**Relatório de aulas do Modulo:** Gerir Segurança de Sistemas de Computadores

O presente relatório visa abordar com relação ao primeiro e o terceiro resultado de aprendizagem do modulo de: Gerir Segurança de Sistemas de Computadores, os critérios de desempenho abordados foram:

* Identificar as principais caraterísticas de segurança e manutenção do sistema operativo
* Utilizar as ferramentas de segurança e manutenção do sistema operativo;
* Udape
* Windows defender
* Controlo contas
* Controlo de parental
* Limpeza do disco e desfragmentação do disco;
* Copia de segurança
* Configurar ferramentas de segurança, nomeadamente antivírus;

No dia 01 e 8 de setembro de 2023, ocorreu primeira sessão no Instituto Industrial e Comercial de Nampula pelas 7:00 que abordou - se sobre o sistemaoperativo, caraterísticas do sistema operativo e sua função assim como fazer a manutenção do próprio sistema operativo. Definiu - se o sistema operativo como é a alma de um computador e que ele é indispensável para o computador porque é o sistema operacional que dá vida a um computador. De seguida fez se a manutenção do Windows:

**Desfragmentação do disco**

A desfragmentação do disco é um processo de otimização que visa o melhor desempenho de um disco rígido ou uma unidade de estado solido do computador.

Abordou-se também que se podemos encontrar diversas formas para a execução do Windows Update, segue aqui em baixo uma das formas:

Selecione Iniciar > Configurações > Windows Update e exiba as atualizações disponíveis. Execute a Solução de problemas do Windows Update. Selecione Iniciar > Configurações > Sistema > Solução de problemas > outros solucionadores de problemas. Em Mais frequente, selecione Windows Update.

Abordamos também sobre Microsoft Defender (também conhecido como Windows Defender  que é um [software](https://pt.wikipedia.org/wiki/Software) que remove [malware](https://pt.wikipedia.org/wiki/Malware" \o "Malware), Trojan, [spyware](https://pt.wikipedia.org/wiki/Spyware) e [adware](https://pt.wikipedia.org/wiki/Adware) instalados no computador.

O Windows Defender foi projetado para que o utilizador remova um spyware ou um software potencialmente indesejado de forma simples.

O programa é composto por opções de verificação (cujos tempos de verificação são proporcionais à qualidade da mesma), opções de registo (em que o utilizador acede às suas acções em relação a execução de certos itens) e também as acções automáticas do Windows Defender, ferramentas que configuram ou ajudam a remover spywares, atualizações que restauram o banco de dados para aumentar a capacidade de deteção do programa em relação aos itens por ele verificados. Possui informações que auxiliam na personalização correta, exibindo quando foi a última verificação e qual o seu tipo, mostrando a data da verificação automática (que é possível configurar); informando o status da proteção em tempo real (descativado ou ativado) e exibe a versão das definições e quando foram criadas. O Windows Defender dispõe também de verificações que podem ser configuradas pelo usuário, podemos encontrar 4 delas:

**Verificação em Tempo Real**

A proteção em tempo real actua na inicialização do sistema, na configuração do sistema, nos complementos, downloads e configurações do [Internet Explorer](https://pt.wikipedia.org/wiki/Internet_Explorer), na execução de serviços e drivers, em execução e registo do aplicativo, e nos complementos do Windows

**Verificação Rápida**

Uma verificação rápida analisará somente as áreas do computador que possuem mais chances de serem infetadas por spywares e outros softwares potencialmente indesejados. Essa verificação não é a mais segura, pela a razão de verificar somente nas pastas principais do sistema.

**Verificação Completa**

Uma verificação completa verificará todos os arquivos do disco rígido e todos os programas em execução no momento, essa análise pode reduzir bastante a performance do computador até a conclusão da verificação.

**Verificação Personalizada**

O utilizador seleciona locais específicos do computador para serem verificados. No entanto, se um software potencialmente indesejado ou mal-intencionado for detectado, o Windows Defender executará uma verificação rápida para que os itens detetados possam ser removidos de outras áreas do computador, se necessário.

O registo no Windows Defender guarda automaticamente as autorizações de execução pelo utilizador e os itens em quarentena com:

**Itens Permitidos**: as configurações de execução serão permitidas pelo utilizador do grupo Administrador. Se confiar no software detectado pelo Windows Defender, poderá impedir que o Windows Defender dê o alerta sobre os riscos que o software pode representar no computador. Para não receber mais alertas, o software deverá ser adicionado à lista de permissões. Se você escolher que deseja monitorizar o software novamente mais tarde, poderá removê-lo da lista de permissões do Windows Defender.

**Itens em Quarentena**: as configurações de quarentena serão permitidas pelo o utilizador do grupo Administrador. Ao o Windows Defender colocar um software em quarentena, ele o move para outro local do computador (pasta do Windows Defender) e, em seguida, impede que o software seja executado até que o utilizador decida restaurá-lo ou removê-lo do computador. E pode ser um bom programa para ser usado como "Antivírus".

Na semana a seguir falamos sobre O **Windows Firewall** é um componente do [Microsoft Windows](https://pt.wikipedia.org/wiki/Microsoft_Windows) que oferece [firewall](https://pt.wikipedia.org/wiki/Firewall) e filtragem de pacotes e funções. Foi incluído pela primeira vez no [Windows XP](https://pt.wikipedia.org/wiki/Windows_XP) e [Windows Server](https://pt.wikipedia.org/wiki/Windows_Server) 2003. Antes do lançamento do Windows XP Service Pack 2 em 2004, era conhecido como **Internet Connection**

**Firewall**.

Como função o próprio nome incita, a firewall serve para impedir que um “incêndio” se propague para outros ambientes, protegendo assim as pessoas e a própria construção. No caso de sistemas ou rede, a ferramenta trabalha para prevenir que malwares se espalhem e infectem outros dispositivos

**Controle parental**

 É um conjunto de ferramentas que dá aos pais a possibilidade de controlar e restringir ações das crianças durante a navegação pela internet.

E para finalizar o primeiro resultado, falamos sobre a limpeza de disco e desfragmentação do disco onde abordávamos sobre a limpeza de disco e desfragmentação da mesma. Dizíamos que a limpeza de disco é um utilitário de

No da 22 de setembro de 2023 entramos ao terceiro resultado, que decorreu no instituto industrial e comercial de Nampula pelas 7. falamos sobre ferramentas de segurança. Onde o resultado pede para instalar e configurar uma ferramenta de segurança, (antivírus). Passo em seguida a explicar como instalar um antivírus (Kaspersky).

1. Abra a janela principal do aplicativo do Kaspersky Internet Security ou Kaspersky Total Security.
2. Clique no botão Mais ferramentas. ...
3. Clique no link Conexão segura para abrir a janela Conexão segura.
4. Clique no botão Baixar e instalar.
5. Siga as instruções do assistente.

Com relação as sessões realizadas afirmou – se que eram muito importantes, além de facilitar a busca de conhecimentos, agilidade e na troca de Informação conseguiu – se perceber alguns conteúdos que decorreram nas sessões como: Utilizar as ferramentas de segurança e manutenção do sistema operativo, Limpeza do disco e desfragmentação do disco; Identificar as principais caraterísticas de segurança e manutenção do sistema operativo entre outros.

Durante as sessões que decorreram, nem todos os conteúdos bordados foram com sucesso porque houve um problema de como criar conta porque não tinha senha de administrador, para poder criar novas contas e também houve um problema na hora de instalar o antivírus porque o aplicativo não era grátis.