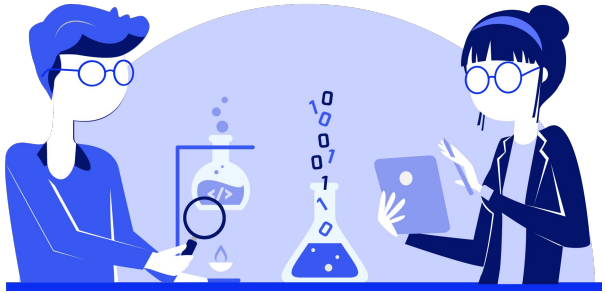
educación IT
CODE YOUR FUTURE

# Criptografía y Blockchain

## Módulo 4 - Laboratorio adicional

# Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.



# Ejercicio 1

## Algoritmos post cuánticos

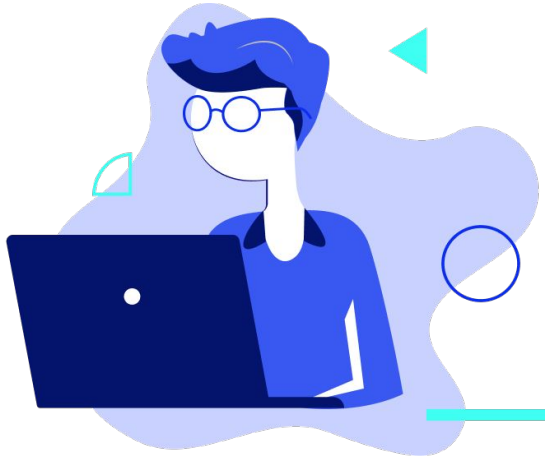
La versión de **openSSL** cargada en la máquina virtual de Kali Linux no es la versión estándar. Tiene incorporada la biblioteca de ***liboqs*** para trabajar con algoritmos post cuánticos mediante **`oqsprovider`**.

1. Verificar los algoritmos de firma soportados:

```
-$ openssl list -signature-algorithms -provider oqsprovider
```

2. Verificar que se encuentra disponible el algoritmo **`dilithium3`**.
3. Utilizar lo aprendido en los módulos anteriores para crear una clave privada `dilithium3`. Mostrarla en la consola.

4. Crear la clave pública `dilithium3`. Mostrarla en la consola.
5. Crear un archivo de texto y  firmarlo con la clave privada `dilithium3`. Guarde la firma.
6. Verificar la firma.
7. Modificar el archivo firmado y comprobar que la verificación de la firma falla.



# Ejercicio 2

## Algoritmos KEM

1. Verificar los algoritmos KEM soportados:

```
-$ openssl list -signature-algorithms -provider oqsprovider
```

2. Verificar que se encuentra disponible el algoritmo `kyber768` con clave ECDSA y curva x25519.

3. En el sitio web de Open Quantum Safe verificar el puerto que acepta intercambio de claves con este algoritmo.

4. Conectar con el servidor con el comando:

```
openssl  s_client -groups  <algoritmo>
-connect  <server:puerto>
```

5. Verificar que la conexión es exitosa.

# ¡Sigamos trabajando!