

## Actividad 2: Uso de software libre y licencias

## UNIDAD 2

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

Listar los programas de diseño y ofimática más populares e investigar el costo de la licencia. Buscar qué alternativas de software libre hay en el mercado para cada alternativa. Pregunte a los estudiantes qué tan seguras son las contraseñas que utilizan para sus activos digitales (correos, cuentas en aplicaciones gratuitas o pagas).

¿Utilizan la misma contraseña y el mismo usuario para todo?

No, dependiendo la plataforma uso contraseñas diferentes y extensas, sin nombres y números conocidos como fechas de cumpleaños o de familiares.

¿Qué pasaría si en un sitio con seguridad pobre, las contraseñas son expuestas?

La exposición de contraseñas en un sitio con medidas de seguridad deficientes desencadenaría una crisis multidimensional. Para los usuarios, implicaría un alto riesgo de robo de identidad, ya que muchos reutilizan contraseñas en múltiples plataformas, permitiendo a los atacantes acceder a cuentas bancarias, correos electrónicos o redes sociales vinculadas. Además, podrían sufrir fraudes financieros (si el sitio almacenaba datos de pago), extorsiones (en casos de servicios sensibles) o ataques de phishing personalizados. Para la empresa responsable, las consecuencias incluirían multas millonarias por incumplir regulaciones como el GDPR, pérdida masiva de clientes por desconfianza, y un daño reputacional permanente que afectaría sus alianzas comerciales.

¿Son las contraseñas combinaciones de sus nombres, números en secuencia, combinaciones de nombres de los familiares y /o fechas de nacimiento?

No, las contraseñas basadas en nombres propios, fechas de nacimiento o nombres de familiares no son seguras, ya que son extremadamente vulnerables a ataques de fuerza bruta y diccionario, siendo descifradas dependiendo la extensión de la contraseña, la velocidad de procesamiento de la máquina, pero puede que no tarde tanto en descifrar la contraseña, si se tiene una buena máquina de ataque. Los cibercriminales utilizan herramientas automatizadas como diccionarios que tienen claves por defectos como "Daniel123" o "Daniel1990"), información disponible públicamente en redes sociales

De ser así, debatan sobre la necesidad de actualizar y dar mantenimiento a sus contraseñas para evitar la pérdida de información.

Pida a los estudiantes que activen el doble factor de autenticación en servicios como Whatsapp.