Listado de cosas esenciales para la seguridad informática:

•**Protección de Software y Accesos:**

•**Antivirus/Antimalware:** Instalado y actualizado para detectar amenazas.

•**Firewall:** Configurado para controlar el tráfico entrante/saliente. **NMAP (cerrar todo noooooo nooo)**

•**Contraseñas fuertes:** Únicas, largas y complejas (mayúsculas, minúsculas, números, símbolos).

•**Autenticación en dos pasos (2FA):** Obligatoria en cuentas importantes.

•**Gestor de contraseñas:** Para almacenar claves de forma segura, sin usar notas o archivos de texto.

•**Bloqueo de pantalla:** Automático al no usar el equipo.

•Chrome o similares con sus extensiones

• Cuidado con las descargas (engaños) NO USAR EL DISPOSITIVO EN MODO ADMINISTRADOR

•Soft pirata... NUNCA JAMÁS

•**Mantenimiento y Datos:**

•**Actualizaciones de software:** Sistema operativo y programas siempre al día para parches de seguridad.

•**Copias de seguridad (Backups):** Periódicas, cifradas y almacenadas en un lugar seguro (nube o disco externo).

•**Cifrado de disco (Disk Encryption):** Para proteger datos si el equipo es robado.

•**Borrado seguro:** De información sensible al desechar equipos o discos.

•**Navegación y Redes:**

•**Navegación segura (HTTPS):** Correo, ssh, ftp Verificar candado en la barra de direcciones.

•**VPN (Red Privada Virtual):** Especialmente al usar redes Wi-Fi públicas.

•**Seguridad Wi-Fi:** Uso de protocolos robustos (WPA3/WPA2) en la red doméstica.

•**Buenas Prácticas de Usuario:**

•**Desconfiar del Phishing:** No abrir enlaces ni archivos adjuntos sospechosos en correos o mensajes.

•**Evitar USBs desconocidos:** Escanear memorias externas antes de abrir archivos.

•**Limitar privilegios:** No usar cuentas con permisos de administrador para tareas diarias.

•**Descargar software seguro:** Solo desde repositorios y sitios web oficiales.

•**Físico:**

•**Seguridad física:** Candados Kensington, ubicaciones seguras, control de acceso físico a los equipos