Con ayuda de los estudiantes, determinar qué herramientas de software se suelen utilizar para la ofimática, el dibujo y la edición multimedia.

**1. Ofimática (procesadores de texto, hojas de cálculo, presentaciones)**

| **Programa** | **Tipo** | **Costo Licencia** | **Alternativa Libre** |
| --- | --- | --- | --- |
| Microsoft Office (Word, Excel, PowerPoint) | Comercial | Desde $69.99 USD/año (Office 365 Personal) | LibreOffice, OnlyOffice, WPS Office |
| Google Docs/Sheets/Slides | Gratuito (en la nube) | Gratis (con cuenta Google) | LibreOffice Online |
| Apple iWork (Pages, Numbers, Keynote) | Gratuito | Gratis en dispositivos Apple | LibreOffice |

Listar los programas de diseño y ofimática más populares e investigar el costo de la licencia.

**2. Dibujo (Ilustración, diseño gráfico, técnico)**

| **Programa** | **Tipo** | **Costo Licencia** | **Alternativa Libre** |
| --- | --- | --- | --- |
| Adobe Illustrator | Comercial | Desde $22.99 USD/mes | Inkscape |
| CorelDRAW | Comercial | Desde $269 USD anual | LibreCAD, Vectr |
| AutoCAD | Comercial | Desde $1,865 USD/año | FreeCAD, LibreCAD |

Buscar qué alternativas de software libre hay en el mercado para cada alternativa.

**3. Edición multimedia (imagen, audio, video)**

| **Programa** | **Tipo** | **Costo Licencia** | **Alternativa Libre** |
| --- | --- | --- | --- |
| Adobe Photoshop | Comercial | Desde $22.99 USD/mes | GIMP |
| Adobe Premiere Pro | Comercial | Desde $22.99 USD/mes | DaVinci Resolve (versión básica gratuita), Kdenlive, Shotcut |
| Audacity | Libre | Gratis | (Es en sí mismo una alternativa libre) |

Pregunte a los estudiantes qué tan seguras son las contraseñas que utilizan para sus activos digitales (correos, cuentas en aplicaciones gratuitas o pagas).

1. **¿Qué tan seguras son tus contraseñas?**
   * ¿Cuántos caracteres tienen?
   * ¿Incluyen letras mayúsculas, minúsculas, números y símbolos?
2. **¿Utilizas la misma contraseña para todo?**
   * ¿Mismo usuario + misma contraseña en todos los sitios?
3. **¿Qué pasa si una contraseña se filtra en un sitio de baja seguridad?**
   * Acceso no autorizado a tus redes sociales, correos, bancos, etc.
   * Robo de identidad.
   * Pérdida de datos o publicaciones ofensivas a tu nombre.
4. **¿Tu contraseña está basada en datos personales fáciles de adivinar?**
   * Nombre de un familiar, mascota, fechas de cumpleaños, 12345, etc.

¿Utilizan la misma contraseña y el mismo usuario para todo? ¿Qué pasaría si en un sitio con seguridad pobre, las contraseñas son expuestas?

Utilizar **contraseñas seguras y únicas** para cada servicio.

Usar un **gestor de contraseñas** como Bitwarden o KeePass.

Activar el **doble factor de autenticación (2FA)** en:

* Gmail
* WhatsApp
* Instagram, Facebook
* Cuentas bancarias
* Plataformas educativas