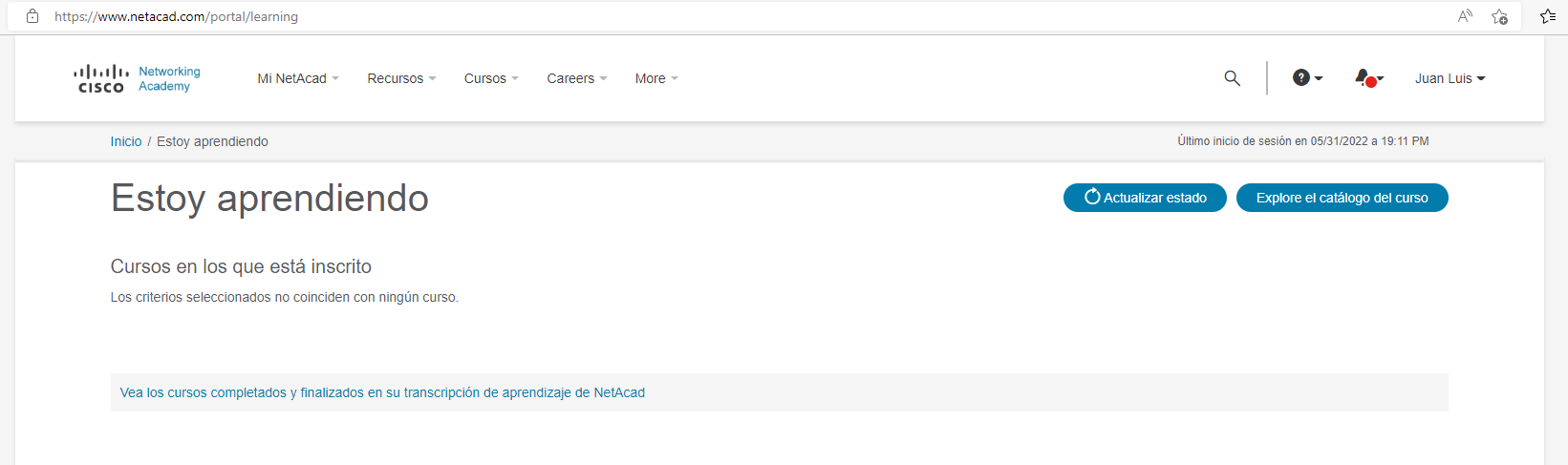
# ¿Qué es packet tracer?

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

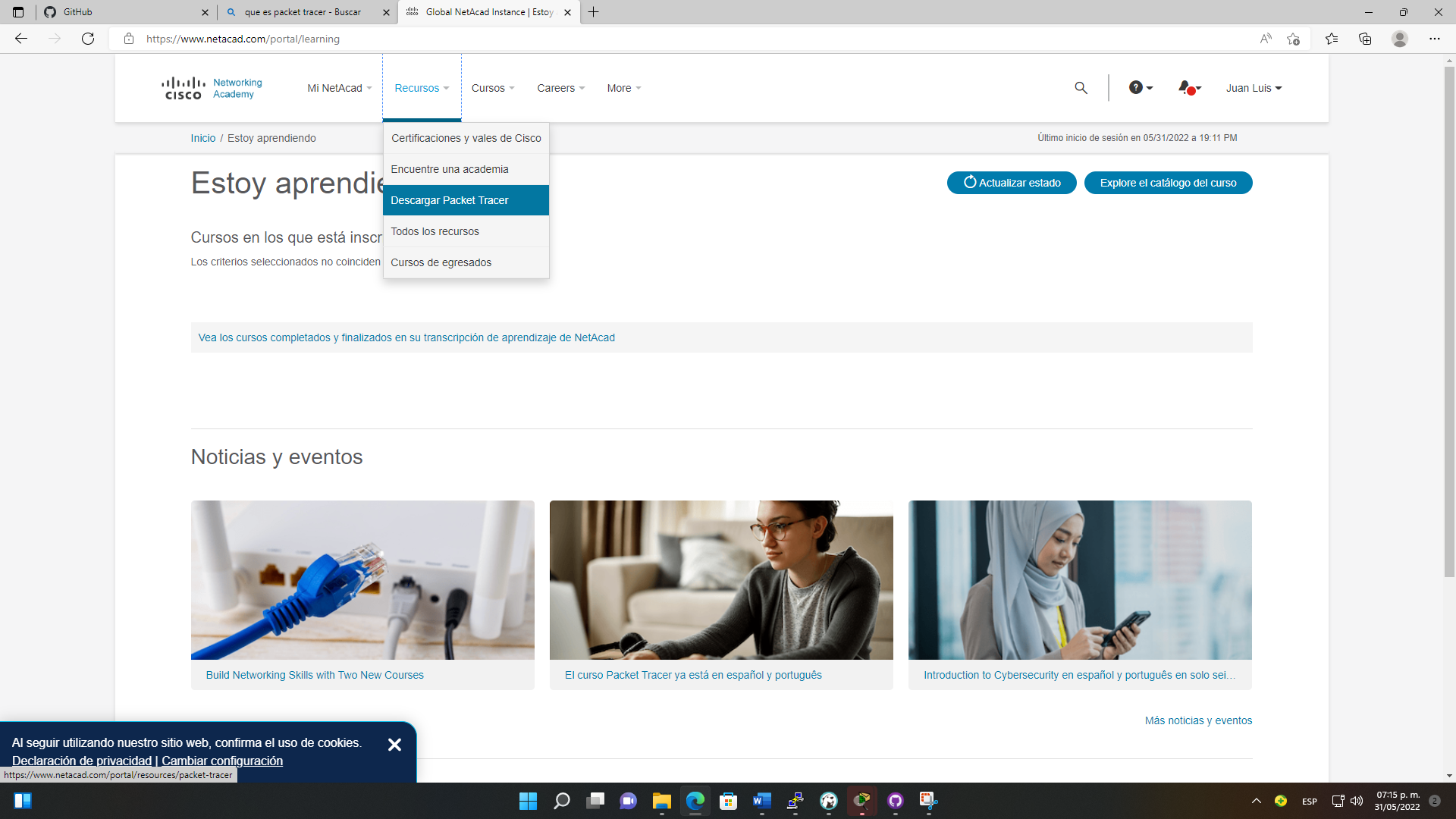
<https://erickosvaldovg.wordpress.com/2014/09/30/que-es-packet-tracer/#:~:text=Que%20es%20Packet%20Tracer%3F%20Packet%20Tracer%20es%20la,y%20simular%20una%20red%20con%20m%C3%BAltiples%20representaciones%20visuales>.

# Instalación de packet tracer.

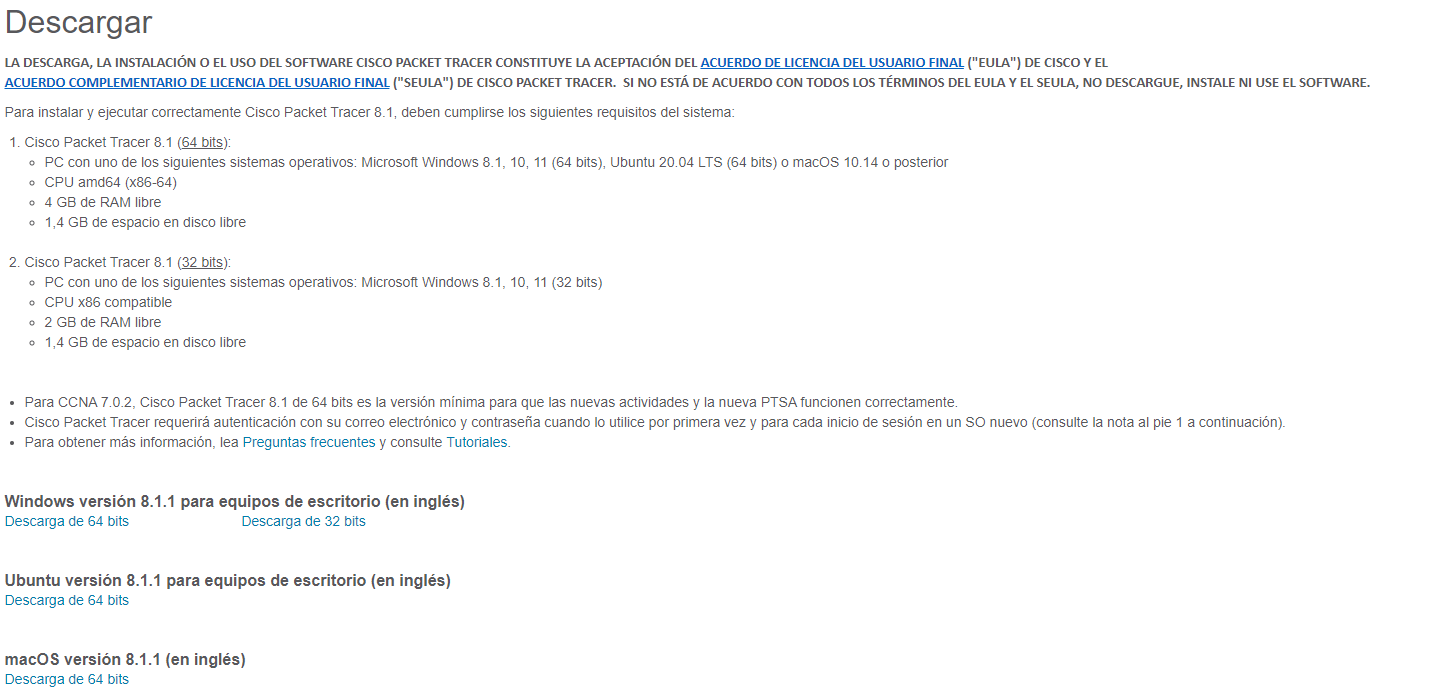
Lo primero que tenemos que hacer es tener una cuenta cisco, luego iremos a este enlace “<https://www.netacad.com/es/courses/packet-tracer>” e iniciaremos sesión.



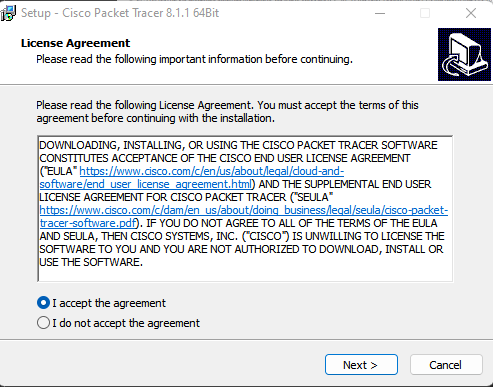
Una vez iniciada la sesión nos dirigimos al apartado de “Recursos” y haremos click en “Descargar Packet Tracer”



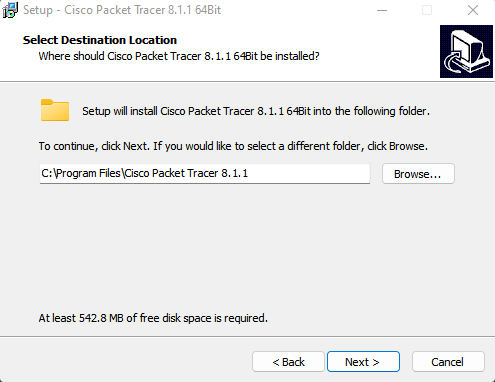
Después de eso nos redireccionará a otra pagina y nos iremos al apartado “Descargar” donde seleccionaremos la versión de acuerdo a nuestro sistema operativo, después de eso el instalador se descargará.



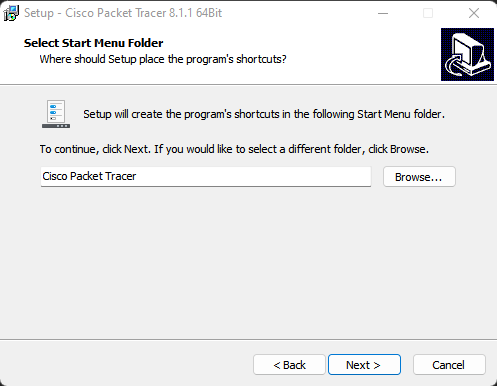
Una vez descargado abrimos el instalador, donde lo primero que saldrá será un cuadro donde aceptaremos los términos de licencia, una vez aceptado le damos en “Next”.

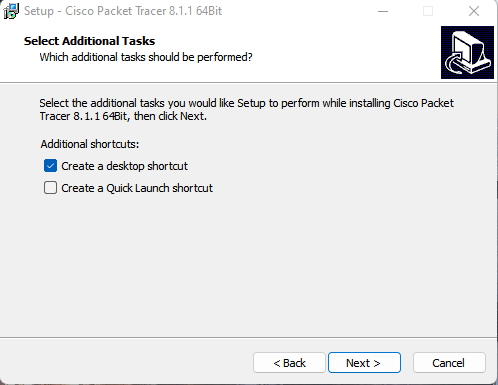


Después nos pedirá la ruta de instalación, se pueda dejar la que sale por defecto, una vez seleccionada le damos en “Next”.

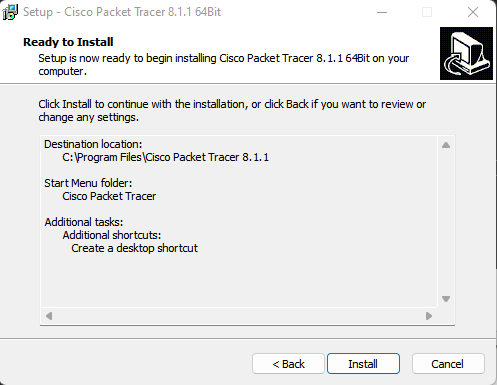


En los sigs. apartados, solo le damos “Next”.

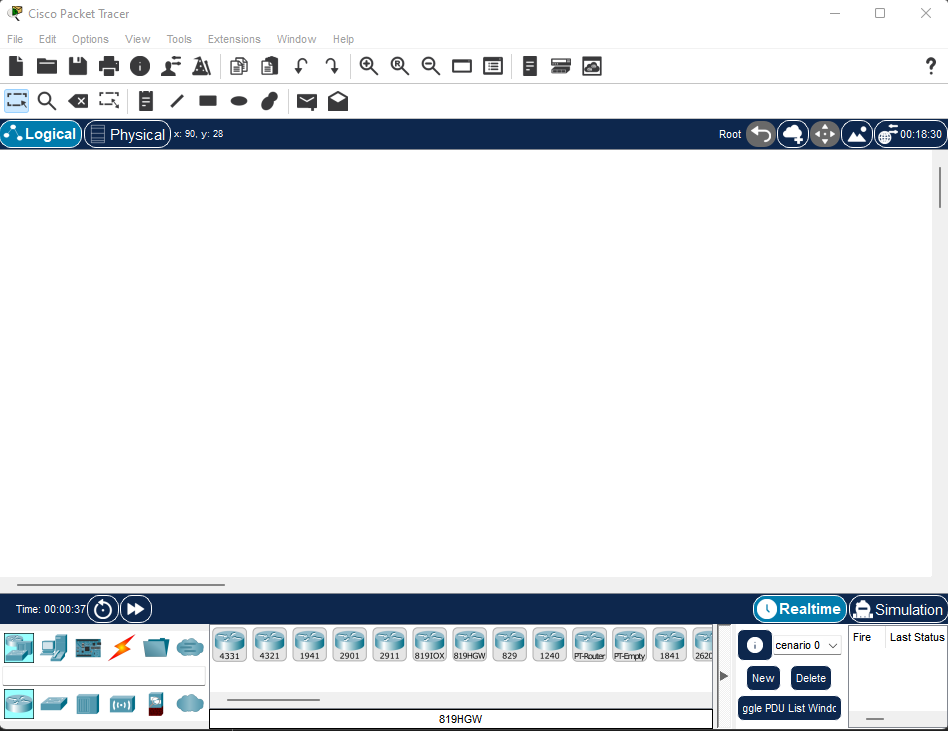




Después le damos en “Install” y esperamos a que termine se instale, al final saldrá un cuadro donde dice que la instalación fue éxitosa y le damos en “Finalizar”.

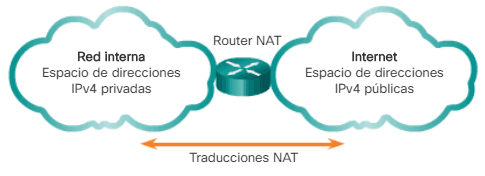


Listo después ya solo tendremos que iniciar sesión con nuestra cuenta Asterisk para poder empezar a usar Cisco Packet Tracer.



# NAT

NAT proporciona la traducción de direcciones privadas a direcciones públicas. Esto permite que un dispositivo con una dirección IPv4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet. NAT tiene el beneficio adicional de proporcionar cierto grado de privacidad y seguridad adicional a una red, ya que oculta las direcciones IPv4 internas de las redes externas.



Según la terminología de NAT, la red interna es el conjunto de redes sujetas a traducción. La red externa se refiere a todas las otras redes.

Al utilizar NAT, las direcciones IPv4 se designan de distinto modo, según si están en la red privada o en la red pública (Internet), y si el tráfico es entrante o saliente.

**Términos interna, externa, global y local**

NAT incluye cuatro tipos de direcciones:

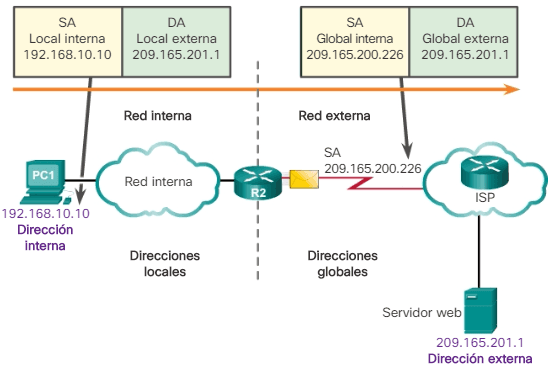
* Dirección local interna
* Dirección global interna
* Dirección local externa
* Dirección global externa

Al determinar qué tipo de dirección se utiliza, es importante recordar que la terminología de NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

* Dirección interna: la dirección del dispositivo que se traduce por medio de NAT.
* Dirección externa: la dirección del dispositivo de destino.

NAT usa los conceptos de local o global con relación a las direcciones:

* Dirección local: cualquier dirección que aparece en la porción interna de la red.
* Dirección global: cualquier dirección que aparece en la porción externa de la red.

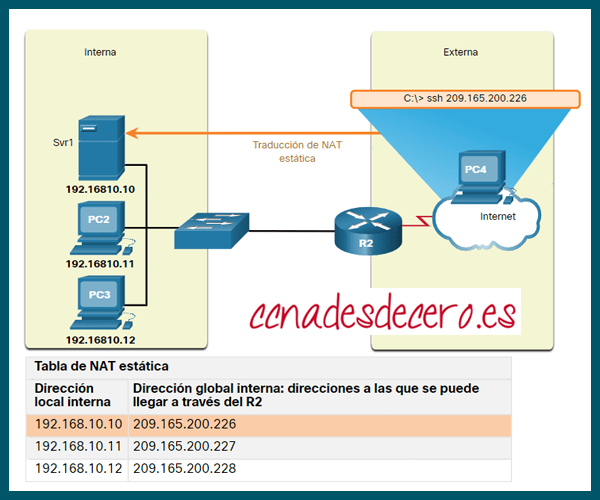


* **Dirección local interna:** la dirección de origen vista desde el interior de la red. En la ilustración, la dirección IPv4 192.168.10.10 se asignó a la PC1. Esta es la dirección local interna de la PC1.
* **Dirección global interna:** la dirección de origen vista desde la red externa. En la ilustración, cuando se envía el tráfico de la PC1 al servidor web en 209.165.201.1, el R2 traduce la dirección local interna a una dirección global interna. En este caso, el R2 cambia la dirección IPv4 de origen de 192.168.10.10 a 209.165.200.226. De acuerdo con la terminología de NAT, la dirección local interna 192.168.10.10 se traduce a la dirección global interna 209.165.200.226.
* **Dirección global externa:** la dirección del destino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en Internet. Por ejemplo, se puede llegar al servidor web en la dirección IPv4 209.165.201.1. Por lo general, las direcciones externas globales y locales son iguales.
* **Dirección local externa:** la dirección del destino vista desde la red interna. En este ejemplo, la PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrutable del destino.

<https://ccnadesdecero.es/nat-network-address-translation/>

**TIPOS DE NAT**

**NAT Estático**



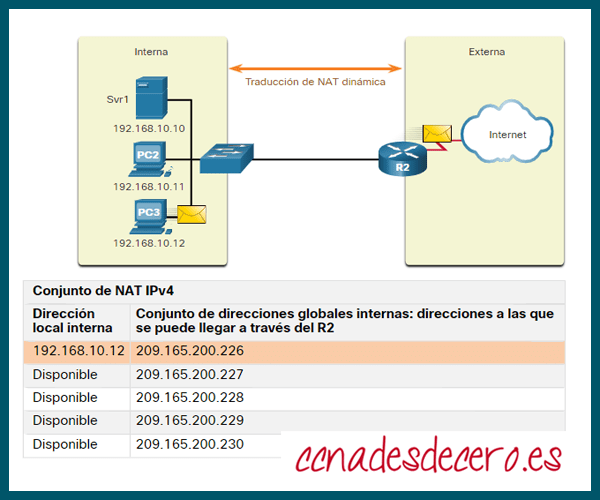
La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes. En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para redes externas, estos dispositivos parecen tener direcciones IPv4 públicas. En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para redes externas, estos dispositivos parecen tener direcciones IPv4 públicas.

Por ejemplo, un administrador de red de PC4 puede usar SSH para obtener acceso a la dirección global interna de Svr1 (209.165.200.226). R2 traduce esta dirección global interna a la dirección local interna 192.168.10.10 y conecta la sesión a Svr1.

La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

**NAT Dinámica**

La NAT dinámica utiliza un pool de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del pool.

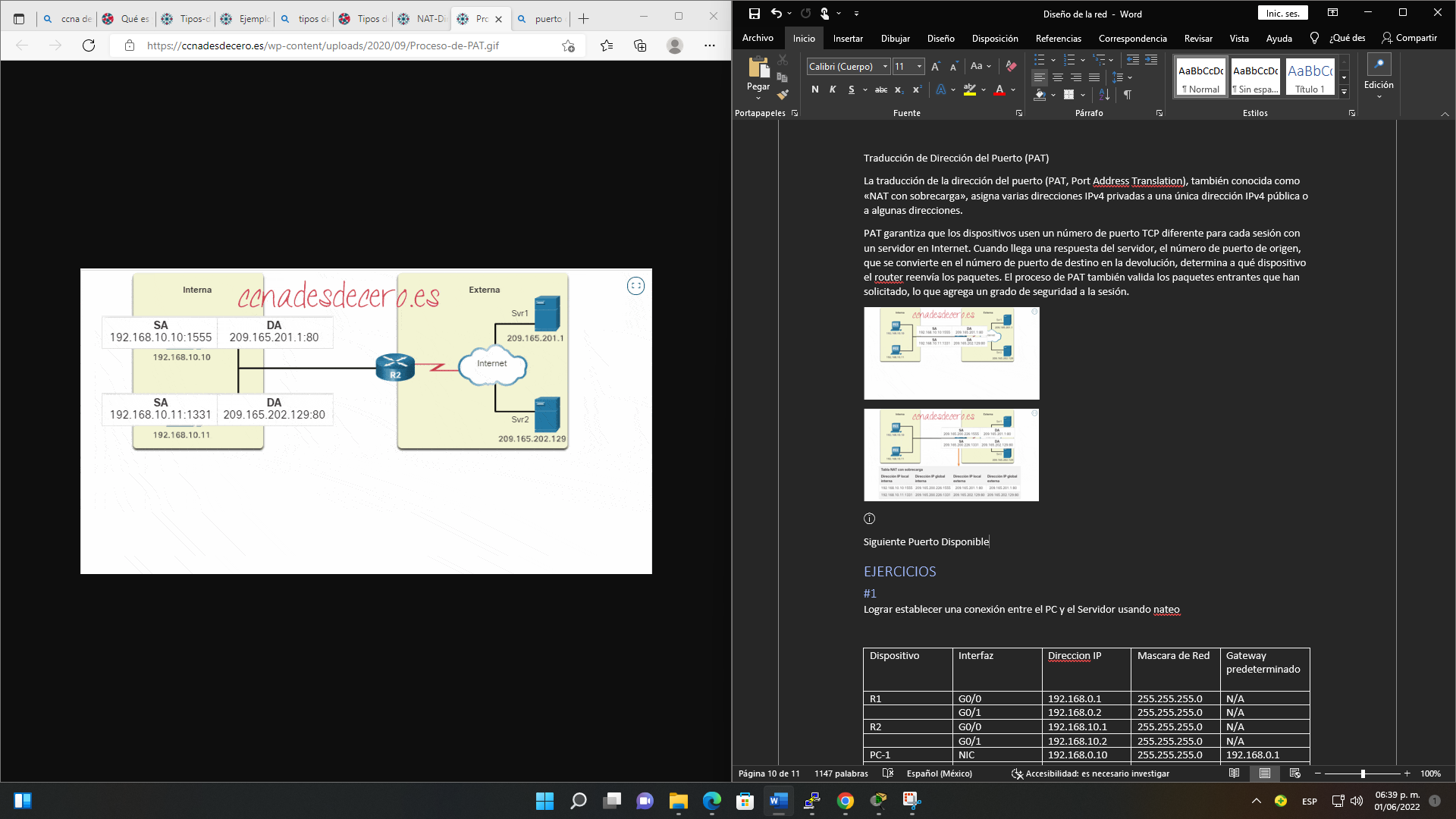


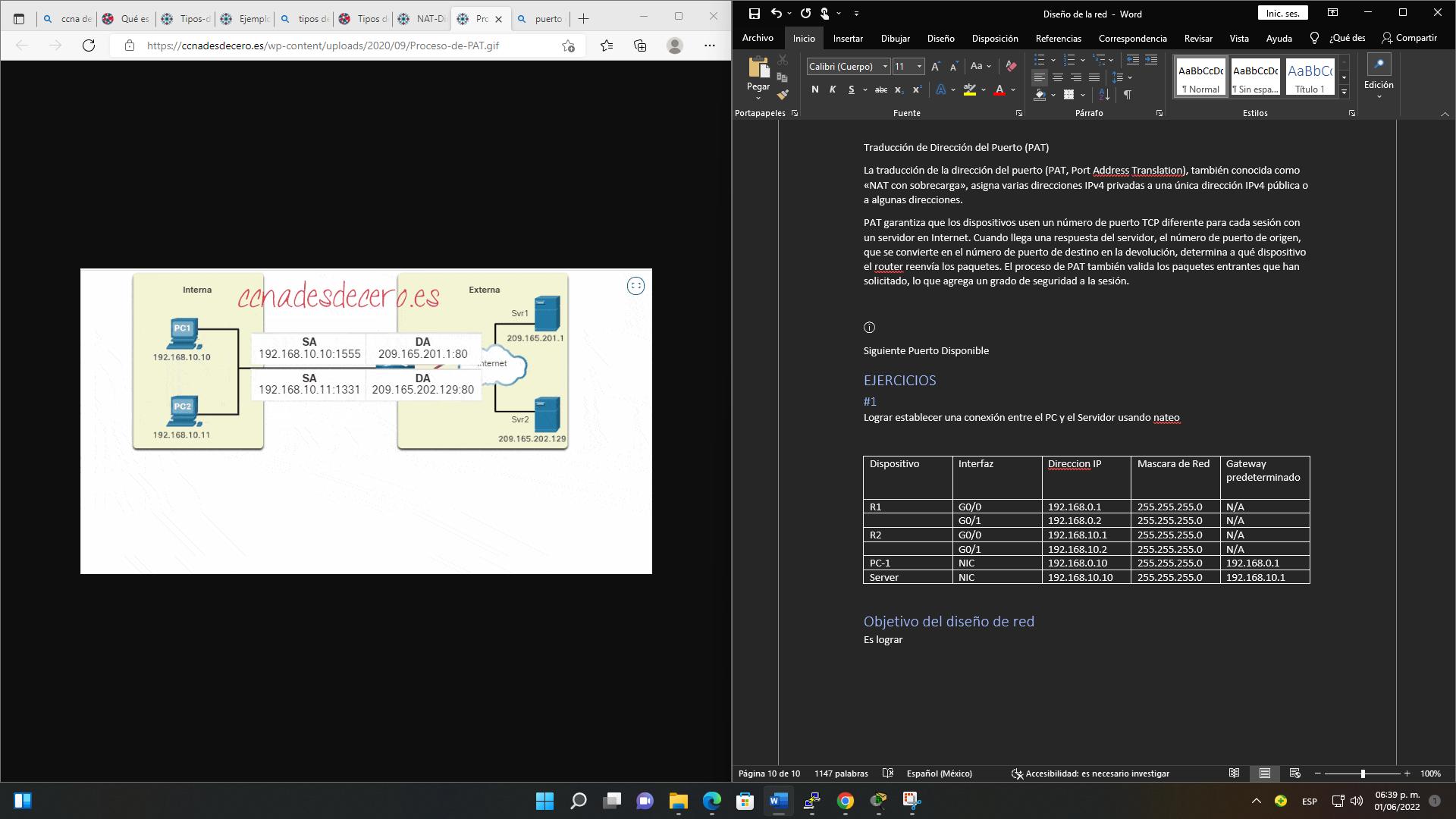
En la figura, PC3 ha accedido a Internet utilizando la primera dirección disponible en el pool NAT dinámico. Las demás direcciones siguen disponibles para utilizarlas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

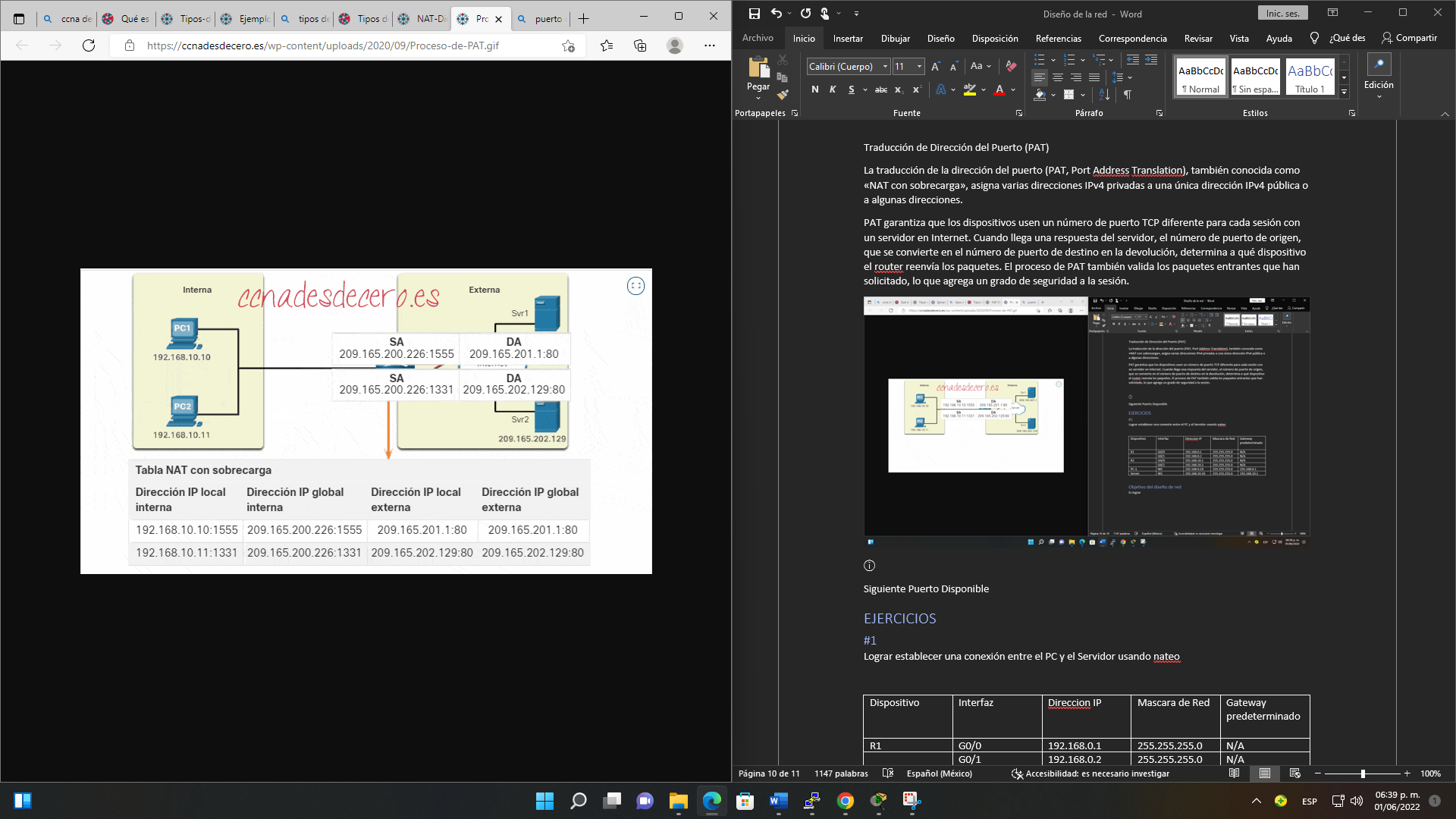
Traducción de Dirección del Puerto (PAT)

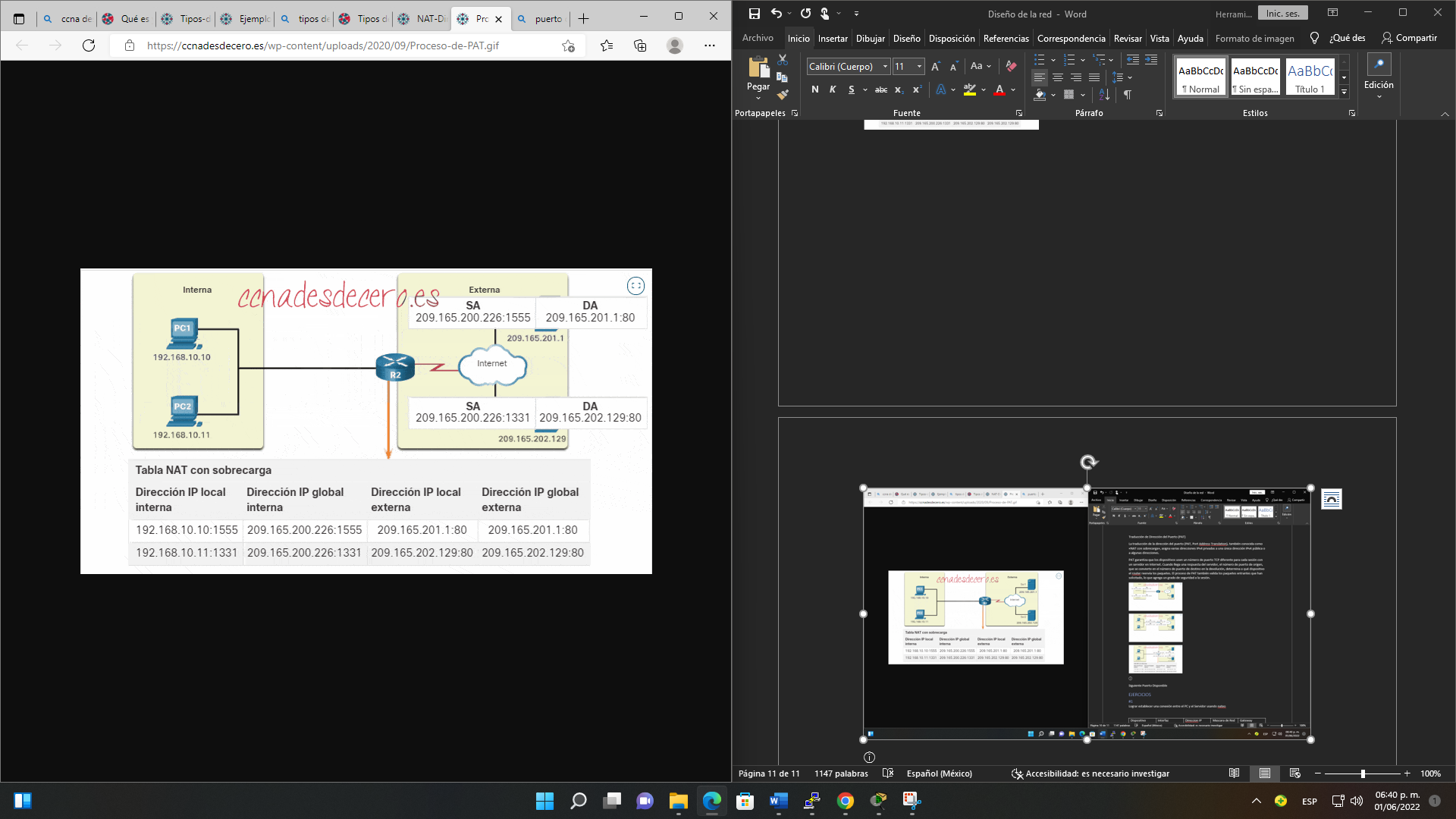
La traducción de la dirección del puerto (PAT, Port Address Translation), también conocida como «NAT con sobrecarga», asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones.

PAT garantiza que los dispositivos usen un número de puerto TCP diferente para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT también valida los paquetes entrantes que han solicitado, lo que agrega un grado de seguridad a la sesión.









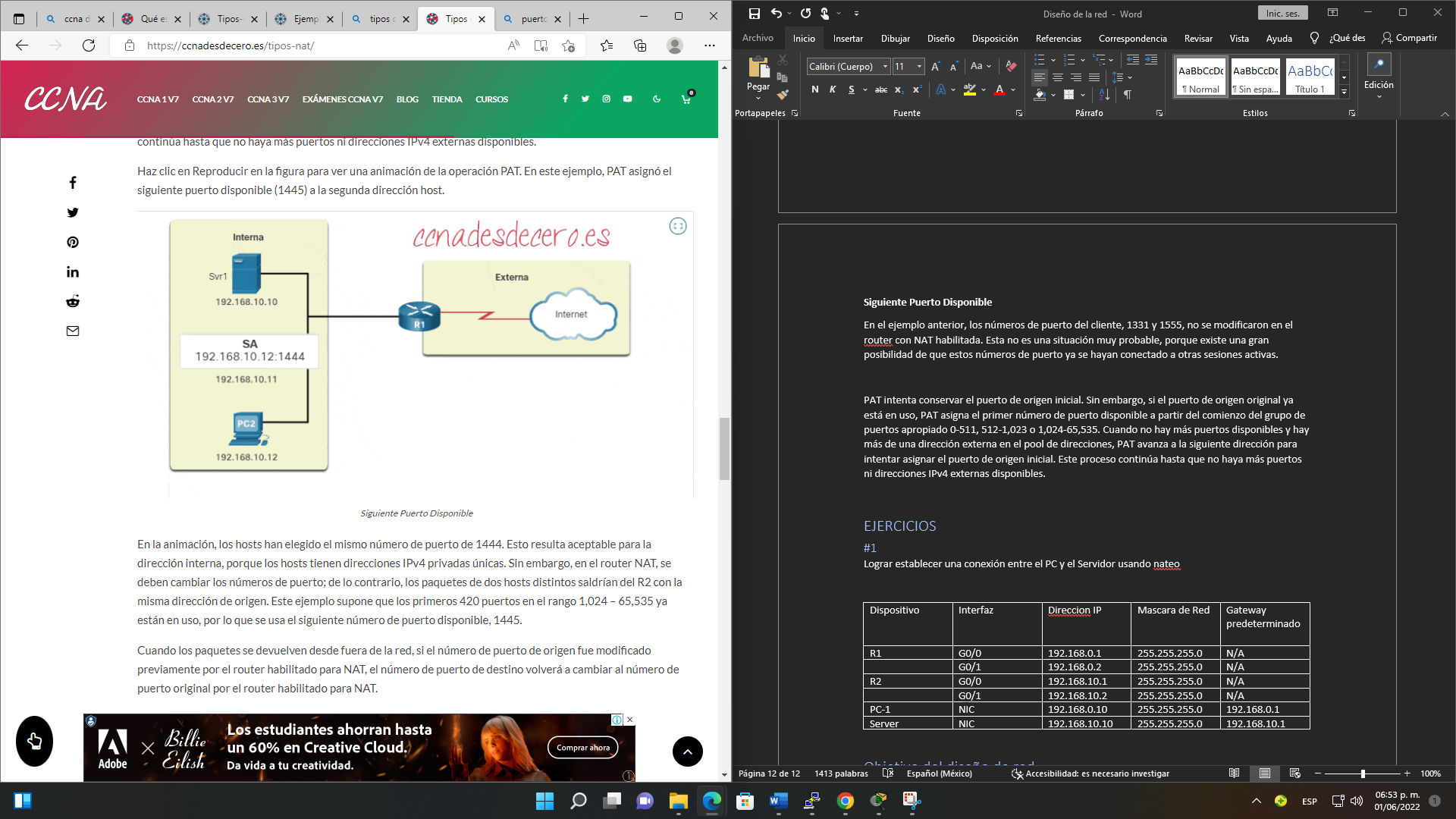
A medida que el R2 procesa cada paquete, utiliza un número de puerto (1331 y 1555, en este ejemplo) para identificar el dispositivo en el que se originó el paquete. La dirección de origen (SA, source address) es la dirección local interna con el número de puerto asignado TCP / UDP agregado. La dirección de destino (DA, destination address) es la dirección global externa con el número de puerto de servicio agregado. En este ejemplo, el puerto de servicio es 80, que es HTTP.

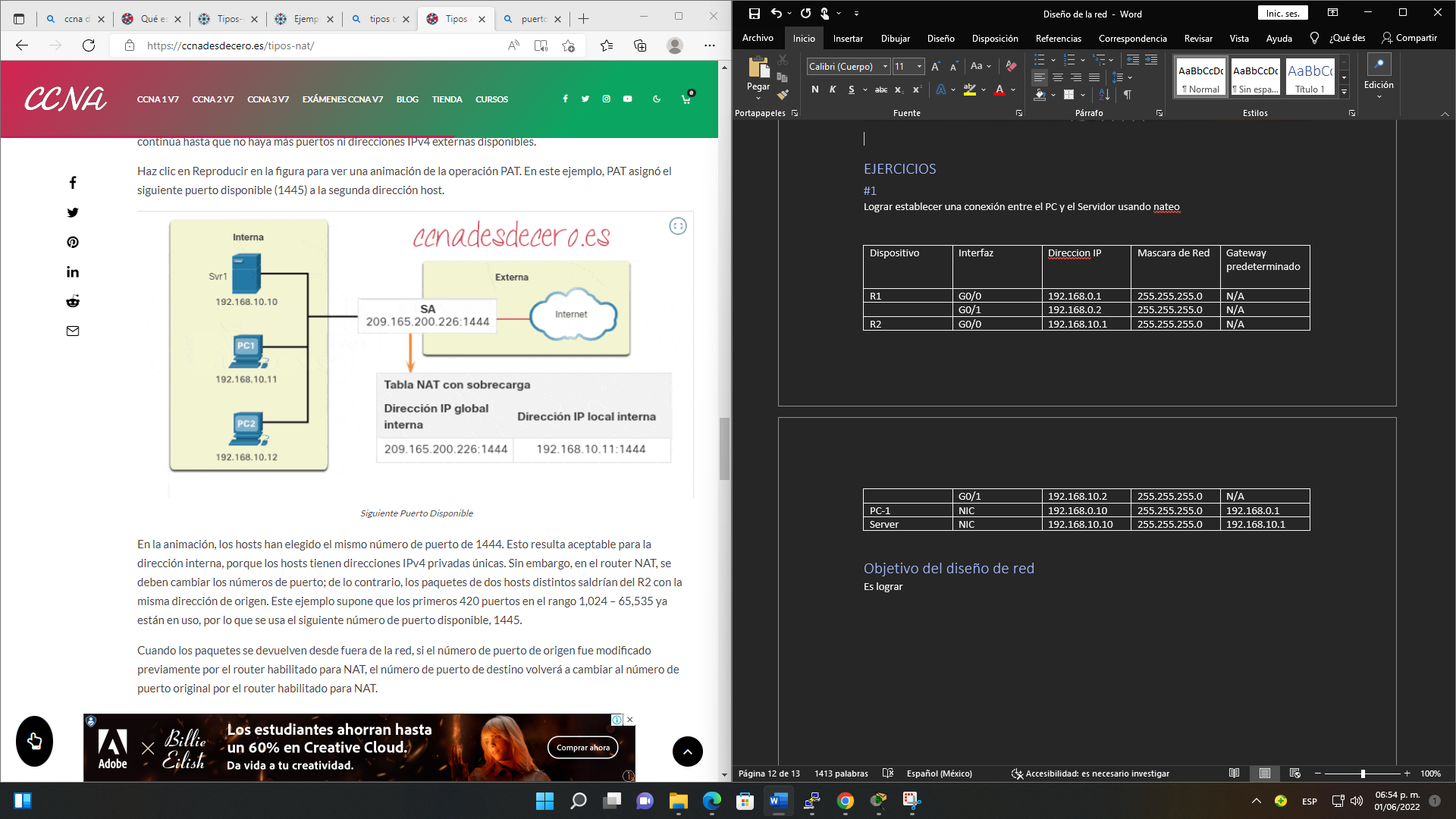
Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado. La dirección de destino no cambia, pero ahora se conoce como la dirección IPv4 global externa. Cuando el servidor web responde, se invierte la ruta.

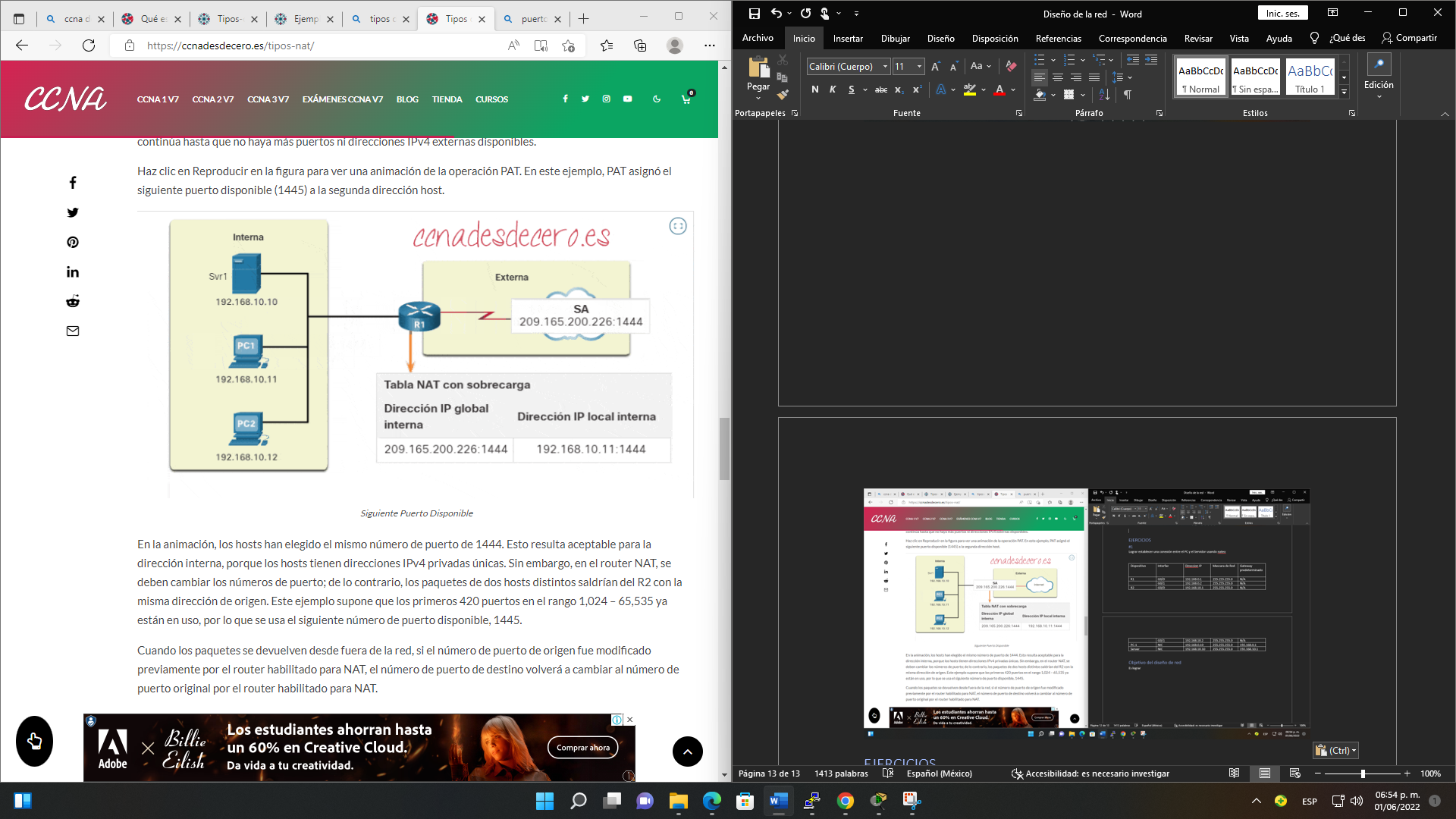
**Siguiente Puerto Disponible**

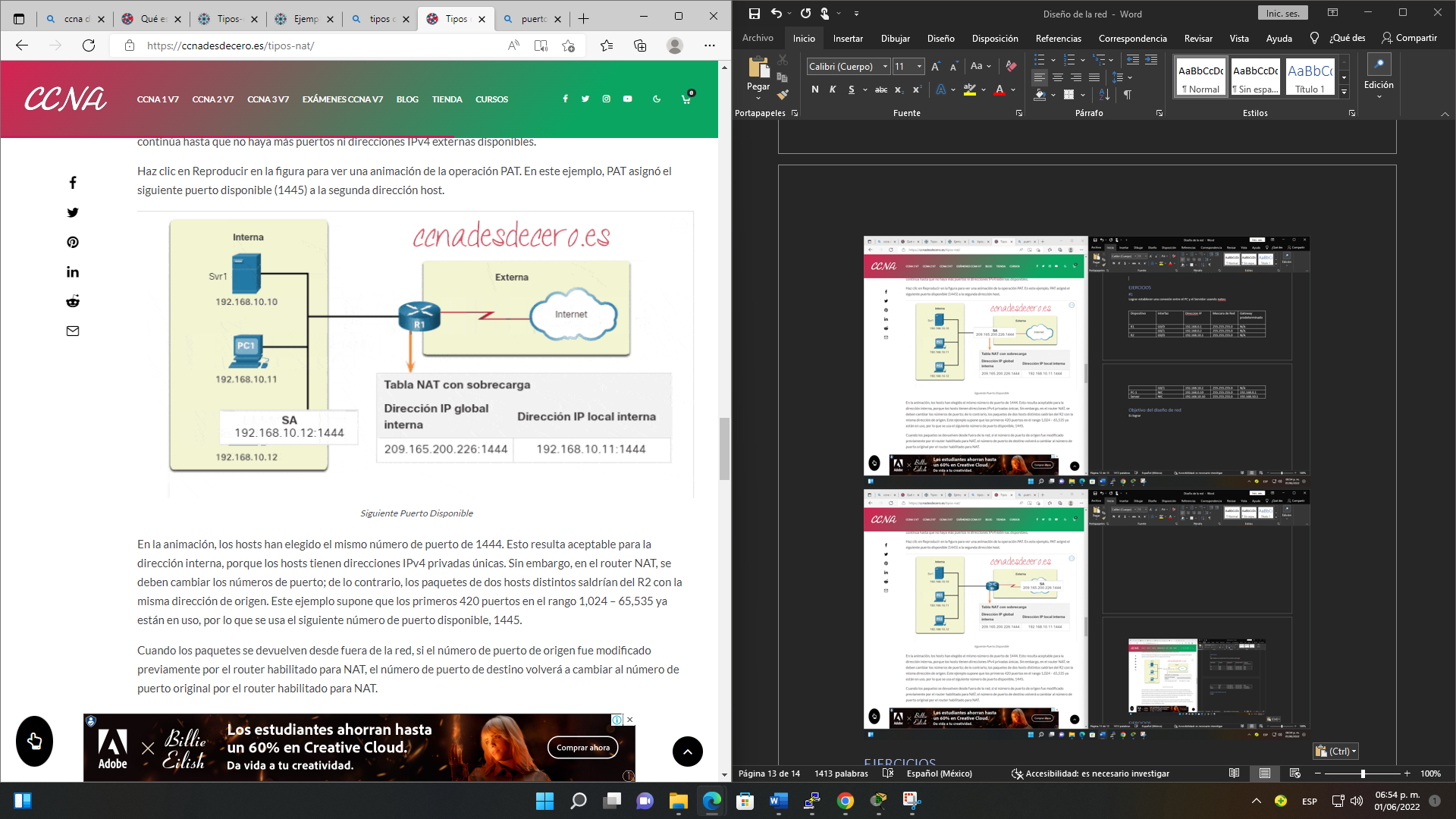
En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

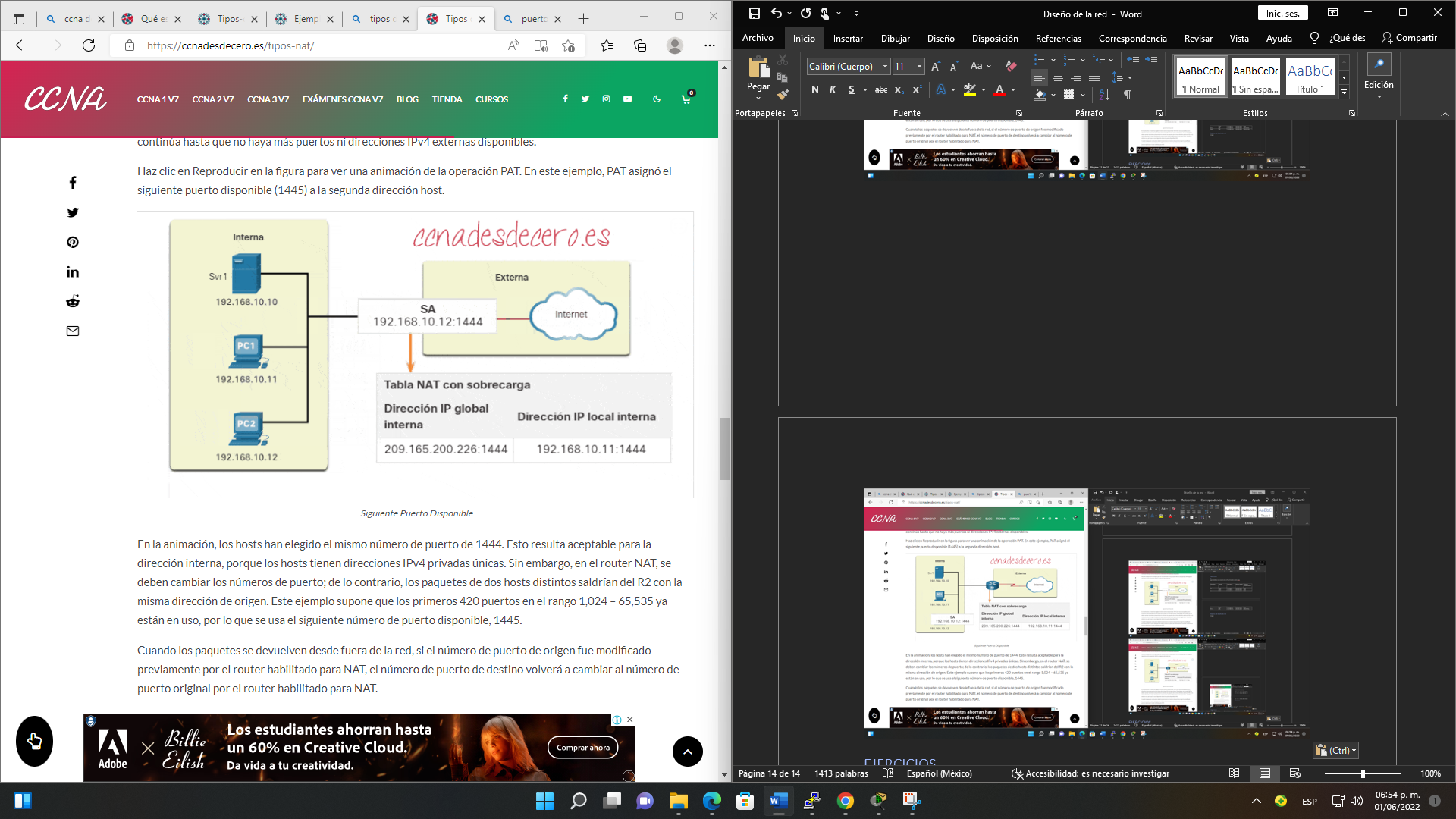
PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen original ya está en uso, PAT asigna el primer número de puerto disponible a partir del comienzo del grupo de puertos apropiado 0-511, 512-1,023 o 1,024-65,535. Cuando no hay más puertos disponibles y hay más de una dirección externa en el pool de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial. Este proceso continúa hasta que no haya más puertos ni direcciones IPv4 externas disponibles.

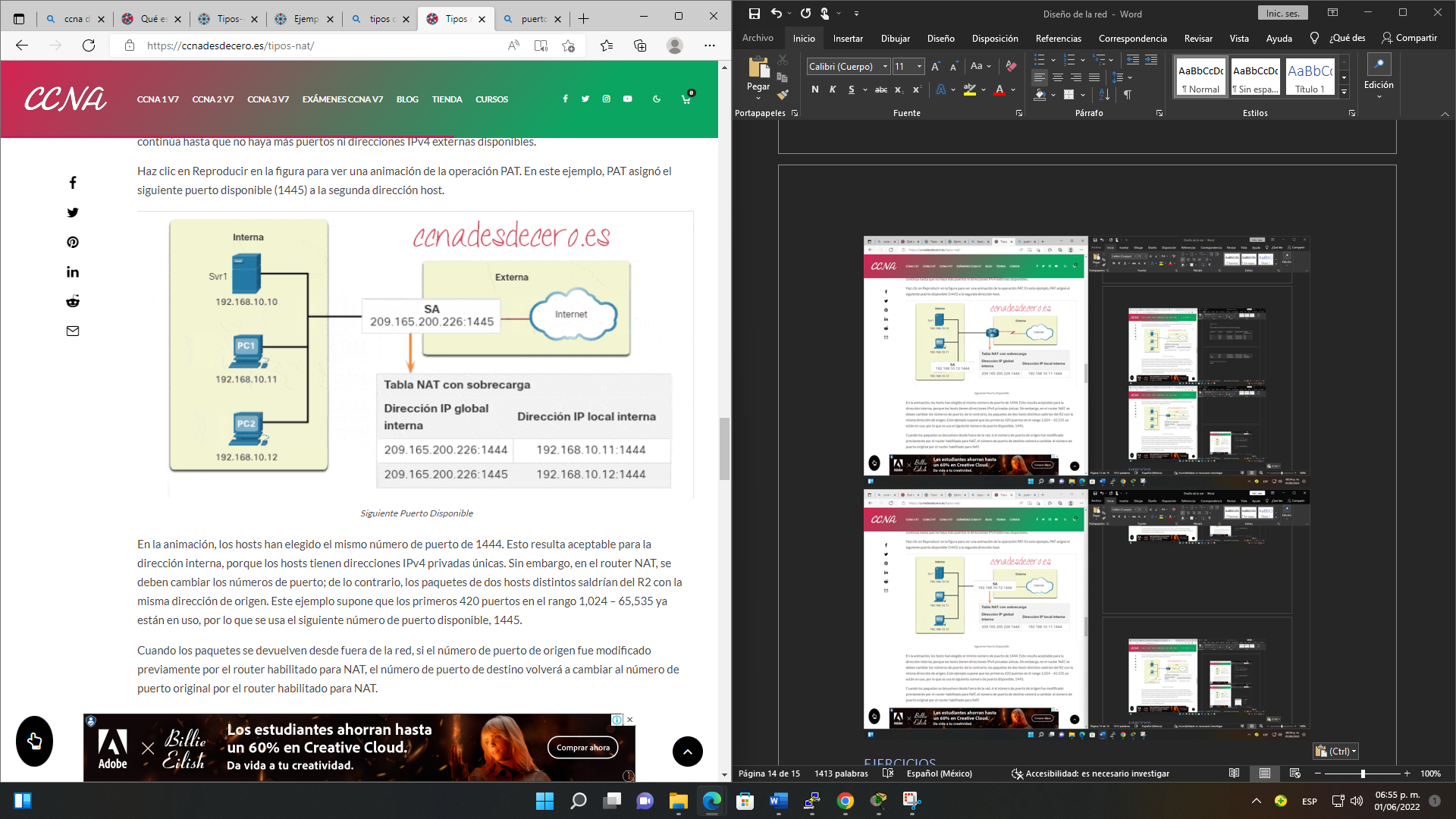


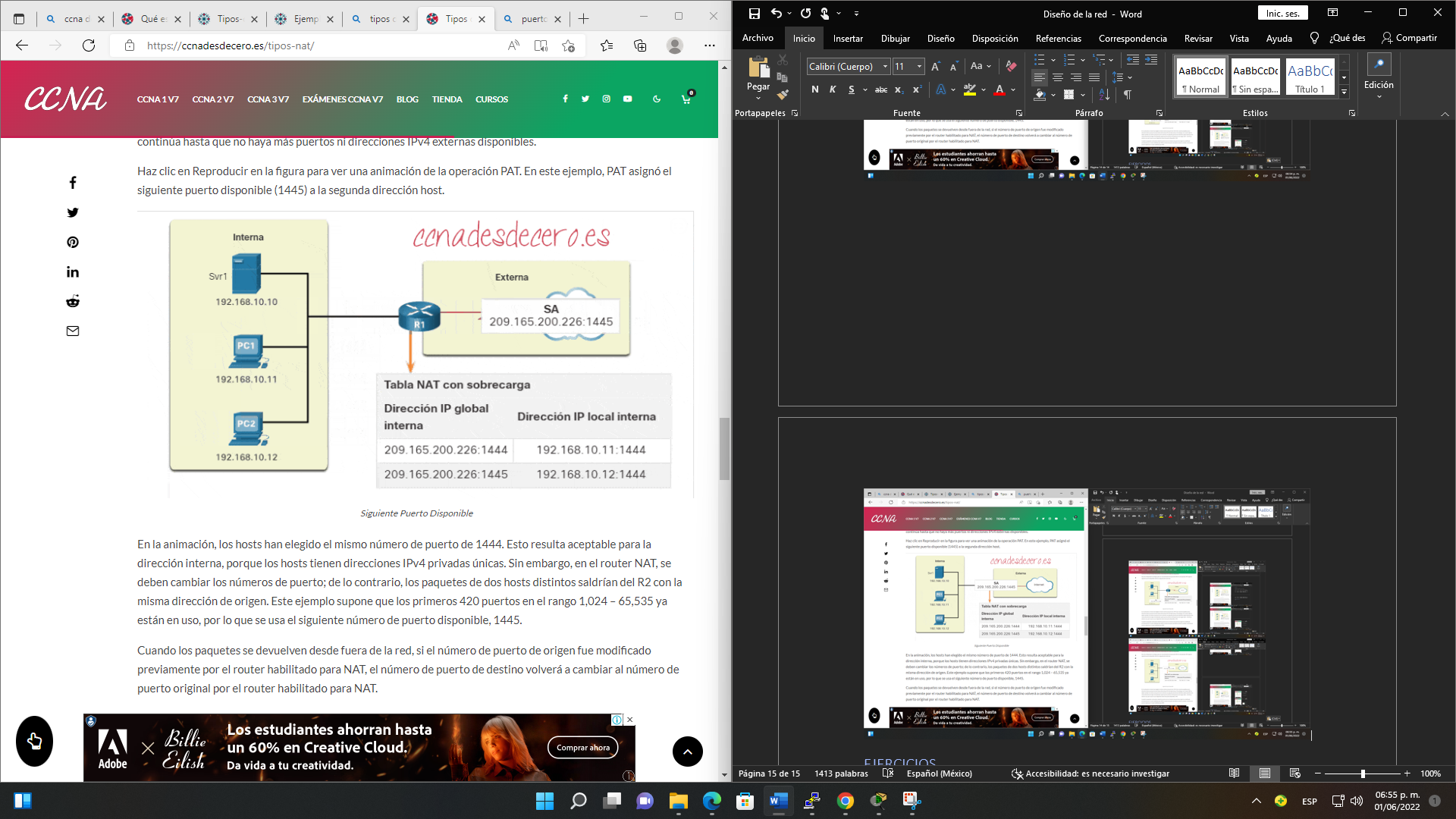












los hosts han elegido el mismo número de puerto de 1444. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IPv4 privadas únicas. Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen. Este ejemplo supone que los primeros 420 puertos en el rango 1,024 – 65,535 ya están en uso, por lo que se usa el siguiente número de puerto disponible, 1445.

Cuando los paquetes se devuelven desde fuera de la red, si el número de puerto de origen fue modificado previamente por el router habilitado para NAT, el número de puerto de destino volverá a cambiar al número de puerto original por el router habilitado para NAT.

<https://ccnadesdecero.es/tipos-nat/>

# EJERCICIOS

## #1

Lograr establecer una conexión entre el PC y el Servidor usando nateo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Direccion IP | Mascara de Red | Gateway predeterminado |
| R1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
|  | G0/1 | 192.168.0.2 | 255.255.255.0 | N/A |
| R2 | G0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | G0/1 | 192.168.10.2 | 255.255.255.0 | N/A |
| PC-1 | NIC | 192.168.0.10 | 255.255.255.0 | 192.168.0.1 |
| Server | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |

# Objetivo del diseño de red

Es lograr