



Certified Tech Developer

The Ultimate Degree

Infraestructura I

Objetivos

En el siguiente ejercicio vamos a hacer uso de la criptografía viendo cómo funciona un certificado. Para ello, vamos a ir a nuestra VPC de AWS, generaremos un dominio propio en **www.noip.com** y seguiremos este tutorial paso a paso que contiene todo lo que vamos a necesitar para completar el ejercicio.

Instrucciones

1. Creación de la instancia EC2 en la VPC.
2. Generación del dominio en noip.
3. Generación del certificado SSL en Let's Encrypt.

Creación de la instancia EC2 en la VPC

Acceso a la consola de gestión AWS

Una vez logueados en la consola de Amazon Educate, seleccionamos la opción **AWS Account**. Allí aparecerá listada la materia y hacemos clic en **Go to Classroom**.

My Classrooms Portfolio Career Pathways Badges Jobs AWS Account Logout

Consecutive Days: **1** Pathways Completed: **0** Badges Earned: **0** Preferred Language: English

ing over 18 million cloud jobs worldwide
ate introduces you to lucrative cloud-
learning pathways, each with content
:ivities and labs, opportunities to earn
of Completion, and access to the AWS
ses at your school or through online
e pathway to your dream job in the

aws educate

If you missed out the "Optimizing your AWS Educate Profile to Help You Find a Cloud Career" webinar and Q&A session, watch it [here](#) !

Suggested Jobs

Entry Level Software Developer
Smoothstack, Inc.
more about this opportunity

See More

Seleccionamos la opción **AWS Educate Starter Account**.

AWS Educate Starter Account

Your cloud journey has only just begun. Use your AWS Educate Starter Account to access the AWS Console and resources, and start building in the cloud!



Luego, presionamos el botón de acceso a **AWS Console** y verificamos que el navegador no bloquee ventanas emergentes en este sitio.

Vocareum My Classes Help introaingenieria@

Welcome to your AWS Educate Account

AWS Educate provides you with access to a wide variety of AWS Services for you to get your hands on and build on AWS! To get started, click on the AWS Console button to log in to your AWS console.

Please read the FAQ below to help you get started on your Starter Account.

- What are the list of services supported?
- What regions are supported with Starter Accounts or Classroom Accounts?
- I can't start any resources. What happened?
- Can I create users within my Starter or Classroom Account for others to access?
- Can I create my own IAM policy within Starter Account or Classroom?

Your AWS Account Status

Active
full access (introaingenieria@gmail.com)

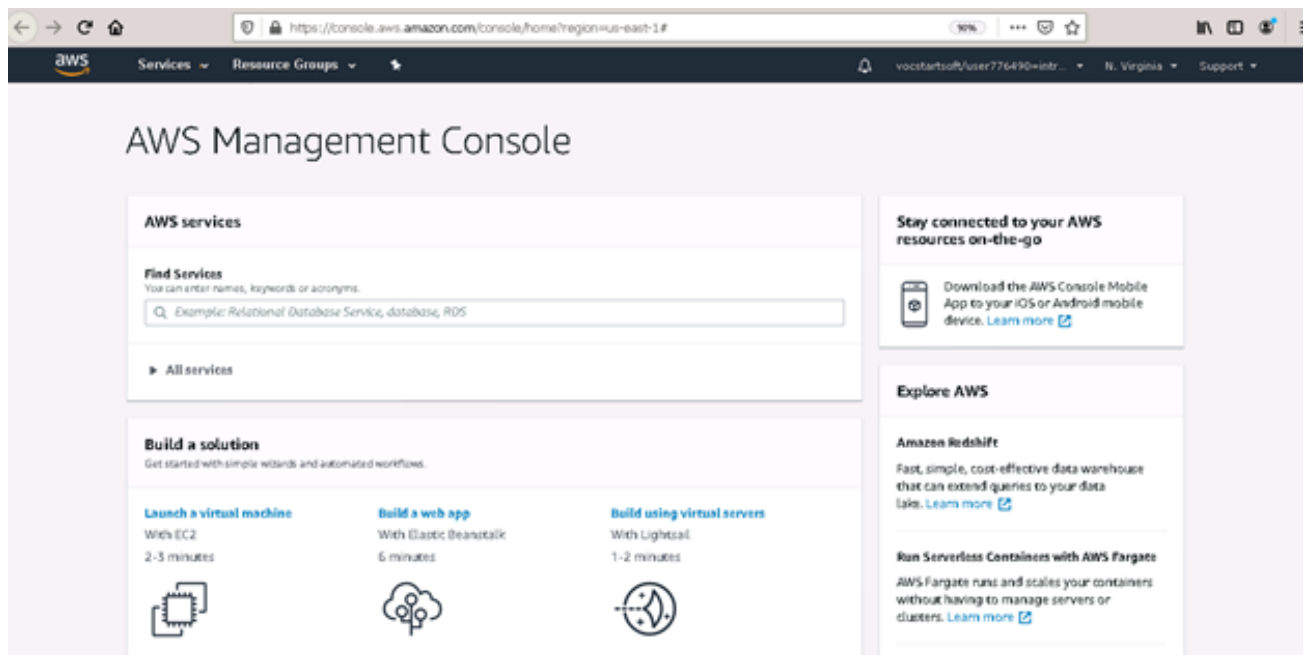
\$30
remaining credits (estimated)

2:59
session time

Account Details **AWS Console**

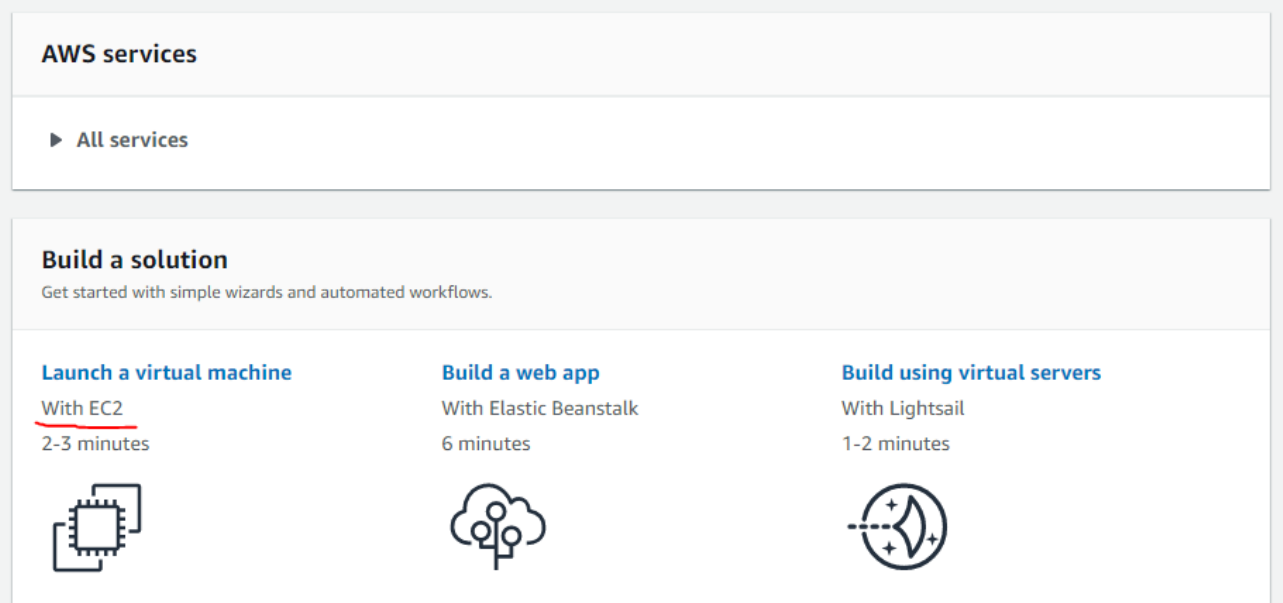
Please use AWS Educate Account responsibly. Remember to shut down your instances when not in use to make the best use of your credits. And, don't forget to logout once you are done with your work!

Nos encontramos con la consola de gestión de la plataforma AWS.



Una vez allí, hacemos clic en **EC2**.

AWS Management Console




Crear una instancia en EC2

Nos posicionamos en la parte superior derecha de la pantalla y hacemos clic en el botón **Launch instances**.

Launch instances

Luego, elegimos **Ubuntu Server 20.04 LTS**.



Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-09e67e426f25ce0d7 (64-bit x86) / ami-00d1ab6b335f217cf (64-bit Arm)

Free tier eligible

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)

☐ 64-bit (Arm)

Seleccionamos el modelo de máquina **Family T2.micro (capa free)** y hacemos clic en **Next**.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are v for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs
<input type="checkbox"/>	t2	t2.nano	1
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1
<input type="checkbox"/>	t2	t2.small	1
<input type="checkbox"/>	t2	t2.medium	2

En la interfaz, el Step 3 lo dejamos tal cual está y apretamos **Next**. En el Step 4, dejamos los discos por defecto de 8 GB, volvemos a presionar **Next**. En el Step 5, hacemos lo mismo. Mientras que en el Step 6 vamos a configurar, por ahora, un grupo de seguridad para el acceso a la instancia.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere 0.0.0.0/0 ::/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere 0.0.0.0/0 ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Anywhere 0.0.0.0/0 ::/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Lo importante es darle un nombre y una descripción que nos ayude a identificarlo y dar acceso a los protocolos.

Reglas de entrada [Información](#)

Security group rule ID	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional	
sgr-06fde1835bbd3b375	HTTP	TCP	80	Person... 0.0.0.0/0		Eliminar
sgr-01818733f74ab9ea4	SSH	TCP	22	Person... 0.0.0.0/0		Eliminar
sgr-0b1c29fe41845842d	HTTPS	TCP	443	Person... 0.0.0.0/0		Eliminar

[Agregar regla](#)

Hacemos clic en **Review and Launch**.

Corroboramos la configuración de la instancia y hacemos clic en **Launch instances**.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

☒ Create a new key pair

Key pair name:

[Download Key Pair](#)

You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

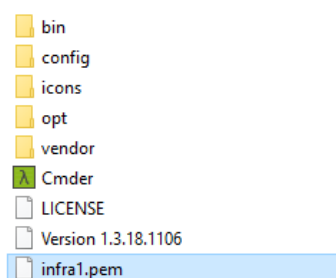
Creamos un nuevo key pair, si no tenemos, y descargamos el archivo **.pem**.

Instance: i-0630dbd3d89230282 (Instancia01)

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
▼ Instance summary Info						
Instance ID i-0630dbd3d89230282 (Instancia01)		Public IPv4 address 3.221.170.223 open address		Private IPv4 addresses 172.31.2.9		
Instance state Running		Public IPv4 DNS ec2-3-221-170-223.compute-1.amazonaws.com open address		Private IPv4 DNS ip-172-31-2-9.ec2.internal		
Instance type t2.micro		Elastic IP addresses -		VPC ID vpc-4cef8131		

Instalar Apache

Para este apartado vamos a necesitar una consola o terminal Bash para comunicarnos vía SSH. En la actualidad, hay muchos productos disponibles y depende del sistema operativo que estemos utilizando. Por el momento, dejamos a tu criterio cuál te parece más cómodo y agradable a la vista. En este ejemplo, utilizamos Windows 10 con Cmder. En caso de no tenerlo, se puede descargar de <https://cmder.net> —recomendamos bajar la versión full que es totalmente portable—. Copiamos el archivo de claves **.pem** en la carpeta raíz del Cmder, solo por comodidad del ejemplo.



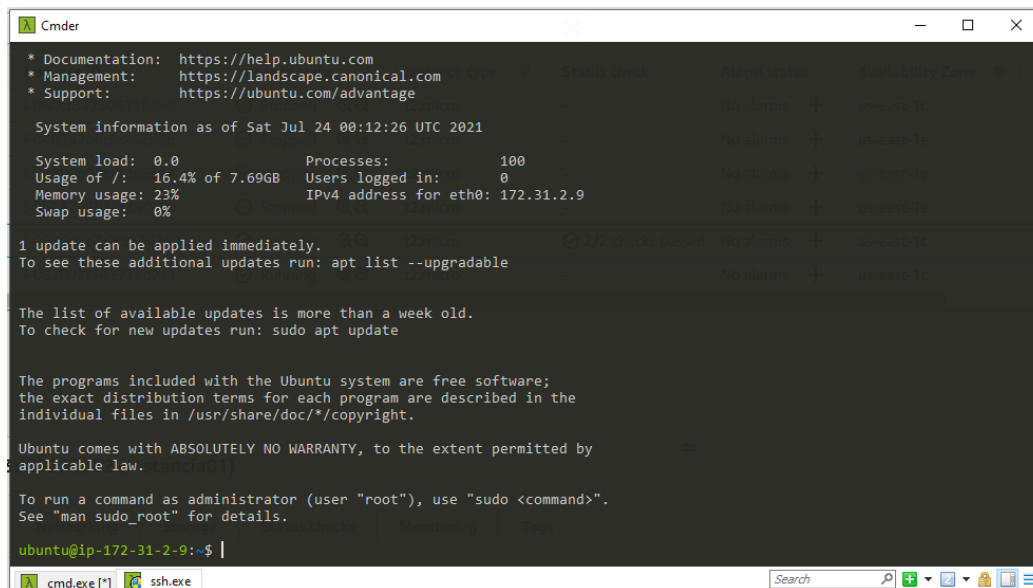
Abrimos la consola. En la parte inferior derecha abrimos un bash como administrador.



Vamos a buscar la IP de la "Instancia01" que está online.



```
david@Escritorio ~/cmdr  
λ ssh -i infra1.pem ubuntu@3.221.170.223
```

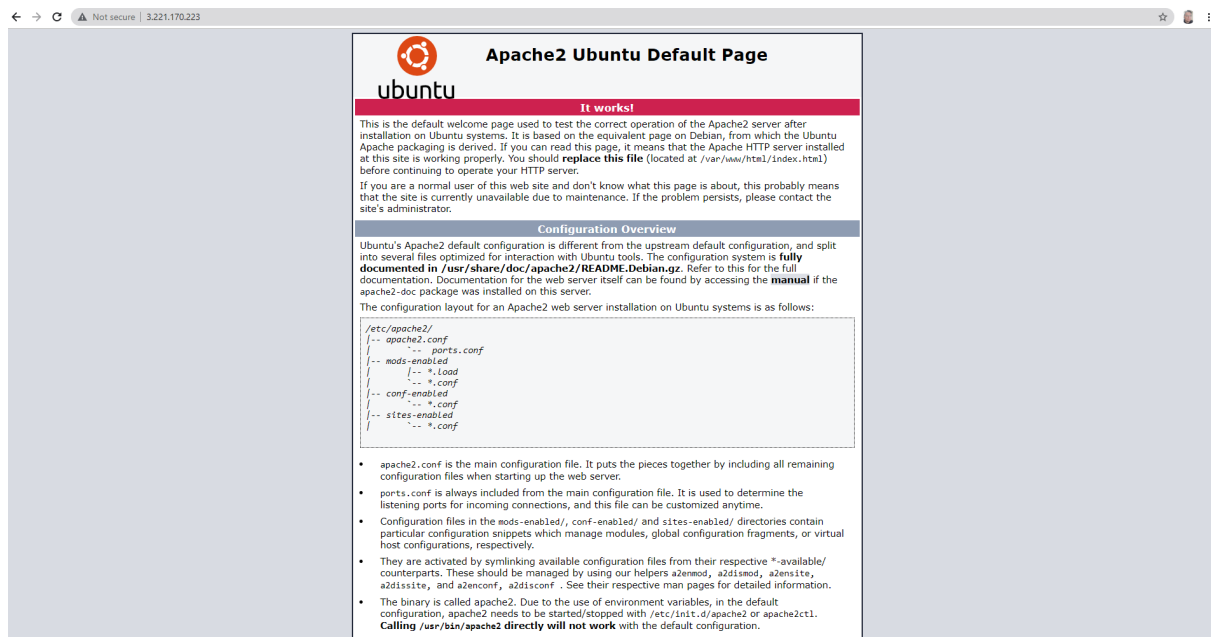


```
Cmder  
* Documentation: https://help.ubuntu.com  
* Management:   https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sat Jul 24 00:12:26 UTC 2021  
  
System load: 0.0      Processes:            100  
Usage of /:  16.4% of 7.69GB   Users logged in:      0  
Memory usage: 23%      IPv4 address for eth0: 172.31.2.9  
Swap usage:  0%  
  
1 update can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-2-9:~$ |
```

Una vez dentro, tenemos que instalar un servidor Apache para deployar nuestro código. Con este objetivo, ponemos el siguiente comando:

```
ubuntu@3.221.170.223:~$ sudo apt update  
ubuntu@3.221.170.223:~$ sudo apt upgrade -y  
ubuntu@3.221.170.223:~$ sudo apt install apache2 -y
```

Comprobamos que el servicio esté andando. Ingresamos a un explorador y colocamos la IP de nuestra instancia y nos debe contestar: **Apache2 recientemente instalado.**



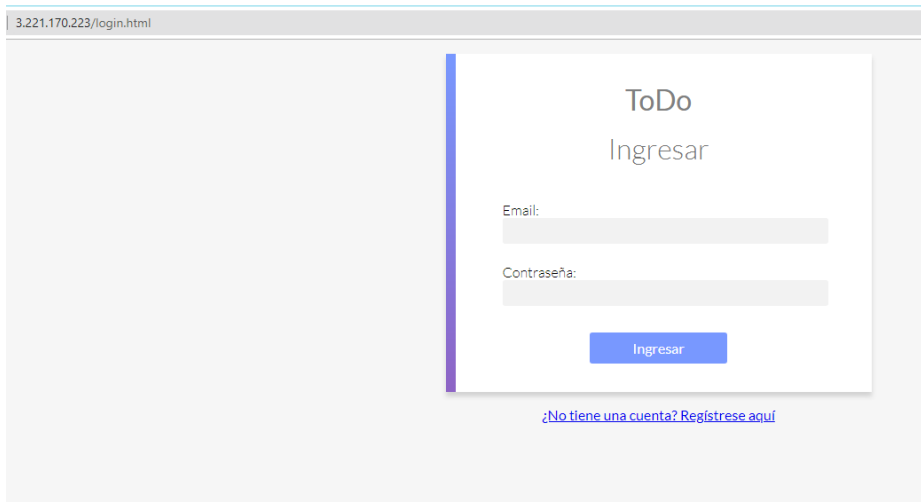
Luego, clonamos el repositorio del proyecto Front End II. En este caso, lo tenemos en el repositorio público de Github.

```
ubuntu@3.221.170.223:~$ sudo git clone
https://github.com/davidroco99/clase25.git

ubuntu@3.221.170.223:~$ sudo chmod 777 -R clase25/

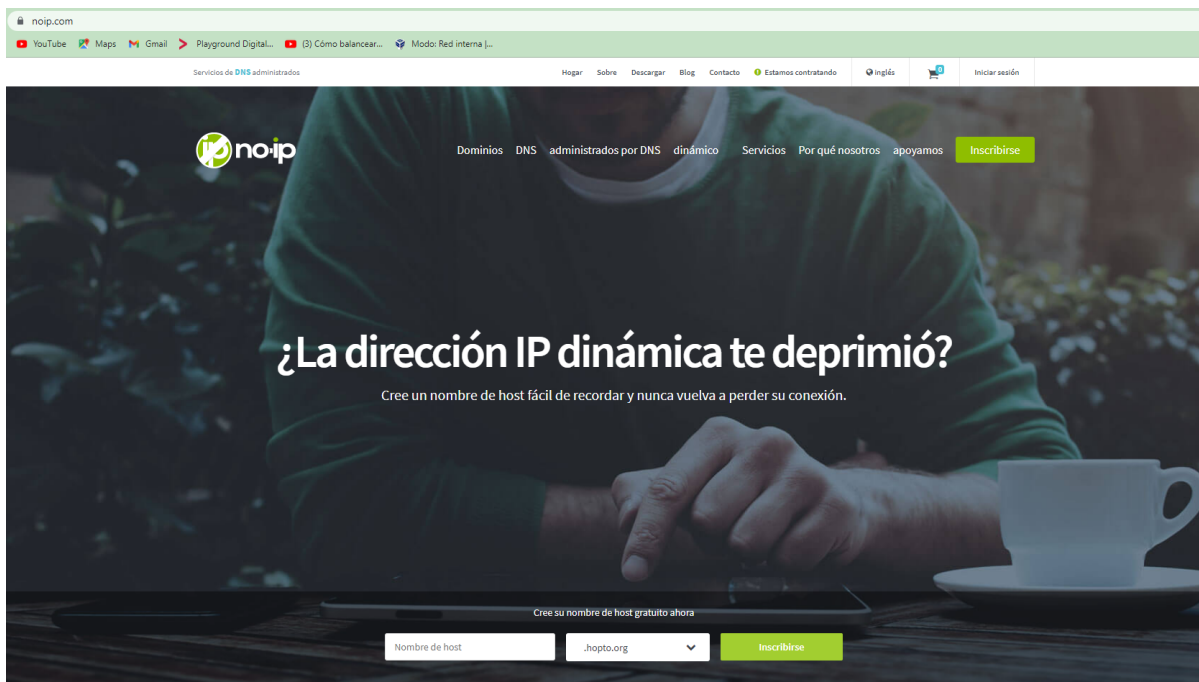
ubuntu@3.221.170.223:~$ sudo cp -rf clase25/* /var/www/html/
```

Ingresamos nuevamente a la instancia a través del navegador web.

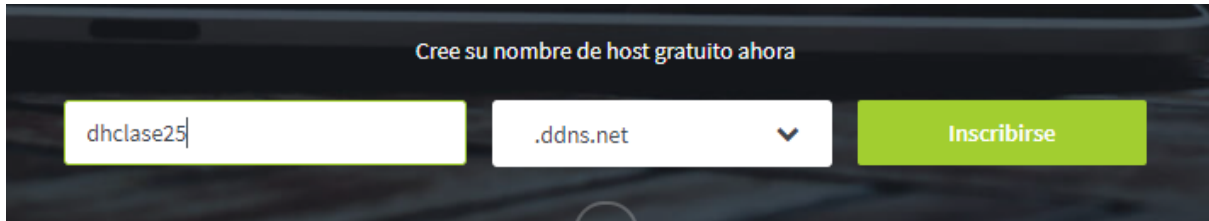


Generación del dominio en noip

Ingresamos en nuestro navegador a www.noip.com.



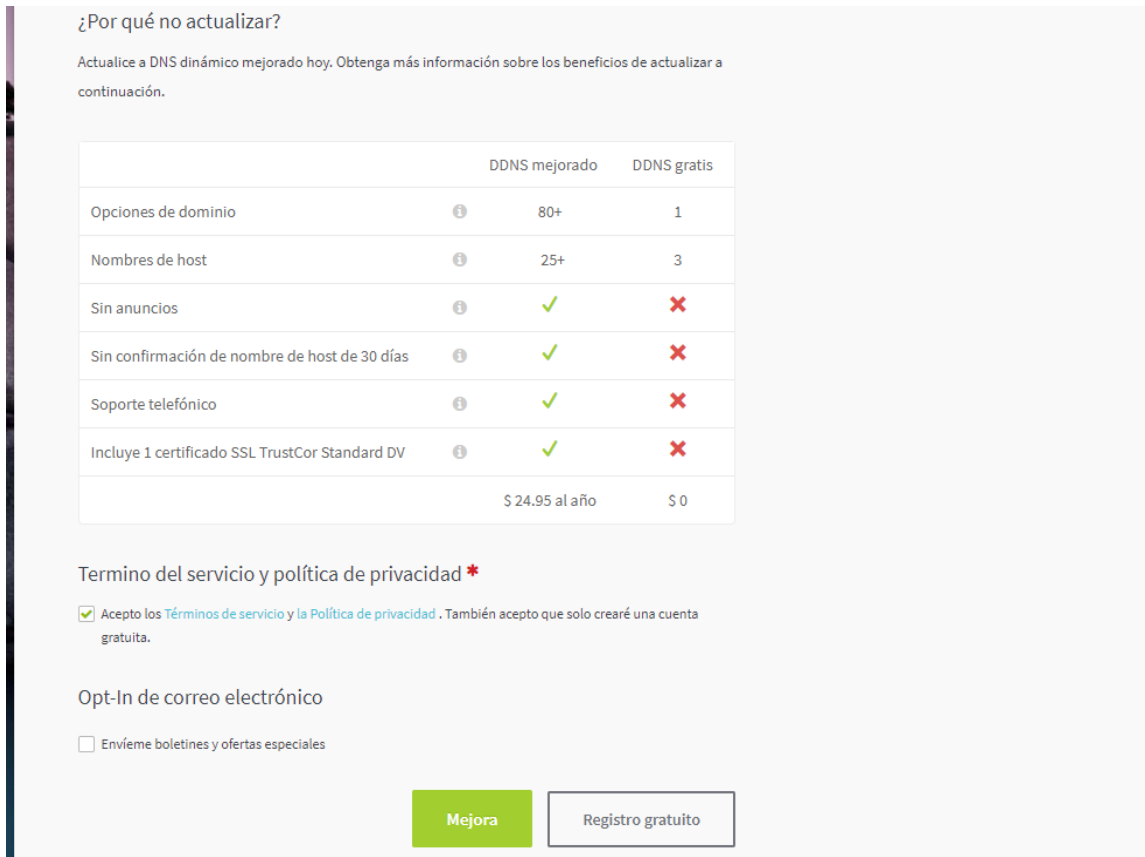
Luego, creamos nuestro nombre de dominio propio. Vale la pena aclarar que en este punto tenemos que colocar nuestro nombre único de dominio para poder redireccionar a nuestra EC2.



Cree su nombre de host gratuito ahora

dhclase25 .ddns.net Inscríbise

Tendremos que crear un registro en el sitio web y crear el registro gratuito.



¿Por qué no actualizar?

Actualice a DNS dinámico mejorado hoy. Obtenga más información sobre los beneficios de actualizar a continuación.

	DDNS mejorado	DDNS gratis
Opciones de dominio	80+	1
Nombres de host	25+	3
Sin anuncios	✓	✗
Sin confirmación de nombre de host de 30 días	✓	✗
Soporte telefónico	✓	✗
Incluye 1 certificado SSL TrustCor Standard DV	✓	✗
	\$ 24.95 al año	\$ 0

Termino del servicio y política de privacidad *

☒ Acepto los [Términos de servicio](#) y la [Política de privacidad](#). También acepto que solo crearé una cuenta gratuita.

Opt-In de correo electrónico

☐ Envíeme boletines y ofertas especiales

Mejora Registro gratuito

Confirmamos en nuestra casilla de correo electrónico y luego vemos lo siguiente:



Cómo acceder de forma remota a su dispositivo:

Paso 1 : crea un nombre de host. (este paso ya está completo)

Paso 2 : [descargue](#) el cliente de actualización dinámica (DUC).
El DUC mantiene su nombre de host actualizado con su dirección IP actual.

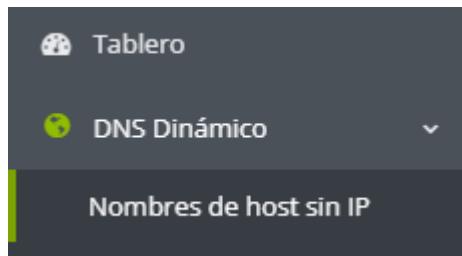
Paso 3 : [reenvíe el puerto de](#) su enrutador.

¿Terminaste con los 3 pasos?

Empiece a utilizar el DNS dinámico

Nuestra Guía de [inicio](#) tiene toda la información que necesita para comenzar.

Iniciamos sesión en www.noip.io , luego nos dirigimos en el menú de la izquierda a **DNS Dinámico** y finalmente **Nombre de host sin IP**.



Modificamos el dominio que creamos con la IP de la instancia de EC2 que creamos.

Nombre de host ▲	Última actualización	IP / destino	Escribe	
dhclase25.ddns.net Confirmar en 26 días	14 de octubre de 2021 10:11 PDT ⓘ	191.81.162.79	A	Modificar

⚙️ **Modificar nombre de host: dhclase25.ddns.net**

Dirección IPv4 ⓘ

4.209.70.39

Última actualización ⓘ

14 de octubre de 2021
10:11 PDT

☐ Desconectado ⓘ **Actualice a Mejorado** para habilitar la configuración sin conexión.

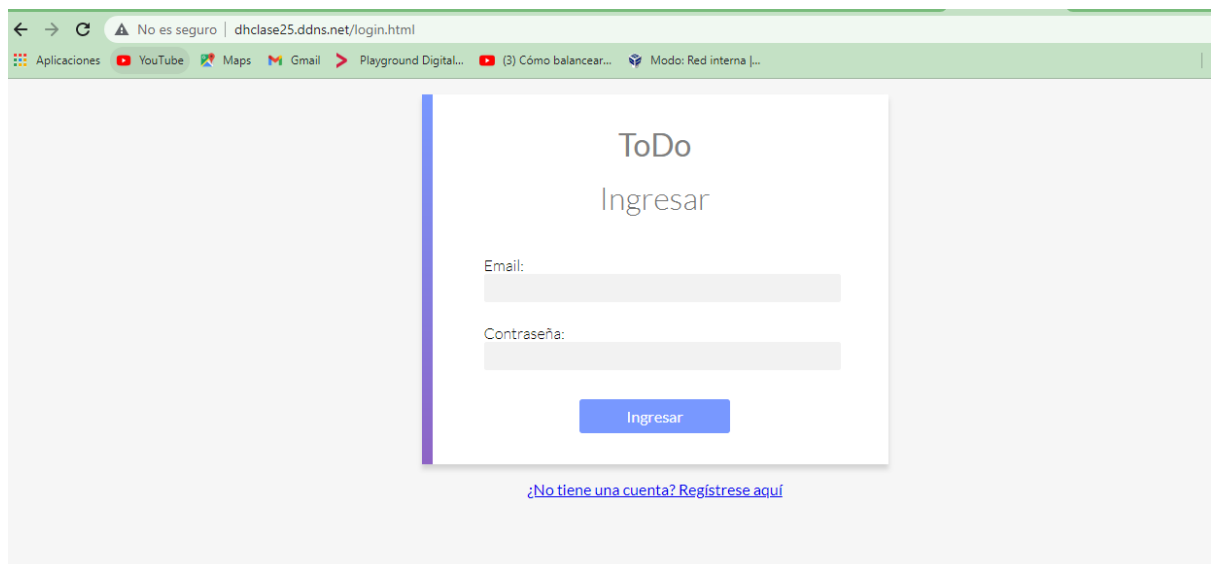
Registros MX

+ Agregar registros MX

Cancelar

Actualizar nombre de host

Damos en actualizar, y ¡listo! Ya tenemos **nuestro dominio online**. En este caso, **dhclase25.ddns.net** (recordá que este es el ejemplo que utilizamos para este tutorial. No podés usar este mismo dominio porque ya está ocupado).





Generación del certificado SSL en Let's Encrypt

Instalar Certbot

El primer paso para utilizar Let's Encrypt para obtener un certificado SSL es instalar el software Certbot en el servidor. Para ello ingresamos nuevamente a nuestra **instancia EC2** por medio de nuestro archivo **.pem** en la **AWS**. Luego, instalamos las dependencias necesarias:

```
ubuntu@3.221.170.223:~$ sudo apt-get install software-properties-common
```

Comprobamos la presencia del repositorio de universe.

```
ubuntu@3.221.170.223:~$ sudo add-apt-repository universe
```

Nuevamente actualizamos la lista de paquetes disponibles.

```
ubuntu@3.221.170.223:~$ sudo apt-get update
```

Certbot para Apache

Ejecutamos este comando desde nuestra línea de comandos para instalar Certbot:

```
ubuntu@3.221.170.223:~$ sudo apt-get install certbot python3-certbot-apache
```



Configuración de firewall (UFW)

Si el firewall UFW está habilitado, debemos crear una nueva regla para permitir el tráfico HTTPS. Para verificar si el firewall está activo, ejecutamos este comando:

```
ubuntu@3.221.170.223:~$ sudo ufw status
```

Para permitir el tráfico HTTPS para Apache:

```
ubuntu@3.221.170.223:~$ sudo ufw allow 'Apache Full'
```

Obtener un certificado SSL

Certbot utiliza el complemento Apache para obtener certificados SSL:

```
ubuntu@3.221.170.223:~$ sudo certbot --apache
```

Nos va a pedir un mail para registrarnos, y la configuración de los directorios que podemos responder "mail", "y" y "a".

```
ubuntu@3.221.170.223:~$ sudo certbot --apache
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
```

```
Plugins selected: Authenticator apache, Installer apache
```

```
Which names would you like to activate HTTPS for?
```

```
- - - - -
```



```
-  
  
1: dhclase25.ddns.net  
  
- - - - -  
-  
  
Select the appropriate numbers separated by commas and/or spaces, or leave  
input  
  
blank to select all options shown (Enter 'c' to cancel): 1  
  
Cert not yet due for renewal  
  
  
You have an existing certificate that has exactly the same domains or  
certificate name you requested and isn't close to expiry.  
(ref: /etc/letsencrypt/renewal/dhclase25.ddns.net.conf)  
  
  
What would you like to do?  
  
- - - - -  
-  
  
1: Attempt to reinstall this existing certificate  
2: Renew & replace the cert (limit ~5 per 7 days)  
  
- - - - -  
-  
  
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1  
  
Keeping the existing certificate  
  
Deploying Certificate to VirtualHost  
/etc/apache2/sites-enabled/000-default-le-ssl.conf
```



Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.

- - - - -
-

1: No redirect - Make no further changes to the webserver configuration.

2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for

new sites, or if you're confident your site works on HTTPS. You can undo this change by editing your web server's configuration.

- - - - -
-

Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2

Enabled Apache rewrite module

Redirecting vhost in /etc/apache2/sites-enabled/000-default.conf to ssl vhost
in /etc/apache2/sites-enabled/000-default-le-ssl.conf

- - - - -
-

Congratulations! You have successfully enabled <https://dhclase25.ddns.net>

You should test your configuration at:

<https://www.ssllabs.com/ssltest/analyze.html?d=dhclase25.ddns.net>

- - - - -



IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
`/etc/letsencrypt/live/dhclase25.ddns.net/fullchain.pem`
Your key file has been saved at:
`/etc/letsencrypt/live/dhclase25.ddns.net/privkey.pem`
Your cert will expire on 2022-01-16. To obtain a new or tweaked version of this certificate in the future, simply run `certbot` again with the "certonly" option. To non-interactively renew **all** of your certificates, run "`certbot renew`"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>

La ejecución de este comando permitirá obtener un certificado SSL y Certbot modificará automáticamente la configuración de Apache. De lo contrario, podríamos obtener el certificado SSL y luego configurar Apache manualmente con el siguiente comando:

```
ubuntu@3.221.170.223:~$ sudo certbot --apache certonly
```



Ingresamos nuestro dominio, en este caso **dhclase25.ddns.net**.

```
ubuntu@3.221.170.223:~$ sudo certbot --apache certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated) (Enter 'c' to cancel):
dhclase25.ddns.net
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for dhclase25.ddns.net
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/dhclase25.ddns.net/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/dhclase25.ddns.net/privkey.pem
  Your cert will expire on 2022-01-16. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
```

*again. To non-interactively renew ***all*** of your certificates, run "certbot renew"*

- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>

Renovación automática (opcional)

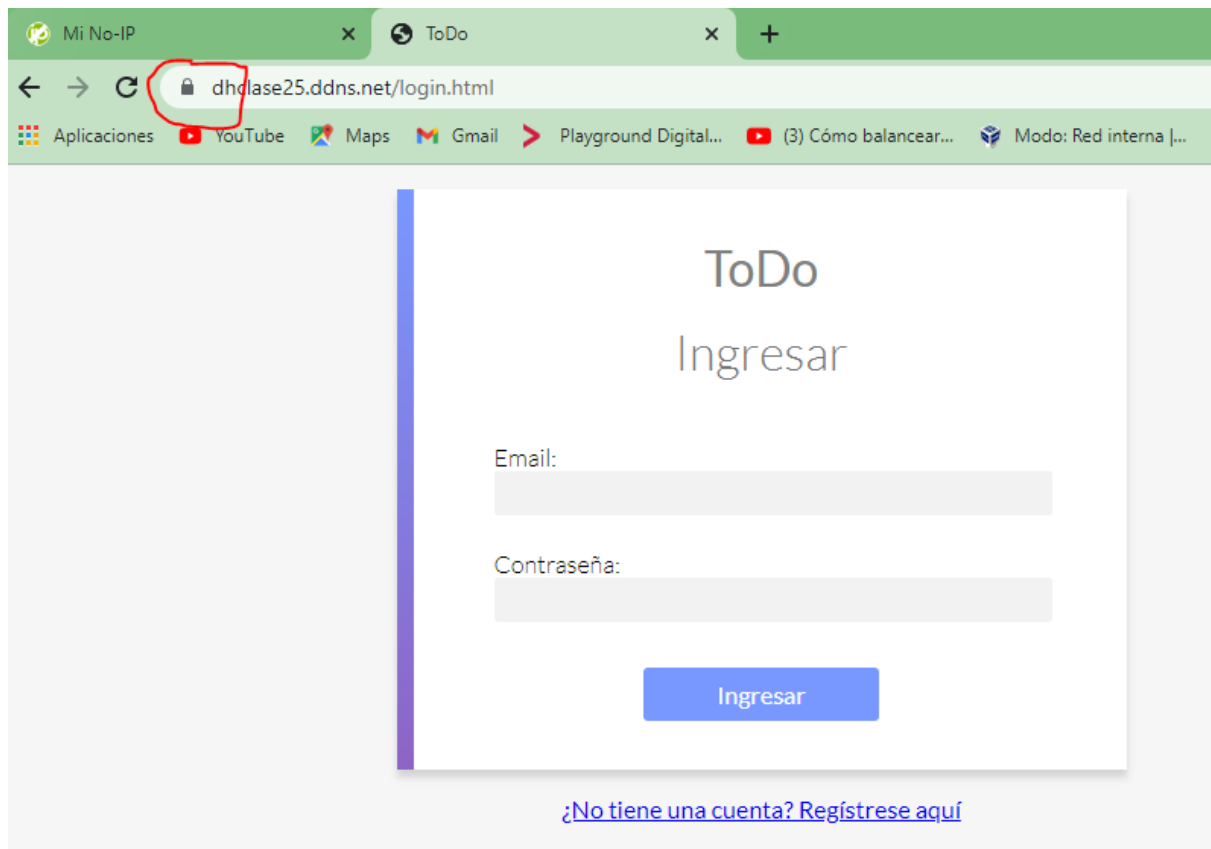
Los paquetes de Certbot vienen con un trabajo Cron que renovará automáticamente sus certificados antes de que caduquen. Dado que los certificados Let's Encrypt duran 90 días, se recomienda encarecidamente aprovechar esta función. Podemos verificar la renovación automática de certificados ejecutando este comando:

```
ubuntu@3.221.170.223:~$ sudo certbot renew --dry-run
```

El comando para renovar Certbot se instala en una de las siguientes ubicaciones:

- */etc /crontab /*
- */etc/cron.*/**
- *temporizadores de lista systemctl*

Para confirmar que Certbot se ha instalado correctamente, podemos visitar el sitio web configurado —**<https://dhclase25.ddns.net>**— en el navegador y buscar el ícono de candado en la barra de URL.



Conclusión

De esta manera hemos concluido con el tutorial para armar nuestro sitio con certificación **Let's Encrypt**. Esta nos permitirá brindar la seguridad necesaria para adjuntar información cifrada.