

**Enviar una cadena segura
(System.Security.SecureString)
entre un cliente y un
servidor cifrando la
comunicación mediante el
protocolo TCP/IP desde
PowerShell utilizando un
certificado X509 autofirmado
creado desde OpenSSL**

**Servidor que envía una cadena
segura cifrando la comunicación**

Utiliza un certificado X509 generado desde OpenSSL
<https://www.jesusninoc.com/03/13/crear-un-certificado-pfx-con-openssl-desde-powershell/>

[crayon-6a9d6954c632c525098102/]

**Cliente que recibe una cadena
segura**

Utiliza un certificado X509 generado desde OpenSSL
<https://www.jesusninoc.com/03/13/crear-un-certificado-pfx-con-openssl-desde-powershell/>

[crayon-6a9d6954c6332216760127/]

Resultado

The image displays two side-by-side screenshots of the Windows PowerShell ISE (Integrated Scripting Environment) interface, showing the execution of a script for secure communication over a network.

Left Window (Server Side):

- Script:** The script defines a certificate, a port (1236), a TCP listener, and an SSL stream. It accepts a TCP client connection, authenticates the server, and creates a message stream. It then receives a password from the client, writes it to the stream, and disposes of the stream and listener.
- Output:** The output shows the message stream being created, the password being received, and the stream being disposed. It also shows the TCP listener stopping and the command prompt prompt.

Right Window (Client Side):

- Script:** The script connects to the server (127.0.0.1, 1236), gets the stream, and creates an SSL stream. It authenticates the client, receives the certificate from the server, and writes the output. It then reads the message stream, converts it to a secure string, and outputs the plain password.
- Output:** The output shows the TCP client connecting, the stream being created, the certificate being received, and the plain password being output. It also shows the message stream being read, the secure string being converted, and the plain password being output.