**Relatório de aula**

No dia 25 de agosto de 2023 pelas 7:00 horas na sala de informática 1 do Instituto Industrial e comercial de Nampula iniciou-se as aulas do modulo gerir segurança de sistemas de computadores onde tivemos como tema ‘**’sistema operativo**’’ dizemos que o **sistema operativo** é um conjunto de programas cuja finalidade é de gerenciar os recursos de hardware e de software, também podemos dizer que o sistema operativo é um mecanismo que permite a interação entre o homem e a máquina. A máquina usa linguagem binaria, mas como o homem seria difícil de entender, o sistema operativo faz a interpretação e transforma na linguagem que o homem possa perceber, quando falamos do sistema operativo estamos a falar do programa mãe do sistema computacional, que sem ela as outras partes não têm como ter utilidade.

Por exemplo: quando conectamos um mouse o sistema operativo é que o reconhece através dos drives que também são pequenos programas que ajudam no reconhecimento do mouse, quando instalamos os programas no computador, para eles funcionarem é através do sistema operativo e também deve haver compatibilidade.

Quando falamos de compatibilidade é por exemplo quando temos um computador que suporta até o Windows 7 por exemplo, e nós queremos instalar o Windows 11, ele pode até instalar, mas o computador ficará lento ou mesmo não vai aceitar executa-lo.

Sabendo que é o sistema operativo que dá vida ao sistema computacional, quando ele tem falhas o nosso sistema computacional fica todo danificado, por isso é necessário zelar pela saúde do nosso sistema operativo, fazendo manutenções ou até mesmo em casos extremos fazer a reparação, usando algumas ferramentas que o próprio sistema operativo fornece como:

* Windows update;
* Windows defender;
* Windows firewall;
* Controlo de contas;
* Controlo parental;
* Copia de segurança;
* Limpeza de disco; e
* Desfragmentação do disco.

Na aula seguinte no dia 1 de setembro de 2023 pela 7:00 na sala de informática 1 do Instituto Industrial e Comercial de Nampula em que tivemos como tema ‘**’utilizar as ferramentas de segurança e** **manutenção** ‘’ e como já acima citadas, começamos por falar do **Windows update** que é uma ferramenta do sistema operativo cuja função é de fazer atualizações ou seja buscar versões atualizadas de programas. Para acessar ao Windows update primeiro acessamos as definições do computador de seguida acessar a atualizações e segurança, mas antes de fazer qualquer atualização é recomendado primeiro activar o ponto de restauração que é ele que guarda as configurações que estão naquele momento antes da instalação, para que quando algo aconteça possamos recuperar as informações ou mesmo devolver o sistema do jeito que estava.

De seguida falamos do **Windows defender**, que também é uma ferramenta de segurança e manutenção do sistema operativo que tem a função de defender o sistema computacional contra vírus ou resumidamente e um antivírus. Para acessar ao Windows defender seguimos os mesmos procedimentos para o Windows update, acessamos as atualizações e segurança e por fim a segurança do Windows.

O Windows defender apresenta algumas opções de analises nomeadamente:

* **Analise rápida** – verifica as pastas do sistema nas quais são encontradas normalmente ameaças.
* **Analise completa** – verifica todos ficheiros e programas em execução no disco rígido, esta análise é um pouco demorada.
* **Analise personalizada** - escolhe os ficheiros e localização que pretende verificar
* **Analise offline da Microsoft** – diz que alguns softwares maliciosos podem ser difíceis de remover do seu dispositivo, o Microsoft defender offline pode ajudar a localizar e remover os mesmos utilizando definições de ameaças atualizadas.

Também falamos do **Windows firewall** como o próprio nome já diz ‘’parede de fogo’’. A firewall é uma espécie de barreira de defesa, que tem o objetivo de bloquear o trafego de dados indesejados, esta barreira pode ser implementada como hardware ou software.

No dia 8 de setembro demos continuidade com o tema ‘’ utilizar as ferramentas de segurança e manutenção’’ demos continuidade falando do **controlo de contas**, Contas do usuário permite que uma pessoa tenha acesso a um ambiente de trabalho pessoal. Para entrar é necessário introduzir um nome para a conta e uma senha, as contas de usuários são criadas pelo administrador do computador, que será responsável em permitir acesso para outras pessoas.

De seguida falamos do **controlo parental** que é um mecanismo para controlar o acesso a diferentes sites, sistemas operativos ou comutadores, por meio do controlo parental, e possível monitorar o acesso a sites, bloquear conteúdos impróprios para a idade, determinar o tempo de tela e limitar ou restringir compras, mensagem e uso de câmeras.

**Copia de segurança** ou backups são definidos como um registro duplicados dos dados contidos nas suas bases de dados. Essas informações podem ser enviadas para uma pasta no seu próprio computador, para a nuvem ou para um dispositivo externo. A principal função desta ferramenta é poder conceder proteção aos dados para que quando precise usa-los os tenha disponíveis.

Um exemplo de armazenamento em nuvem é o google drive, que nos permite fazer backup de informações dos nossos telemóveis ou computadores gratuitamente.

**Limpeza de disco**, devemos fazer a limpeza do disco porque quando usamos o PC, tem certos ficheiros que ficam de formas residuais que por algum momento atrapalha no processo do bom funcionamento do computador permite localizar os programas, ver quanto espaço em disco eles ocupam e remove-los para libertar espaço no disco rígido.

Para fazer a limpeza do disco, acessamos este PC, normalmente fazer a limpeza do disco na partição onde contêm o sistema operativo, damos um clique e clicamos em propriedades.

**Desfragmentação do disco** é uma ferramenta presente no sistema operativos que permite analisar o status e desfragmentar unidades de disco rígido tornando o computador mais rápido e eficiente.

No dia 15 de setembro de 2023 pelas 7:00 horas na sala de informática 1 do Instituto Industrial e Comercial de Nampula falamos dos ataques **DOS** (ataque de negação) é um tipo de ataque cibernético em que um actor malicioso tem por objetivo tornar um computador ou outro dispositivo para os usuários a que se destinam, ou seja a ideia deste ataque é derrubar um servidor para coloca-lo fora do ar. Uma das coisas que acontece no ataque DOS é usar uma série de computadores como Bot net para atacar um determinado Host, desta forma pelo servidor estar a receber uma série de informações em simultâneo acaba entrando em Dead look.

No dia 22 de setembro pelas 7:00 horas na sala de informática do instituto industrial e comercial de Nampula tivemos como tema ‘’ instalação de antivírus’’ dizendo que um antivírus e um software que identifica e protege os dispositivos de malwares também conhecidos como vírus. Esses programas podem ser instalados em computadores e dispositivos moveis como celulares e tablets.

A função mais simples de um antivírus e monitorar arquivos e outros programas de um dispositivo para detectar vírus.

**Considerações** **finais**

Chegando ao fim da elaboração do meu relatório da aula do modulo gerir segurança de sistemas de computadores falarei um pouco do impacto no processo de formação que proporciona na minha vida estudantil, de principio dizer que a informática não foi no curso que sempre quis fazer mais por outros motivos tive que fazer e levei isso como um desafio em minha vida, mas depois de um tempo me adaptei com a ideia e acabei me apaixonando pelo curso e isso tem trazido impactos positivos em minha vida, novos conhecimentos como por exemplo na aula do modulo gerir segurança de sistemas de computadores deu para ter o conhecimento primeiro o que e um sistema operativo e ter também o conhecimento que devemos zelas pelo bem estar dele, porque se o sistema operativo estiver danificado as outras partes do computador não terá como ter utilidade. Usamos algumas ferramentas para a sua manutenção e o outro impacto positivo foi a aprendizagem da instalação do antivírus.