

<b>Nombre de la práctica</b>	<b>Practica: Instancia W2019S y conexión remota desde escritorio remoto</b>			<b>No.</b>	<b>7</b>
<b>Asignatura:</b>	<b>Administración de Redes</b>	<b>Carrera:</b>	<b>INGENIERÍA EN SISTEMAS COMPUTACIONALES</b>	<b>Duración de la práctica (Hrs)</b>	<b>2 horas</b>

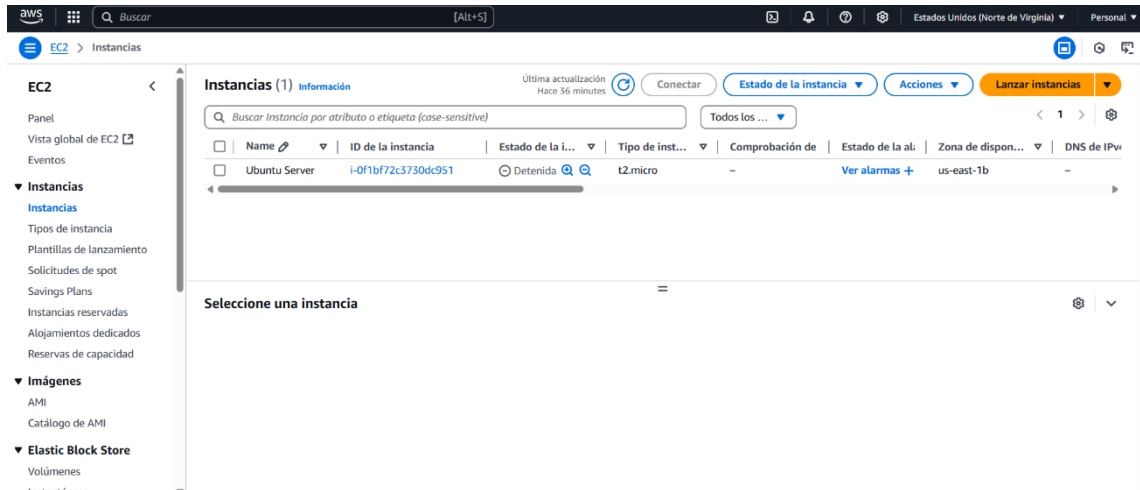
**GRUPO: 3601**

**NOMBRE: Vanesa Hernández Martínez**

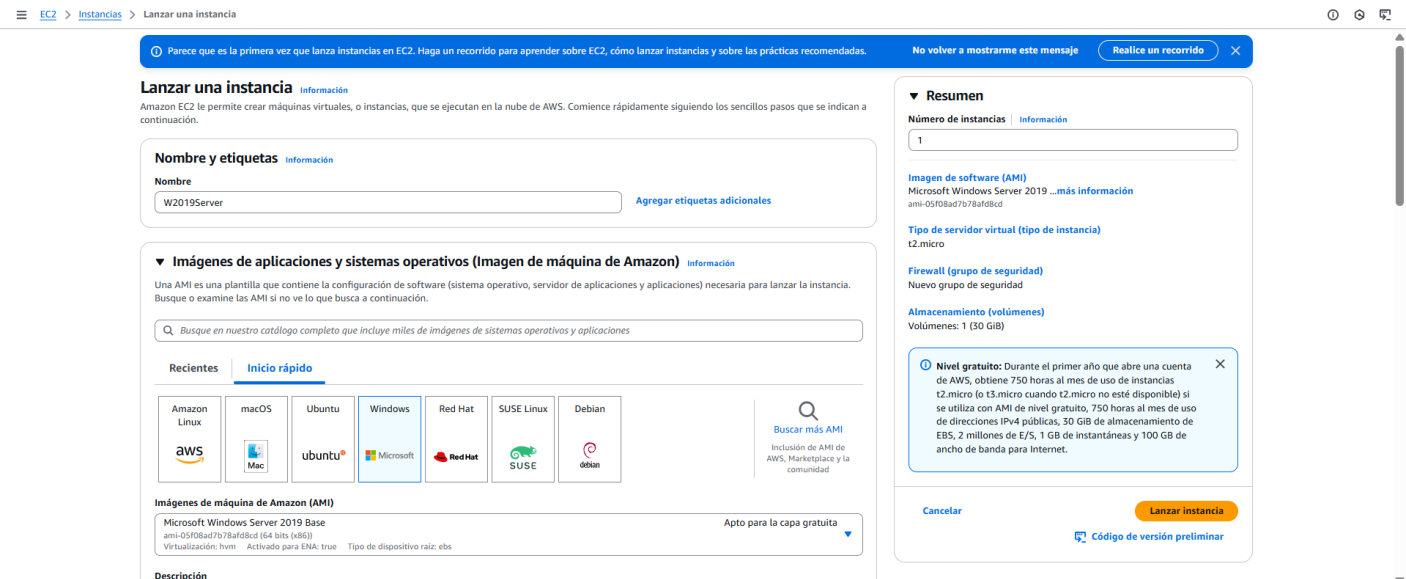
## Encuadre con CACEI

No. atributo	Atributos de egreso del PE que impactan en la asignatura	Criterio de desempeño	Indicadores	
A2	El estudiante diseñará esquemas de trabajo y procesos, usando metodologías congruentes en la resolución de problemas de ingeniería en sistemas computacionales	CD1. IDENTIFICA METODOLOGÍAS Y PROCESOS EMPLEADOS EN LA RESOLUCIÓN DE PROBLEMAS	I1	IDENTIFICACION Y RECONOCIMIENTO DE DISTINTAS METODOLOGIAS PARA LA RESOLUCION DE PROBLEMAS
			I2	MANEJO DE PROCESOS ESPECIFICOS EN LA SOLUCION DE PROBLEMAS Y/O DETECCION DE NECESIDADES
		CD2 DISEÑA SOLUCIONES A PROBLEMAS, EMPLEANDO METODOLOGÍAS APROPIADAS AL AREA	I1	USO DE METODOLOGIAS PARA EL MODELADO DE LA SOLUCION DE SISTEMAS Y APLICACIONES
A7	El estudiante desarrolla proyectos y trabajos en equipo basándose en metodologías preestablecidas para lograr mayor calidad y eficiencia.	CD2. ASUME SU RESPONSABILIDAD EN EL DESARROLLO DE TRABAJOS Y/O PROYECTOS EN EQUIPO Y EN LA ENTREGA DE RESULTADOS	I1	PARTICIPACIÓN ACTIVA EN EL DESARROLLO DE TRABAJOS Y PROYECTOS EN EQUIPO
			I2	DIRIGIR Y ORGANIZAR TRABAJO EN EQUIPO
			I3	PRESENTACION Y/O EXPOSICION DE TRABAJOS Y PROYECTOS EN EQUIPO

1. Entramos a aws con nuestra cuenta en la sección de instancias para dar clic en el botón amarillo que dice **“Lanzar instancias”**

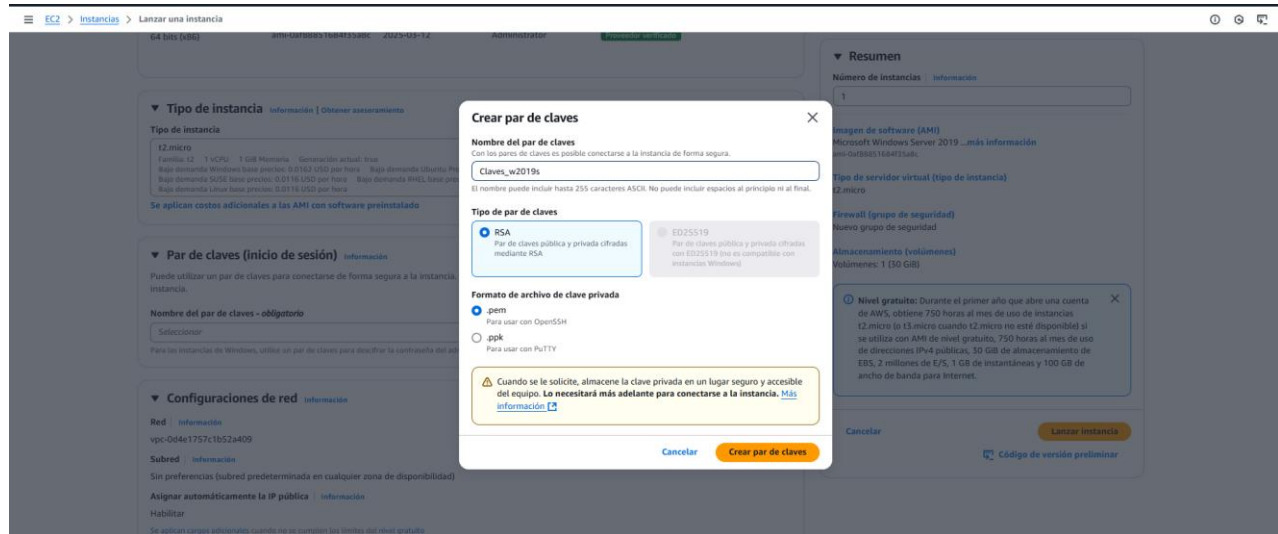


2. Colocamos el nombre a la instancia de W2019Server, que sea 1 instancia, de **Windows server 2019 base**.

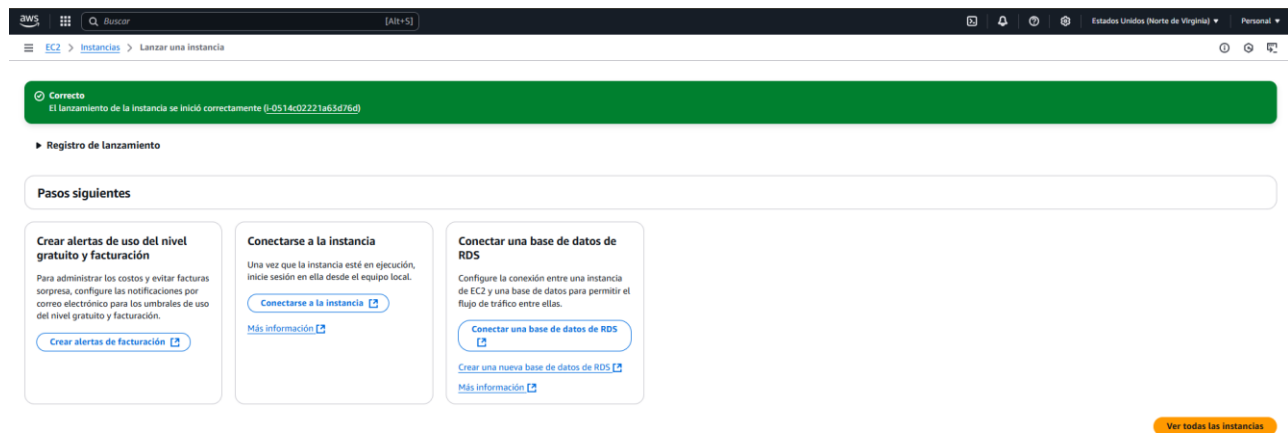




3. Generamos nuestro par de claves que nos servirán mas adelante para conectarnos remotamente.



4. Si la instancia se creo correctamente nos aparecerá la siguiente pantalla en la cual debemos de dar clic en el botón de “Ver todas las instancias”



5. Esto nos llevara a que en la sección de instancia ya podamos ver la nueva instancia creada.

The screenshot shows the AWS Management Console interface. On the left, there is a navigation menu with categories like EC2, IAM, and Elastic Block Store. The main content area displays the details of a security group. The 'Reglas de entrada' (Inbound rules) tab is selected, showing a table with one rule. The rule has an ID of 'sgr-0eab8022eef2e8911', is of type 'RDP', and allows traffic from '0.0.0.0/0' on port '3389' using the 'TCP' protocol.

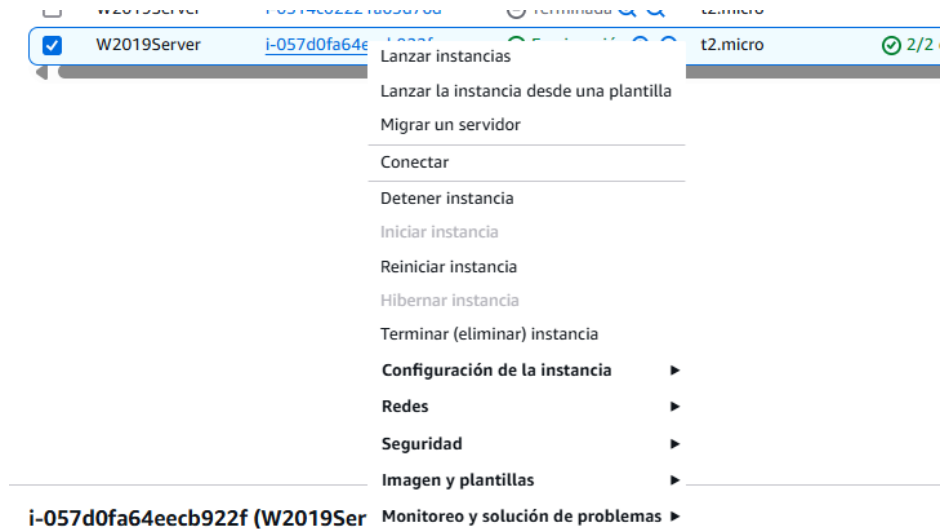
ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
sgr-0eab8022eef2e8911	RDP	TCP	3389	0.0.0.0/0	-

6. Primero revise si en la seguridad que la instancia ya tenga la regla 3389 que es la que permite la conexión remota.

The screenshot shows the 'Editar reglas de entrada' (Edit inbound rules) page in the AWS Management Console. It displays a form for adding or editing inbound rules. The rule ID is 'sgr-0eab8022eef2e8911'. The rule type is 'RDP', the protocol is 'TCP', and the port range is '3389'. The source is set to 'Persona...' (Personal). There is a search bar and a button to 'Agregar regla' (Add rule). A warning message at the bottom states: 'Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.' (Rules whose origin is 0.0.0.0/0 or ::/0 allow all IP addresses to access the instance. We recommend configuring security group rules to allow access only from known IP addresses.)



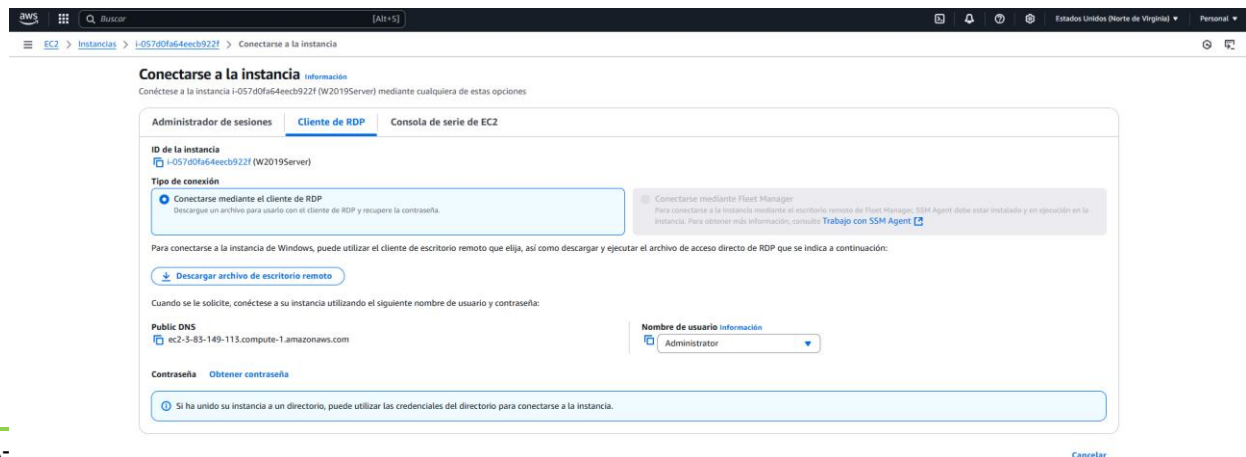
7. Hago clic sobre el nombre de la instancia y selecciono la opción de conectar.



8. Abriré la siguiente pantalla, pero nos tenemos que dirigir a el segundo apartado que se llama “Cliente de RDP”



9. Nos aparecerá la siguiente pantalla en la cual daremos clic en descargar archivo de escritorio remoto y en obtener contraseña.



10. Eso nos abrirá un apartado en el cual tendremos que cargaran las claves que se nos generaron al momento de crear la instancia.

EC2 > Instancias > i-057d0fa64eeeb922f > Obtener la contraseña de Windows

### Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia  
i-057d0fa64eeeb922f (W2019Server)

Par de claves asociado a esta instancia  
Claves\_W2019Server

Clave privada  
Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.


[Cargar archivo de clave privada](#)

Contenido de la clave privada: *opcional*

Contenido de la clave privada

[Cancelar](#) [Descifrar contraseña](#)

11. Cuando las claves esten subidas, daremos clic en descifrar contraseñas.

aws   [Alt+S]

EC2 > Instancias > i-057d0fa64eeeb922f > Obtener la contraseña de Windows

### Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia  
i-057d0fa64eeeb922f (W2019Server)

Par de claves asociado a esta instancia  
Claves\_W2019Server

Clave privada  
Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.

[Cargar archivo de clave privada](#)

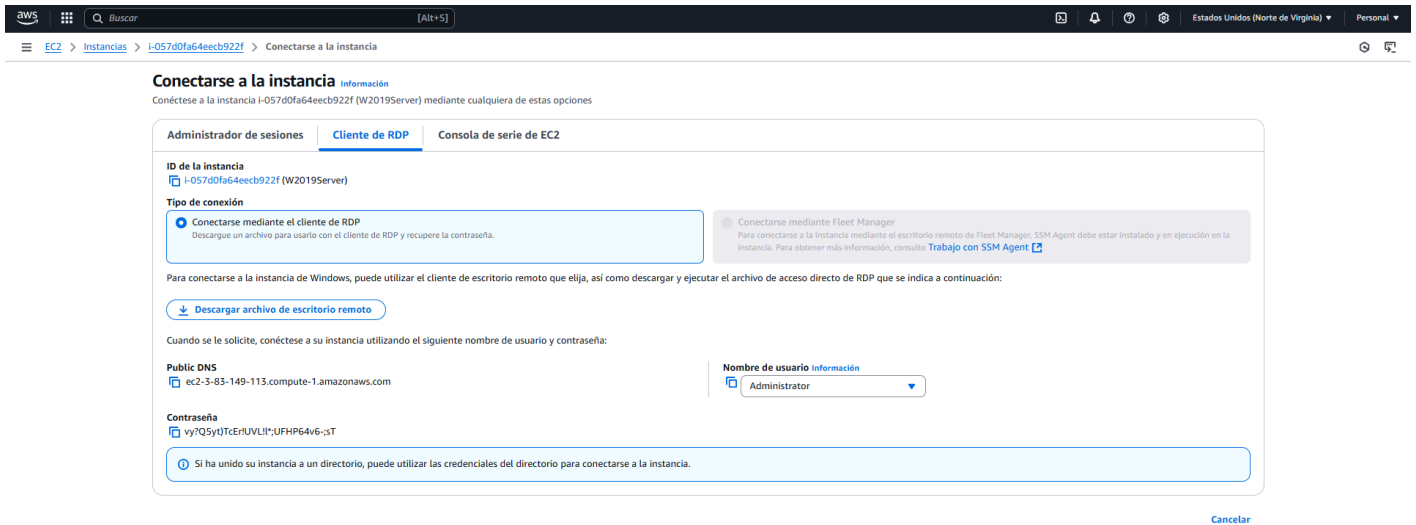
Claves\_W2019Server.pem  
1.678KB

Contenido de la clave privada: *opcional*

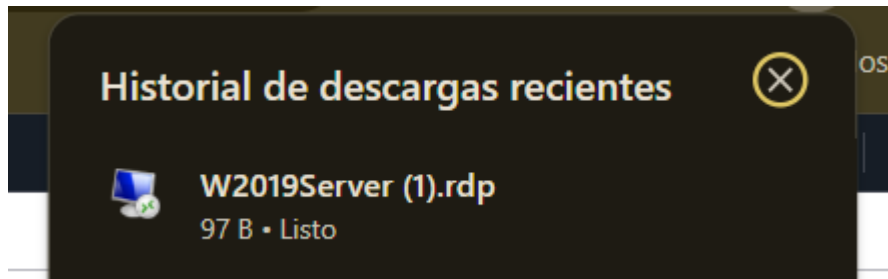
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2w6lQUR3E9Hva1u36TlVlvaqmNR2XqQPD+gpxXalIGf57O
56f7HnKCAUwS0D8dIAJkQULkzHbQ9uZv+WR8EZahJA6955XpOulaaEYjrumP
PaBYRC8oCDE4INuTfTuvRfJ0AqgR8ZorR1msEiQJxQqNqgR853H81LLZgwb
ZLKQJZNe/fXL29FqbOUUddI36qDFAgcd8PLSL4VqLW/hqGaQZ0NLsJ7x048RSE1
OYBlmtLwIRKFFQFTGTyDwnnnf47or8HfHVdepOfem882yWlsOnUbPI8Ymitkeu
T8b+C/tqrqxv+G4Ura5UZqORnU50RSWMCnM45QIDAQABaoBAQDKuPECR8QQTWZNC
PW0jqEeZ/nNs+G9bh8LwNTQYy55FtgO6ZrBV6dHH8YzPHDH29EUBPG8X7CD460
-----
```

[Cancelar](#) [Descifrar contraseña](#)

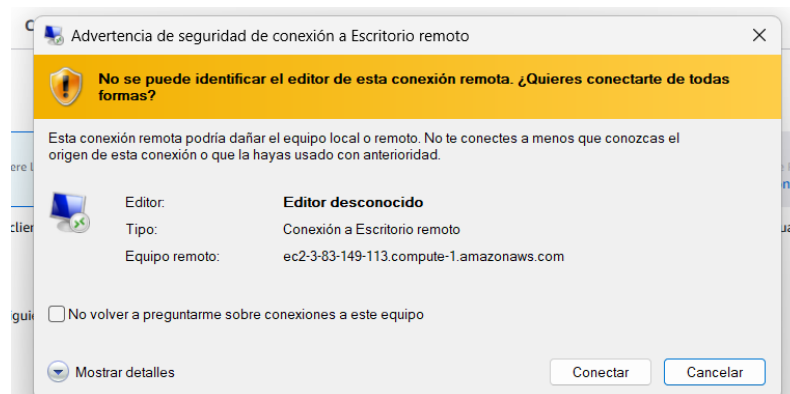
12. Esto nos mostrara ahora esta pantalla en donde podremos copiar la contraseña para conectarnos remotamente.



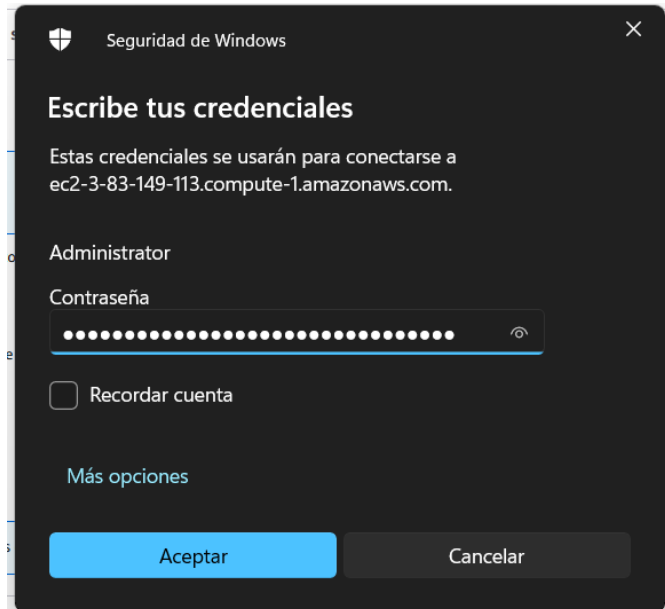
13. Vamos a las descargas y abrimos el escritorio remoto que descargamos



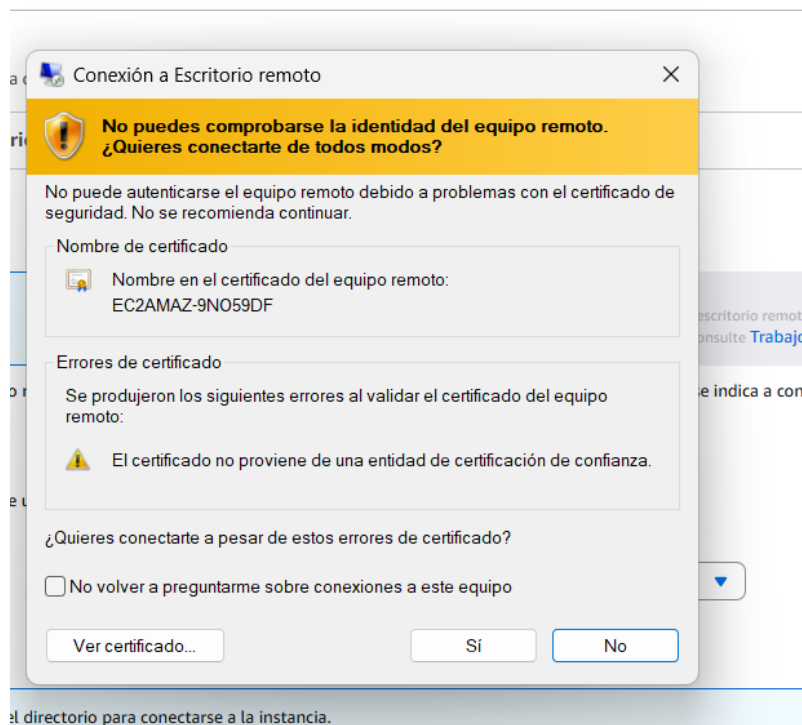
14. Al principio nos aparecera el siguiente mensaje en donde le daremos clic en conectar.



15. Aparecerá este mensaje en donde colocaremos la contraseña que se genero en el paso 12 para después darle clic en aceptar.

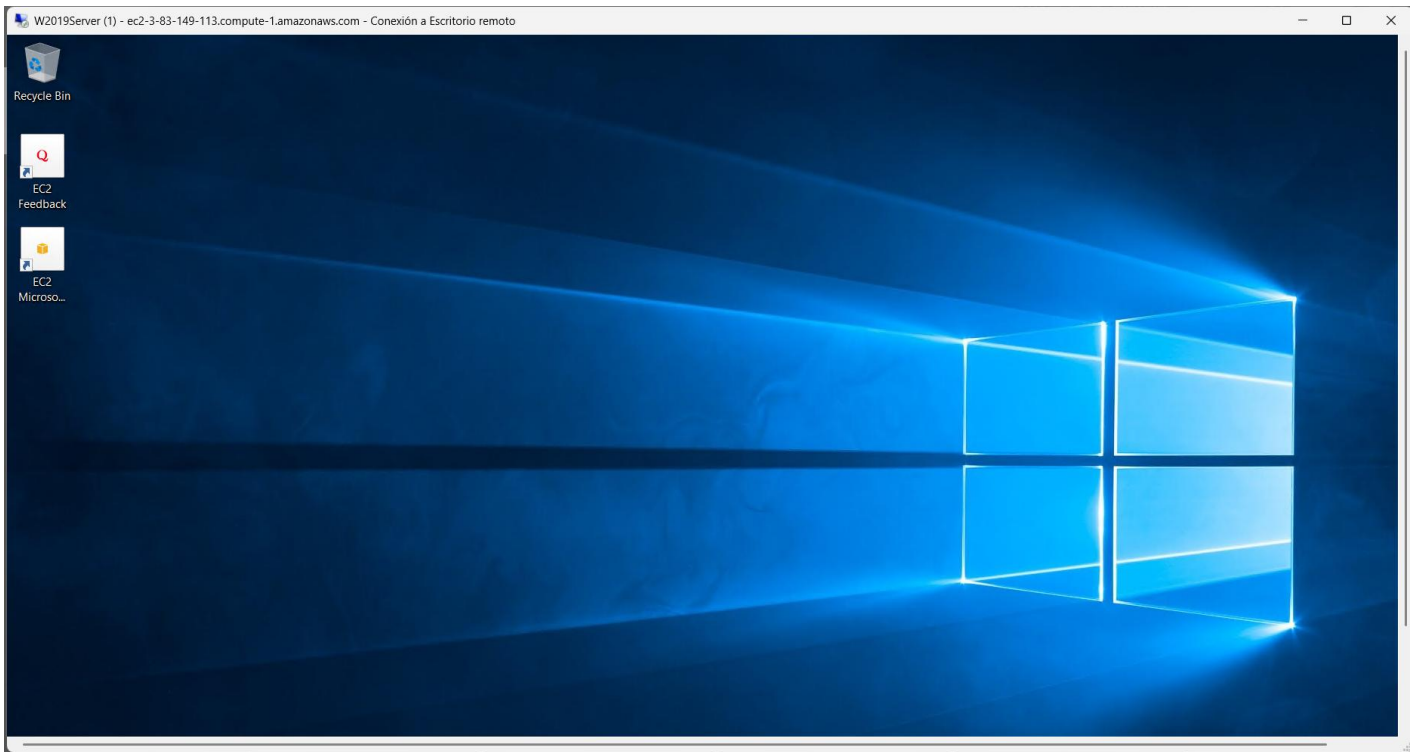


16. Finalmente nos aparecerá el siguiente mensaje de advertencia la cual le damos si.





## 17. Esto abrirá de manera remota Winows 2019 Server



## Conclusiones

El uso de una instancia en Windows Server 2019 en AWS permite disponer de un servidor remoto confiable, escalable y accesible desde cualquier lugar con conexión a internet. Establecer la conexión mediante Escritorio Remoto (RDP) es un proceso directo que requiere habilitar el puerto adecuado en el grupo de seguridad, obtener las credenciales mediante la clave PEM, y usar la IP pública de la instancia.

Esta capacidad facilita la administración remota de servidores, pruebas de software, ejecución de aplicaciones empresariales y otros servicios en un entorno controlado y seguro. Es fundamental seguir buenas prácticas de seguridad, como restringir el acceso por IP y usar contraseñas fuertes, para proteger el acceso al servidor.