawarehouse*, base de dados e segurança de dados;
- **Serviços de segurança cibernética:** incluo controlos de segurança, orquestração de segurança, automação, resposta e gestão de risco;
- **Soluções de segurança electrónica: i**nclui soluções de CCTV, controlo de acesso e sistemas de detecção de incêndio;
- **Soluções para gestão documental:** inclui arquivo de documentos, catálogo, integração, etc.;

- **Serviços de suporte técnico:** inclui serviços de suporte de primeira linha, segunda linha e terceira linha;
- Soluções de voz e videoconferência.

3.1.2. Política de qualidade

Como forma de evidenciar o comprometimento da gestão de topo perante os seus colaboradores, clientes e outras partes interessadas, a ALTEL reconhece a importância da Qualidade na gestão das suas actividades e, desta forma, institui a presente Política no sentido de implementar e manter um Sistema de Gestão, em conformidade com os requisitos da norma ISO 9001:2015, com vista à melhoria contínua de todos os processos da empresa, satisfação dos Clientes e análise dos riscos inerentes. A Direcção Geral compromete-se desta forma a zelar pelo cumprimento escrupuloso da Política de Qualidade estabelecida e péla designação de um responsável (Gestor da Qualidade) que fará a sua actualização periódica, de acordo com as necessidades futuras da empresa. A presente Política encontra-se disponível a todos os Colaboradores e é divulgada pelos meios de comunicação interna da empresa para sua consciencialização, juntamente com a restante estrutura documental do sistema.

Visão

Ser líder de referência no mercado nacional na área das TICs, pela qualidade e inovação dos serviços e soluções que proporciona aos seus clientes, contribuindo para o seu crescimento sustentável.

Missão

Proporcionar aos seus clientes soluções ambiciosas e compatíveis com os seus requisitos, sendo reconhecida como um parceiro de confiança, capaz de acompanhar e promover a evolução das suas necessidades.

Princípios

- Garantir um ambiente para a operacionalização eficaz e eficiente dos processos que permita aos Colaboradores o desenvolvimento das suas competências, a sua criatividade e a sua motivação para benefício comum;
- Cumprir os requisitos legislativos, normativos e regulamentares aplicáveis;

- Aperfeiçoar e manter continuamente o SGQ, sensibilizando, formando e envolvendo todos os Colaboradores e todas as partes envolvidas que se considere relevante;
- Analisar e melhorar constantemente a eficácia e a eficiência do SGQ, com vista à satisfação dos Clientes e outras partes interessadas.

Valores

- Liderança;
- Ética e profissionalismo;
- Trabalho em equipa;
- Competência;
- Comprometimento.

3.2. APRESENTAÇÃO DO GRUPO MERIDIAN 32

O Grupo Meridian 32 é uma holding de empresas e incubadora de projectos, contando neste momento com empresas de diferentes áreas sob sua gestão. Actualmente, localiza-se no Edifício TVSD – Avenida Vladimir Leninenº 3071, 5º Andar Maputo, Moçambique.

O Grupo Meridian 32 oferece as suas empresas, vários serviços, nomeadamente: serviços administrativos, serviços de recursos humanos, serviços de contabilidade e finanças, serviços jurídicos e estatutários, serviços de tecnologia da informação e serviços de logística.

O Grupo Meridian 32 teve início de actividade em 2000 e conta com mais de 100 colaboradores em áreas de especialidade bastante diferenciadas: business center; imobiliário, engenharia, arquitectura, ambiente, gestão social, sistemas de gestão, formação, contabilidade, fiscalidade, auditoria, cobranças, softwares de gestão, redes e telecomunicações e manutenção de edifícios.

A seguir algumas das principais empresas do Grupo Meridian 32:

- **Accsys -** É uma empresa moçambicana que se dedica à prática de consultoria e prestação de serviços em quatro principais sectores, nomeadamente o

Outsourcing e Assurance, consultoria financeira, consultoria de negócio e consultoria fiscal, com uma vasta experiência e know-how em Moçambique.

- **REC -** Real Estate Consulting, Lda é uma empresa moçambicana regulada pelo RICS (Royal Institution of Charted Surveyors) e que opera no mercado moçambicano desde 2000. Tem como principais serviços, gestão imobiliária, avaliação de equipamentos, avaliação de frotas, avaliação de activos biológicos e desenvolvimento de projectos de engenharia e arquitectura.
- **Incentea –** é a maior representante das soluções Primavera em Moçambique. Dedica-se a prestação de serviços profissionais nas áreas das tecnologias de informação e comunicação, marketing e inovação, consultoria de negócio, e engenharia de produto**.**
- **ZAE -** é uma empresa moçambicana que opera no mercado desde 2004 e dedica-se a inventariação, conformidade com registos contabilísticos, etiquetagem e valoração de equipamentos, frotas, imobilizados e maquinarias.
- **Ambveritas -** é uma empresa que opera desde 2007 em todo o território nacional, especializada em consultoria e prestação de serviços ambientais, sociais e formação orientadas às empresas.
- **Predial -** é uma empresa especializada em transacções de arrendamento, compra e venda, estratégia e gestão de portfólios, sindicatos de Investidores, procurement e relocation abrangendo os segmentos comercias, retalho, escritórios, logística / armazéns / industrial, hotelaria, residencial, non-Profit e Boutique.
- **Serenus -** é uma empresa moçambicana que opera desde 1992, especializada em prestação de serviços de segurança privada, incluindo o fornecimento de agentes especializados, sistemas electrónicos, central de recepção, resposta armada e e emergência médica.
- **Fantoffice -** é uma empresa que oferece soluções de mobiliário para escritórios, como móveis, divisórias, auditórios, tapetes modulares, revestimentos de parede, estantes compactas, entre outras.

3.2.1. Política integrada da qualidade e do ambiente

A Direcção da Meridian 32 compromete-se a manter o Sistema Integrado de Gestão (SIG) da Qualidade e Ambiente de acordo com os requisitos das Normas ISO 9001 e ISO 14001 e a desenvolver o seu negócio de uma forma ambientalmente sustentável, de acordo com as seguintes instalações:

- Adoptar um modelo de gestão ético e socialmente responsável, procurando considerar nas suas decisões, de forma equilibrada, os aspectos económicos, sociais e de preservação do ambiente;
- Promover, satisfazer e superar as expectativas dos Clientes, assegurando que as suas actividades se desenvolvam em conformidade com os requisitos das Normas ISO 9001 e ISO 14001, com a legislação e todos os requisitos aplicáveis às actividades definidas e aspectos ambientais;
- Manter-se a par das mais modernas técnicas disponíveis para o seu sector e, sempre que justificado e oportuno, desenvolver e incorporar tecnologias e práticas direccionadas à prevenção da poluição e melhoria contínua do seu desempenho ambiental;
- Estabelecer e rever periodicamente os objectivos e as metas, tendo em conta os processos, os impactos e os riscos ou aspectos significativos de modo a garantir um desenvolvimento sustentável e a melhoria contínua;
- Minimizar os impactos ambientais decorrentes das suas actividades, prevenindo a poluição, promovendo a reciclagem e uma gestão dos recursos naturais; e
- Assumir pró-activamente uma atitude de melhoria contínua do SIG;
- Envolver no respeito pelas propostas e compromissos referidos, não apenas todos os colaboradores da Meridian 32, mas também os fornecedores e falar de serviços que com a empresa cooperam nas diferentes actividades.
  A Direcção da Meridian 32 assegura assim que a Política Integrada da Qualidade e Ambiente é rompida, mantida, comunicada e garantida a todos os níveis da organização e disponibilizada a outras partes interessadas.

3.3. SITUAÇÃO ACTUAL DO GRUPO MERIDIAN 32

3.3.1. Infra-estrutura de TI

O grupo Meridian 32 conta no seu parque tecnológico com servidores, switches, firewalls, entre outros activos de TI. Abaixo (na tabela 1) são apresentados os activos de TI presentes na sala de servidores.

Tipo de Activo	Quant.	Função
Servidor físico	6	Hipervisores Tipo 1
Servidor de armazenamento	1	Repositório de máquinas virtuais
NAS	3	Servidores de ficheiros e de backup
Switch	5	Switches de core e distribuição
Firewall	1	Firewall de perímetro
Servidor virtual	14	Servidor *ERP*, controlador de Domínio, Service Desk, etc.

Tabela 1: Tabela de activos

Fonte: autor

Os serviços locais como controlador de domínio, rede de voz, rede de dados, servidor de ficheiros, serviço *ERP*, serviço de impressora, entre outros, estão assentes na infraestrutura de TI que está localizado na sala de servidores.

Adicionalmente, existem outros serviços como serviços de email e armazenamento de dados, que estão localizados na nuvem.

3.3.2. Acesso a rede

O acesso a rede corporativa no grupo Meridian 32 é protegido e controlando, sendo que para aceder a impressora, aplicações corporativas, servidores, entre outros serviços da rede, os utilizadores devem antes se autenticar a rede seja via WIFI ou via cabo.

A rede WIFI corporativa é protegida por um mecanismo de autenticação WPA2-802.1X[1], onde é necessário utilizar as credencias do *Active Directory* para poder se autenticar na rede.

[1] WPA2-802-1X é um padrão de segurança em redes sem fio que exige que cada utilizador tenha seu nome de utilizador e palavra-passa para poder se autenticar a rede WiFi.

Para o acesso à internet, os dispositivos corporativos se autenticam no computador através do *Single Sign-On* (SSO) da Firewall, que é um protocolo de autenticação pelo qual os utilizadores podem se autenticar usando as credencias do *Active Directory*.

Existe uma rede WIFI dedicada para smartphones e tablets, que permite que estes tenham acesso somente à internet. Esta rede usa um mecanismo de autenticação *WPA2-Personal*[2], sendo necessária uma senha para autenticação.

O departamento de TI é responsável por configurar o acesso à rede, monitorar e controlar os dispositivos corporativos e pessoais na rede. Para o efeito, todos os dispositivos são inventariados (laptops, smartphones ou tablets) e registados na firewall.

Através da firewall é possível monitorar os dispositivos que estão conectados a rede e também é possível ver informações relacionadas ao dispositivo, como o fabricante do dispositivo, IP, sistema operativo, última conexão à rede, entre outras e é possível bloquear temporariamente o acesso à rede.

Para os convidados, existe uma rede WIFI que permite que estes tenham acesso somente à internet. Para aceder esta rede, os utilizadores autenticam-se num portal web usando o nome de utilizador e palavra-passe fornecido pelo departamento de TI.

3.3.3. Segurança física

O acesso físico as instalações do grupo Meridian32 é protegido por meio de sistemas de controlo de acesso, que são responsáveis por garantir que somente pessoas autorizadas acedam as instalações. Adicionalmente existe um sistema de CCTV através do qual é possível monitorar todos os movimentos dentro das instalações em tempo real, assim como consultar gravações em caso de suspeita de uma actividade ilegal.

3.3.4. Segurança Lógica

A infra-estrutura de TI do grupo Meridian 32 é protegida por uma *Next-Generation Firewall* (NGFW) que é responsável por garantir a segurança por perímetro, através do monitoramento e controlo de todo o tráfego que entra e sai da rede.

[2] WPA2-Personal é um padrão de segurança em redes sem fio onde a rede WiFi é protegida por uma única palavra-passe compartilhada entre os utilizadores.

Esta firewall conta com vários recursos avançados como filtro de websites, sistema de detecção e intrusão, antivírus, inspecção SSL, entre outros recursos, que garantem a protecção da rede interna contra ameaças externas.

Adicionalmente, foram configurados em todos os postos de trabalho, um software de detecção e resposta de endpoints (EDR), que ajuda a mitigar ameaças cibernéticas através da detecção e reposta à activdades suspeitas graças ao monitoramento contínuo e em tempo real de todos os eventos do *Endpoint*[3]*.*

3.4. DESCRIÇÃO DAS ACTIVIDADES DESENVOLVIDAS

Antes do início do estágio foi elaborado um plano de actividades (vide em anexo 4) junto do supervisor da instituição para uma melhor gestão das actividades a serem realizadas dentro da organização.

Gestão de CCTV e controlo de acesso

Em relação a gestão de CCTV, era feito o controlo diário do sistema de CCTV de forma a validar o correcto funcionamento do sistema. Era feita a verificação da operacionalidade das cameras assim como o armazenamento das gravações.

No que diz respeito ao controlo de acesso, eram configurados acessos para novos colaboradores quando solicitado, assim como também eram removidos os acessos dos ex-colaboradores.

Gestão da Firewall

Como mencionado no capítulo 3.3.4, todo o tráfego que entrava e saía da rede era gerido por uma *Next-Generation Firewall.* Através da firewall era possível bloquear acessos a sites indevidos, garantindo acesso somente a sites específicos.

Adicionalmente, era feita a gestão da largura de banda de internet, assim como o monitoramento da utilização da internet e dos acessos de cada utilizador.

[3] *Endpoint* refere-se a qualquer dispositivo, como *desktop, laptop, smartphone, entre outros,* conectado a uma rede.

Durante o período de estágio foi feita a revisão de algumas regras da Firewall de forma a garantir a segurança nos acessos a rede. Foi feito também o upgrade da versão do *firmware* da firewall.

Gestão da VPN

O grupo Meridian32 permite que os seus colaboradores tenham acesso remoto a infraestrutura de TI pelo uso da VPN. Para o uso de VPN, era necessário configurar os acessos VPN assim como configurar o cliente de VPN no posto de trabalho do colaborador.

Era dado suporte ao utilizador, quando este tinha problema de conexão com a VPN ou quando este não conseguia aceder a um determinado serviço da rede.

Gestão do EDR

Era monitorado o estado do agente em todos os Endpoints, eram monitorados e corrigidos os alertas dependendo da criticidade, era feito o agendamento do scan dos endpoints e era feita a instalação do EDR em novos dispositivos.

Gestão de Backup

A gestão de backup era feita através do Veem Backup, que é um software que permite realizar backup de forma automática de máquinas virtuais de acordo com o agendamento do utilizador. O Veeam Backup conta com outras funcionalidades como restauração e replicação.

Era também feito o backup manual dos ficheiros do servidor de ficheiros para um disco externo com recurso ao *robycopy* que é uma ferramenta disponível da Microsoft utilizada para realização de backups e que conta com recursos avançados como espelhamento, retomada de transferências interrompidas, sincronização de diretórios, etc.

No que diz respeito a gestão de backup, dependendo da criticidade das VMs, os backups eram diários, semanais e mensais. Era feito o monitoramento dos backups e em caso de alguma incidência, era analisado e corrigido o problema.

A seguir é apresentado o diagrama (figura 4) da rede do grupo Meridian 32.

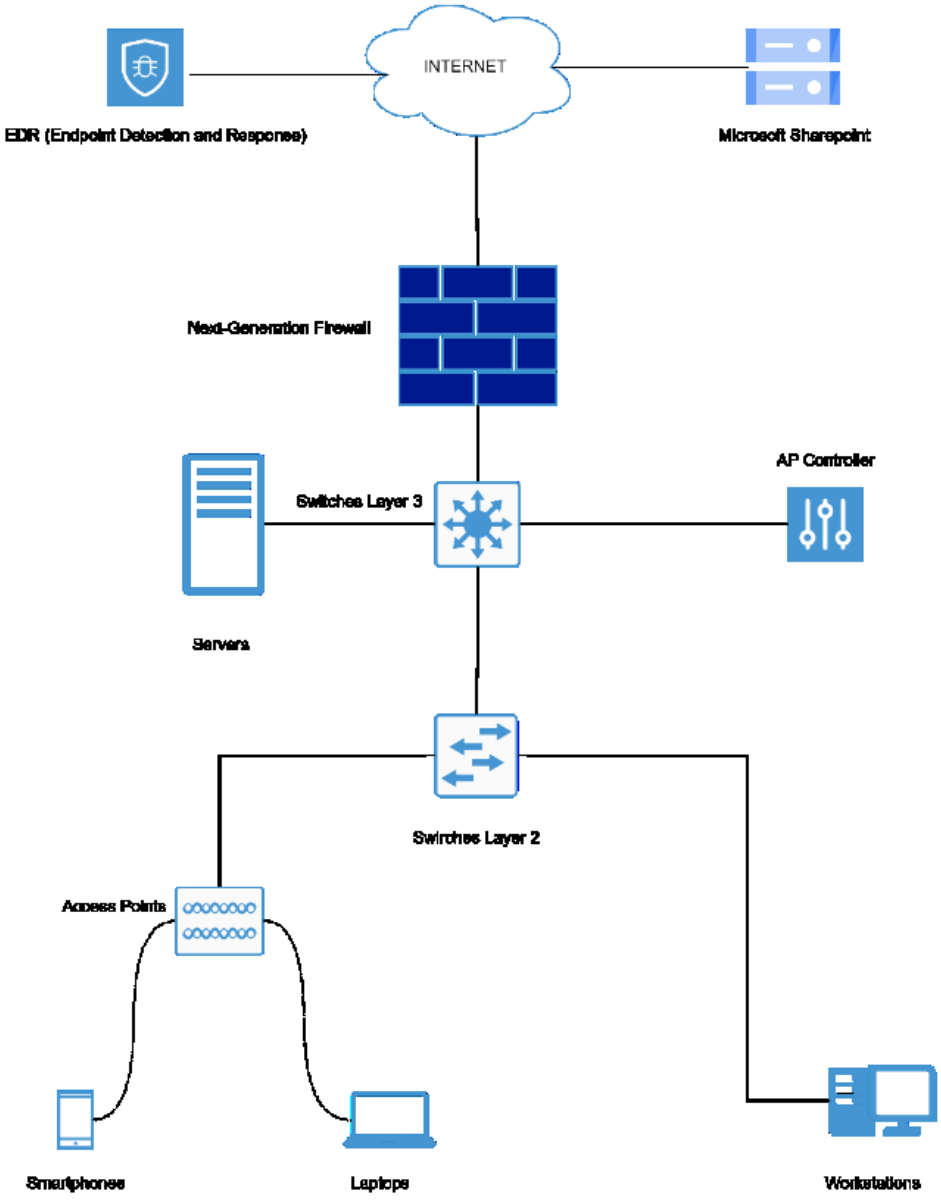

Figura 4: diagrama da rede.

Fonte: autor

4. CAPÍTULO IV - ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1. IDENTIFICAÇAÕ E AVALIAÇÃO DE RISCOS DOS SHADOW IT

Para identificação de riscos foi usada uma metodologia baseada em activos, ameaças e vulnerabilidades, método identificado no padrão de segurança da informação ISO/IEC 27001, que consiste nas seguintes fases:

- Identificação de riscos – consiste na listagem de activos, ameaças e vulnerabilidades;
- Atribuição de proprietários de riscos – consiste em identificar a pessoa que será responsável pelo risco;
- Análise do risco – consiste na avaliação de consequências e probabilidade;
- Cálculo de risco – consiste em determinar o nível do risco;
- Avaliação de risco – consiste em definir a acção sobre o risco com base em critérios.

4.1.1. Identificação de riscos

Para identificação de riscos, foram feitas entrevistas com os principais responsáveis de negócios e proprietários de processos do Altel.

Para identificação dos activos relacionado ao *Shadow IT*, foi criada um quadro (tabela 2) com o nome do activo e descrição deste. Activos iguais foram agrupados para simplificar a avaliação de risco.

Activo	Descrição
Servidor físico	Hipervisores Tipo 1.
Servidor de armazenamento	Repositório de máquinas virtuais.
NAS	Servidor de ficheiros.
Switch	Switches de acesso, distribuição e core.
Firewall	Firewall de próxima geração.
Servidor virtuais	*ERP*, controlador de Domínio, Service Desk, etc.
BYOD	Dispositivos móveis pessoais usados para execução de alguma tarefa da organização.
Laptops	Estações de trabalho móveis atribuídas aos colaboradores.
Desktops	Estações de trabalho fixas atribuídas aos colaboradores.
Redes sociais	Meios de comunicação usadas para troca de informação. Exemplo: Facebook, WhatsApp, Instagram, etc.
Dispositivo de armazenamento externo	Flash USB e Disco HDD Externo

Aplicações freewarwe	Aplicações gratuitas.
Aplicações web	Aplicações que rodam na internet, geralmente via um navegador.
Colaboradores	Todo o trabalhador da organização.
Serviços de email	Microsoft office 365.
Serviço de armazenamento em nuvem.	Microsoft office OneDrive e Sharepoint.

Tabela 2: Activos do grupo Meridian 32

Fonte: autor

Para identificação de ameaças e vulnerabilidades, foi utilizado como base o catálogo de ameaças e a vulnerabilidade apresentadas pelo autor Kosutic (2016), que contém uma lista de ameaças e vulnerabilidades mais comuns. (vide anexo 2),

Após a identificação dos activos, das ameaças e das vulnerabilidades, foi elaborado um quadro (tabela 3) que consiste no mapeamento da relação entre os activos, ameaças e vulnerabilidades, resultando na identificação do risco.

ID (Risco)	Activo	Ameaça	Vulnerabilidade	Risco
R1	Colaboradores	Colaboradores mal treinados sobre a matéria do *Shadow IT*	Falta de treinamento em relação ao *Shadow IT*	Perda ou roubo de dados da organização
R2		Instalação não autorizada do software (*Shadow IT)*	Gerenciamento de rede inadequado	Introdução de malware
R3		Utilização não autorizada do *Shadow IT*	Ausência de política de *Shadow IT*	Roubo de dados
R4	BYOD	Pessoas mal-intencionadas	falta de controle de dados de entrada e saída	Vazamento de informação

R5		Pessoas mal-intencionadas	equipamentos móveis sujeitos a furto	Perda de dados
R6	Dispositivo de armazenamento externo (Flash USB e Disco HDD)	Código malicioso	Ausência de antivírus nos postos de trabalho	Introdução de malware
R7		Pessoas mal-intencionadas	Ausência de criptografia	Perda ou roubo de dados
R8	Web Apps	Hackers	Códigos maliciosos	Vazamento de informação
R9	Aplicações freeware	Hackers	Introdução de malware	Vazamento de informação
R10	Redes sociais	Pessoas mal-intencionadas	Ausência de políticas	Vazamento de informação

Tabela 3: Identificação dos riscos

Fonte: autor

4.1.2. Proprietário do risco

Após a identificação dos riscos, a fase a seguir foi de atribuição de proprietário aos riscos que consiste na identificação da pessoa ou entidade responsável por gerir o risco, garantindo o devido tratamento dos mesmos. Para os identificados na tabela acima, o proprietário do risco é o departamento de TI.

4.1.3. Análise do risco

Esta fase consistiu na análise de cada risco tendo como referência a avaliação do impacto em caso do risco se materializar e a avaliação da probabilidade em caso do risco acontecer.

A avaliação do impacto do risco e da probabilidade do risco foi feita com base nas tabelas 4 e 5, a seguir.

Avaliação de probabilidade

Classificação	Descrição
5 - Frequente	Frequente Probabilidade de ocorrência mais do que uma vez por mês (P> 1 ocorrência / mês)
4 - Provável	Provável Probabilidade de 1 ocorrência por mês (1 ocorrência / ano <P ≤ 1 ocorrência / mês)
3 - Improvável	Improvável Probabilidade de 1 ocorrência em cada ano (1 ocorrência / 5 anos <P ≤ 1 ocorrência / ano)
2 - Remota	2 Remota Probabilidade de 1 ocorrência em cada 5 anos (1 ocorrência / 50 anos <P ≤ 1 ocorrência / 5 anos)
1 - Muito remota	Probabilidade de 1 ocorrência até uma vez em cada 50 anos (P ≤ 1 ocorrência / 50 anos)

Tabela 4: Avaliação de probabilidade

Fonte: autor

Avaliação de Impacto

Classificação	Descrição
5 - Muito Grave	Paralisação de operações, actividades, projectos, programas ou processos da organização, que causam impactos irreversíveis nos objectivos.
4 - Grave	Interrupção de operações, actividades, projectos, programas ou processos da organização, que causam impactos de reversão muito difícil nos objectivos.

3 - Moderado	Interrupção de operações ou actividades da organização, de projectos, programas ou processos, que causam impactos significativos nos objectivos, porém recuperáveis.
2 - Ligeiro	Degradação de operações, actividades, projectos, programas ou processos da organização, causando impactos pequenos nos objectivos.
1 - Baixo	Degradação de operações, actividades, projectos, programas ou processos da organização, que causam impactos mínimos nos objectivos (prazo, custo, qualidade, imagem, etc.) relacionados com as metas ou padrões ou com a capacidade de entrega de produtos/serviços às partes interessadas (clientes, externos/internos, beneficiários).

Tabela 5: Avaliação de impacto

Fonte: autor

A seguir são apresentados resultados da análise de Risco (tabela 6):

ID (Risco)	Probabilidade	Impacto
R1	3	3
R2	4	3
R3	4	3
R4	3	3
R5	3	3
R6	2	3
R7	3	3
R8	4	3
R9	4	3
R10	2	3

Tabela 6: Análise de risco

Fonte: autor

4.1.4. Cálculo do nível de risco

Para o cálculo do nível foram multiplicados valores referentes a probabilidade e o impacto de cada, usando a fórmula:

Medida de Risco = Probabilidade x Impacto

Com base na fórmula apresentada acima, a seguir é apresentado (tabela 6) é os resultados do cálculo dos riscos.

ID (Risco)	Nível de Risco
R1	9
R2	12
R3	12
R4	9
R5	9
R6	6
R7	9
R8	12
R9	12
R10	6

Tabela 7: Nível de risco

Fonte: autor

4.1.5. Avaliação de risco

Após o cálculo do nível do risco, o passo a seguir foi classificar o risco de acordo com o resultado, podendo ser classificado: como risco baixo, significativo, alto, muito alto e inaceitável.

Avaliação	Medida do risco	Descrição da avaliação
1-Baixo	[1-4]	O baixo nível de risco não justifica a implementação de controles adicionais. Nenhuma actividade adicional é necessária.
2-Significativo	[5-9]	A gestão fará análise se os riscos são aceitáveis ou não. Os controles serão aplicados conforme necessário.
3-Alto	[10-15]	A gestão seleccionará os controles apropriados com prioridade e actuação a curto prazo
4-Muito Alto	[16-20]	A gestão seleccionará os controles apropriados com prioridade a actuação urgente
5-Inaceitável	[25]	A gestão seleccionará os controles apropriados com prioridade e actuação imediata

Tabela 8: Metodologia para classificação de risco

Fonte: autor

Com base na tabela 8, na tabela 9 é apresentada a classificação dos riscos de acordo com o nível de cada risco.

ID (risco)	Nível de risco	Classificação
R1	9	Significativo
R2	12	Alto
R3	12	Alto

R4	9	Significativo
R5	9	Significativo
R6	6	Significativo
R7	9	Significativo
R8	12	Alto
R9	12	Alto
R10	6	Significativo

Tabela 9: Resultados da avalição de riscos

Fonte: autor

4.2. APRESENTAÇÃO DOS RESULTADOS DO INQUÉRITO

Foi elaborado um inquérito dirigido aos colaboradores do grupo Meridian 32, sendo que a maior parte dos respondentes do inquérito são do departamento de TI, correspondente a 55%. As outras áreas afectas são a área de gestão, segurança electrónica e suporte a aplicação, com percentagens respectivas de 18%, 9% e 18%.

4.2.1. Utilização das redes sociais

Em relação a utilização das redes socias, 60% dos colaboradores que responderam ao inquérito utilizam alguma rede social para partilhar a informação da organização. Sendo o LinkedIn e o WhatsApp as redes sociais mais usadas para a partilha da informação. (vide figura 5)

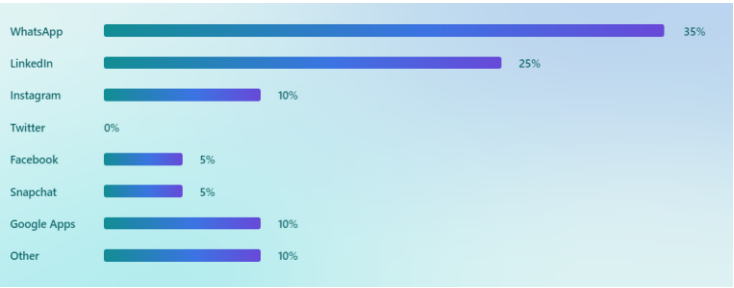

Figura 5: Resultados do inquérito - utilização de redes sociais

Fonte: autor

4.2.2. Utilização de dispositivos electrónico pessoais

Em relação a utilização de dispositivos electrónicos pessoais, 72% dos colaboradores que responderam ao inquérito utilizam os seus dispositivos para partilha ou armazenamento de alguma informação da organização. Os dispositivos electrónicos mais usados são o smartphone e o flash USB de acordo com figura 6.

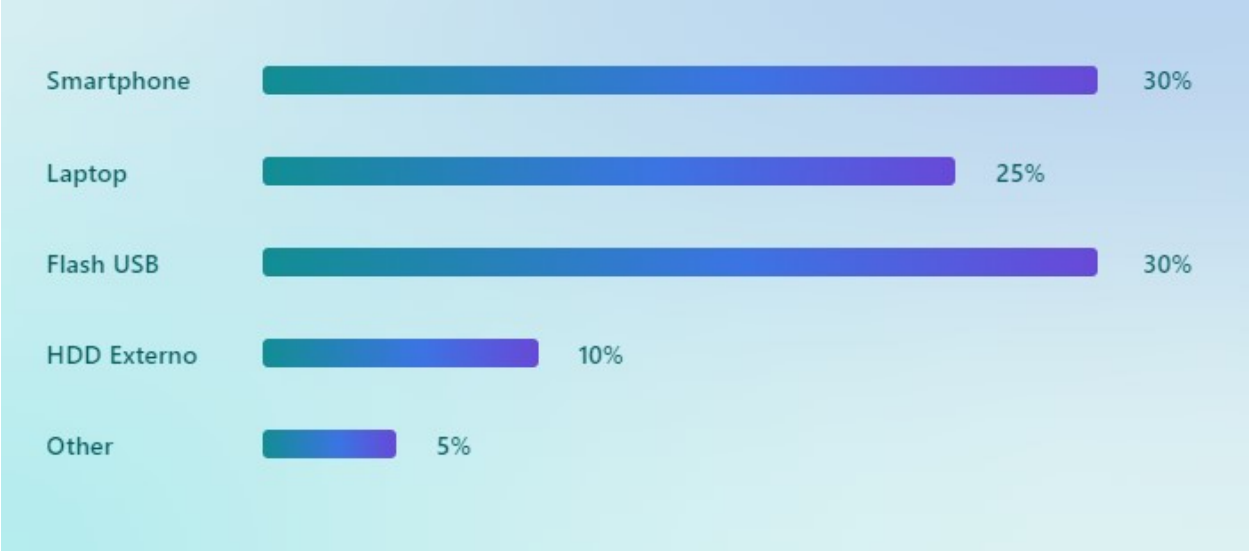

Figura 6: Resultados do inquérito - utilização de dispositivos electrónicos pessoais

Fonte: autor

4.2.3. Utilização de web apps

Em relação a utilização de aplicações web, 50% dos colaboradores que responderam ao inquérito já utilizaram uma aplicação web sem o conhecimento do TI para execução de uma tarefa da organização.

Figura 7: Resultados do inquérito - utilização de web apps

Fonte: autor

4.2.4. Desenvolvimento de software/ planilha excel

Em relação ao desenvolvimento de uma planilha excel ou um outro software, 50% dos colaboradores que responderam ao inquérito já desenvolveram alguma planilha para facilitar em alguma tarefa da organização sem informar a equipa de TI.

Figura 8: Resultados do inquérito - desenvolvimento de planilha ou software

Fonte: autor

4.3. DISCUSSÃO DE RESULTADOS

O presente trabalho procurou analisar o *Shadow IT* e os seus riscos para segurança cibernética no grupo Meridian 32, e para este feito recorreu-se a revisão bibliográfica, onde foram apresentados aspectos teóricos relativamente a segurança da informação.

Ainda sobre a revisão bibliográfica, foram analisados aspectos teóricos no que concerne ao assunto central do trabalho – *Shadow IT*, onde foi possível conhecer os tipos de *Shadow IT,* os factores que levam a sua utilização, os riscos, os benefícios e as medidas que podem ser implementadas para mitigação dos seus riscos.

No capítulo 6.1, foram apresentados resultados de um inquérito dirigido aos colaboradores como forma de aferir sobre a utilização do *Shadow IT*, onde foi possível constatar a ocorrência do *Shadow IT* no grupo Meridian 32.

As principais ocorrências do *Shadow IT* foram a utilização de dispositivos pessoais para partilha ou armazenamento de informação da organização sem o conhecimento do departamento de TI e utilização de redes sociais para partilha de informação, classificadas respectivamente como dispositivos de rede e aplicações *SaaS*, de acordo com Haber (2023).

De acordo com a revisão da literatura, as ocorrências do *Shadow IT* podem representar riscos no que tange a segurança da informação, como por exemplo o risco de vazamento de dados, podendo resultar em custos para organização, de acordo com Haber (2023).

Assim sendo, é importante analisar os riscos dos *Shadow TI,* assim como estabelecer medidas para sua implementação segura.

Foi realizada uma avaliação de risco, onde resultados mostraram a existência de riscos de *Shadow IT* no grupo Meridian 32, sendo que estes variaram de significativo para alto. De acordo com os resultados da avaliação de risco, os principais riscos encontrados são o risco de vazamento de dados e o risco de introdução de malware.

O risco de vazamento de dados (o que mais se destacou), de acordo com Morey J. Haber (2023), resulta da inexistência de controlos de segurança em dispositivos pessoais ou software não geridos pela organização, o que dificulta a recuperação da informação em caso de perda.

Com base no guião de entrevista (Anexo 1), foi possível obter informação relativamente a segurança da informação no grupo Meridian 32, em caso concreto, das políticas e mecanismos de segurança implementados na organização.

Dos resultados obtidos, foi possível verificar que o grupo Meridian 32 apresenta uma infra-estrutura minimamente protegida, graças a implementação de uma *Firewall Next-Generation* e a implementação do *EDR* nos postos de trabalho.

Contudo, foi possível constatar também, que apesar da existência de algumas tecnologias de segurança, não existem políticas e programas de treinamento e conscientização sobre segurança da informação na organização, sendo que estes elementos são cruciais para a implementação da segurança da informação de acordo com Whitman & Mattord (2021).

De acordo com Klotz et al. (2019), o estabelecimento de políticas e programas de treinamento de segurança da informação constituem as principais medidas para mitigação dos riscos de segurança da informação. A ausência destes elementos constitui uma vulnerabilidade no que diz respeito a segurança do *Shadow IT* e a segurança da informação no geral.

4.4. PROPOSTA DE MEDIDAS DE MITIGAÇÃO

Para propostas de medidas de mitigação, teve-se em contas as cincos estratégias para controlo de risco abordadas na revisão de literatura, nomeadamente: defender, transferir, aceitar, mitigar e eliminar.

O quadro mostra as medidas para mitigação dos riscos identificados tendo como base os controlos da ISO 27001.

ID (risco)	Acção	Descrição	ISO/IEC 27001 (Anexo A)
R1	Mitigar	Capacitação de utilização sobre *Shadow IT.*	A6.3 - Conscientização, educação e treinamento em segurança da informação.
R2	Mitigar	Instalação de antimalware e antivírus.	A8.7 - Proteção Contra Malware.
R3	Mitigar	Implementação de uma política de *Shadow IT.*	A5.1 - Políticas para segurança da informação.
R4	Mitigar	Firewall e Sistemas de detecção, prevenção de intrusão.	A8.20 - Segurança da rede.
R5	Mitigar	Implementação de uma política de BYOD e existência de backups.	A5.1 - Políticas para segurança da informação. A8.13 - Cópia de segurança das informações.
R6	Mitigar	Instalação de antimalware e antivírus.	A8.7 - Proteção Contra Malware.

R7	Mitigar	Implementação de uma política de segurança para reduzir ou evitar o armazenamento de informação confidencial nos dispositivos pessoais.	A5.1 - Políticas para segurança da informação.
R8	Mitigar	Firewall e Sistemas de detecção, prevenção de intrusão; Antimalware.	A8.20 - Segurança da rede. A8.7 - Proteção Contra Malware.
R9	Mitigar	Firewall e Sistemas de detecção, prevenção de intrusão (A12.6.1) Antimalware (A12.2.1)	A8.20 - Segurança da rede. A8.7 - Proteção Contra Malware.
R10	Mitigar	Sensibilização dos colaboradores, Conscientização, educação e treinamento em segurança da informação	A6.3 - Conscientização, educação e treinamento em segurança da informação.

Tabela 10: Proposta de medidas de mitigação

Fonte: autor

5. CAPÍTULO V – CONCLUSÕES E RECOMENDAÇÕES

5.1. CONLCLUSÕES

O presente trabalho abordou sobre os riscos do *Shadow IT* e propôs medidas de segurança para os riscos identificados, tendo sido necessário fazer uma avaliação de risco de acordo com a norma ISO 27001:2022, que é o padrão de segurança da informação.

Para realização deste trabalho recorreu-se a uma pesquisa descritiva do *Shadow IT*, onde fez-se uma revisão bibliográfica, análise dos documentos da organização, inquérito e entrevistas.

Para análise da utilização do *Shadow IT* e as suas implicações para segurança cibernética, foram definidos três objectivos, tendo estes sido alcançados, pois foi possível através da revisão da literatura abordar sobre as características do *Shadow,* os seus riscos, benefícios e medidas que possam ser utilizadas.

Foi possível também descrever a utilização do *Shadow IT* no grupo Meridian e a identificação dos seus riscos, através do inquérito e das entrevistas. Tendo sido que verificado que não existem políticas, medidas ou programas de treinamento no que diz ao *Shadow IT.*

Foram propostas medidas de segurança da informação de acordo com os resultados da avaliação do risco e com base nos controlos de segurança presentes na norma ISO 27001:2022 Anexo A.

5.2. RECOMENDAÇÕES

O presente trabalho permitiu analisar o uso de *Shadow IT* e as suas implicações na segurança cibernética no grupo Meridian 32. Com base nas conclusões, recomenda-se que o grupo Meridian 32:

- Estabeleça políticas de segurança de informação, incluindo políticas relacionadas ao uso do *Shadow IT,* de forma a salvaguardar a confidencialidade, a integridade e disponibilidade da informação, e recomenda-se que estas políticas sejam divulgadas aos colaboradores.

- Estabeleça programa programas de treinamento e conscientização dos utilizadores na matéria de segurança cibernética, de forma que estes não sejam vectores de entradas de malwares.
- Estabeleça medidas de segurança de informação de acordo com as políticas estabelecidas, garantindo principalmente a segurança da informação em todos dispositivos, incluindo dispositivos de armazenamento como flash USB e disco externos.

BIBLIOGRAFIA

[1] ALVES, G. A. (2006). Segurança da informação: Uma visão inovadora da gestão. *Rio de Janeiro: Ciência Moderna*.

[2] Ferreira, F. N. F. (2003). *Segurança da informação*. Ciência Moderna Rio de Janeiro.

[3] Ferreira, F. N. F. (2008). *Política de segurança da informação: Guia prático para elaboração e implementação*. Ciência Moderna.

[4] Fontes, E. L. G. (2017). *Segurança da informação*. Saraiva Educação SA.

[5] Gil, A. C. (2002). Como classificar as pesquisas. *Como elaborar projetos de pesquisa*, *4*(1), 44–45.

[6] Haag, S., & Eckhardt, A. (2014). *Normalizing the shadows–The role of symbolic models for individuals' shadow IT usage*.

[7] Haber, M. J. (2023). *The Most Common & Most Dangerous Types of Shadow IT*. BeyondTrust. https://www.beyondtrust.com/blog/entry/most-common-and-dangerous-types-of-shadow-it

[8] Klotz, S., Kopper, A., Westner, M., & Strahringer, S. (2019). Causing factors, outcomes, and governance of shadow IT and business-managed IT: A systematic literature review. *International Journal of Information Systems and Project Management*, *7*(1), 15–43.

[9] Konzen, M. P. (2013). *Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança*. https://repositorio.ufsm.br/handle/1/8276

[10] Kosutic, D. (2016). *Free List of Information security threats and vulnerabilities*. https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/

[11] Kosutic, D. (2023). *O que é a ISO 27001? Um guia detalhado e direto*. https://advisera.com/27001academy/what-is-iso-27001/

[12] LAUREANO, M. A. (2012). *Gestão de Segurança da Informação. 2005*.

[13] Leão, L. M. (2019). *Metodologia do estudo e pesquisa: Facilitando a vida dos estudantes, professores e pesquisadores*. Editora Vozes.

[14] Messias, L. C. da S. (2005). *Informação: Um estudo exploratório do conceito em periódicos científicos brasileiros da área de Ciência da Informação*.

[15] Peixoto, M. C. P. (2006). *Engenharia social e segurança da informação na gestão corporativa*. Brasport.

[16] SANTOS, E. E. dos, & Soares, T. M. M. K. (2018). *Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações*.

[17] Sêmola, M. (2003). *Gestão da segurança da informação: Uma visão executiva. Rio de Janeiro: Ed*. Campus.

[18] Sêmola, M. (2014). *Gestão da segurança da informação: Uma visão executiva. 2ª edição*. Brasil: Elsevier.

[19] Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of shadow IT on innovation in organizations. *Complex Systems Informatics and Modeling Quarterly CSIMQ*, *8*, 68–80.

[20] Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

ANEXOS

ANEXO 1 – GUIÃO DE ENTREVISTA AO GESTOR DE TI DO GRUPO MERIDIAN32

1. Quais são as políticas são políticas e mecanismos de segurança existentes na organização?

2. Quais são as medidas tomadas pelo IT para que os utilizadores não sejam a porta de entrada para um ataque cibernético?

3. Quais são as medidas usadas para garantir a segurança da informação nos dispositivos pessoais que acedem a segurança da informação?

4. Quais são as medidas existentes na organização para garantir a segurança da informação nos dispositivos corporativos que estão fora de trabalho?

5. Qual é o procedimento para instalação de um novo software requisitado pelo um utilizador?

6. Como é feito controle das aplicações ou sites acedidos pelos colaboradores nos computadores da organização?

7. Qual é o plano de resposta da organização em caso de um ataque cibernético?

ANEXO 2 – CÁTOLOGO DE VULNERABILIDADES E AMEAÇAS

Lista de vulnerabilidades

A seguir a lista de principais vulnerabilidades:

- Acesso à rede por pessoas não autorizadas
- Ataque a bomba
- Ameaça de bomba
- Quebra de relações contratuais
- Violação da legislação
- Comprometer informações confidenciais
- Ocultando a identidade do usuário
- Danos causados por terceiros
- Danos resultantes de testes de penetração
- Destruição de registos
- Desastre (causado pelo homem)
- Desastre (natural)
- Divulgação de informações
- Divulgação de senhas
- Escuta
- Desfalque
- Erros na manutenção
- Falha nos links de comunicação
- Falsificação de registos
- Fogo
- Enchente
- Fraude
- Espionagem industrial
- Vazamento de informação
- Interrupção de processos de negócios
- Perda de electricidade
- Perda de serviços de suporte
- Mau funcionamento do equipamento
- Código malicioso

- Uso indevido de sistemas de informação
- Uso indevido de ferramentas de auditoria
- Poluição
- Engenharia social
- Erros de software
- Batida
- Ataques terroristas
- Roubo
- Trovão
- Alteração não intencional de dados em um sistema de informação
- Acesso não autorizado ao sistema de informação
- Alterações não autorizadas de registos
- Instalação não autorizada de software
- Acesso físico não autorizado
- Uso não autorizado de material protegido por direitos autorais
- Uso não autorizado de software
- Erro do usuário
- Vandalismo.

Lista de principais ameaças

- Interface de usuário complicada
- Senhas padrão não alteradas
- Descarte de mídia de armazenamento sem exclusão de dados
- Sensibilidade do equipamento a mudanças de tensão
- Sensibilidade do equipamento à umidade e contaminantes
- Sensibilidade do equipamento à temperatura
- Segurança de cabeamento inadequada
- Gestão de capacidade inadequada
- Gestão de mudanças inadequada
- Classificação inadequada das informações
- Controle inadequado de acesso físico
- Manutenção inadequada
- Gerenciamento de rede inadequado

- Backup inadequado ou irregular
- Gerenciamento inadequado de senhas
- Protecção física inadequada
- Protecção inadequada de chaves criptográficas
- Substituição inadequada de equipamentos mais antigos
- Consciência de segurança inadequada
- Segregação inadequada de funções
- Segregação inadequada de instalações operacionais e de testes
- Supervisão inadequada dos funcionários
- Supervisão inadequada de fornecedores
- Treinamento inadequado dos funcionários
- Especificação incompleta para desenvolvimento de software
- Testes de software insuficientes
- Falta de política de controle de acesso
- Falta de mesa limpa e política de tela limpa
- Falta de controle sobre os dados de entrada e saída
- Falta de documentação interna
- Falta ou má implementação da auditoria interna
- Falta de política para o uso de criptografia
- Falta de procedimento para remover direitos de acesso após rescisão do contrato de trabalho
- Falta de protecção para equipamentos móveis
- Falta de redundância
- Falta de sistemas de identificação e autenticação
- Falta de validação dos dados processados
- Local vulnerável a inundações
- Má selecção de dados de teste
- Cópia única
- Muito poder em uma pessoa
- Cópia não controlada de dados
- Download descontrolado da Internet
- Uso descontrolado de sistemas de informação
- Software não documentado

- Funcionários desmotivados
- Conexões de rede pública desprotegidas
- Os direitos do usuário não são revisados regularmente

ANEXO 3 – INQUÉRITO SOBRE A UTILIZAÇÃO DO *SHADOW IT*

Shadow IT é uma prática que consiste na utilização de programas, softwares, dispositivos ou serviços sem o conhecimento da equipa de TI, como forma a flexibilizar um conjunto de actividades dentro da organização.

O presente questionário tem como objectivo avaliar o uso de Shadow IT por parte dos colaboradores do Grupo Meridian 32, de forma a identificar os possíveis impactos causados por esta prática assim como propor medidas de reforço para segurança cibernética dos sistemas do grupo. As questões são apresentadas de forma clara e simples.

1 - Por favor, identifique o departamento onde se encontra a trabalhar:

_____

2 - Utiliza alguma rede social (ex: WhatsApp, Facebook ou LinkedIn) para partilhar informações relacionadas a organização?

2.1. Sim_____ 2.2. Não

3 - Caso tenha respondido "Sim" para questão anterior (questão 2), cite por favor as redes socias que utiliza:

3.1. Facebook ___

3.2. WhatsApp ___

3.3. LinkedIn ___

3.4. Instagram ___

3.5. Twitter ___

3.6. Snapchat ___

3.7. Google Apps ___

3.7. Outro_____

4- Já utilizou algum dispositivo pessoal para partilhar ou armazenar informação relacionada a organização?

4.1. Sim_____ 4.2. Não

5 - Caso tenha respondido "Sim" para questão anterior (questão 4), por favor cite o tipo dispositivo pessoal usado para partilha ou armazenamento.

5.1. Smartphone____

5.2. Laptop____

5.3. Disco Duro Externo____

5.4. Flash USB____

5.5. Outro____

6 - Já instalou algum programa no computador para pode executar uma tarefa da organização sem informar a equipa de TI?

6.1. Sim_____ 6.2. Não

7 - Caso tenha respondido "Sim" para questão anterior (questão 6), por favor cite os programas instalados:

_____

8 - Já utilizou alguma aplicação Web (Web App) para pode executar uma tarefa da organização sem informar a equipa de TI?

8.1. Sim_____8.2. Não

9 - Caso tenha respondido "Sim" para questão anterior (questão 8), por favor cite as aplicações utilizadas:

_____

10 - Já desenvolveu algum programa ou planilha (excel) para facilitar em alguma tarefa da organização sem informar a equipa de TI?

10.1. Sim_____10.2. Não

ANEXO 4 – PLANO DE ACTIVIDADES DO ESTÁGIO PROFISSIONAL

Nº	Actividades	Semanas															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
01	Reunião c/ supervisor da Instituição.																
02	Colecta da informação da organização																
03	Submissão do Anexo 5																
04	Reunião com o supervisor da UEM																
05	Definição do tema, problema e objectivos.																
06	Justificativa																
07	Definição da Metodologia																
08	Revisão da Literatura																
09	Descrição do caso de Estudo																
10	Desenvolvimento do trabalho																
11	Discussão de resultados																

12	Conclusões e recomendações																
13	Revisão final do relat.																
14	Submissão do Relatório de EP																