**UNIVERSIDADE EDUARDO MONDLANE**

**FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA**

**CURSO DE ENGENHARIA INFORMÁTICA**

# Desenvolvimento de Políticas de Segurança da Informação para Faculdade de Engenharia da UEM (FEUEM)

**Autor**

Ricardo Orlando Manhice

**Supervisor**

Dr. Sérgio Mavie

**Co-supervisores**

Dr. Alfredo Covele

Engº Cristiliano Maculuve

Maputo, Setembro de 2022

**UNIVERSIDADE EDUARDO MONDLANE**

**FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA**

**CURSO DE ENGENHARIA INFORMÁTICA**

# Desenvolvimento de Políticas de Segurança da Informação para Faculdade de Engenharia da UEM (FEUEM)

**Autor**

Ricardo Orlando Manhice

**Supervisor**

Dr. Sérgio Mavie

**Co-supervisores**

Dr. Alfredo Covele

Engº Cristiliano Maculuve

Maputo, Setembro de 2022

**UNIVERSIDADE EDUARDO MONDLANE**

**FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA**

**CURSO DE ENGENHARIA INFORMÁTICA**

## TERMO DE ENTREGA DE RELATÓRIO DO TRABALHO DE LICENCIATURA

Declaro que o estudante **Ricardo Orlando Manhice** entregou no dia ___/___/2022 as ___cópias do relatório do seu Trabalho de Licenciatura com a referência: **2021EITLD112** intitulado: **Desenvolvimento de Políticas de Segurança da Informação para Faculdade de Engenharia da UEM (FEUEM)**

Maputo, ___ de Setembro de 2022

O chefe de Secretaria

_____

**UNIVERSIDADE EDUARDO MONDLANE**

**FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA**

**CURSO DE ENGENHARIA INFORMÁTICA**

## DECLARAÇÃO DE HONRA

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

Maputo, ___ de Setembro de 2022

O autor

_____

(Ricardo Orlando Manhice)

## ÍNDICE DE FIGURAS



## ÍNDICE DE TABELAS

## ÍNDICE

**Dedicatória**

*Aos meus pais,*
*Orlando Manhice e*
*Júlia Chécua.*

**Agradecimentos**

Agradeço em primeiríssimo lugar a Deus todo poderoso pelo dom da vida, e por permitir que eu realizasse este trabalho, que constitui uma alegria a mim, aos meus pais e a todos que contribuíram directa ou indirectamente para a realização do mesmo.

Aos meus supervisores e docentes da FEUEM o Dr. Sérgio Mavie, Dr. Alfredo Covele, Engº Cristiliano Maculuve, Engº Ruben Manhiça pela boa supervisão, pela ajuda e recomendações para ultrapassar as dificuldades que foram surgindo e pelo apoio em todas situações durante o percurso do trabalho.

Ao departamento de TIC's, especificamente aos técnicos deste que se disponibilizaram para dar informações que foram sendo necessárias para a realização do trabalho.

Aos meus pais pelo apoio incondicional que me deram durante o percurso acadêmico. Por terem acreditado e investido em mim. Pelos valores que me transmitiram e pelas palavras de conforto em momentos de tensão.

Aos docentes da Faculdade de Engenharia da UEM, especificamente os do Departamento de Electrotecnia pelos conhecimentos que me passaram durante os anos de formação e os seus esforços para que pudesse alcançar os objectivos que eram desejados.

Aos colegas da turma de Engenharia Informática – 2017, pelos anos de convivência, pelos momentos que juntos passamos, desde os de tristeza (muito poucos) até aos de alegria, que foram os mais destacados, e as experiências trocadas durante o tempo de formação.

Aos meus familiares e amigos, que apesar da minha ausência em diversos momentos, continuaram acreditando em mim e dando o seu apoio de forma totalmente incondicional.

A todos que deram o seu contributo directa ou indirectamente vai o meu muito obrigado.

*“It always seems impossible, until it is done”*

***Nelson Mandela***

**Resumo**

A Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM) é uma instituição de ensino superior, que possui uma infraestrutura informática e constituída por recursos humanos, desde os funcionários aos estudantes. Ao nível da FEUEM não existe um guia de uso correcto dos recursos tecnológicos lá existente. Política de Segurança da Informação (PSI) constitui o guia anteriormente referido. Neste âmbito surge a necessidade de se desenvolver uma PSI que será responsável pela gestão da segurança da informação.

O presente trabalho visa apresentar normas e políticas de utilização de recursos informáticos da FEUEM que permitam garantir os princípios de segurança da informação e que minimizem as vulnerabilidades dos sistemas de informação da FEUEM.

Para o alcance deste objectivo, fez-se um levantamento bibliográfico sobre a segurança da informação bem como os seus princípios. Este levantamento auxiliou no processo da criação da proposta de PSI para FEUEM. Foram paralelamente feitas entrevistas ao DTIC's com vista a perceber as principais janelas de vulnerabilidades da FEUEM e as principais necessidades no que concerne a segurança da informação. Neste contexto, o presente trabalho culmina com criação de uma PSI para a FEUEM baseando-se nos controles da norma ISO/IEC 27002, que servirá de um guia para os colaboradores da instituição bem como para os estudantes. Na PSI são inclusas as normas de utilização dos recursos tecnológicos da instituição, com foco nas camadas de segurança da informação. Espera-se, portanto, como resultado uma garantia de Integridade, Disponibilidade e Confidencialidade dos activos institucionais, e minimização das vulnerabilidades nos sistemas de informação da FEUEM, como também se espera uma melhoria no entendimento dos aspectos de segurança da informação por parte dos recursos humanos da instituição.

**Palavras-chaves:** Informação; Segurança da Informação; Política de Segurança; normas e padrões.

**Abstract**

The Faculty of Engineering of Eduardo Mondlane University (FEUEM) is a higher education institution, which has a computer infrastructure and consists of human resources, from employees to students. At the FEUEM there is no guide for the correct use of the technological resources there. Information Security Policy (ISP) is the guide previously mentioned. In this context the need arises to develop an ISP that will be responsible for managing information security.

The present work aims to present norms and policies for the use of FEUEM's IT resources that can guarantee the principles of information security and minimize the vulnerabilities of FEUEM's information systems.

To achieve this objective, a bibliographic survey was made about information security and its principles. This survey helped in the process of creating the ISP proposal for FEUEM. In parallel, DTIC's were interviewed in order to understand the main vulnerability of FEUEM and the main needs regarding information security.

In this context, the present work culminates with the creation of a ISP for FEUEM, based on the ISO/IEC 27002 controls, which will serve as a guide for the institution's collaborators as well as for the students. The ISP includes rules for the use of the institution's technological resources, focusing on the layers of information security. It is expected, therefore, as a result a guarantee of Integrity, Availability and Confidentiality of the institutional assets, and minimization of vulnerabilities in the information systems of FEUEM, as well as an improvement in the understanding of the information security aspects by the human resources of the institution

**Key-words:** Information; Information Security; Security Security Policies;

**Siglas e abreviaturas**

| | |
|---|---|
| CEE-UP | **Centro de Estudos de Engenharia – Unidade de Produção** |
| CIUEM | Centro de Informática da Universidade Eduardo Mondlane |
| DAF | Departamento de Finanças |
| DCG | Departamento das Cadeiras Gerais |
| DECI | Departamento de Civil |
| DEEL | Departamento de Electrotecnia |
| DEMA | Departamento da Mecânica |
| DEQUI | Departamento da Química |
| DIB | Departamento de Informação e Biblioteca |
| DRA | Departamento do Registo Académico |
| FEUEM | Faculdade de Engenharia da Universidade Eduardo Mondlane |
| ISO/IEC | Organização Internacional de Estandardização/Comissão Internacional Electrónica |
| ISACA | Associação de Auditoria e Controle de Sistemas de Informação |
| PSI | Política de Segurança da Informação |
| SI | Sistema de Informação |
| TI | Tecnologia de Informação |
| VPN | Rede Privada Virtual |

**Glossário de termos e expressões**

| | |
|---|---|
| Ameaça | **É um objecto, pessoa ou outra entidade que representa um perigo permanente para um activo** |
| *Extranet* | Rede interna que pode ser acedida pelas pessoas autorizadas de forma remota |
| *Internet* | é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos (*Internet Protocol Suite* ou TCP/IP) com o propósito de servir progressivamente utilizadores no mundo inteiro |
| *Intranet* | Rede empresarial interna, voltada exclusivamente para a comunidade de uma empresa |
| Risco | É a probabilidade de algo não desejado acontecer |
| Sistema Operativo | É um programa ou um conjunto de programas cuja função é gerir os recursos do computador (definir qual programa recebe atenção do processador, gerir memória, criar um sistema de arquivos, etc.), fornecendo uma interface entre o computador e o utilizador |
| *Software* | Programa de computador, uma sequência de instruções escritas para serem interpretadas por um computador com o objectivo de executar tarefas específicas |
| Usuário | Todos utilizadores do ambiente de TI, independente do cargo ocupado |
| Wi-Fi | Wireless fidelity (fidelidade sem fio) |
| *Web sites* | É um conjunto de páginas web, isto é, de hipertextos acessíveis com diversos protocolos |

# 1 Introdução

## 1.1 Contextualização

Com o avanço das Tecnologias de Informação (TI's), a informação se torna cada vez mais importante para as organizações, surgindo assim a necessidade de uma adequada protecção para a informação, que constitui um essencial activo na tomada de quaisquer decisões, no processo de garantia da continuidade dos negócios, no aumento das oportunidades bem como em diversos parâmetros de negócio de uma dada organização.

Administrar a informação é cada vez mais vital em seus diferentes níveis estratégico, tático ou operacional. Daí que Pontes (2014) afirma que a informação envolve riquezas (tangíveis ou não), e por isso, os sistemas que a produzem e a mantém precisam estar seguros para se evitar que ela caia em mãos erradas. A segurança da informação é uma das responsabilidades do profissional de sistemas de informação.

Tendo em conta que a informação é um activo muito importante para qualquer instituição e tomando que esta é um recurso patrimonial, Fontes (2015) sublinha que informações adulteradas, não disponíveis, sob conhecimento de pessoas de má fé ou de concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. Sem uma devida segurança da informação é possível que a continuidade de negócio da instituição se inviabilize.

Santos (2011) relembra que as organizações se preocupam com a segurança de suas informações a partir do momento que passam por algum incidente que gerou algum tipo de impacto aos seus negócios. Todas as actividades são de alguma forma regidas por regras e leis que visam controlar o comportamento humano como também colocar limites às pessoas e de modo que saibam distinguir o certo do errado.

O presente trabalho propõe Políticas de Segurança da Informação (PSI) na FEUEM, descrevendo como os recursos computacionais devem ser manipulados e protegidos bem como a formalização das acções que devem ser tomadas na instituição. Essas políticas servirão de um modo geral, como um código de conduta ao qual os colaboradores da instituição devem se adaptar inteiramente garantindo desta feita os princípios de segurança da informação.

## 1.2 Descrição do Problema

A tecnologia da informação evolui de forma rápida, a *Internet* é um exemplo desta evolução. O uso da *Internet* constitui uma grande janela de vulnerabilidade quando se trata de segurança da informação (Epaminondas, 2010). A interligação de redes públicas e privadas assim como o compartilhamento de recursos de informação tornam difícil o controle e a segurança.

No que tange as instituições de ensino superior a segurança da informação não só protege a informação contra ameaças à sua disponibilidade, integridade, confidencialidade, como também minimiza o risco ao negócio e maximiza o retorno sobre os investimentos e as oportunidades de negócio (ISO/IEC 27002).

A Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM) é uma instituição de ensino superior que não está fora perante esta necessidade de garantir a protecção dos seus activos, desde os tangíveis aos intangíveis. Ela é constituída por departamentos, que possuem infraestrutura informática e cada um deles tem colaboradores que fazem o uso da infraestrutura. Para que os colaboradores institucionais possam fazer o uso correcto dos recursos computacionais, é necessário que se estabeleçam princípios, valores, compromissos e orientações de modo a se alcançar um padrão desejável de protecção para as informações. Portanto, essas regras e princípios constituem Políticas de Segurança da Informação (PSI), e de acordo com os estudos e as entrevistas feitas na instituição constatou-se que não existem Políticas de Segurança da Informação desenvolvidas e implementadas ao nível da Faculdade de Engenharia.

## 1.3 Justificativa

Muitos recursos de informação que são disponíveis e mantidos em sistemas de informação distribuídos através de redes, têm um alto valor para seus usuários. Maior parte destes sistemas de informação são projectados de tal forma que só armazenam as informações e fazem as transações e manipulação destas, porém não são projectados para proteger as informações que portam.

A informação constitui um activo de muito valor para as instituições, e esta precisa de uma adequada protecção. Muitas organizações e instituições para fazerem a protecção das suas informações recorrem à segurança da informação.

A FEUEM está equipada por uma infraestrutura tecnológica que ajuda na criação, processamento e armazenamento das suas informações. Com isso, para uma instituição de ensino de dimensão da FEUEM é de extrema importância existirem mecanismos responsáveis pela garantia da segurança das informações.

O desenvolvimento de PSI constitui um avanço para a garantia da segurança da informação dos activos da FEUEM. Com o desenvolvimento aliado a implementação destas politicas o autor acredita que pode reduzir ou minimizar as vulnerabilidades da FEUEM.

Portanto a grande motivação para a realização do presente trabalho, é o factor de segurança, principalmente em instituições de ensino, pois estas estão directa ou indirectamente ligadas ao funcionamento de empresas ao formarem quadros nas várias áreas de conhecimento. Tomando em consideração que estas empresas atraem investimento ao país é necessário que funcionem adequadamente, e este funcionamento o autor acredita que começa com os aspectos de segurança da informação estarem óptimos.

Uma das maneiras de atingir este feito é pela implantação de uma Política de Segurança da Informação, a qual regula como uma instituição protege a sua informação estabelecendo regras e procedimentos.

## 1.4 Objectivos

### 1.4.1 Objectivo Geral

- Desenvolver Políticas de Segurança da Informação para a FEUEM.

### 1.4.2 Objectivos específicos

- Apresentar os princípios de segurança da informação
- Identificar normas e políticas de utilização de recursos informáticos que permitam garantir os princípios de segurança da informação;
- Descrever as vulnerabilidades dos sistemas de informação da FEUEM;
- Formular PSI para FEUEM.

## 1.5 Metodologia do Trabalho

A realização de um trabalho científico é sempre sustentada por uma certa metodologia de pesquisa, e para a mesma existem diversas classificações, no entanto, o presente trabalho sustenta-se nas metodologias que Gil (2002 e 2008) e Marconi e Lakatos (2008) sugerem. A mesma é classificada segundo os seguintes critérios: quanto à abordagem; quanto aos objectivos; quanto aos procedimentos e quanto aos métodos.

### 1.5.1 Classificação da Metodologia

#### 1.5.1.1 Quanto a natureza

Um trabalho de pesquisa quanto à natureza pode ser classificado em uma pesquisa básica e pesquisa aplicada (Gerhardt e Silveira 2009).

- **Pesquisa básica**

Objectiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista. Envolve verdades e interesses universais.

- **Pesquisa aplicada**

Tem por objectivo gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais.

Portanto o presente trabalho tem pesquisa de natureza aplicada, por gerar conhecimentos que têm aplicação prática imediata, no caso, o desenvolvimento de uma proposta de Política de Segurança da Informação, que não existe ao nível da FEUEM.

### 1.5.1.2 Quanto aos objetivos

Para Gil (2002) uma pesquisa quanto aos objectivos classifica-se em: pesquisas exploratórias, descritivas e pesquisas explicativas.

- **Pesquisas exploratórias**

Para o autor estas pesquisas têm como objectivo proporcionar maior familiaridade com o problema, com vista a torna-lo mais explícito ou a construir hipóteses.

- **Pesquisas descritivas**

Têm como objectivo primordial a descrição das características de determinada população ou fenómeno ou, então, o estabelecimento de relações entre variáveis.

- **Pesquisas explicativas**

A preocupação central destas pesquisas é a identificação de factores que determinam ou que contribuem para a ocorrência de fenómenos.

De acordo com a classificação anterior o presente trabalho tem objectivos de natureza exploratórios por viabilizar uma maior familiaridade entre o pesquisador e o caso de estudo. Foi possível com esta pesquisa explorar várias bibliografias com o objectivo de fazer uma análise profunda sobre políticas bem como segurança da informação.

### 1.5.1.3 Quanto a abordagem

Quanto à abordagem um trabalho de pesquisa científica pode classificar-se em: pesquisa qualitativa e pesquisa quantitativa.

Segundo Gerhardt e Silveira (2009) uma pesquisa qualitativa é aquela que não se preocupa com a representatividade numérica, mas sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc. este tipo de pesquisa preocupa-se, portanto, com aspectos da realidade que não podem ser quantificados. Gerhardt e Silveira (2009) afirmam que uma pesquisa é quantitativa sempre que os seus resultados poderem ser quantificados. Esta forma de pesquisa recorre à linguagem matemática para a descrição de um dado fenómeno.

O presente trabalho apresenta uma pesquisa de abordagem qualitativa, por não recorrer à linguagem matemática para a descrição do problema em causa.

### 1.5.1.4 Quanto aos procedimentos

Quanto aos procedimentos, a metodologia para a realização de um trabalho classifica-se segundo os tipos que Gil (2002 e 2008) sugere:

a) **Pesquisa experimental** - esta pesquisa segundo Gil (2008) citado por Gerhardt e Silveira (2009) consiste na determinação de um objecto de estudo, na selecção de variáveis que seriam capazes de influenciá-lo, definir as formas de controle e de observação dos efeitos que a variável produz no objecto.
b) **Pesquisa bibliográfica** – segundo Fonseca (2002) citado por Gerhardt e Silveira (2009) é uma pesquisa feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e electrónicos, o exemplo de livros, artigos científicos, páginas de web sites. Acrescenta o autor ainda que qualquer trabalho científico se inicia com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto em causa.
c) **Pesquisa documental** – esta pesquisa segundo Gerhardt e Silveira (2009) assemelha-se à pesquisa bibliográfica, não sendo fácil por vezes distingui-las. Enquanto a pesquisa bibliográfica utiliza fontes constituídas por material já elaborado, a pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, etc.
d) **Pesquisa de levantamento** – é utilizada em estudos exploratórios e descritivos, e o levantamento pode ser de dois tipos: levantamento de uma amostra ou levantamento de uma população (Gerhardt e Silveira, 2009).
e) **Estudo de caso** – é caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social (Gerhardt e Silveira, 2009).

Para a realização do presente trabalho recorreu-se à pesquisa bibliográfica, à pesquisa documental e ao estudo de caso.

Pesquisa bibliográfica, pois, uma revisão bibliográfica foi necessária, recorrendo-se a vários materiais que já foram publicados e analisados, que podem estar em vários formatos, desde o electrónico, físico bem como páginas *web.* Os aspectos chaves que tratados neste levantamento bibliográfico foram sobre: segurança da informação, políticas de segurança da informação e sua importância, padrões de segurança para que se pudesse dentre os vários abarcados pela pesquisa, identificar o padrão que se adequasse às necessidades da FEUEM no que concerne aos aspectos de segurança.

O estudo de caso permitiu uma interação com a FEUEM de modo que se pudesse levantar as principais fragilidades no que concerne a segurança da informação dentro

da instituição. O estudo de caso permitiu também conhecer melhor a instituição, que constitui o foco da realização do presente trabalho.

### 1.5.2 Técnicas de recolha de dados

Para Marconi & Lakatos (2003, p.173), técnica é um conjunto de preceitos ou processos de que se serve uma ciência ou arte e também a habilidade de usar esses preceitos ou normas na parte prática. Para as mesmas autoras (2003, p.165), técnica de recolha de dados corresponde a etapa de pesquisa em que se inicia a aplicação dos instrumentos elaborados e das técnicas selecionadas, a fim de se efectuar a colecta de dados previstos.

#### 1.5.2.1 Entrevistas

Para a materialização do presente trabalho uma das ferramentas usadas foi a recolha de dados em forma de entrevistas.

Uma das entrevistas foi feita aos responsáveis de Segurança da Informação ao nível da CIUEM para que fosse possível primeiro saber da existência de uma Política de Segurança da Informação conforme consta no Anexo 1 e entender das principais janelas de vulnerabilidades.

Outras entrevistas foram feitas ao nível da Faculdade de Engenharia que é o caso de estudo para que se pudesse fazer o levantamento de todos os problemas e fragilidades que poderão ser resolvidos com a proposta da Política de Segurança da Informação.

De acordo com Marconi & Lakatos (2003, p.196) a entrevista “é um encontro entre duas pessoas, afim de que uma delas obtenha informações a respeito de determinado assunto, mediante uma conversação de natureza profissional”.

De acordo com Marconi & Lakatos (2003, p.197), dependendo do propósito do entrevistador a entrevista pode ser:

Estruturada “é aquela em que o entrevistador segue um roteiro previamente estabelecido; as perguntas feitas ao indivíduo são pré-determinadas”.

Não estruturada é aquela em que “o entrevistador tem liberdade para desenvolver cada situação em qualquer direcção que considere adequada. É uma forma de poder explorar mais amplamente uma questão”.

Para a recolha de dados para o presente trabalho foi usada uma abordagem mista, por ter sido usado as duas formas de entrevistas. As entrevistas possibilitaram um

entendimento profundo do problema em questão e apurar medidas necessárias para a minimização de vulnerabilidades.

#### 1.5.2.2 Pesquisa bibliográfica

É uma pesquisa feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e electrónicos (Gerhardt e Silveira, 2009). Para a realização deste trabalho foram consultadas diversas bibliografias que tratam temáticas ligadas à segurança da informação ou que tratam de temas próximos. Esse levantamento visou compreender como é feita a elaboração de uma política de segurança, bem como compreender aspectos chaves de sucesso aquando da elaboração de uma política de segurança.

#### 1.5.2.3 Observação

Para Marconi & Lakatos (2003), a observação é uma técnica de recolha de dados para conseguir informações e utiliza os sentidos na obtenção de determinados aspectos da realidade. Neste contexto o autor usou também os órgãos de sentido para a recolha de dados, como forma de alavancar os dados levantados pelas entrevistas.

### 1.5.3 Metodologia de pesquisa

Para a concepção do presente trabalho foi necessária uma série de passos, sendo o que o primeiro de todos foi a escolha e aprovação do tema pelos supervisores. De seguida foi sendo desenvolvido gradualmente e com encontros frequentes com os supervisores que tinham como objectivo a análise do progresso do trabalho. Este desenvolvido foi possibilitado pela análise prévia do caso de estudo, a FEUEM, sendo que esta análise consistia em entrevistas com técnicos de DTIC's e com alguns funcionários da instituição com vista a levantar os dados que ajudariam na percepção e desenvolvimento do tema com foco na instituição, a FEUEM. As entrevistas deram uma visão geral do que seria o escopo da proposta de politica de segurança da informação, do que eram os principais pontos em que a PSI focar-se-ia.

## 1.6 Estrutura do trabalho

O presente trabalho está organizado do seguinte modo:

- **Capítulo 1 – Introdução**

  Este capítulo aborda todos os capítulos introdutórios ao caso de objectivos, descrição do problema, justificativa da escolha ou realização de trabalho com esta temática, a metodologia usada para a realização e materialização deste trabalho.

- **Capítulo 2 – Revisão da Literatura**

  Neste capítulo é feita a descrição teórica de todos os aspectos a abordar em todo o relatório, bem como a avaliação dos mesmos. É neste capítulo que é feita a análise e comparação dos conhecimentos produzidos em outros trabalhos de temática igual ou semelhante, dando se mais ênfase aos conceitos, procedimentos, discussões e conclusões com relevância para o trabalho. Os tópicos neste capítulo abordados em conjunto auxiliam na elaboração da proposta de solução.
- **Capítulo 3 – Caso de estudo**

  Neste capítulo é feita uma descrição do caso do estudo em causa, especificamente o estudo da instituição em causa e é feita a descrição da situação actual com relação ao problema identificado. É neste capítulo onde são descritas as vulnerabilidades dos sistemas de informação da FEUEM.
- **Capítulo 4 – Processo de desenvolvimento da proposta de solução**

  É neste capítulo onde são apresentados os passos seguidos para a materialização da proposta de solução, onde são listados os controles usados para o desenvolvimento da PSI.
- **Capítulo 5 – Conclusões e recomendações**

  Neste capítulo é onde são feitas as conclusões sobre o processo da realização do trabalho, onde se discute a questão de alcance ou não dos objectivos traçados. É no mesmo capítulo onde se dão recomendações para trabalhos futuros de mesma temática.
- **Bibliografia**

  Este capítulo serve especialmente para indicar todas as fontes consultadas para se materializar o trabalho, bem como alcançar os objetivos traçados.
- **Anexos**

  Nesta secção é onde são apresentados elementos adicionais que facilitam a compreensão do trabalho

# 2 Revisão de Literatura

## 2.1 O valor da informação em uma organização

Muitos recursos de informação que são disponíveis e mantidos em sistemas de informação distribuídos através de redes, têm um alto valor para seus usuários.

“O sangue da empresa é a informação. Distribuída por todos os processos de negócio, alimentando-os e circulando por diversos ativos, ambientes e tecnologias, a informação cumpre o importante papel de fornecer instrumentos para a gestão do negócio” (Sêmola, 2014, p.8).

Sêmola (2014) afirma ainda que:

> Apesar de ter grande volume momentaneamente armazenado e processado de forma centralizada nos grandes computadores e servidores, toda a informação está acessível dos pontos mais distantes através da Internet, Intranet, Extranet, VPNs, culminando com as tecnologias sem fio, como Wi-Fi, 3G, 4G.

A informação é armazenada de forma temporária nos computadores de grande porte e em servidores. E a mesma é acedida remotamente em redes globais bem como locais de forma centralizada, e a mesma e acedida por meio de redes virtuais privadas.

A tecnologia da informação (TI) está cada vez mais alinhada com o planeamento estratégico das organizações, garantindo em muitos aspectos a competitividade das mesmas.

Segundo a norma ISO/IEC 27002:2005, a informação é um activo que, como qualquer outro activo importante, é essencial para negócios de uma organização e consequentemente necessita ser adequadamente protegida.

Informação é todo e qualquer conteúdo ou lado que tenha valor para alguma organização ou pessoa, ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição (Andrade, 2009).

Podemos com isto afirmar que a informação é um órgão vital das organizações, garante a continuidade de negócio.

Toda informação tem valor e precisa ser protegida contra acidentes ou ataques.

### 2.1.1 Ciclo de vida do desenvolvimento da informação

A informação possui um ciclo de vida. Ela nasce com a produção, tem um tempo de vida útil, na qual é manuseada, utilizada internamente bem como externamente, transportada por diversos meios, armazenada, e ela morre com a sua destruição.

Sendo a informação muito valiosa para um negócio, é preciso analisar os aspectos ligados à sua segurança, as suas propriedades por preservar e proteger para que ela esteja efectivamente sob controle, e destacadamente os envolvidos no seu ciclo de vida.

Qualquer e toda a informação tem influência de três propriedades principais: a confidencialidade, integridade, disponibilidade, sendo que os aspectos autenticidade e legalidade fazem o complemento da influência. Estas propriedades serão abordadas e desenvolvidas em tópicos posteriores do presente trabalho.

O ciclo da vida da informação é também identificado por momentos vividos pela informação e que a colocam em risco. Estes momentos são presentes a quando ao uso da informação pelos activos físicos, tecnológicos e humanos.

Os momentos vividos pela informação, segundo Sêmola (2014) destacam-se a seguir.

#### 2.1.1.1 Manuseio

É o momento no qual a informação é criada, manipulada. Pode se tomar como exemplo a digitação da mesma.

#### 2.1.1.2 Armazenamento

É o momento pelo qual a informação é armazenada, seja em um banco de dados, seja em uma anotação no papel, seja em um CD-ROM, DVD-ROM ou mesmo um *pen-drive*.

#### 2.1.1.3 Transporte

O transporte é o momento no qual a informação é transportada, ou enviada de um ponto para o outro, quer seja encaminhamento por e-mail, quer seja por disponibilizar a mesma em uma plataforma web.

#### 2.1.1.4 Descarte

Momento em que a informação é descartada ou destruída, seja ao depositar numa lixeira um material impresso, seja ao eliminar um arquivo do seu computador, seja ao descartar um CD-ROM usado que apresentou uma falha de leitura.

## 2.2 Segurança da Informação

Segurança da informação é a protecção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO/IEC 27002:2005).
Para Beal (2005) citado por Netto & Silveira (2007) a segurança da informação é o processo de protecção da informação das ameaças à sua integridade, disponibilidade e confidencialidade.
Para Sêmola (2005) citado por Netto & Silveira (2007) a segurança da informação constitui uma área de conhecimento dedicada à protecção de activos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.
A segurança da informação refere-se à protecção existente sobre informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto os pessoais (Andrade, 2009).
Com isto pode-se dizer que a segurança da informação é um sentido bem-informado de garantir que os riscos e controlos de informação estão balanceados. É a qualidade ou o estado de estar livre do perigo ou de adversários.
Segundo a norma (ISO/IEC 27002:2005):

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.
> Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objectivos do negócio e de segurança da organização sejam atendidos.

Portanto para garantir que haja uma segurança efectiva da informação é necessário que haja muito controle, é necessário que se implementem políticas, e muitos processos, processos esses que são fortemente auxiliados pelas funções das aplicações em coordenação com o hardware.
Sendo a informação um ativo que, como qualquer outro ativo importante, segundo afirma a norma ISO/IEC 27002:2005, é necessário que haja uma segurança desta nos negócios de uma organização, portanto precisa ser adequadamente protegida.
Santos (2011) acrescenta que a implantação de metodologias de segurança da informação (SI) precisa ter total e constante apoio dos gestores e colaboradores das organizações, pois isso é uma forma deles participarem frequentemente na identificação das necessidades e da conscientização de usuários.

### 2.2.1 A necessidade de segurança da informação

A informação e os processos de apoio, sistemas e redes são importantes activos para os negócios (ISO/IEC 27002:2005).

As organizações e os seus sistemas de informação que armazenam os seus activos estão expostas a diversos tipos de ameaças à segurança da informação, incluindo ataques ou fraudes electrónicas, espionagens, vandalismo ou mesmo sabotagem. Portanto a segurança da informação é muito importante para os negócios em todos os sectores, sejam eles públicos ou privados, e também para a protecção das infraestruturas críticas. Ela viabiliza os negócios e evita ou reduz riscos relevantes, conforme a norma ISO/IEC 27002:2005 sublinha.

Peltier (2000) considera que em uma organização os activos são protegidos pois quando perdidos ou danificados diminuem as chances de sucesso da empresa. Da mesma forma protegendo a empresa activos de informação aumentam sua chance de sucesso.

Por outro lado, Whitman (2012) afirma que a segurança da informação desempenha quatro funções importantes para uma organização, a saber:

#### 2.2.1.1 Proteger a funcionalidade de uma organização

Ambos administração geral e gestão de TI são responsáveis pela implementação da segurança da informação que protege a capacidade de a organização funcionar. A gestão de segurança da informação tem mais a ver com a política e sua aplicação do que com a tecnologia de sua implementação.

#### 2.2.1.2 Garantir uma operação segura das aplicações

As organizações de hoje estão sob imensa pressão para adquirirem e operarem com aplicações de forma integrada, eficiente. Essas organizações precisam criar um ambiente capaz de proteger as aplicações, em particular aquelas que são as mais importantes.

#### 2.2.1.3 Protecção de dados que a organização coleciona e usa

Quando uma organização não tiver dados automaticamente o seu registo de transações é perdido, bem como a sua capacidade de satisfazer aos clientes. Nisso nota-se que os dois aspectos críticos de segurança de informação são a protecção dos dados em repouso bem como dos em movimento.

Quanto mais valor os dados tiverem, mais motivação é dos atacantes para roubá-los, sabotá-los ou mesmo corrompê-los. Portanto é necessário que haja um plano eficaz de SI para proteger a integridade e o valor dos dados.

#### 2.2.1.4 Salvaguardar os activos tecnológicos da organização

Para que uma empresa tenha um desempenho efectivo é preciso que contrate serviços de infraestrutura segura apropriadas para o tamanho e o escopo da empresa. Uma vez que a rede de uma organização cresce, para acomodar mudanças relativas ao crescimento da rede, os programas vigentes de segurança da informação devem ser substituídos por soluções de tecnologia mais robustas.

### 2.2.2 Classificação da informação

As organizações classificam as informações a fim de estabelecer os níveis de protecção destas. Com a limitação dos recursos é necessário que se priorize e se faça a identificação do que realmente precisa de protecção (Peltier, 2000).

Maior parte das organizações e instituições não possuem informações com o mesmo valor, com isso é necessário que o alto nível destas desenvolva uma tentativa inicial de classificação. Os funcionários e colaboradores precisam não só proteger as informações como também devem saber o valor de cada informação por estes protegida como forma de garantir uma protecção mais adequada para as informações mais sensíveis.

A informação, para ser protegida, precisa receber um determinado nível de segurança, que se baseie no valor dela e da necessidade da mesma para a organização.

> A classificação da informação tem o objectivo de assegurar que ela receba um nível adequado de proteção. Ela precisa ser classificada para indicar a necessidade, prioridade e o nível esperado de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar de um nível adicional de proteção ou um tratamento especial (ISO/IEC 27002:2005).

A informação é classificada com o objectivo de atender duas necessidades, sendo uma de proteção contra revelação e a outra de prevenção da mesma.

Na necessidade de proteção contra a revelação segundo Caruso e Stefan (1999) citado por Santos (2011) a informação pode ser classificada como: secreta, confidencial e uso interno.

#### 2.2.2.1 Secreta

Quando a informação é assim classificada é quando é de extrema importância para a organização e que a sua integridade precisa ser preservada. Deve ser acedida por um número restrito de pessoas e sendo controladas sobre o uso das tais informações.

#### 2.2.2.2 Confidencial

Essas são informações que trazem danos irreparáveis para a organização se forem acedidas de forma não autorizada, como danos no ambiente financeiro, brechas para a concorrência e como consequência, a perda da confiança dos clientes.

Devido a esses danos, esse tipo de informação deve ficar restrita ao ambiente da empresa, onde as mesmas só devem ser acedidas perante uma necessidade que seja fundamental para o desenvolvimento de uma determinada tarefa de um ou mais usuários que possam acede-las (Spanceski, 2004).

#### 2.2.2.3 Interna

As informações internas são aquelas que devem ficar disponíveis apenas para a organização evitando-se o acesso externo destas. Quando essas vazam no âmbito da empresa não trazem nenhum dano crítico para a mesma, porém, podem causar algum prejuízo indirectamete para a organização e de certa forma denigrir minimamente a imagem desta.

#### 2.2.2.4 Pública

Essa categoria de classificação é sugerida por Spanceski (2004) e este é um tipo de informação que pode ser trazida ou divulgada ao público da organização ou instituição sem restrição nenhuma, tanto que não traz prejuízos com a sua publicação.

### 2.2.3 Medidas de segurança de informação

As medidas de segurança constituem acções que minimizam a existência de riscos e os custos dos impactos, através da redução e eliminação de vulnerabilidades e de ameaças. O conjunto de medidas de segurança e sua prática constituem a essência da Segurança da Informação.

Existem, segundo Da Costa (2010) três tipos básicos de medidas de segurança.

#### 2.2.3.1 Medidas preventivas

São aquelas planejadas e executadas no intuito de evitar a ocorrência de danos aos activos de informação. Reduzem as vulnerabilidades e mantêm as ameaças sob

controle. Essas medidas são aplicadas às vulnerabilidades conhecidas e ameaças identificadas.

#### 2.2.3.2 Medidas prospectivas

São as medidas planejadas e executadas durante o ciclo normal de actividades da empresa. A prospeção busca identificar vulnerabilidades e ameaças ocultas ou que façam parte de produtos e soluções que a empresa pretende adquirir.

#### 2.2.3.3 Medidas corretivas

São as executadas após o dano ao activo de informação. Eliminam ou minimizam os impactos sofridos, bem como colaborar para a criação de outras medidas de segurança que evitem a repetição do problema.

### 2.2.4 Princípios da segurança da informação

> "Quando se pensa em segurança da informação, a primeira ideia que nos vem à mente é a protecção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de actuar exactamente como o esperado. Porém a segurança não é apenas isto.
> A expectativa de todo usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo" (Dias, 2000, p.42 citado por Spanceski, 2004, p.18).

Para o usuário a informação tem que estar disponível no momento e local que ele determina, espera ainda que a informação esteja sempre correcta e não seja alcançada por pessoas sem a devida autorização. Esse conjunto de expectativas do usuário se traduzem em princípios da segurança da informação**.**

#### 2.2.4.1 Autenticidade

"O controle de autenticidade está associado com a identificação de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo" (Spanceski, 2004, p.19).

Para Whitman (2012), a autenticidade é a qualidade ou estado de genuíno ou original, ao invés de uma reprodução ou fabricação. As informações são autênticas quando estão no mesmo estado em que foram criadas, colocadas, armazenadas ou transferidas.

Os dois conceitos visam essencialmente dizer que a autenticidade visa evitar a falsificação da informação.

#### 2.2.4.2 Confidencialidade

“As informações têm confidencialidade quando são protegidas da divulgação ou exposição a indivíduos ou sistemas não autorizados. Garante que apenas aqueles com direitos e privilégios para acessar informações são capazes de fazê-lo” (Whitman, 2012, p.13).

Quando sistemas ou indivíduos não autorizados puderem ver a informação, a confidencialidade é quebrada.

Conforme afirma o Whitman (2012), para proteger a confidencialidade ou a informação, você pode usar uma série de medidas, incluindo as seguintes:

- Classificação de informações
- Armazenamento seguro de documentos
- Aplicação de políticas gerais de valores mobiliários
- Educação de guardiões de informações e usuários finais.

A confidencialidade como as demais características da informação, é interdependente com outras características e é relativamente próxima às características conhecidas como privacidade. O valor da confidencialidade da informação é especialmente alto quando se trata de informações pessoais sobre funcionários, clientes ou pacientes.

Portanto a confidencialidade visa a protecção das informações contra acesso por alguém não autorizado, interna ou externamente.

#### 2.2.4.3 Integridade

A integridade é um dos princípios de segurança que consiste em evitar que de alguma forma os dados ou a informação sejam alterados, e sem a permissão do sujeito proprietário da informação. Os dados em referência podem ser programas, documentos e/ou registos.

#### 2.2.4.4 Disponibilidade

“Permite que usuários autorizados – pessoas ou sistemas de computadores – para que acedam a informação sem interferência ou obstrução, e receberem-na no formato desejado” (Whitman, 2012, p.12).

> “Um sistema indisponível, quando um usuário autorizado necessita dele, pode resultar em perdas tão graves quanto as causadas pela remoção das informações daquele sistema.
> Atacar a disponibilidade significa realizar acções que visem a negação do acesso a um serviço ou informação, como por exemplo: bloqueando no canal de comunicação ou do acesso a servidores de dados” (Spanceski, 2004, p.21).

Entende-se que a disponibilidade consiste em proteger os serviços que um dado sistema presta de tal forma que os mesmos não possam se degradar ou mesmo se tornarem indisponíveis sem autorização, e desta forma assegurando que o usuário aceda aos dados a qualquer momento que precisar dos mesmos.

Toda a informação deve chegar aos usuários de uma forma íntegra e confiável. Para a garantia deste feito, os elementos envolvidos na rede por onde a informação transita para chegar aos destinos precisam estar disponíveis, preservando também a integridade das informações.

Segundo Hintzbergen (2018 as características de disponibilidade são:

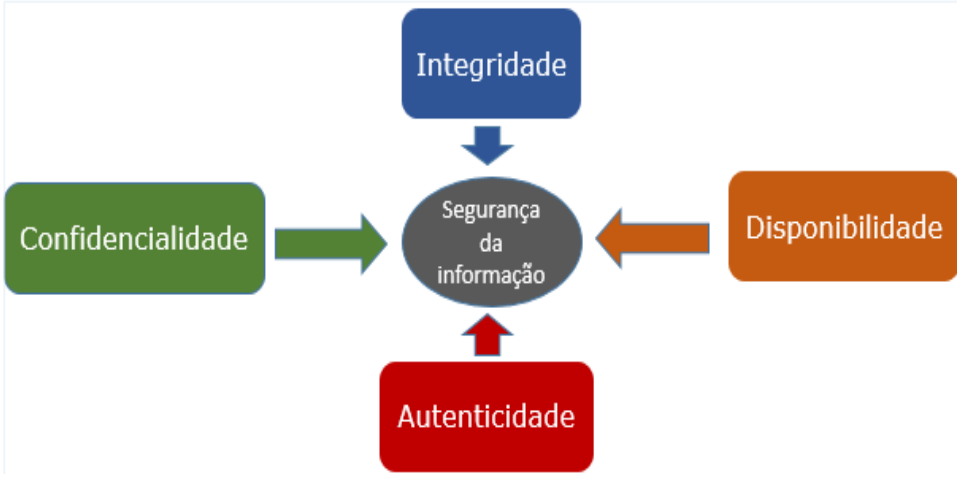
**Oportunidade:** a informação está disponível quando necessário.

**Continuidade:** a equipe consegue continuar trabalhando no caso de falha

**Robustez:** existe capacidade suficiente para permitir que toda a equipe trabalhe no sistema.

É importante ressaltar que essas propriedades, embora isoladas, apenas têm valor se complementares. Por exemplo, não adianta nada a informação estar disponível no momento da solicitação, mas não estar íntegra.

*Figura 1: Elementos de Segurança da Informação*




*Fonte: O autor, 2021*

### 2.2.5 Camadas da Segurança da Informação

Conforme referido por Netto & Silveira (2007), a todo instante os negócios, seus processos e activos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda a ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua acção. Quando essa possibilidade aparece, a quebra de segurança é consumada, conforme defende (Sêmola, 2001) citado por (Netto & Silveira, 2007).

Schneier (2001) citado por Netto & Silveira (2007) afirma que as ameaças do mundo digital espalham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça, se os bancos físicos são roubados, então os bancos digitais são roubados. Portanto o crime no ciberespaço inclui também tudo o que do mundo físico se pode esperar, como: extorsão, roubo, exploração, etc.

"A gestão da SI pode ser classificada em três aspectos: tecnológicos, físicos e humanos" (Netto & Silveira 2007, p.5).

Muitas organizações preocupam-se com aspectos tecnológicos principalmente, como caso de redes, computadores, vírus, *Internet*, e se esquecem dos aspectos físicos e humanos, que são muito relevantes para uma boa segurança do negócio quanto os aspectos tecnológicos.

#### 2.2.5.1 Camada física

É o ambiente onde está instalado fisicamente o hardware – computadores, servidores, meio de comunicação – podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis. Para Netto & Silveira (2007, p.5) "a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação".

O controle de acesso aos recursos de TI, equipamentos para a não interrupção do fornecimento da energia e firewalles são algumas formas de se gerir a segurança desta camada.

#### 2.2.5.2 Camada lógica

Esta camada caracteriza-se principalmente pelo uso de softwares, responsáveis pela funcionalidade do hardware, pela realização de transações em bases de dados organizacionais, criptografia de senhas, etc.

Para Adachi (2005) citado por Netto & Silveira (2007) é nessa camada que estão as regras, normas, protocolos de comunicação e onde, ocorrem efectivamente as transações e consultas.

A segurança em relação ao nível lógico é basicamente o acesso que os indivíduos têm às aplicações em ambientes informáticos organizacionais ou institucionais, sem se importar com o tipo de aplicação, muito menos o tamanho do computador. As ferramentas de controle nesta camada são segundo Caruso (1999) citado por Netto & Silveira (2007), invisíveis aos olhos de pessoas externas aos ambientes de informática; estas só se reconhecem quando têm o seu acesso barrado pelo controle de acesso.

Manter o software do sistema operativo actualizado é uma forma de minimizar os riscos de segurança nesta camada.

#### 2.2.5.3 Camada humana

Esta camada é formada por todos os recursos humanos presentes na organização, sendo principalmente os que possuem acesso aos recursos de TI, seja para a manutenção ou uso. Para esta camada é importante a percepção do risco pelas pessoas, sobre como elas lidam com todos os incidentes de segurança que ocorrem. É importante perceber se os usuários são ou não ignorantes em relação ao uso da TI.

Schneier (2001) conforme citado por Netto & Silveira (2007) defende que esta é a mais difícil camada de se avaliar os riscos e gerir a segurança, pois envolve o factor humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual.

Mais que gerir os recursos de tecnologia – software e hardware – a gestão da segurança da informação envolve pessoas e processos, e, isso é por muitas organizações negligenciado. Portanto uma PSI bem como a conscientização dos usuários são algumas formas de controlar a segurança ao nível da camada humana.

*Tabela 1: Visão conceitual das camadas de Segurança da Informação*

| **Visão conceitual das camadas de segurança da informação** | |
|---|---|
| **Humana** | • Segurança em recursos humanos<br>• Documentação de procedimentos<br>• Políticas de tecnologia da informação<br>• Treinamento e conscientização<br>• Gestão de continuidade de TI |
| **Lógica** | • Firewalls<br>• Antivírus<br>• Segurança de redes<br>• Controle de acesso<br>• Monitoramento<br>• Criptografia<br>• Backup |
| **Física** | • Estrutura física<br>• Localização<br>• Energia eléctrica<br>• Cabeamento<br>• Climatização<br>• Protecção contra incêndios |

*Fonte: o autor (adaptado da norma ISO/IEC 27002, 2021)*

A tabela acima resume os conceitos das camadas de segurança da informação trazendo os mesmos de uma forma sintetizada.

Conforme ilustra a tabela a camada humana é formada por todos os recursos humanos que estão presentes na organização, e descreve como estes lidam com os incidentes de segurança que ocorrem.

A camada lógica é constituída pelos softwares em uso para o monitoramento das informações da organização ou instituição. Está relacionada com o acesso ao determinado local onde a informação está. É nesta camada onde são adotadas medidas como:

- Backup dos dados
- Firewall para a filtragem do tráfego das informações que entram e saem
- Instalação de sistemas de detenção de intrusões nos programas
- Actualização dos aplicativos

A camada física constitui o ambiente onde o hardware está fisicamente instalado e nela adotam-se medidas que visam:

- Na prevenção de acesso não autorizado às instalações
- Prevenção contra desastres naturais
- Protecção contra queda de energia
- Protecção de acesso à sala de servidores, etc.

## 2.3 Políticas de segurança da informação

Política significa muitas coisas para pessoas diferentes. Para Peltier (2000) a política é definida como sendo uma declaração de alto nível de convicções empresariais, objectivos e metas bem como os meios para a realização desta para uma dada área de estudo. O mesmo autor reforça ainda dizendo que uma política não é uma descrição específica e com detalhes do problema e cada etapa necessária para a implementação desta, mas sim uma declaração de alto nível das metas e objectivos e meios gerais para a sua realização em uma área específica.

Para Dantas (2011) citado por Cardoso F. & Oliveira P, pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de protecção para as informações. Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação.

Dantas (2011) defende ainda que a sua forma, escopo e detalhes estão directamente relacionados com as actividades de negócio e decisão da organização do nível e padrão de segurança que se pretende alcançar.

Segundo Dias (2000, p.48) citado por Mocelin (2008),

> A política de segurança é um mecanismo preventivo de protecção de informações e processos importantes de uma organização, que define um padrão de segurança a ser seguido pelo corpo técnico. A politica deve estabelecer os princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e consequentemente, as informações manipuladas.

Para Marciano e Lima-Marques (2006) citado por Candeias (2018), a política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e utilizadores que com ela interagem.

Para Caruso (1999) citado por Epaminondas (2010) uma política de segurança é um conjunto de directrizes gerais destinadas a governar a protecção a ser dada a activos da companhia.

A política de segurança pode significar também delegar responsabilidades para os funcionários de uma organização, e que estes passam a responder pelos seus actos. É o conjunto de leis, regras e práticas que regulam como uma organização gere, protege e distribui suas informações e recursos (Soares, 1977 citado por Epaminondas, 2010).

Uma PSI deve representar os objectivos da organização, e é importante que todos os colaboradores participem no desenvolvimento da PSI a ser adotada.

Existem várias directrizes para a implementação de uma política de segurança da informação, e para tal, a norma ISO/IEC 27002:2005 afirma que este documento deve conter:

a) Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
b) Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objectivos e estratégias do negócio;
c) Uma estrutura para estabelecer os objectivos de controle e os controles, incluindo a estrutura de análise/avaliação e gestão de risco;
d) Breve explanação das políticas, princípios normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
    1) Conformidade com a legislação e com requisitos regulamentares contratuais;
    2) Requisitos de conscientização, treinamento e educação em segurança da informação;
    3) Gestão da conformidade do negócio;

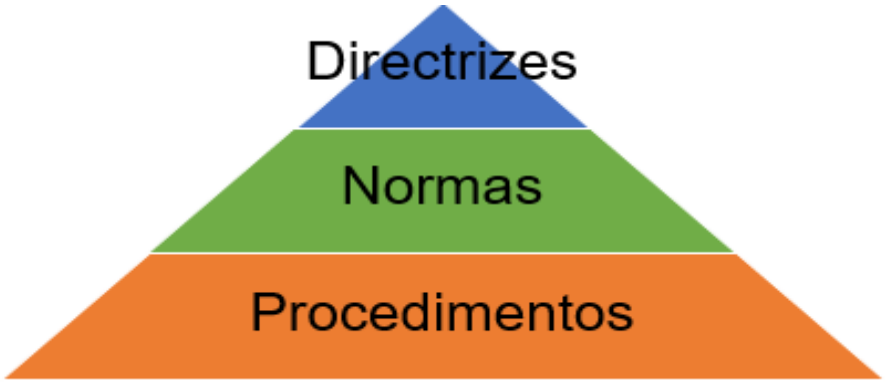
4) Consequências das violações na política de segurança da informação;

e) Definição das responsabilidades gerais na gestão da segurança da informação, incluindo o registo dos incidentes de segurança da informação;

f) Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

A mesma norma recomenda que a política de segurança da informação seja comunicada através de toda a organização para os usuários de forma que seja relevante, acessível e compreensível para o leitor em foco.

*Figura 2: Visão conceitual de uma Política de Segurança da Informação*




*Fonte: O Autor, 2021*

Na figura acima, a diretriz é o que deve ser feito, e é um documento que é elaborado pela camada gestora da segurança da informação com base no planeamento estratégico e informacional descrito pela administração da empresa.

A norma especifica a forma e controle em que será feita a SI na organização. E os procedimentos constituem a descrição passo a passo das actividades. Cada procedimento é documentado a partir de uma norma.

### 2.3.1 Características de Política de Segurança da Informação

Para a elaboração de uma Política de Segurança da Informação (PSI) é necessário que se faça uma análise de riscos e entender os pilares de segurança. Além disso deve-se ter conhecimento profundo da organização bem como os seus processos todos.

Para isso é necessário se conhecer o objectivo central da empresa, e, entender cada um dos processos passo a passo, compreendendo como cada sector funciona com vista a encontrar melhorias na segurança dos activos.

Posteriormente é preciso que se faça a listagem de todos os activos da empresa, os internos bem como os externos, para cada processo entender os pontos chaves, e desenvolver regras que serão cumpridas, com vista a estabelecer dentre os processos realizados um padrão, garantindo assim nível de segurança alto e zelar pelos recursos de TI e por todas as informações que estão dentro da empresa.

Outro aspecto importante para uma PSI é que esta possa ser redigida com uma linguagem simples e de entendimento fácil pelo facto de o público alvo abranger a organização toda desde o nível operacional até o mais alto nível da organização.

Desenvolvido o documento, no caso a PSI, é importante que se realize a sua apresentação para todos os colaboradores da empresa, pois a sua divulgação é tão importante tanto quanto a própria PSI, sendo que para a sua adaptação e cumprimento de todos os itens que ela contém, a mesma deve ser conhecida e bem esclarecida.

Portanto, uma PSI importa que ela seja publicada e esclarecida para os funcionários todos em uma organização, para em caso de algum incumprimento, seja possível fazer a cobrança.

### 2.3.2 Tipos de políticas

Existem três tipos de políticas: Regulatória, Consultiva e Informativa

#### 2.3.2.1 Política Regulatória

Este tipo de política pode ser entendido como uma série de especificações legais.

Descreve com detalhes o que deve ser feito, quem deve fazer e ainda relata qual a acção é importante. Esta é uma política geralmente direcionada para um ramo de actividade.

#### 2.3.2.2 Política Consultiva

É um tipo de política que não é obrigatória, mas muito recomendada. As organizações devem conscientizar seus funcionários a considerar esta política como se ela fosse obrigatória. Esta política esclarece as tarefas diárias dos funcionários de uma maneira clara e directa.

#### 2.3.2.3 Política Informativa

É uma política de carácter informativo e sem riscos associados ao não cumprimento da mesma. Ela traz informações importantes bem como advertências severas.

### 2.3.3 Importância de uma Política de Segurança da Informação

Segundo Siewert citado por Andrade (2009)

> A PSI tem como principal objectivo definir padrões de comportamento que sejam largamente informados e conhecidos por todos na organização e que sirva de base para a alta administração em decisões relacionados a SI, proporcionando coerência e menos complexidade, refletindo também em decisões mais justas e mais facilmente aceitas, já que se baseiam em uma política largamente difundida, e não apenas no critério pessoal de quem toma a decisão.

De acordo com o mesmo autor a Política de Segurança da Informação (PSI) contribui não só para a redução de incidentes de SI, mas também para o aumento da produtividade, já que a busca de orientações sobre comportamento será menor e cada um poderá se concentrar mais em suas actividades em vez de procurar as possibilidades de uso ou acesso às informações, fazendo com que as pessoas se sintam mais confortáveis conhecendo os limites.

Quando não se tem uma política estabelecida as actividades actuais e passadas em si se tornam política. Sem uma política formal uma organização pode estar em um maior perigo de quebra de segurança perdendo assim a sua vantagem de competitividade, segundo defendido por (Peltier, 2000).

Portanto uma PSI tem um impacto considerável para uma organização, garante que os colaboradores da mesma conheçam a PSI e não apenas um grupo de pessoas na organização.

## 2.4 Padrões e normas de Segurança da Informação

A norma é aquilo que se estabelece como base ou medida para a realização de alguma coisa. E a padronização é uma referência de qualidade.

O profissional em Segurança da Informação precisa desenvolver acções que estejam alinhadas com melhores práticas no contexto de segurança para a protecção e o controle da informação.

Portanto existem muitas normas e padrões para diferentes contextos. No contexto do presente trabalho serão abordados normas e padrões no ramo da Segurança da Informação.

### 2.4.1 Série ISO 27000

A ISO/IEC 27001 e a ISO/IEC 27002 são normas internacionais publicadas pela *Standardization Organization* (ISO) e pela *International Electrotechnical Commission* (IEC). Elas definem respectivamente, os requisitos e as melhores práticas para o Sistema de Gestão de Segurança da Informação (SGSI).

Empresas que aplicam orientações dessas normas garantem um SGSI conforme orientações internacionais e usufruem de benefícios destes tomando a redução de riscos e processos bem organizados como exemplo.

As normas desta família são projectadas com focos diferentes dentro da Segurança da Informação. Elas podem ser para implementações do SGSI, métricas, controles, avaliação e tratamento de riscos, auditoria, gestão.

#### 2.4.1.1 Norma ISO 27001

Essa é uma norma de gestão que define os requisitos para uma organização possuir e administrar um Sistema de Gestão de Segurança da Informação certificado. Esta norma leva em consideração os activos da organização e todas as necessidades referentes à área de negócio para melhor definir a forma de administração do sistema.

Esta norma possui vários benefícios dentre os quais se destacam:

- A redução de risco de responsabilidade pela não implementação de políticas e procedimentos
- Oportunidade de identificar e corrigir os pontos fracos da organização
- A alta gestão da organização é responsável pela segurança da informação
- Permissão de maior confiabilidade aos clientes
- Permite medir o sucesso do sistema
- Permite revisão independente do sistema de gestão da segurança da informação
- Aumenta a maior conscientização interna sobre a segurança
- Combina recursos com outros sistemas de gestão

#### 2.4.1.2 Norma ISO 27002

Esta norma estabelece um código de melhores práticas para o apoio na implantação de um Sistema de Gestão de Segurança da Informação nas organizações e/ou instituições e tem por objectivo o estabelecimento de directrizes e princípios para iniciar, implementar, manter e melhorar a gestão da segurança da informação de uma organização.

Ela funciona como um guia completo de implementação, em que faz a descrição de que controles devem ser estabelecidos e de que forma. Se baseia na avaliação de riscos de activos mais importantes da organização.

Esta possui vários benefícios a destacar:

- Maior controle de activos e informações estratégicas
- Identificação e correção dos pontos fracos do sistema
- Melhora a organização dos processos
- Redução de custos com a prevenção de incidentes de segurança da informação
- Conformidade com a legislação e outras regulamentações

A norma ISO 27002 contém 11 secções de controles de segurança da informação que juntas formam as categorias de segurança que são:

- Política de Segurança da Informação
- Organizando a Segurança da Informação
- Gestão de activos
- Segurança em Recursos Humanos
- Segurança Física e do Ambiente
- Gestão das Operações e Comunicações
- Controle de Acesso
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- Gestão de Incidentes de Segurança da Informação
- Gestão de Continuidade do Negócio
- Conformidade

Segundo afirma a norma, a ordem destas secções não significa o seu grau de importância. Dependendo das circunstâncias, todas as secções podem ser importantes. Cada organização ou instituição que utiliza esta norma é que identifica quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio desta.

### 2.4.2 COBIT

COBIT significa Obejctivos de Controle de Informação e Tecnologia Relacionada. É uma estrutura criada pela ISACA (Associação de Auditoria e Controle de Sistemas de Informação) para governança e gestão de TI. O COBIT serve de modelo para gerentes de negócios que oferece valor às organizações e praticar melhores práticas

de gestão de risco associados aos processos de TI. É um integrador de boas práticas de TI e a metodologia de governança de TI que auxilia no entendimento e gestão de todos os riscos e todos os benefícios que estão associados com a Tecnologia de Informação.

O COBIT é um padrão que começou em 1996 como um *framework* para auditoria e controle de TI, com foco nos objectivos de controle conforme sustenta Dourado, 2014. É um padrão que foi evoluindo sendo que agora encontra-se na sua quinta versão com a designação de COBIT 5 com foco na Governança Corporativa de TI. O COBIT 5 baseia-se em cinco princípios básicos para governança e gestão de Tecnologia de Informação de uma organização que são:

- **1º Princípio:** Atender às Necessidades das Partes Interessadas
- **2º Princípio:** Cobrir a Organização de Ponta a Ponta
- **3º Princípio:** Aplicar um Modelo Único Integrado
- **4º Princípio:** Permitir uma Abordagem Holística
- **5º Princípio:** Distinguir a Governança da Gestão

O COBIT está dividido em 4 domínios, nos quais 34 processos estabelecem os objectivos de controle necessários para a manutenção de uma estrutura de controles internos que possibilitem à organização atingir seus obejctivos de negócio de maneira confiável. Esses domínios são:

- **Planeamento e Organização** – Provê direcção para a entrega de soluções e de serviços. É neste domínio onde se define o plano estratégico da TI, a arquitetura e informação, direcionamento da tecnologia, gestão dos investimentos, riscos, gestão de projectos e da qualidade.
- **Aquisição e Implementação** – Provê as soluções e estas são transferidas, para entrega de serviços, identificam as soluções automatizadas que serão aplicadas e reutilizadas na organização, aquisição e manutenção de todos os sistemas e infraestruturas, instalação e gestão de mudanças.
- **Entrega e Suporte** – Neste domínio são recebidas as soluções e são tornadas passíveis aos usuários finais; garantia de desempenho, continuidade e segurança de sistemas; faz-se também neste domínio o treinamento dos usuários; alocação de serviços; gestão de configurações e de dados, problemas e incidentes.

- **Monitoramento e Avaliação** – Faz o monitoramento dos processos para garantir que a direcção que foi definida seja seguida, é uma supervisão de todas as actividades dos outros processos; é feita a colecta e análise de todos os dados dos níveis operacional e estratégico para a auditoria e controle da organização.

Cada um dos domínios engloba um conjunto de processos para garantir uma gestão completa da TI, somando no total os 34 processos, e estão divididas do seguinte modo:

**Planeamento e Organização**

- Define o plano estratégico da TI
- Define a arquitetura da informação
- Determina a direcção tecnológica
- Define a organização de TI, os seus processos e seus relacionamentos
- Gerência dos investimentos de TI
- Comunicação dos objectivos e direcionamentos gerenciais
- Gerencia os recursos humanos
- Gerencia a qualidade
- Avalia e gerencia os riscos de TI
- Gerencia os projectos

**Aquisição e implementação**

- Identifica as soluções de automação
- Adquire e mantém os softwares
- Adquire e mantém a infraestrutura tecnológica
- Viabiliza a operação e utilização
- Adquire recursos de TI
- Gerencia as mudanças
- Instala e aprova soluções e mudanças

**Entrega e suporte**

- Define e mantém os acordos de níveis de serviços
- Gerencia os serviços de terceiros
- Gerencia a performance e capacidade do ambiente
- Assegura a continuidade dos serviços
- Assegura a segurança dos serviços

- Identificação e alocação de custos
- Educação e treinamento de usuários
- Gerencia a central de serviços e incidentes
- Gerencia a configuração
- Gerencia os problemas
- Gestão de dados
- Gestão da infraestrutura
- Gerencia as operações

**Monitoramento e avaliação**

- Monitoramento e avaliação do desempenho da TI
- Monitoramento e avaliação dos controles internos
- Assegura a conformidade com requisitos externos
- Prove governança para a TI

#### 2.4.2.1 Componentes do COBIT

Os vários componentes do COBIT incluem:

***Framework – IT*** - ajuda a organizar os objectivos da governança de TI trazendo as melhores práticas nos processos e domínios de TI, ao mesmo tempo que vincula os requisitos do negócio.

**Descrições de processo** – é o modelo de referência e também actua como uma linguagem comum para cada indivíduo da organização. As descrições do processo incluem planeamento, construção, execução e monitoramento de todos os processos de TI.

**Objectivos de Controle** – fornecem uma lista completa de requisitos considerados pela gestão para controle efectivo de TI.

**Modelos de maturidade** – acessa a maturidade e a capacidade de cada processo enquanto abordam as lacunas.

**Directrizes de gestão** – ajudam na atribuição de responsabilidades melhores, na medição de desempenhos, concordar com objectivos comuns e ilustrar melhores inter-relações com todos os outros processos.

### 2.4.3 ITIL

ITIL *(Information Technology Infrastructure Library)* significa Biblioteca de Serviços de Tecnologia de Informação (TI) e tem como objectivo a gestão da TI e seus recursos através da execução dos processos e serviços que precisam ser levados em consideração para uma execução efectiva da tecnologia da informação alinhada ao negócio da organização. Essa biblioteca de boas práticas foi elaborada pelo *Office of Government Commerce/UK* com objectivo de que as organizações que se relacionassem com o governo britânico seguissem esse padrão.

A filosofia deste padrão adota estratégia que esteja orientada a processos para o atendimento de qualquer que seja o tipo de organização. Considera o Gestão de Serviços em TI um conjunto de processos relacionados e integrados.

Os serviços de suporte do ITIL dão um forte auxílio no atendimento das necessidades do cliente, e desta forma apoiar aos seus objectivos do negócio. Este padrão faz a descrição de todos os processos necessários para dar suporte à utilização e à gestão da infraestrutura de TI. Fornecer qualidade de serviço aos clientes de TI com custos justificáveis e relacionar estes com os custos dos serviços é mais um princípio do ITIL.

Esta biblioteca contempla os seguintes assuntos: Gestão de Configuração, Central de Serviços, Gestão de Incidentes, de Problemas, de Mudanças, de Liberações, da Capacidade, da Disponibilidade, da Continuidade dos Serviços de TI, Gestão Financeiro para Serviços de TI, Gestão do Nível de Serviço, da Infraestrutura e de Aplicações.

#### 2.4.3.1 Características do ITIL

- É um modelo de referência para processos de Tecnologia de Informação não proprietário
- Adequado para todas as áreas de actividade
- Independente da tecnologia e fornecedor
- Baseia-se nas melhores práticas
- Modelo de referência para a implementação de processos de TI
- Padronização de terminologias
- Independência de processos
- Interdependência de processos
- Directivas básicas para implementação

- Directivas básicas para funções e responsabilidades dentro de cada processo

#### 2.4.3.2 Benefícios do ITIL

Com o ITIL podem-se ter muitos resultados dentre os quais se destacam:

- Fortalecimento dos Controles e da Gestão dos ambientes de TI
- Orientação a processos com significativa redução nos tempos de execução e distribuição de serviços
- Diminuição gradativa da indisponibilidade dos recursos e sistemas de tecnologia da informação, causados por falha no planeamento das mudanças e implantações em TI
- Os níveis de satisfação do clientes e usuários internos se elevam com relação à disponibilidade e qualidade dos serviços de TI
- Os custos operacionais de TI são reduzidos
- Há um reconhecimento da capacidade de gestão pelos acionistas, colaboradores e clientes
- Aderência às instruções normativas das entidades reguladores e certificadoras

### 2.4.4 Análise comparativa entre os *frameworks* COBIT, ITIL e o padrão ISO/IEC 27001 e 27002

Os *frameworks* COBIT e ITIL constituem melhores práticas para governança em TI. ITIL é um conjunto de melhores práticas para gestão de serviços e operações em TI E e o COBIT é um conjunto de directrizes que se baseiam em auditoria para processos, controles bem como práticas em TI.

Os padrões da série ISO 27000 constituem boas práticas para a gestão da Segurança da Informação. A norma ISO/27001 permite às empresas demonstrarem conformidade com sistema de gestão de segurança da informação obrigando estas a melhorar de forma contínua o controle dos seus activos de informação, principalmente os mais sensíveis ao passo que a norma ISO/IEC 27002 é usada para segurança da informação. Esta possibilita a prevenção e proteção das ameaças e vulnerabilidades nas informações. Perante esta análise, o autor usou a norma ISO/IEC 27002 para a definição dos controles que se adequam a realidade da FEUEM, por esta se comprometer com melhores práticas em segurança da informação.

# 3 Caso de Estudo

## 3.1 Faculdade de Engenharia da Universidade Eduardo Mondlane - FEUEM

A Faculdade de Engenharia foi fundada em 1962 com uma estrutura de chefia centralizada, com cada curso associado a um Departamento específico. Logo após a Independência, os departamentos assumiram o estatuto de Faculdade com um corpo directivo não centralizado, mas com uma coordenação interfaculdade. Esta estrutura permaneceu até 1980, quando a estrutura foi de novo mudada para a situação de 1962. Em 1962 existiam 4 cursos, nomeadamente Engenharia Civil, Engenharia Electrotécnica, Engenharia Mecânica e Engenharia Química. No início, os cursos duravam 6 anos sendo os 3 primeiros anos virados para matérias gerais-básicas e os últimos 3 anos, para disciplinas de Engenharia, incluindo disciplinas de gestão. Em 1970 a duração do curso foi encurtada para 5 anos, com os dois primeiros anos virados para matérias gerais-básicas. As horas de ensino foram estendidas e as disciplinas eram tipicamente semestrais ao contrário de anuais como eram em 1962. Dois novos cursos foram introduzidos em 1970 Engenharia de Minas e Engenharia Metalúrgica. Estes novos cursos não duraram muito visto serem de longa duração (5 e 8 anos respectivamente).

Foram introduzidos mais quatro (4) cursos na Faculdade Engenharia, totalizando, actualmente, oito (8) no conjunto dos seus Departamentos, nomeadamente:

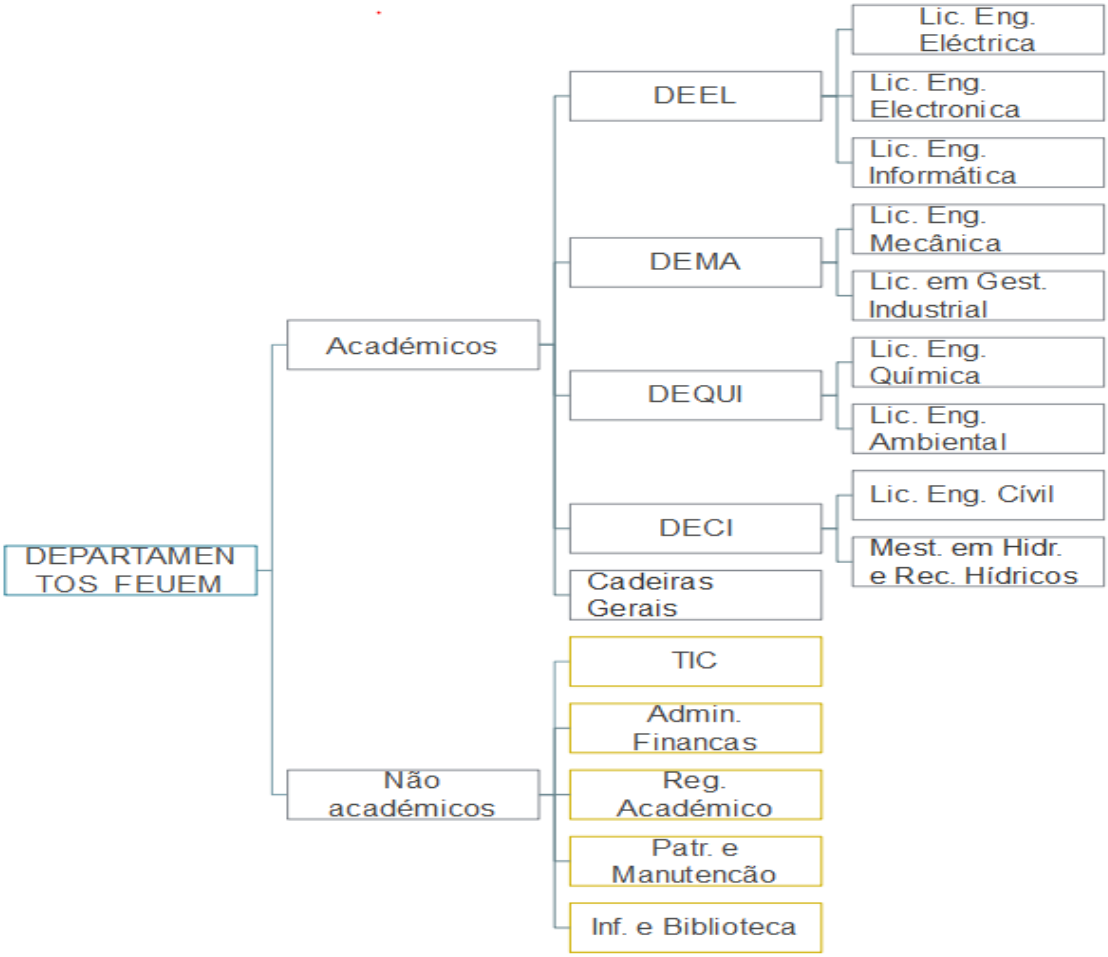
- Engenharia Eléctrica
- Engenharia Informática
- Engenharia e Gestão Industrial
- Curso de Ciências de Engenharia do Ambiente

A medida que o tempo foi passando a faculdade tem vindo apresentar várias mudanças em termos de cursos, períodos, aspectos curriculares, e outros elementos, entretanto de lá até cá a faculdade conta com 5 departamentos nomeadamente: Departamento da Mecânica (DEMA), Departamento da Civil (DECI), Departamento de Química (DEQUI), Departamento de Electrotecnia (DEEL), e Departamento de Cadeiras Gerais (DCG).

Esta conta também com cinco departamentos não académicos, nomeadamente: O Património e Manutenção, Departamento de Tecnologias de Informação e Comunicação, Departamento do Registo Académico (DRA), Departamento de Administração e Finanças (DAF) e Departamento de Informação e Biblioteca (DIB) e

um Centro de Estudos de Engenharia - Unidade de Produção (CEE-UP). A seguir é ilustrada a organização dos departamentos da FEUEM, na *Figura 3.*

*Figura 3: Organização dos departamentos da FEUEM*




*Fonte: [http://www.engenharia.uem.mz/index.php](http://www.engenharia.uem.mz/index.php)*

Os cursos no período laboral têm no geral uma duração de 5 anos sendo que em 4 anos ocorre o estudo de cadeiras gerais e de engenharia e o no quinto ano é realizado a preparação do trabalho de licenciatura.

*Figura 4: Faculdade de Engenharia da UEM*

*Fonte: http://www.engenharia.uem.mz*

## 3.2 Descrição da situação actual

A Faculdade de Engenharia da Universidade Eduardo Mondlane, também designada por FEUEM, actualmente se encontra sem uma Política de Segurança da Informação (PSI) traçada ou implementada. Uma proposta de uma Política de Segurança de Informação, será de grande importância para a faculdade. Com ela poderá se garantir a segurança dos principais activos que a faculdade dispõe, que são de grande valor para a mesma. Portanto a segurança destes activos é muito fundamental.

A Faculdade de Engenharia é um dos órgãos da Universidade Eduardo Mondlane (UEM). No que diz respeito à Segurança da Informação a UEM predispõe de um órgão específico que é o Centro de Informática da UEM (CIUEM) que se encarrega pelos aspectos de segurança para todas faculdades da universidade bem como todos os órgãos com activos informacionais com necessidade de protecção.

O CIUEM neste contexto faz o controle e supervisão dos activos da informação de uma forma centralizada, ou seja, este adota as medidas de segurança centralmente. O CIUEM não predispõe de uma Política de Segurança da Informação implementada ou documentada, porém possui uma política de Estratégias das TIC's que tem por objectivo geral estabelecer princípios e padrões no que concerne a adopção e exploração das Tecnologias de Informação e Comunicação, tendo em conta o seu

papel no processo de transformação da Universidade Eduardo Mondlane numa universidade de investigação.

Neste contexto este trabalho visa dar proposta de algumas políticas que podem ser implementadas e vigorarem na instituição (FEUEM) como meio que contribui para a efectivação da Segurança da Informação.

### 3.3 Descrição das vulnerabilidades dos sistemas de informação da FEUEM

O departamento de TIC's da FEUEM é o órgão que zela pelo bem-estar dos activos da instituição.

A instituição tem acesso à *Internet,* e usa serviços de e-mail. Os funcionários possuem senhas que lhes dão acesso aos sistemas internos, bem como aos e-mails, e os estudantes têm acesso livre para os computadores dos laboratórios.

Os computadores das salas de máquinas não possuem software de segurança, o que pode colocar esses em perigo. Sem mecanismos de segurança nos computadores pode ser fácil instalar-se qualquer tipo de vírus, que pode se espalhar pela rede e causar danos.

Ainda sobre os computadores nos laboratórios, e não só, estes possuem entradas para leitores de mídias como USB, e essas entradas não são bloqueadas, e ao introduzir algum dispositivo externo infectado, pode passar o "malware" para o computador, pode ter consigo um tipo de vírus especialmente desenhado para o roubo de dados.

Constitui também um ponto fraco no que diz respeito a segurança, a partilha de credenciais entre funcionários e a não alteração periódica da senha.

# 4 Processo de Desenvolvimento da proposta de PSI para FEUEM

Durante o processo de desenvolvimento do seguinte trabalho, teve-se como objectivo principal trazer uma proposta de Política de Segurança da Informação como resultado. A mesma foi desenvolvida com objectivo de ser aplicada realidade da FEUEM no que concerne a segurança da informação.

A proposta de PSI desenvolvida neste trabalho é uma política regulatória, conforme os tipos de políticas que constam no Capítulo 2, no ponto 2.3.2.1, e a mesma tem definições que se basearam na norma ISO/IEC 27002.

**Identificação e descrição das vulnerabilidades da FEUEM no que concerne à Segurança de Informação**

## 4.1 Política de Segurança da Informação (PSI) para a FEUEM

A PSI proposta neste trabalho, a constar no Anexo 2 deste trabalho, vela pelos aspectos da segurança da informação da FEUEM, com a finalidade de protecção dos activos de informação da instituição, os físicos e lógicos, definindo, portanto, um padrão desejável de segurança a ser seguida pelos usuários.

O processo da criação da PSI seguiu os seguintes passos:

- Indicação dos objectivos e definição de termos que ajudam no entendimento da PSI;
- Definição da abrangência e/ou público alvo da PSI;
- Descrição para a classificação das informações;
- Definições de direito de acesso às informações;
- Procedimentos para a utilização dos recursos de TI da FEUEM;
- Procedimentos para o uso da Internet;
- Definições para o uso correcto do correio electrónico;
- Indicação de procedimentos seguros para o descarte das informações;
- Definições para o uso de senhas;

### 4.1.1 Definição de controles usados no processo de desenvolvimento da PSI

Conforme citado em pontos anteriores, para o desenvolvimento da proposta da PSI apresentada neste trabalho baseou-se na norma ISO/IEC 27002. Esta norma contém secções, as mesmas com vários controles, no entanto, os controles são usados de acordo com a necessidade de cada organização ou instituição, não havendo deste modo a necessidade de uso de todos os controles desta norma.

A seguir está a indicação dos controles da norma ISO/IEC usados para o desenvolvimento da PSI para a FEUEM.

*Secção 5 – Política de Segurança da Informação*

- Categoria 5.1 – Política de segurança da informação
  - Controle 5.1.1 – *Documento de política de segurança da informação*

*Secção 7 – Gestão de activos*

- Categoria 7.2 – Classificação da informação
  - Controle 7.2.1 – *Recomendações para classificação*

*Secção 9 – Segurança física e do ambiente*

- Categoria 9.1 – Áreas seguras
  - Controle 9.1.2 – *Controles de entrada física*
- Categoria 9.2 – Segurança de equipamentos
  - Controle 9.2.4 – *Manutenção de equipamentos*

*Secção 10 – Gestão das operações e comunicações*

- Categoria 10.6 – Gestão da segurança em redes
  - Controle 10.6.1 – *Controles de redes*
- Categoria 10.7 – Manuseio de mídias
  - Controle 10.7.1 – *Gestão de mídias removíveis*
- Categoria 10.8 – Troca de informações
  - Controle 10.8.1 – *Políticas e procedimentos para troca de informações*
  - Controle 10.8.4 – *Mensagens electrónicas*

*Secção 11 – Controle de acessos*

- Categoria 11.2 – Gestão de acesso do usuário

Controle 11.2.2 – *Gestão de privilégios*

Controle 11.2.3 – *Gestão de senha do usuário*

- Categoria 11.3 – Responsabilidades dos usuários

Controle 11.3.1 – *Uso de senhas*

Controle 11.3.3 – *Política de mesa limpa e tela limpa*

# 5 Conclusões e Recomendações

## 5.1 Conclusão

As Políticas de Segurança da Informação são indispensáveis para o sucesso em um negócio. Estas permitem que as instituições bem como organizações tenham um controle dos seus activos de informação bem como o controle da camada humana, o elo mais fraco no que concerne a Segurança da Informação.

Com a introdução e implementação de normas e políticas na FEUEM será possível se preservar os elementos de segurança, a integridade, disponibilidade e confidencialidade das suas informações, e restringir o acesso às informações, principalmente as mais sensíveis. As PSI's exigem menos poder financeiro, e revelam-se eficientes, garantem o funcionamento do sistema todo, e podem fazer com que não hajam problemas recorrentes.

O desenvolvimento desta PSI foi feito de acordo com a realidade da FEUEM, fazendo abrangência de várias áreas de segurança na instituição, e visa definir normas e procedimentos para a garantia da segurança da informação.

## 5.2 Recomendações

Por se tratar de uma primeira proposta de Política de Segurança da Informação a mesma não apresentou muitas políticas, e as que foram apresentadas são de certa forma generalizadas, tendo-se focado mais para funcionários da instituição, os que lidam com informações críticas e sistemas de informação que portam dados sensíveis. Portanto recomenda-se que em próximos trabalhos se apresentem políticas de forma específica, ou seja, haver directrizes especificamente selecionadas para estudantes e outras para os funcionários no geral.

Recomenda-se o uso das políticas presentes neste trabalho para ajudar na visão de outras políticas que sejam necessárias, e de acordo com as mudanças nas infraestruturas computacionais as presentes neste trabalho podem sofrer modificações e melhorias, para que futuramente se tenham políticas mais sólidas.

## Bibliografia

### Referências Bibliográficas


1. Abner, N. S., Silveira, M. A (2007). *Gestão da segurança da informação: factores que influenciam sua adoção em pequenas e médias empresas.* Universidade Municipal de São Caetano do Sul – IMES, Brasil.
2. Andrade, C. F. (2009). *Política de segurança da Informação*. Estudo de caso: Assembleia Nacional
3. Candeias, I., Pinheiro, F. M. (2018). *Política de segurança da informação em uma instituição de ensino superior pública*
4. Epaminondas, J. M. (2010). *Política de segurança da informação aplicada à instituição de educação superior*
5. Da Costa N, J.P. (2010). *Software de Segurança da Informação.* Manaus - AM
6. Dantas, M. L. (2011). *Segurança da Informação – Uma abordagem focada em gestão de riscos.*
7. Dourado, L. (2014). *COBIT 5. Framework de Governança e Gestão Corporativa de TI.*
8. Fontes, E. L. G. (2015). *Políticas de segurança da informação.*
9. Gerhardt, T. E., Silveira, D. T. (2009). *Métodos de pesquisa.* 1ª ed.
10. Gil, A. C. (2002). *Como elaborar projectos de pesquisa.* 4ª ed. São Paulo. ATLAS S.A.
11. Gil, A. C. (2008). *Métodos e técnicas de pesquisa social.* 6ª ed. São Paulo. ATLAS S.A.
12. Gross, C. M. & Gross C. J. (2013). *Segurança em Tecnologia da Informação*
13. Hintzbergen, J. et al (2018). *Fundamentos de Segurança da Informação* – Com base na ISO 27001 e na ISSO 27002
14. Manaus/AM (2012). *Política de Segurança da Informação (PSI).* Instituto Federal de Educação, Ciência e Tecnologia do Amazonas
15. Marconi, M. A., Lakatos, E. M. (2003). *Fundamentos de Metodologia Científica.* 5ª ed. ATLAS S.A.
16. Mesquita, L. H. (2015). *Política de segurança da informação – desenvolvimento de um modelo para uma empresa de plano de saúde ambulatorial.* Centro Universitário de Brasília

**17.** Mocelin, S. S. (2008). *Controles de segurança de dados acessados via aplicação web.*

**18.** NBR ISO/IEC 27002:2005. *Tecnologia da Informação – Código de Prática para Gestão da segurança de Informações*. 2ª ed. Rio de Janeiro

**19.** Netto, A. S. & Silveira, M. A. P. (2007). *Gestão da Segurança da Informação: factores que influenciam sua adoção em pequenas e médias empresas.* Rio de Janeiro.

**20.** Novo, J. P da C. (2010). *Softwares de Segurança da informação.*

**21.** Peltier, T. R. (2000). *Information Security: Policies and Procedures - A Practioner's Reference.*

**22.** Pontes, M. V. (2014). *Política de Segurança da Informação: uma contribuição para o campus IV.*

**23.** Santos, A. L. (2011). *Política de segurança da informação. Uma proposta de política de segurança da informação para a companhia melhoramentos norte do Paraná.* Universidade Estadual do Norte do Paraná.

**24.** Sêmola, M. (2014). *Gestão da Segurança da Informação.* Uma visão executiva. 2ª ed. Elsevier Editora Ltda

**25.** Spanceski, F. R. (2004). *Política de Segurança da informação – desenvolvimento de um modelo voltado para instituições de ensino*.

**26.** Whitman, M. E. & Mattord, H. J. (2012). *Principles of Information Security*. 4th ed.

## Outra bibliografia consultada

**1.** Hermann, D. S. *A practical guide to Security Engineering and Information Assurance.*

**2.** Peltier, T. R. *Information Security: Policies and Procedures - A Practioner's Reference.* 2th ed.

**3.** www.anyconsulting-com-br-wp-content-cache-page_enhanced-www-anyconsulting-com-br-o-que-sao-iso-27001-e-iso-27002-index_ssl-html_gzip – acedido em 15/07/2021

***4.*** www.gestaodesegurancaprivada.com.br/politica-de-seguranca-da-informacao - Políticas de Segurança – acedido em 12/02/2021

5. www.uem.mz
6. www.b4K1BphABn6CaKb_2013-5-3-11-17-0 – acedido em 06/08/2021
7. www.ostec-blog-padronizacao-seguranca-iso-27002-boas-praticas-gsi- - acedido em 15/07/2021
8. https://pt.strephonsays.com/iso-27001-and-vs-iso-27002-14693 - acedido em 15/07/2021

# ANEXOS

## Anexo 1: Proposta de Política de Segurança da Informação para FEUEM

### 1. Proposta de solução: políticas para a gestão de segurança da informação na FEUEM

Para a criação desta proposta de Política de Segurança da Informação usou-se como padrão a norma ISO/IEC 27002:2005. Esta norma conforme mencionado no Capítulo 2 em seu ponto 2.4.1.2, estabelece directrizes e princípios para iniciar, implementar, manter e melhorar a gestão da segurança da informação de uma organização.

### 1.1. Introdução

A implementação de políticas, normas e procedimentos que visam a garantia de segurança da informação deve constituir uma prioridade para a Faculdade de Engenharia, reduzindo-se os riscos de falhas, danos ou prejuízos que podem comprometer os objectivos da FEUEM.

A informação constitui um bem valioso que existe e é manipulada por várias maneiras, por meio de arquivos electrónicos, mensagens, internet, base de dados, em formato físico (em meio impresso), em forma de áudios e de vídeos e muito mais.

Uma boa segurança da informação deve ter em consideração três aspectos básicos de extrema importância, que são:

Confidencialidade: somente pessoas com devida autorização em uma dada organização ou instituição devem ter acesso à informação.

Integridade: somente alterações autorizadas pela organização podem ser feitas na informação.

Disponibilidade: a informação deve estar sempre disponível para as pessoas que têm a devida autorização.

### 1.2. Objectivos

Esta Política de Segurança da Informação tem como objectivo estabelecer directrizes que permitam à FEUEM fazer a preservação e protecção das suas informações contra vários tipos de ameaças e riscos relacionados à Segurança da Informação. Tem também por objectivo fazer a implementação de controles e procedimentos que visam na redução das vulnerabilidades da FEUEM contra seus activos.

Outro objectivo da PSI proposta é o da conscientização dos usuários de informação sobre a sua segurança e a protecção e preservação da integridade, confidencialidade e a disponibilidade da informação com vista a proteger as actividades da FEUEM.

### 1.3. Abrangência

Esta Política de Segurança da Informação é destinada a todos os colaboradores, toda camada de gestão, funcionários, estudantes, visitantes da FEUEM. Abrange requisitos de segurança lógica, requisitos de segurança física e requisitos de segurança dos recursos humanos.

Todos os requisitos de segurança que esta Política de Segurança abrange terão a sua regulamentação por meio de normas e procedimentos específicos que se adequam à realidade da Faculdade de Engenharia.

### 1.4. Conceitos

**Activo –** qualquer coisa que tenha valor para a organização.

**Controle –** forma de gerir o risco, incluindo políticas, procedimentos, directrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

**Directriz –** descrição que orienta o que deve ser feito e como, para se alcançarem os objectivos estabelecidos nas políticas.

**Perímetro de segurança –** área que contém informações críticas bem como informações sensíveis usado para a guarda e processamento de informação

**Política –** intenções e directrizes globais formalmente expressas pela direcção.

**Segurança da Informação –** preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente outras propriedades como autenticidade, responsabilidade, não repúdio e confidencialidade, podem também estar envolvidos.

**Vulnerabilidade –** É uma fraqueza identificada num sistema controlado, onde não existem controlos ou estes já não tenham efeito

## 1.5. Directrizes gerais

### 1.5.1. INTERNET

Poucas organizações e instituições podem fazer os seus negócios bem como as suas actividades sem o acesso à Internet. A rede tem um papel muito fundamental no dia a dia de uma organização seja ela uma instituição de ensino. O uso dela pode constituir ameaça para os activos, portanto é importante que a Internet seja usada observando certas medidas.

A FEUEM e os seus departamentos dispõem de uma rede de comunicação sem fio (Wi-Fi) que é oferecida a toda comunidade académica e administrativa, em todos os ambientes com a devida autorização e que estão no limite do perímetro físico institucional. Esta rede é destinada a finalidades educacionais e administrativas da instituição.

É necessário que todos os recursos e todas as operações envolvidas na rede sejam protegidos. Deve-se garantir a protecção das informações em redes e a protecção da infraestrutura de suporte.

A norma no seu ponto 10.6.1 sugere o seguinte controle: convém que as redes sejam adequadamente gerenciadas e controladas, de forma a protege-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.

#### 1.5.1.1. Directrizes específicas sugeridas

- A Internet não pode ser usada para a divulgação de informações confidenciais
- É proibido o acesso a sites não permitidos
- É expressamente proibido o acesso a sites de conteúdos inadequados
- Os usuários só podem fazer o *download* de conteúdos ligados a instituição e/ou as actividades desta, ou seja, conteúdos académicos para o caso de estudantes, e profissionais para os funcionários e demais colaboradores.
- Devem ser estabelecidos controles especiais para a protecção da confidencialidade e integridade dos dados trafegando sobre redes públicas ou sobre redes sem fio (*wireless*) e para proteger os sistemas e aplicações a elas conectadas

### 1.5.2. Computadores e recursos tecnológicos

Os computadores e todos os recursos tecnológicos que estão disponíveis aos colaboradores e toda a comunidade institucional para a execução das actividades ou acesso a *Internet* são propriedade da FEUEM, que esta pode se reservar o direito de se necessário restringir o acesso a esses equipamentos, fazer o bloqueio de qualquer arquivo que nestes se encontra armazenado, bloquear site, correio electrónico com vista a garantir o cumprimento desta Política de Segurança da Informação.

Os laboratórios de informática existentes na FEUEM foram instalados para fins académicos, tanto que é necessário que os usuários destes, maioritariamente estudantes, façam o bom uso destes bem como dos equipamentos neles existentes. Para isso abaixo estão algumas regras e boas práticas de uso destes com vista ao cumprimento dos requisitos de segurança da informação.

#### 1.5.2.1. Directrizes específicas

- Sendo que os estudantes são os maiores usuários dos laboratórios, eles devem usá-los para fins estritamente académicos
- Se o estudante encontrar ficheiros ou pastas no computador que pretenda usar, este está proibido de apagar ou remover os mesmos para outro diretório, pois estes ficheiros são de grande importância para quem os armazenou
- Após a instalação de uma aplicação e esta não ser mais necessária, o gestor de sala deve fazer a remoção da mesma, com vista a liberar espaço de armazenamento no computador
- Se for caso de ficheiros armazenados, que constituem informação importante para o estudante que fez o armazenamento num dado computador, após o fim da vida útil daquela informação, deve se prosseguir para a fase do descarte ou destruição da informação segundo o seu ciclo de vida
- É proibida a ocupação de um computador, ou qualquer outro equipamento existente em um dado laboratório para fins não académicos. Portanto deve se limitar o tempo de ocupação da máquina por estudante
- É proibido o acesso a sites de conteúdos que não sejam académicos, o caso deste feito, o estudante é interdito a continuar usando a sala em causa por um tempo previamente determinado

- Para os usuários que tenham recursos particulares ou individuais, mesmo que façam o uso do laboratório para a realização das suas tarefas, a responsabilidade pelos seus utensílios recai para os mesmos usuários. Os utensílios do utente devem ser registados na entrada pelo gestor da sala e orientá-lo na ligação ou activação da *Internet* ou corrente eléctrica
- É necessário que todo o usuário dos laboratórios seja ciente de que os equipamentos lá disponíveis são propriedade da Faculdade de Engenharia
- É da responsabilidade de cada estudante garantir a integridade de cada equipamento, a confidencialidade bem como a disponibilidade da informação que é contida no equipamento
- Todos os utentes da sala devem assinar a ficha de presença na sala para facilitar o rastreio em caso de haver algum incidente

### 1.5.3. Correio Electrónico (E-mail)

Esta política visa definir as normas e procedimentos de utilização de e-mail, incluindo o envio, recebimento e a gestão das contas e-mail.

O que torna esta política muito necessária é o facto de que o envio de um e-mail exige a *Internet*, e esta constitui um meio público, e grande parte dos ataques chega através da *Internet*, e esta pode não estar totalmente sobre o controle do departamento das TIC's, portanto isso é necessário que seja de conhecimento de todos os utilizadores deste meio de comunicação para que façam o uso deste com precauções. Por outro lado, é notório que o e-mail tem se tornado um meio de comunicação muito usado pelas organizações ou instituições. A FEUEM não está fora dessas tendências, esta também faz algumas das suas transações electronicamente por e-mail, tomando como exemplo a transferência de informações entre os departamentos e instituições parceiras

Para esta política o controle é sugerido pela norma no seu item 10.8.1 das políticas e procedimentos para a troca de informações e, segundo este, convém que políticas, procedimentos e controles sejam estabelecidos e formalizados para proteger a troca de informações em todos os recursos de informações. Outro controle que reforça esta política está na mesma norma no item 10.8.4 que sugere que as informações que trafegam em mensagens electrónicas sejam adequadamente protegidas.

#### 1.5.3.1. Directrizes sugeridas

- Protecção das mensagens contra acesso não autorizado, modificação ou negação de serviço
- Assegurar que o endereçamento e o transporte da mensagem estejam correctos, ou seja, depois da escrita da mensagem (e-mail) é necessário que se faça uma revisão desta bem como verificar se o destinatário marcado é o correcto
- Confiabilidade e disponibilidade geral do serviço
- Aprovação prévia para o uso de serviços públicos externos, tais como sistemas de mensagens instantâneas e compartilhamento de arquivos.
- Evitar o envio de uma quantidade de mensagens que possa comprometer o desempenho da rede, ou que possa afectar o uso dos recursos da rede dos demais usuários
- Deve-se fazer a limpeza das caixas de e-mail, e periodicamente eliminar os e-mails desnecessários
- Para as mensagens recebidas, se o remetente destas é desconhecido é necessário que se tenha cuidado ao clicar em links que possam estar inclusos no e-mail
- Adicionalmente, sempre que possível é necessário que se evite o envio de e-mail para vários destinatários em simultâneo

### 1.5.4. Política de Senhas

Muitos sistemas usam as senhas como um meio de autenticação, contudo, em algum momento são tidas como perigosas pois estas dependem na maior parte das vezes do usuário do sistema, que em algum momento pode escolher senhas muito fáceis de se descobrirem. Estas validam a identidade do usuário que pretenda aceder um sistema para a realização das suas actividades. O uso inapropriado de privilégio pode ser um grande factor de contribuição para falhas ou violações de sistemas.

A norma em seu item 11.2.3 (gestão de senha do usuário) sugere o seguinte controle: convém que a concessão de senhas seja controlada através de um processo de gestão formal e sugere em seu item 11.3.1 de uso das senhas, um controle que alerta os usuários para que estes sejam solicitados a seguir as boas práticas de segurança da informação na selecção e uso das senhas.

#### 1.5.4.1. Directrizes sugeridas para a implementação

- Solicitar aos usuários a assinatura de uma declaração, para manter a confidencialidade de sua senha pessoal e das senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições da contratação;
- Garantir, onde os usuários necessitam manter suas senhas, que sejam fornecidas inicialmente senhas seguras temporárias, o que obriga o usuário a alterá-la imediatamente;
- Senhas temporárias sejam únicas para uma pessoa e não sejam fáceis de serem adivinhadas;
- As senhas nunca podem ser armazenadas nos sistemas de um computador de forma desprotegida;
- Alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- Selecionar senhas de qualidade com um tamanho mínimo que sejam:
    - Fáceis de lembrar;
    - Não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, tomando nomes, números de celulares e datas de aniversário como exemplo;
    - Isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
    - Não vulneráveis a ataques de dicionário (não consistir por exemplo em palavras inclusas no dicionário);
- Modificar senhas regularmente ou com base no número de acessos (convém que senhas de acesso a contas privilegiadas sejam modificadas mais frequentemente que senhas normais) e evitar a reutilização do ciclo de senhas antigas;

### 1.5.5. Acesso aos Sistemas e Recursos da Rede

Os sistemas de informação e o acesso a estes, bem como aos bancos de dados e todos os recursos da Faculdade de Engenharia precisam ser restritos a pessoas que tenham a devida autorização, segundo o princípio da confidencialidade. De acordo com as entrevistas que se fizeram no caso de estudo (FEUEM) notou-se que alguns sistemas de informação têm pessoas exclusivamente indicadas para que só elas

façam o uso destes para a realização das suas funções, pelo facto destes sistemas portarem dados e informações extremamente sensíveis. Mas tem acontecido que de uma vez a outra, pessoas diferentes da indicada para a gestão destes sistemas fazem o uso destes sistemas, embora é com conhecimento da pessoa indicada. Conforme os entrevistados, este facto acontece por motivos estritamente profissionais, tanto que existe uma confiança entre essas duas partes (os dois usuários do sistema). Esta é uma grande janela de vulnerabilidade, que podem comprometer os dados sigilosos que estes sistemas portam. As partes confiadas, não serão sempre confiadas, não serão sempre as mesmas. Conforme mencionado no Capítulo 2 no seu ponto 2.2.5.2, a camada humana constitui o elo mais fraco quando se trata da Segurança da Informação, deve ser a camada na qual mais se investe no que concerne à segurança. E uma maneira eficaz é fazendo o treinamento e conscientização em matérias de segurança da informação.

Para este tipo de vulnerabilidade, a norma em seu item 11.2.2 sugere o seguinte controle: convém que a concessão e o uso de privilégios sejam restritos e controlados.

#### 1.5.5.1. Directrizes sugeridas para implementação

Convém que os sistemas multiusuários que necessitam de protecção contra acesso não autorizado tenham a concessão de privilégios controlada por um processo de autorização formal.

Privilégio de cada produto de sistema e de categorias de usuários para os quais estes necessitam ser concedido, seja identificado

Privilégios sejam concedidos a usuários conforme a necessidade de uso, o acesso necessário para o desempenho de uma função deve ser mínimo

### 1.5.6. Descarte seguro das informações e mídias

No processo de destruição ou descarte da informação conforme definido no ponto 2.1.1.4 deste trabalho nas etapas do ciclo de vida da informação, é necessário que se usem procedimentos seguros para o efeito, para evitar o reuso da informação por uma outra entidade podendo ou não trazer danos à instituição. Ao nível da FEUEM não existe uma política que tem a responsabilidade de ditar normas e procedimentos de descarte da informação. Conforme consta na norma (ISO/IEC 27002:2005) numa das suas secções no ponto 10.7., convém que procedimentos apropriados sejam estabelecidos para proteger documentos, mídias magnéticas de computadores, dados de entrada e saída e documentação dos sistemas contra divulgação não

autorizada, modificação, remoção e destruição. Portanto o controle no item 10.7.1 sugere que existam procedimentos implementados para a gestão de mídias removíveis.

#### 1.5.6.1. Directrizes sugeridas

- Mídias contendo informações sensíveis sejam guardadas e destruídas de forma segura e protegida, como, por exemplo, através da incineração ou trituração, ou da remoção dos dados para uso por uma outra aplicação dentro da instituição;
- Procedimentos sejam implementados para identificar os itens que requerem descarte seguro;
- Pode ser mais fácil implementar a coleta e descarte seguro de todas as mídias a serem inutilizadas do que tentar separar apenas aquelas contendo informações sensíveis;
- Muitas organizações oferecem serviços de coleta e descarte de papel, de equipamentos e de mídias magnéticas; convém que se tenha o cuidado na selecção de um fornecedor com experiência e controles adequados;
- Descarte de itens sensíveis seja registado em controles sempre que possível para se manter uma trilha de auditoria.

### 1.5.7. Controle de acesso

Colocar senhas fortes nos Sistemas de Informação já é um avanço no que concerne à segurança, mas não deixar que nenhuma pessoa sem autorização chegue perto destes é melhor ainda.

A norma no seu ponto 9.1.2 propõe o seguinte controle: convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

#### 1.5.7.1. Directrizes para a implementação

- Convém que as permissões de acesso sejam concedidas somente para finalidades específicas e autorizadas;
- Acesso às áreas em que são processadas ou armazenadas informações sensíveis seja controlado e restrito às pessoas autorizadas;
- Os visitantes que pretendam usar umas das salas com conteúdo sigiloso devem ser acompanhados e monitorados. Ou quando estes são permitidos a

entrar em uma área considerada segura, a saída destes desta sala deve ser supervisionada;

- Aos terceiros que realizem serviços de suporte, seja concedido acesso restrito às áreas seguras ou às instalações de processamento da informação sensível quando necessário; este acesso deve ser autorizado e monitorado;
- Os direitos de acesso a áreas seguras sejam revistos e actualizados em intervalos regulares, e revogados se necessário.

### 1.5.8. Classificação da Informação

A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar de um nível adicional de protecção ou tratamento especial (ISO/IEC 27002:2005). Conforme sugerido pelo controle do item 7.2.1 da norma, convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

O nível de valor, sensibilidade e criticidade da informação podem ser facilmente percebidos quando esta for classificada segundo as categorias de classificação que constam no Capítulo 2 em seu item 2.2.2 deste trabalho, porém uma vez que a informação tem o seu tempo de vida útil segundo a última etapa do ciclo de vida da informação a constar no Capítulo 2 em seu subcapítulo 2.1.1, esta não terá a mesma classificação ao longo do tempo. Com isso convém que as directrizes de classificação incluam convenções para classificação inicial e reclassificação ao longo do tempo.

Convém que seja de responsabilidade do proprietário do activo definir a classificação de um activo, analisando-o criticamente a intervalos regulares, e assegurar que ele está actualizado e no nível apropriado.

Toda a informação precisa de uma adequada protecção, não importa o critério da classificação em que esta se enquadre. Mas importa referir que, dependendo do critério da classificação, o nível de risco em caso de quebra de segurança é diferente para cada tipo de classificação, sendo maior para aquelas informações que são tidas como internas, secretas ou confidenciais.

Quando se tratar de informações confidenciais a segurança deve ser maior, o sigilo destas deve ser absoluto e deve se garantir maior confidencialidade para elas e precisam estar sempre disponíveis para as pessoas que tenham a devida autorização para fazer a manipulação destas informações.

Para a Faculdade de Engenharia as informações que devem ser confidenciais resumem-se nas seguintes:

- Os sistemas de informação que portam dados referentes aos estudantes, funcionários e todos colaboradores da FEUEM. Estes sistemas devem ser acedidos por pessoas com a devida autorização
- As senhas – estas de forma alguma devem ser partilhadas por nenhuma circunstância, devem ser intransferíveis
- Todas as estações de trabalho
- Toda a informação estratégica, que se apresente em formato impresso, que esteja armazenado nos sistemas de informação, etc.

De um modo geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida.

### 1.5.9. Manutenção de equipamentos

O ponto 2.2.3 deste trabalho, sobre medidas de segurança faz a menção de três medidas de segurança que são aplicadas consoante a situação. Recomenda-se o uso de medidas preventivas, uma vez que estas visam controlar as ameaças e reduzir as vulnerabilidades. Evitam que danos irreparáveis aconteçam sobre os activos de informação. Neste sentido, os equipamentos que portam informações precisam de uma manutenção antes mesmo que parem de funcionar.

O controle que a norma propõe no seu item 9.2.4 sugere que os equipamentos tenham manutenção correcta para assegurar sua disponibilidade e integridade permanentes.

#### 1.5.9.1. Directrizes para implementação

A manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor, e de acordo com as especificações;

A manutenção e os consertos dos equipamentos sejam realizados somente por pessoal de manutenção autorizado;

Sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo de a manutenção ser realizada pelo pessoal da instituição ou por pessoal externo à ela; onde necessário, as informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança.

### 1.5.10. Mesa limpa e tela limpa

- Todas as informações críticas ou confidenciais, podem estar em forma de papel ou outra mídia de armazenamento, devem ser guardadas em lugar seguro quando não uso, especialmente quando o escritório está desocupado, segundo sustenta a norma no seu item 11.3.3.
- Documentos que contém informação sensível ou classificada sejam removidas de impressoras imediatamente.

## 1.6. Responsabilidades

### 1.6.1. Direcção

- A alta direcção da FEUEM tem a responsabilidade de apreciar e aprovar esta Política de Segurança da Informação
- Tomar decisões e medidas em caso de não cumprimento desta Política de Segurança

### 1.6.2. Departamento das TIC's

- Este departamento tem por responsabilidade zelar pelo cumprimento das directrizes que estão nesta PSI
- Indicar os responsáveis pela manutenção dos activos de informação
- Garantir que todos os colaboradores da FEUEM tenham acesso a esta Política de Segurança da Informação

### 1.6.3. Usuários

- Os usuários e todos os colaboradores da Faculdade de Engenharia têm a responsabilidade de conhecer a Política de Segurança seguindo todas as suas normas e directrizes.
- Adotar um comportamento seguro e ter uma boa atitude no que concerne à protecção das informações da FEUEM.

## 1.7. Sanções pelo descumprimento da Política de Segurança da Informação

Em caso de não cumprimento ou violação desta política, não se deve prosseguir com a sanção de quem a violou. Em uma primeira instância é necessário que se determine a razão, isto é, a violação pode não ter ocorrido intencionalmente, pode ter sido por um acidente, por algum erro, no pior caso por desconhecimento da política.

Como forma de minimizar o descumprimento da política é necessário que haja o devido treinamento dos usuários e todos colaboradores da Faculdade de Engenharia no que concerne a Segurança da Informação.

O treinamento e conscientização deve se fazer sempre que novos funcionários forem integrados na instituição, bem como quando novos estudantes ingressarem para que estes tenham o conhecimento da política e façam o devido cumprimento das regras e directrizes da mesma e evitar-se menos violações desta.

**Anexo 2: Guiões de Entrevistas**

**Entrevista ao Director do CIUEM – 21/06/2021**

1. Com o avanço das tecnologias de informação (TI's), a informação se torna cada vez mais importante para as organizações, e com esta importância surge uma necessidade de uma adequada protecção para a informação, e a política de segurança é um dos elementos para a gestão da segurança da informação. Existe alguma Política de Segurança da Informação em vigor ao nível da UEM?

2. Os activos (tecnológicos) da FEUEM que estão sobre supervisão/controle da CIUEM como são protegidos ou que mecanismos são usados para o controle se não for por uma Política de Segurança da Informação?

3. Sabe-se que com o avanço das tecnologias as informações das instituições estão sob constantes ameaças. Alguma vez os activos intangíveis já estiveram em uma ameaça ou sofreram algum ataque que comprometera as actividades da instituição?

4. Existe alguma capacitação da camada humana no contexto da segurança da informação ou uma conscientização destes no destaque que têm ao se tratar de Segurança da Informação ao nível da CIUEM/UEM? E como esta capacitação é feita? Até que ponto esta camada contribui como um ponto de vulnerabilidade ao nível da UEM no contexto de segurança de informação?

5. Que tipo de medidas de segurança (preventivas, prospectivas ou correctivas) são adotadas pela CIUEM em relação aos seus activos?

6. Até que ponto a falta de uma PSI constitui um problema/desafio para uma instituição de ensino superior/CIUEM?

**Entrevista ao Departamento de TIC's da Faculdade de Engenharia (Técnico do DTIC) – 17/08/2021**

1. Existe alguma Política de Segurança da Informação ao nível da FEUEM?

2. Como é feita a salva-guarda dos activos intangíveis da FEUEM?

3. Existe uma política de back up? E com que frequência este é feito?

4. Como é feita a troca de informações entre os departamentos da Faculdade?

5. O DTI's é o responsável pelas Base de Dados da Faculdade?

6. Existe uma política de emails?
    1. O email institucional é usado para fins pessoais?
    2. Com que frequência é feita a limpeza da caixa de email?
    3. Já recebeu email desconhecido e com link malicioso?
    4. Já fez o envio de email para mais de 5 destinatários em simultâneo?

7. Existe uma política de senhas para os funcionários?
    1. Com que frequência faz a troca da senha em uso?
    2. Já partilhou senha com algum colega de trabalho?
    3. A senha possui um comprimento de pelo menos 8 caracteres?
    4. Como a mesma é formada? De números, letras, caracteres especiais ou mistura?

8. Existe uma política de descarte segura das informações?

9. O que seria necessário que a Política de Segurança da Informação a propor abrangesse?

**Entrevista ao Técnico Administrativo do DEEL – 18/08/2021**

1. Tem usado o email institucional para fins pessoais?

2. Com que frequência é feita a limpeza da caixa de email?

3. Já recebeu email desconhecido e com link malicioso?

4. Já fez o envio de email para mais de 5 destinatários em simultâneo?

5. Com que frequência faz a troca da senha em uso?

6. Já partilhou senha com algum colega de trabalho?

7. A senha possui um comprimento de pelo menos 8 caracteres?

8. Como a mesma é formada? De números, letras, caracteres especiais ou mistura?

**Entrevista ao Departamento de TIC's da Faculdade de Engenharia (Técnico do DTIC) – 30/08/2021**

1. Existe alguma formação ou treinamento interno dos colaboradores com relação a questões de Segurança da Informação?

2. As contas dos funcionários são imediatamente desactivadas após o término ou suspensão do vínculo contratual?

3. Existe algum contrato de manutenção dos equipamentos ao nível da FEUEM?

4. Existe um sistema interno de combate a incêndios?

5. Em caso de queda de energia enquanto se estiver trabalhando com informações sensíveis, como garantir a continuidade das actividades?

6. Nas salas com equipamentos que portam informações críticas existem UPS's?

7. Caso haja dano resultante de fenómenos naturais existe um seguro para os equipamentos?

**Anexo 3: Secções da norma ISO/IEC 27002 e seus objectivos relacionadas às camadas de Segurança da Informação**

| Camada | Secção | Objectivos |
|---|---|---|
| Física | Gestão das operações e comunicações | Garantir a operação segura e correcta dos recursos de processamento da informação |
| | Segurança física do ambiente | Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furto ou comprometimento de activos e interrupção das actividades da organização. |
| | Controle de acesso | Controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede. |
| | Gestão de acesso | Assegurar que um enfoque consistente e efectivo seja aplicado à gestão de incidentes da segurança da informação. |
| Lógica | Aquisição, desenvolvimento e manutenção de SI's | Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrências de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou integridade das informações por meios criptográficos;<br>Garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação.<br>Reduzir riscos resultantes de exploração de vulnerabilidades técnicas conhecidas. |

| | | |
|---|---|---|
| Humana | Organizando a segurança da informação | Gerir a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação da organização, que são acedidos, processados, comunicados ou gerenciados por partes externas. |
| | Gestão de activos | Alcançar e manter a protecção adequada dos activos da organização; assegurar que a informação receba um nível adequado de protecção. |
| | Segurança em recursos humanos | Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos. |
| | Gestão de continuidade do negócio | Não permitir a interrupção das actividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso. |
| | Conformidade | Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação |
| | Política de segurança da informação | Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. |