

## Parte 3: Preguntas sobre Telnet, SSH y diferencias entre ambos

### Instrucciones:

Con tu grupo reflexiona sobre las siguientes preguntas relacionadas con los protocolos Telnet, SSH y las diferencias entre ellos:

#### Telnet:

a) Pregunta: ¿Cuáles son las ventajas y desventajas de utilizar el protocolo Telnet?

R: Las ventajas son que te puedes conectar a algún servidor remotamente, la desventaja es que es una conexión no encriptada.

b) Instrucciones: Responde la pregunta en base a tu conocimiento y experiencia. Menciona al menos dos ventajas y dos desventajas de utilizar Telnet como protocolo de acceso remoto.

Ventajas: Poder acceder a equipos remotamente, casi todas las plataformas lo tienen incorporado.

Desventajas: Conexión no segura. No todos los servidores permiten el uso de Telnet.

#### SSH:

a) Pregunta: ¿Cuáles son las ventajas y desventajas de utilizar el protocolo SSH?

Poder acceder a servidores remotamente de manera segura, ya que los datos van encriptados.

b) Instrucciones: Responde la pregunta en base a tu conocimiento y experiencia. Menciona al menos dos ventajas y dos desventajas de utilizar SSH como protocolo de acceso remoto.

Ventajas: Tiene capa de encriptación. Todos los servidores actuales lo incorporan ya que es seguro.

Desventajas: Es a través de línea de comandos.

#### Diferencias entre SSH y Telnet:

a) Pregunta: ¿Cuáles son las principales diferencias entre SSH y Telnet?

La seguridad, SSH es seguro y Telnet no lo es.

b) Instrucciones: Responde la pregunta destacando al menos tres diferencias clave entre SSH y Telnet en términos de seguridad, cifrado de datos y características funcionales.

Autenticación. SSH utiliza un cifrado de clave pública como modo de autenticación, Telnet no tiene ningún mecanismo.

Puertos: SSH usa el puerto 22, pero se puede cambiar al que se requiera para mayor seguridad. Telnet usa por defecto el puerto 23.

Seguridad: Telnet no es seguro, SSH utiliza mecanismos de cifrado para la seguridad.