

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

REDES DE COMPUTADORAS

SERVICIOS EN LA NUBE

Profesor: Paulo Contreras Flores

Ayudante: Virgilio Castro Rendón

Ayudante Lab: Daniel Campuzano Barajas

## Objetivo

- El alumno implementará una infraestructura de servidores en la nube para ofrecer un servicio web.
- El alumno conocerá el proceso para contratar, configurar y poner en un ambiente de producción una aplicación web completa.
- El alumno pondrá en práctica los conceptos vistos en las clases de teoría y laboratorio como protocolos HTTP, HTTPS, DNS, SSH, de manejador de bases de datos, servidor proxy para caché, registro de un dominio, registros DNS, entre otros.

## Desarrollo

### I. Obtener un nombre de dominio

- I.1 Obtener un dominio que será utilizado para todo el proyecto, por ejemplo el dominio `proyectoredes.tk`.
- I.2 Se recomienda que sea a través de un proveedor que lo ofrezca de forma gratuita como Freenom <https://www.freenom.com>, este proveedor ofrece dominios gratuitos para ciertos dominios de nivel superior o TLD (*Top Level Domain*).

### II. Contratación de servidores virtuales

#### II.1 Contratación de dos servidores virtuales para albergar los siguientes servicios:

- un servidor, el que tenga asociado el dominio a su dirección IP, tendrá el servidor web y el servidor de correo electrónico.

- el otro servidor tendrá el servidor de aplicación y el servidor de base de datos.

II.2 Existen diferentes empresas para contratar los servidores, se recomienda alguna de éstas:

- Amazon Web Services (AWS), dentro del programa AWS Educate - Facultad de Ciencias. El servicio Amazon Elastic Compute Cloud (EC2).
- OVH. El servicio Virtual Private Server (VPS)

II.3 Cada servidor deberá contar con direcciones IP públicas y estáticas, tanto IPv4 como IPv6 <sup>1</sup>.

II.4 Cada servidor con la posibilidad de usar todos los puertos de la capa de transporte.

II.5 Instalar un sistema operativo en cada servidor, se recomienda Debian 9.

### III. Instalación y configuración del servidor Web

III.1 Instalar un servidor web, se recomienda Apache HTTPD.

III.2 Instalar los módulos necesarios para que se ejecute la aplicación.

III.3 Instalar los módulos necesarios para conexiones a través de HTTPS.

### IV. Configuración de los registros DNS, de una CDN y HTTPS

IV.1 Configuración de los registros DNS necesarios, se recomienda usar un servicio gratuito como Cloudflare <https://www.cloudflare.com>.

IV.2 Deberá estar asociado el nombre de dominio a la dirección IP de su servidor web.

IV.3 Se podrá consultar su sitio web de forma exitosa a través de por ejemplo, `proyectoredes.mx` o `www.proyectoredes.mx`.

IV.4 También se podrá consultar su sitio web usando una dirección IPv6, es decir su registros DNS deberán estar configurados para este tipo de peticiones.

IV.5 Para el punto anterior se recomienda usar Teredo para probar la conexión del cliente hacia el sitio web a través de IPv6.

IV.6 Deberán configurar una CDN (Content Delivery Network), se recomienda usar el servicio gratuito de Cloudflare.

IV.7 Cloudflare permite la configuración gratuita de hasta tres reglas de la caché de su sitio web en la CDN, deberán configurar estas reglas con base en su aplicación del sitio web. Esta configuración la pueden realizar una vez que ya tengan programada su aplicación. Se recomienda que las reglas sean para hojas de estilo (CSS), imágenes y/o programas en javascript.

IV.8 Cloudflare ofrece un certificado HTTPS gratuito, es compartido con otros sitios web, para el proyecto pueden utilizar éste.

---

<sup>1</sup>El contar con IPv6 es un punto pendiente que revisará el profesor

- IV.9 Se darán puntos sobre la calificación del proyecto si obtienen el certificado HTTPS a través de Let's encrypt <https://letsencrypt.org>, que también es gratuito.

Hasta este punto su sitio web ya podría ser consultado desde cualquier lugar colocando su URL en un navegador web, usando una conexión de direcciones IPv4. Debido a que aún no se realiza la aplicación, se mostrará la pantalla inicial de Apache. Las pruebas con IPv6 se pueden dejar al final del proyecto.

## V. Instalación y configuración del servidor de aplicación y de base de datos

- V.1 Instalar un manejador de base de datos, se recomienda MySQL.
- V.2 La lógica de la aplicación residirá en este servidor, por lo que se tendrá que configurar el servidor web para que se conecte a este servidor en donde se estará ejecutando los programas de la aplicación y regresarán el resultado al servidor web para que este último envíe la respuesta al usuario. Es decir, se deberá de configurar un Reverse proxy entre el servidor web y el servidor de aplicación.
- V.3 Las conexiones a la base de datos desde la aplicación se harán a través de un canal cifrado.

## VI. Programación de la aplicación

- VI.1 Al menos la aplicación consistirá en un Login, es decir, al menos deberá contar con autenticación de los usuarios a través de contraseñas, los usuarios y las contraseñas residirán en la base de datos, por lo que se tendrán que hacer consultas a ésta.
- VI.2 Se otorgarán puntos extras sobre la calificación del proyecto si la aplicación tiene más funcionalidades. Se recomienda una aplicación sencilla que no les involucre demasiado tiempo.
- VI.3 El lenguaje de programación, y en su caso el framework de desarrollo se dejará a elección de cada equipo.

## VIII. Configuración de un servidor de correo electrónico.

- VI.1 Configurar un servidor de correo electrónico para recibir y enviar correo electrónico con el mismo dominio que obtuvieron.
- VI.2 Para este punto la seguridad cobra mayor relevancia, por lo que deberán configurar correctamente el servidor para que no sea usado por terceros para mandar spam.
- VI.3 No debe estar en *open relay*.
- VI.4 Se deberán de configurar también los registros DNS para correo electrónico: para dirigir el correo electrónico del dominio al servidor de correo electrónico; para verificar la propiedad del dominio; para identificar qué servidor de correo puede enviar correos a nombre del dominio configurado.
- VI.5 Puntos extras sobre la calificación del proyecto si se usa el certificado creado con Let's encrypt para el servidor de correo electrónico usando SMTPS, IMAPS y/o POP3S.

## VII. Consideraciones sobre seguridad de la información

Debido a que sus servidores estarán expuestos en Internet, deberán de realizar unas configuraciones mínimas de seguridad.

- VII.1 Configurar el servidor de aplicación para que solamente acepte conexiones del servidor web.
- VII.2 Para la administración conectarse a través de SSH a los servidores, deberán cambiar el puerto predeterminado 22 al 2200.
- VII.3 No permitir la conexión remota por SSH al usuario root.
- VII.4 Crear un usuario dentro del manejador de bases de datos que solamente tenga permisos sobre la base de datos de la aplicación, no usar root para las conexiones de la aplicación.
- VII.5 No almacenar en claro la contraseña de los usuarios en la base de datos.
- VII.6 El servidor web no deberá de listar ni archivos ni directorios.
- VII.7 Instalar y configurar fail2ban para bloquear intentos de conexión no autorizados por fuerza bruta.
- VII.8 Programar de forma segura al menos la autenticación de usuario y contraseña, filtrando el contenido de los campos que se reciben desde el usuario para evitar un SQL injection.
- VII.9 Desinstalar servicios que no se usen en los servidores.

## Condiciones de entrega

- El proyecto lo podrán realizar en equipos de tres alumnos.
- Entregar un breve reporte en PDF que contenga
  - Diagrama de red de los servidores, indicando direcciones IP.
  - Registros DNS que se hicieron.
  - Resumen de las configuraciones del servidor web, servidor de aplicación, servidor de correo electrónico y base de datos.
  - Esquema de la base de datos.
  - Objetivo de la aplicación (redactado para un usuario).
  - Uso de la aplicación (breve descripción de como usarla con capturas de pantalla, pensando en un usuario).
  - Comentarios sobre el desarrollo del proyecto.
- Subir el documento a Moodle.
- Se podrán hacer preguntas por medio del foro de Moodle creado para este propósito. Si es necesario se podrá solicitar una o varias sesiones de preguntas y respuestas en los horarios de clase o del laboratorio.
- Cada equipo deberá de programar su sesión de revisión usando Google Calendar, se harán revisiones de tres equipos por día.
- Se usará la Rúbrica del final de este documento para calificar la exposición del equipo.

- El día de la revisión se harán preguntas de cualquier parte del proyecto a cualquier integrante del equipo, su respuestas influirán en la calificación, en la sección de puntos obtenidos de la Rúbrica.
- Se hará una prueba de estrés al sitio usando jmeter. Si está bien configurada la CDN, el sitio web debería seguir funcionando sin problema.
- La fecha de entrega de la documentación será el día lunes 29 de octubre antes de las 10 hrs., a través de Moodle.
- La fecha de revisión se hará en la semana del lunes 29 al viernes 3 de noviembre a la hora de clase.
- NO habrá prórroga.

## Rúbrica para el proyecto Servicios en la nube

*Nombre de los integrantes del equipo*


*Dominios*

Web	
Correo	

Requerimiento	Valor (ptos.)	Ptos. obtenidos
---------------	---------------	-----------------

<i>Configuración del dominio y registros</i>		
Dominio	5	
Registro A	5	
Registro CNAME	5	
Registro AAAA	5	
Registro SPF	10	
Registro TXT (para DKIM)	10	

<i>Configuración del servidor Web</i>		
Instalación	5	
Reverse Proxy	10	
Certificados para HTTPS	5	
Redirección de HTTP a HTTPS	5	
No permite listar ni directorios ni archivos	5	
Certificados de Let's Encrypt	+10	

<i>Configuración del servidor de Aplicación</i>		
Instalación	5	
Aplicación	5	
Funcionalidad de Autenticación	10	
No permite SQL injection	10	
No almacena las contraseñas en claro	10	
Sólo acepta peticiones del servidor Web	10	

Requerimiento	Valor (ptos.)	Ptos. obtenidos
---------------	---------------	-----------------

<i>Configuración del servidor de Base de datos</i>		
Instalación	5	
Conexiones cifradas hacia la BD	10	
Usuario de BD para consultas de la Aplicación	5	

<i>Configuración de la CDN</i>		
Reglas de CDN	10	

<i>Configuración del servidor de Correo</i>		
Instalación	5	
Envía correo electrónico	15	
Recibe correo electrónico	15	
Sin open relay	10	
Configuración de SMTPS	+15	
Configuración de IMAPS	+15	
Configuración de POP3S	+15	

<i>Otras configuraciones de seguridad</i>		
El puerto de SSH deberán cambiarlo a puerto 2200	5	
No permitir la conexión remota al usuario root	5	
Fail2ban para el puerto 2200	10	
Desinstalación de servicios sin utilizar en servidores	5	

<i>Pruebas</i>		
registro SPF <a href="https://tools.sparkpost.com/spf/inspector">https://tools.sparkpost.com/spf/inspector</a>	10	
prueba DKIM <a href="https://tools.sparkpost.com/dkim">https://tools.sparkpost.com/dkim</a>	10	
prueba Jmeter <a href="https://jmeter.apache.org/">https://jmeter.apache.org/</a>	10	