4 GESTIÓN DE SERVICIOS DE CORREO ELECTRÓNICO

Gracias al correo electrónico es posible intercambiar distintos mensajes haciendo uso de los sistemas de configuración electrónicos. Para realizar este proceso, se utiliza el protocolo **SMTP** (***simple mail transfer protocol***), es decir, protocolo simple de transferencia de **correo**.

El correo electrónico recurre a una forma análoga a la del correo postal para poder funcionar.

Ambos pueden enviar y recibir información (mensajes) con el fin de que lleguen al buzón correspondiente al que son enviados (direcciones personales).

El correo electrónico utiliza como buzón un servidor de correo.

APLICACIÓN	← **Correo**
Transporte	
Red	
Enlace	
Físico	

¿SABÍAS QUE...?

En 1961, el MIT (Massachussett Institute of Technology) ya pensaba en la necesidad de que varios usuarios pudieran acceder a un equipo de forma remota y que los datos pudieran almacenarse de la misma manera. Aunque esta idea no fue consolidándose hasta 1965, cuando el concepto de correo electrónico ya se englobaba dentro de una red informática.

4.1. Protocolos y servicios De Descarga De correo

Protocolos de descarga de correo

POP **IMAP**

Losdosprotocolosdecorreoelectrónicomásutilizados son **POP** e **IMAP**.

- **POP *(post office protocol)*:** este protocolo de oficina de correos se utiliza a la hora de recibir correos.

Ofrece al usuario la posibilidad de descargar, en su ordenador, los correos recibidos por si necesita realizar cualquier cambio o modificación sobre ellos sin necesidad de que esté conectado a la red.

Se utiliza desde el año 1980, aunque desde entonces ha mejorado algunos de sus aspectos como:

– RFC 918 → define el protocolo POP1

– RFC 937 → define el protocolo POP2

- RFC 1081 y 1039 → define el protocolo POP3
- RFC 1734 → Fija el mecanismo de autentificación y cifrado

Algunas de las versiones anteriores apenas se utilizan y otras, incluso, han desaparecido.

Hoy en día, el **POP3** es el más utilizado y su funcionamiento consiste en:

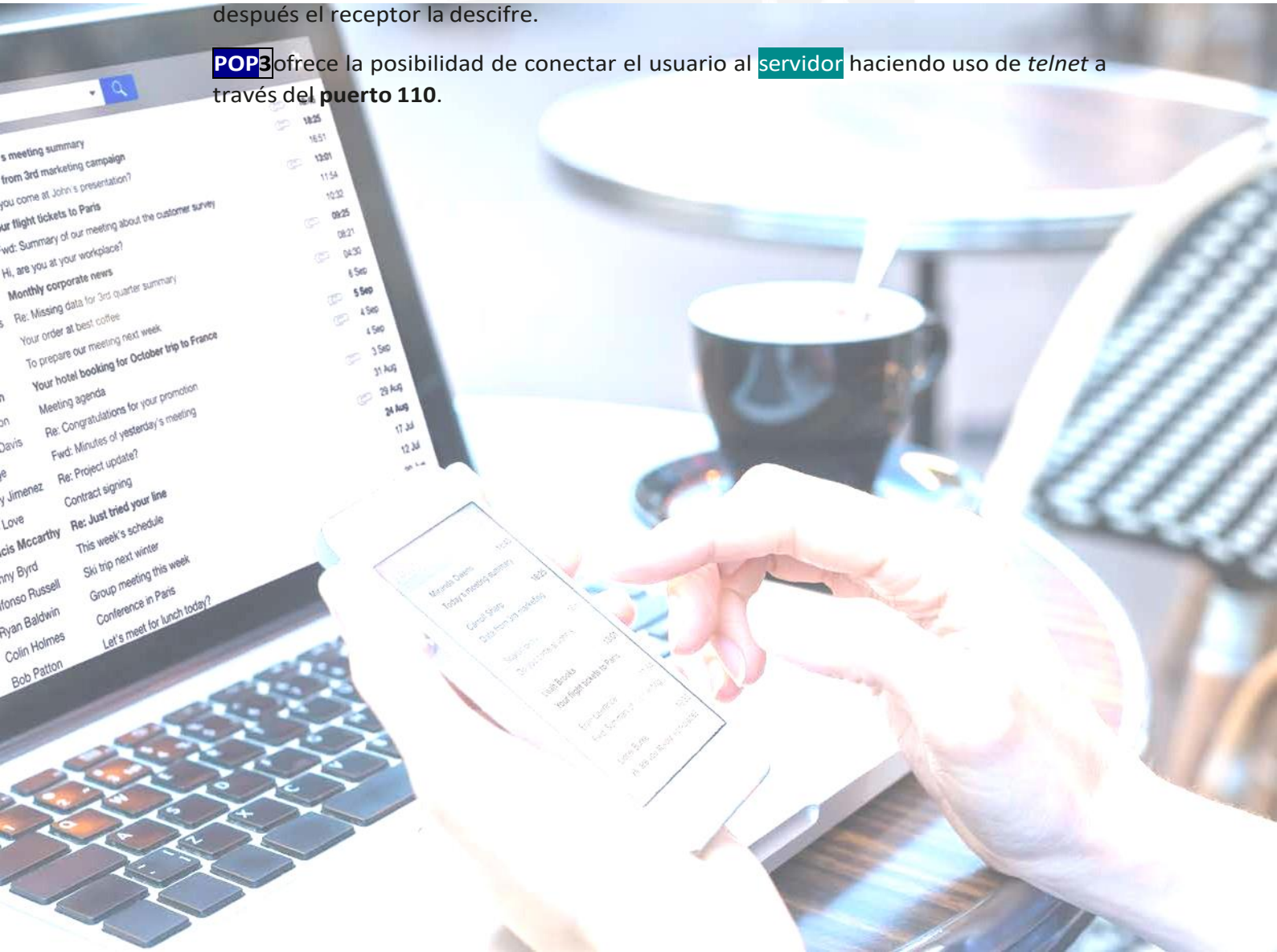
- *Al principio*, el usuario se conecta al servidor para descargar los mensajes.
- *A continuación*, los graba en un equipo local y los marca para que se almacenen como si fueran nuevos.
- *Finalmente*, ya los puede eliminar del servidor y se puede desconectar.

El **protocolo POP3** se basa en una autentificación sin cifrado.

Para conseguir una mayor seguridad, existe la **extensión APOP *(authenticatied POP)*** o **POP** autenticado.

Estas extensiones ofrecen al emisor la posibilidad de cifrar la contraseña para que después el receptor la descifre.

POP3 ofrece la posibilidad de conectar el usuario al servidor haciendo uso de *telnet* a través del **puerto 110**.



- **IMAP**

(Internet Message Access Protocol):

Este protocolo de acceso a mensajes de internet se utiliza, sobre todo, para recibir correos.

Ofrece al usuario la posibilidad de acceder al servidor de correo desde cualquier equipo mediante el acceso a internet.

De esta forma, puede definir una serie de carpetas en el servidor para poder ir

almacenando los distintos mensajes. Este proceso ayuda a disminuir la incidencia de virus.

Este protocolo se creó en el año 1984 con la idea de poder ser una alternativa al protocolo POP. Hoy en día, la versión más utilizada es la **IMAP4**.

– RFC 3501 → define esta versión

Los usuarios (IMAP4) pueden estar conectados todo el tiempo que su enlace permanezca activo y los mensajes se irán descargando según sean demandados. De esta forma, se mejora el tiempo de respuesta.

IMAPS utiliza como referencia el protocolo IMAP cifrado mediante la utilización de SSL (secure cockets) o mediante una capa de conexión segura.

Protocolo de envío de correo SMTP

- **SMTP *(simple mail trasfer protocol)***: este protocolo de transferencia de correo simple tiene como objetivo principal definir ciertos comandos y funciones que permitan el intercambio de información (mensajes) entre dos dispositivos diferentes a través del correo electrónico.

  Diseñado desde el año 1982 para conseguir la transferencia de mensajes en código ASCII. A lo largo de los años, ha ido incorporando una serie de mejoras, como:

  – RFC 2821 → define ESMTP o SMTP extendido.

  – Gestiona mensajes mayores de 64 KB y utiliza temporizadores para que no se interrumpan mensajes entre servidores.

  – RFC 2920 → al utilizar diferentes comandos en un único envío, consigue aumentar la productividad del servidor SMTP.

  – RFC 3030 → permite utilizar mensajes MIME.

Funcionamiento del protocolo

Su objetivo principal es conseguir entregar un mensaje determinado a su destinatario. Para ello, se deben seguir los siguientes pasos:

1. El cliente estructura el mensaje de correo y lo envía a través del puerto 25 desde el servidor SMTP, denominado **servidor de correo saliente**.
2. El servidor saliente lanza una petición hasta un servidor DNS. Se asocia la IP del servidor emisor con el del receptor. Cuando tengamos la confirmación de que existe un enlace, entonces podemos enviar el paquete.

3. El servidor saliente (SMTP) reenvía el mensaje al servidor de correo (SMTP) del receptor.
4. El servidor SMPT destinatario que recibe el correo, lo tiene que procesar para, posteriormente, dejarlo en el buzón de entrada.

Comandos

El origen del SMTP se encuentra en los protocolos del FTP, por lo que hace uso de sus comandos. En la siguiente tabla, se detallan algunos de los más importantes:

Comandos SMTP	
Comando	Definición
HELO/ EHLO	Identifica al cliente
MAIL FROM	Identifica la remitente
RCPT TO	Identifica a los destinatarios
DATA	Generado por el cliente para indicar que el envío ha comenzado

Códigos de respuesta

La respuesta que ofrece el servidor se expresa mediante un **código formado por tres dígitos**. En la siguiente tabla, se ve cómo el primero de ellos puede tomar cinco valores distintos:

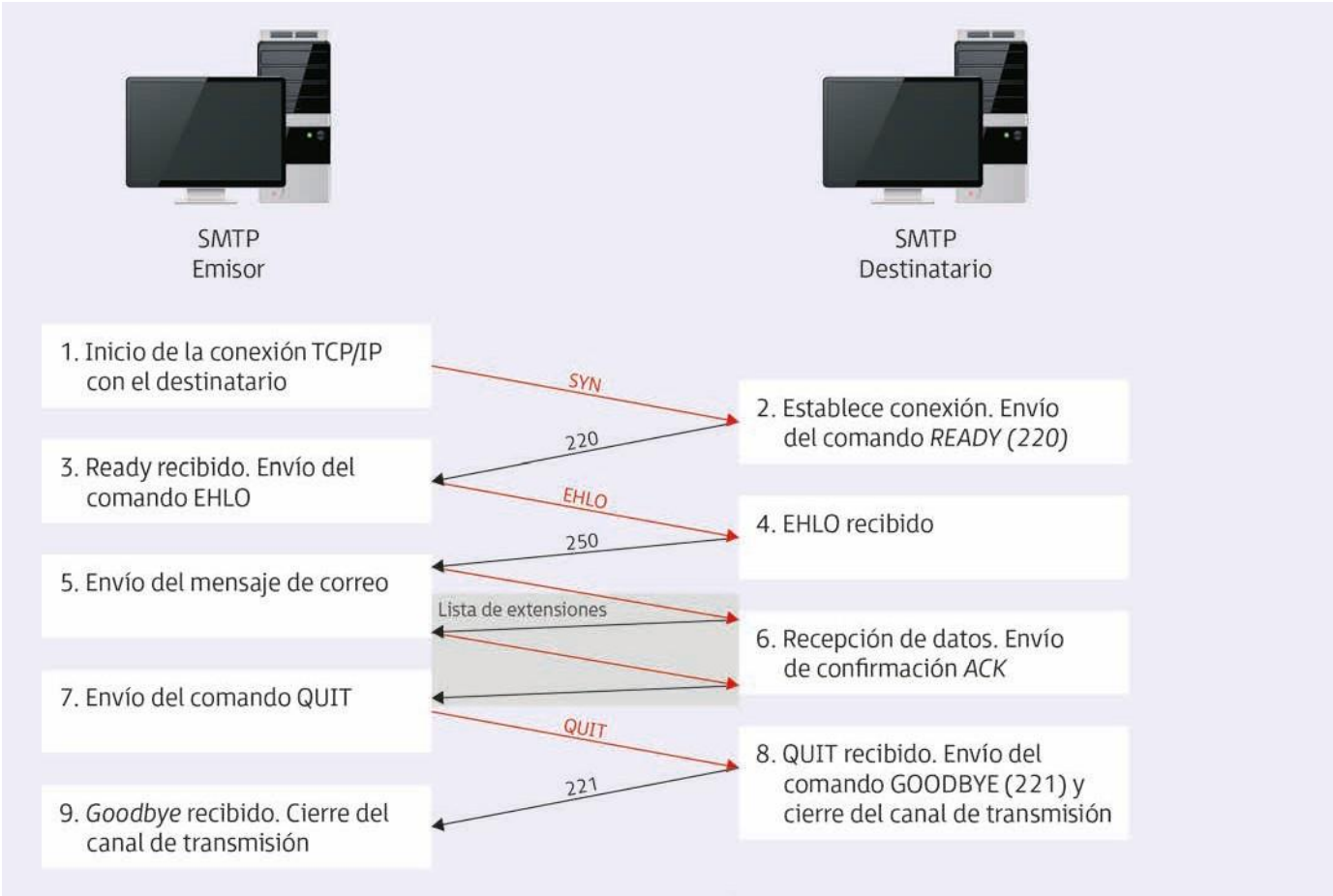
Códigos de respuesta SMTP	
Dígitos Xyz	**Definición**
1yz	Si se acepta el comando, se suspende la acción hasta que el cliente determine si va a continuar o no.
2yz	Si se realiza la acción con éxito.
3yz	Si se acepta el comando, la acción queda pendiente hasta que el cliente haga otro envío con más información.
4yz	Si no se acepta el comando, el cliente puede volver a iniciar la secuencia de comandos.
5yz	Si no se acepta el comando y es necesario que alguna persona intervenga para corregir la petición.

Procedimiento

Cuando los mensajes de correo electrónico se transmiten, lo hacen en tres fases:

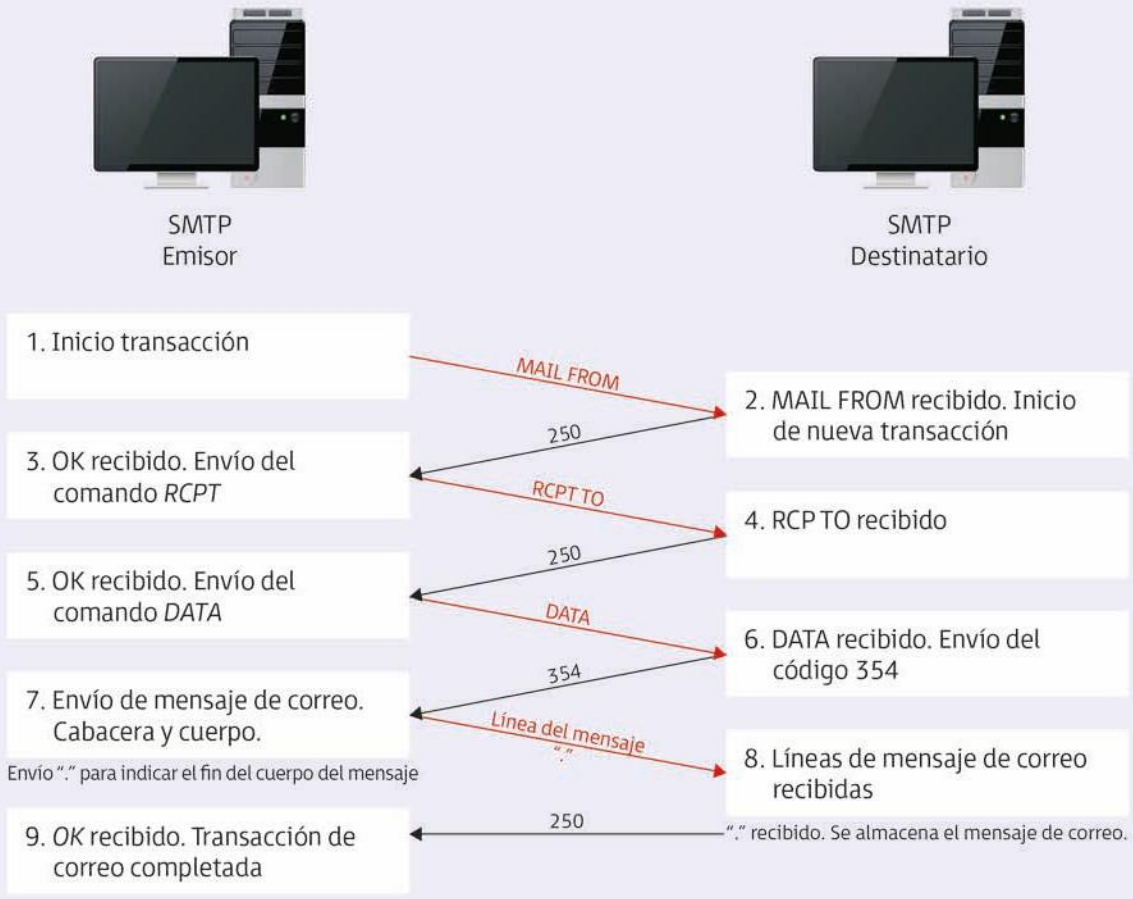
1. Se crea la conexión SMTP para iniciar sesión.
2. Se pone en marcha la transacción SMTP mediante el envío del correo electrónico.
3. Por último, se cierra sesión y se finaliza la conexión SMTP.

Cuando se realiza la transacción se utiliza una serie de comandos que permiten transmitir el contenido del mensaje. Para cada comando, el destinatario **SMTP** genera una respuesta que determina si el comando ha sido aceptado, si sigue esperando comandos o si existe algún error.



Envía por correo el contenido del mensaje mediante el comando **DATA**. Si el receptor acepta el mensaje, remite un código de respuesta 354 para considerar a las demás líneas del mensaje como texto del mensaje. Cuando finalice el envío, se puede identificar con ***<CRLF>.<CRLF>*.**

Una vez se reciba el final del mensaje, ya se puede almacenar y confirmar que se ha recibido.

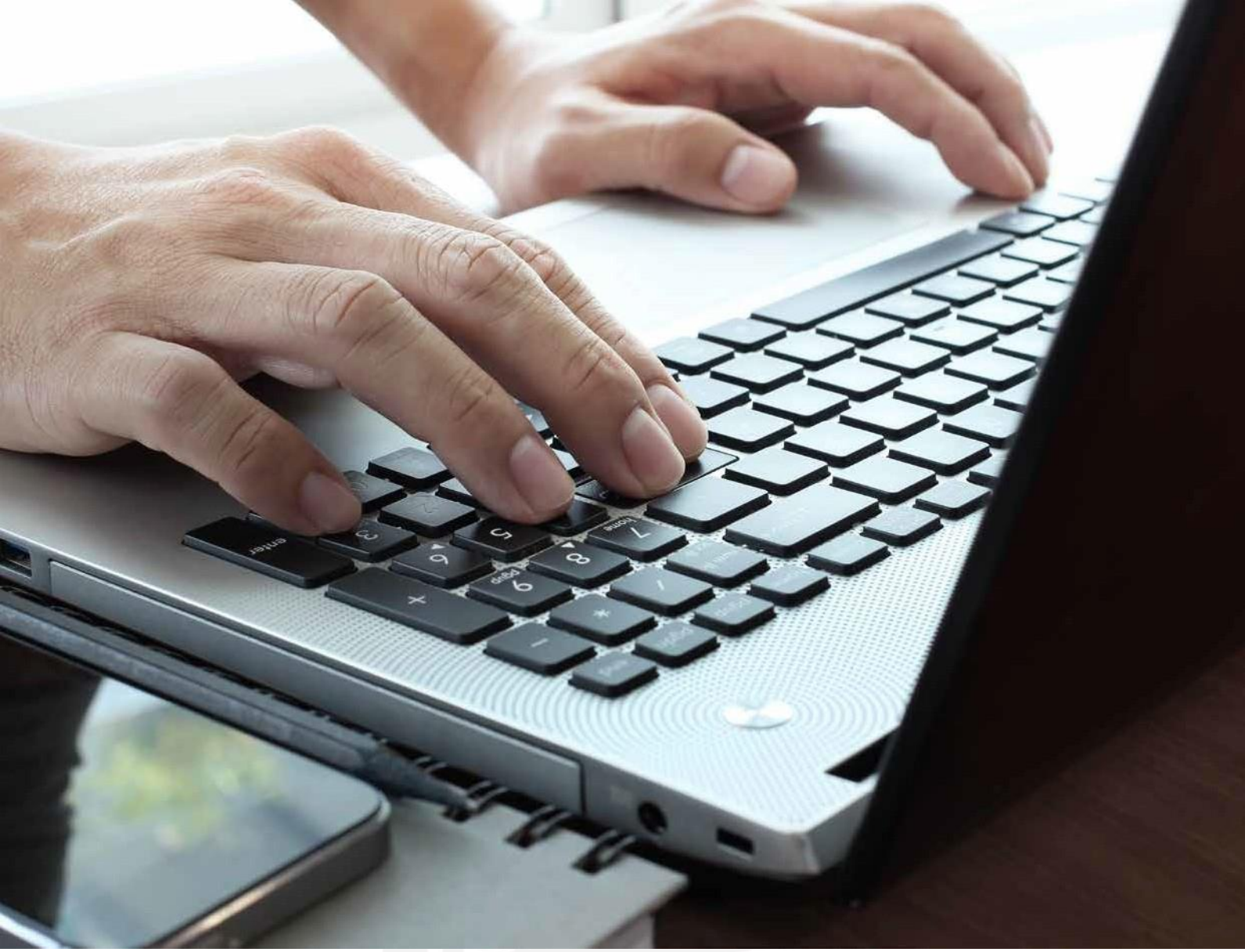


4.2. Instalación De un servicio De correo electrónico

Para poder instalar esta herramienta del correo electrónico se ha de tener en cuenta que el servidor de correo no viene instalado previamente en el sistema **Windows Server**, así que antes de la instalación, se debe adquirir alguna aplicación extra para llevar este proceso a cabo.

Asimismo, hay que conocer una serie de **requisitos** previos al proceso de instalación:

- Todos los trabajadores deben conocer la herramienta mediante la cual van a poder hacer uso del correo electrónico.
- Este correo electrónico va a tener acceso de la intranet hasta cualquier equipo conectado a la red.
- Cada usuario debe tener asignada su propia cuenta de correo electrónico privada y, para entrar a ella, debe autentificarse.



Instalación del servidor

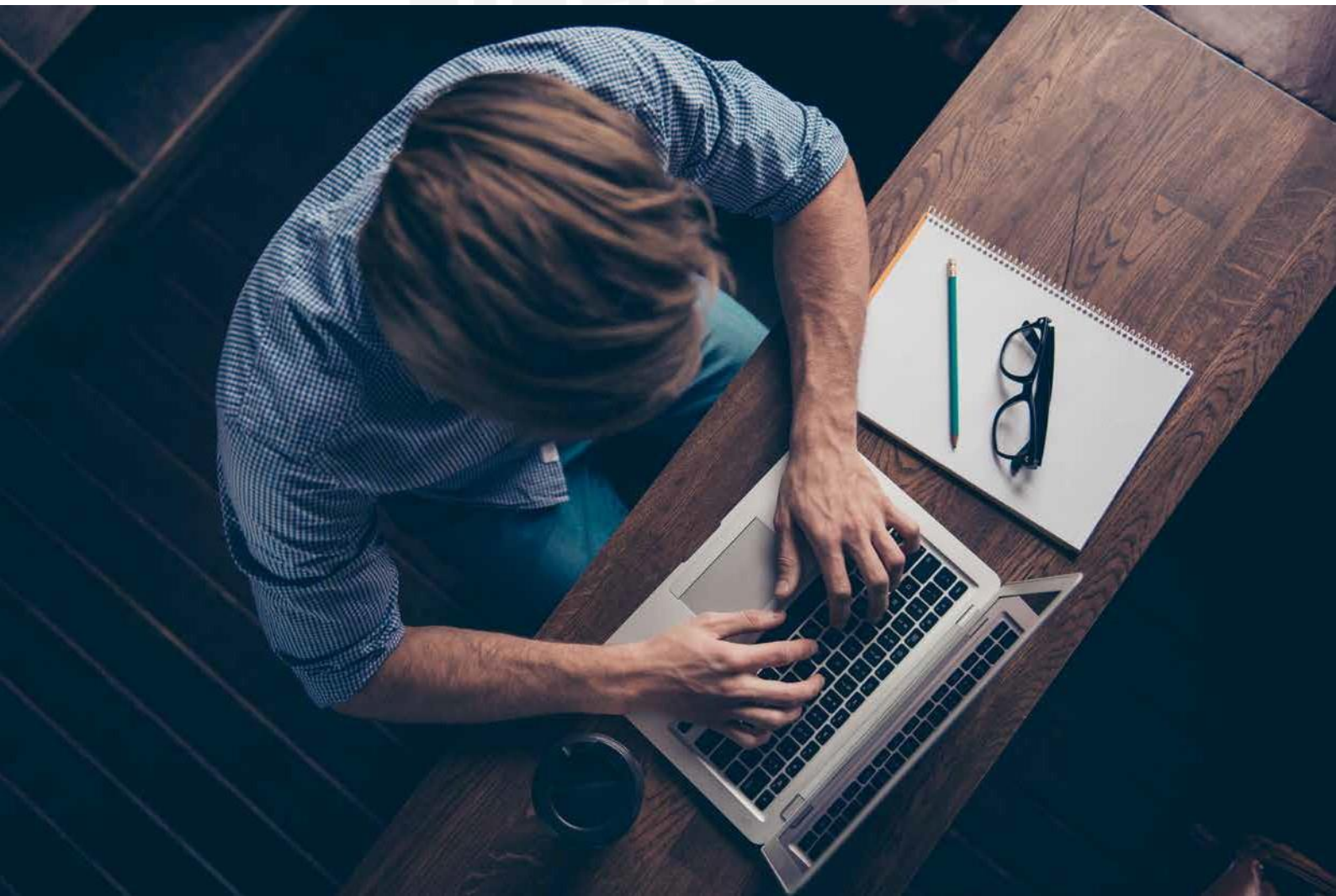
Preparación del sistema

Antes de empezar con la instalación de **Exchange Server**, es necesario:

1. Hacer clic en *Inicio* y seleccionar *Administrador del servidor.*
2. En la ventana que se muestra, en la parte de la izquierda, seleccionar *Administrador del servidor/SERVIDOR/ Funciones* y elegir la opción *Servidor web (IIS).*
3. A continuación, en la parte de *Resumen/Servicios de función* elegir *Agregar servicios de función.*
4. En la ventana *Seleccionar servicios de función,* marcar la opción *ASP. NET*. Una vez hecho esto, se marcan de forma automática las demás opciones de *Extensibilidad de .NET, Extensiones ISAPI y Filtros ISAPI.*

5. La opción *ASP. NET* necesita añadir una serie de servicios más para conseguir un correcto funcionamiento. Así que hay que clicar en *Agregar servicios de función requeridos.*
6. En la ventana *Seleccionar servicios de función*, marcar:
   - Inclusión del lado servidor.
   - En el apartado de *Seguridad*, seleccionar *Autenticación de Windows y Autenticación implícita.*
   - En el apartado *Rendimiento*, seleccionar la opción *Compresión de contenido dinámico.*
   - Marcar también la opción *Compatibilidad con la administración de IIS 6.*
   - A continuación, se muestra la ventana *Confirmarselecciones de instalación* con un resumen de las opciones seleccionadas hasta el momento. Clic en *Instalar.*
   - Pasado el tiempo de instalación, clic en *Cerrar* para finalizar.

Ya hemos terminado de preparar el sistema, pero, necesitamos también instalar **Windows PowerShell** antes de seguir avanzando, por lo que, ahora seguimos los pasos que, detallamos a continuación:



1. En *Inicio* seleccionar la opción *Administrador del servidor.*
2. Del bloque *Resumen de características/Características* elegir la opción *Agregar características.*
3. En la nueva ventana que aparece, marcar la casilla para verificar *Windows PowerShell*. Clic en *Siguiente.*
4. Seleccionar el botón *Instalar* para comenzar la instalación.
5. Una vez trascurrido el tiempo estimado para realizar la instalación, se finaliza haciendo clic en *Cerrar.*

Llegados a este punto, ya es posible iniciar el proceso de instalación.

Instalación de Microsoft Exchange Server

Para comenzar a instalar **Microsoft Exchange Server,** hay que seguir estos pasos:

1. Ejecutar el archivo previamente descargado. Seleccionar una carpeta para extraer los archivos y hacer clic en *Aceptar.*
2. Comenzar la instalación clicando en *Setup.*
3. Seleccionar *Paso 5: instalar Microsoft Exchange Server.*
4. Comienza el asistente de instalación. Clic en *Siguiente.*
5. En la casilla *Informe de errores*, marcar la opción *No.* Clic en *Siguiente.*
6. Elegir la instalación típica de *Exchange Server.* Clic en *Siguiente.*
7. A continuación, aparece la ventana de *Organización de Exchange* en la que se debe indicar el nombre de la organización que corresponda. Clic en *Siguiente.*
8. Marcamos la casilla *No* ya que no existen equipos con versiones anteriores. Clic en *Siguiente* y después *Instalar.*
9. Cuando se ha terminado el proceso de instalación, clic en *Finalizar.*
10. Hecho esto, es conveniente *reiniciar el equipo*.

4.3. Cuentas De correo

CONCEPTO

Mediante las cuentas de correo podemos identificarnos dentro del servicio para que podamos enviar y recibir información.

Existe un **proveedor de servicio de Internet ISP *(Internet Service Provider)*** que ofrece la posibilidad de obtener una cuenta de correo electrónico en sus servidores mediante un **agente de correo MUA *(Mail User Agent)*.**

Las diferentes cuentas de correo se dividen en dos partes, separadas entre ellas por medio del símbolo @.

- La primera parte hace referencia al **nombre de usuario** de la cuenta.
- La segunda parte al **dominio del servidor de correo** en el que se encuentra alojada la cuenta.

Por ejemplo, **ilerna@servidor1.com**

Esta dirección de correo electrónico indica que la dirección de correo del **usuario ilerna** se encuentra en el servidor "servidor1". En él no pueden existir dos direcciones iguales, aunque el **usuario ilerna** puede tener más de una dirección de correo siempre que sean de servidores diferentes.

Las diferentes formas que existen a la hora de configurar las descargas de las cuentas de correo electrónico, según el protocolo, son las siguientes:

- **IMAP *(Internet Message Access Protocol)***: protocolo de acceso a los mensajes de internet. Guarda los mensajes en el servidor de correo.
- **POP *(Post Office Protocol)*:** protocolo de oficina de correos. Guarda los mensajes en el equipo del usuario.

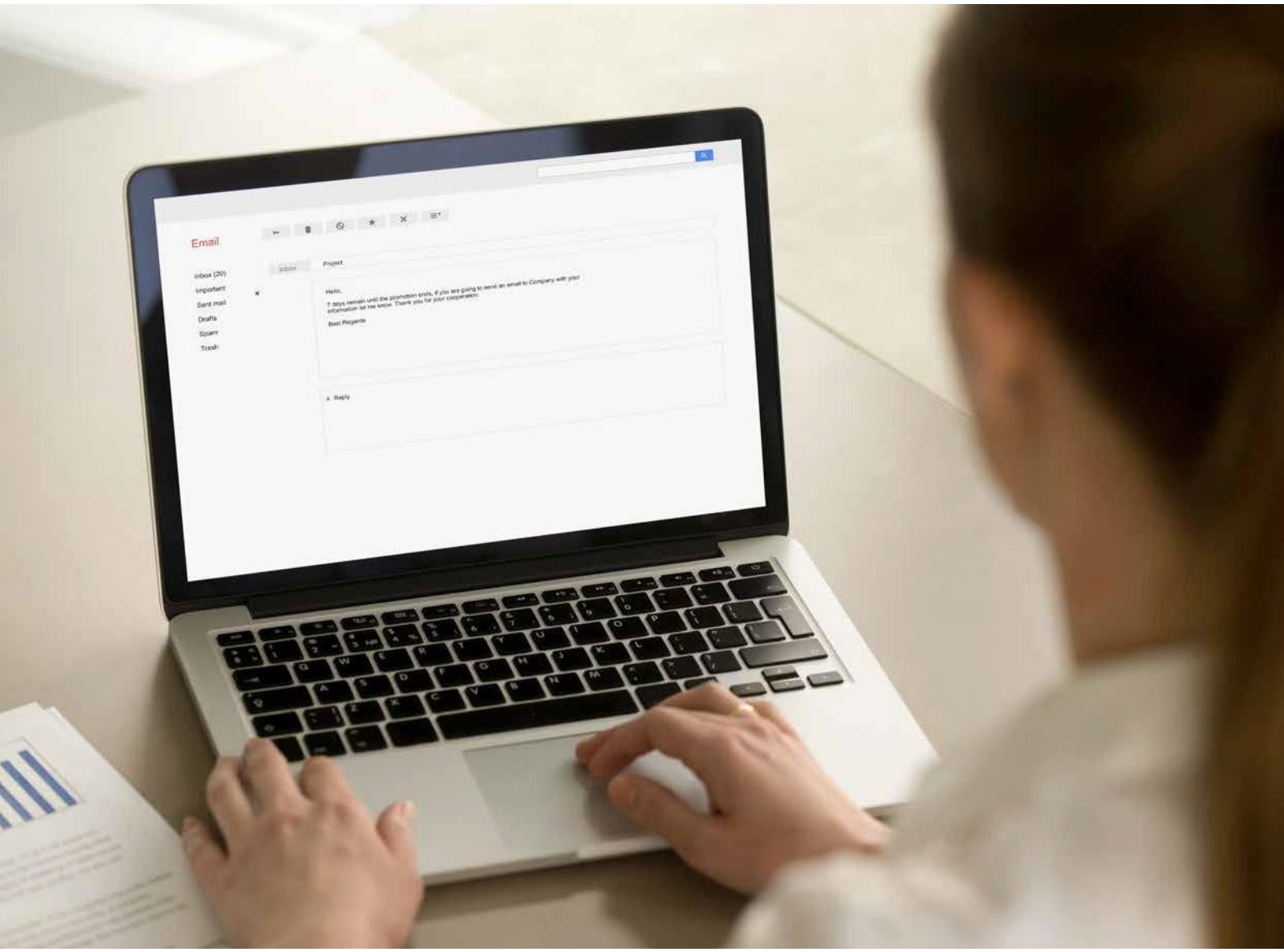
4.4. Alias y buzones De usuario

Alias de buzón

Los alias son una especie de apodo o sobrenombre que suele utilizarse para llamar alguien de una forma más cercana o familiar. Los alias de correo electrónico se utilizan, entre otras cosas, para reenviar correos sin tener que utilizar la dirección original completa.

Existen dos tipos diferentes de alias para los correos electrónicos:

- Los que pueden reemplazar a uno o más de un correo específico.
- Los denominados **universales**, "de sistema" o "sumidero", que se encargan de recoger el correo de todas aquellas direcciones posibles que no estén asignadas a ningún usuario que esté dado de alta.

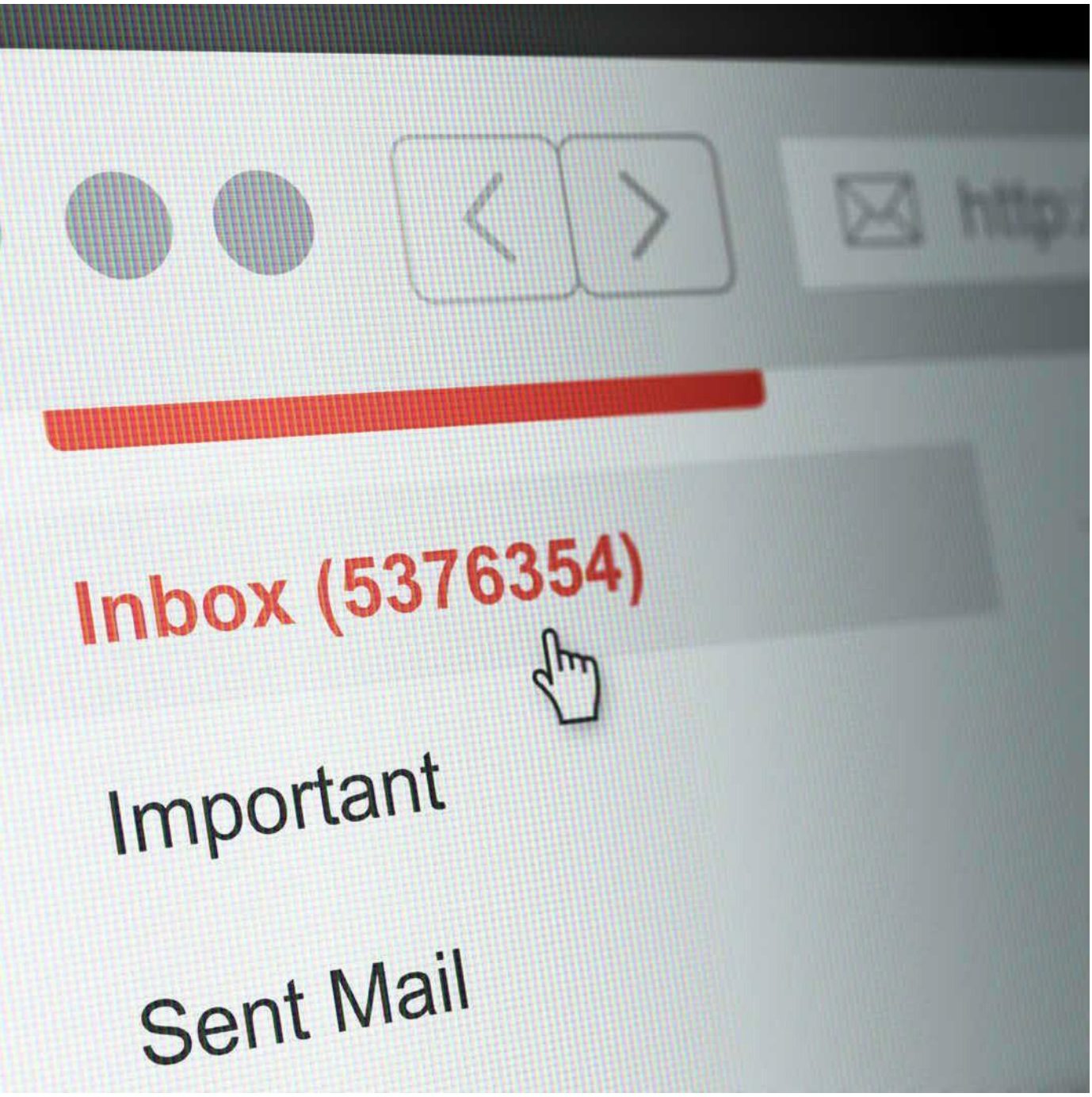


Buzones de usuario

Son una serie de subcarpetas del sistema de correo electrónico del usuario en las que se pueden almacenar los mensajes recibidos. Por tanto, ya que un usuario puede tener diferentes cuentas, así también puede tener varias carpetas de una misma cuenta o diferentes usuarios de un servidor de correo específico. Estas carpetas se pueden crear de forma real o virtual.

4.5. Protección Del serviDor Para imPeDir usos inDebiDos

En un primer momento, cuando se diseñaron los diferentes protocolos de correo electrónico no era imprescindible que se llevaran a cabo mediante mecanismos de seguridad,



por lo que estaba permitido que cualquier servidor pudiera aceptar peticiones desde cualquier origen. Este es uno de los motivos por los que los SMTP no necesitaban autentificarse, lo cual posibilitaba que el *spam* o correo no solicitado.

Las principales características del *spam* son:

- **Anónimo:** no envía la dirección de correo del emisor y, en algunos casos, utiliza la de otra persona para no mostrar su identidad.
- **Duplicativo:** cuando se reciben correos que tienen contenido bastante parecido.

Las diferentes formas de *spam* son:

- **Publicidad no deseada:** no dañan la información y su característica principal es que son mensajes que se utilizan para temas comerciales.
- ***Hoax* (bulo):** mensajes que contienen noticias falsas pidiendo colaboración al usuario para determinadas tareas, con el fin de conseguir el mayor número de direcciones de correo electrónico posibles.
- ***Phishing:*** pretenden engañar a los usuarios haciéndoles creer que los correos recibidos vienen de una entidad oficial o pública.

Para no caer en el engaño de ningún *spam*, se debe tener en cuenta una serie de características:

- Es conveniente no facilitar información personal a través del correo electrónico.
- No pinchar en los distintos hiperenlaces que aparezcan, incluso si vienen de algún usuario conocido.
- No publicar la dirección de correo electrónico.
- Ignorar los mensajes que se van reenviando.
- No dar contestación a los correos basura.
- Comprobar siempre que la conexión es segura.

4.6. Configuración Del servicio De correo

Como ya se ha detallado en apartados anteriores, el acceso de los clientes a través del correo electrónico debe constar de una **dirección de correo electrónico** y una **contraseña.**

Las direcciones de correo electrónico son únicas (no se pueden repetir) dentro de un mismo servidor y es recomendable que la contraseña no sea descifrable fácilmente. Siempre ofrecen una mayor seguridad cuando se mezclan caracteres con números y con algún símbolo de los permitidos.

Creación de un buzón de usuario para el correo electrónico

Para llevar a cabo el proceso de configuración, es necesario seguir los siguientes pasos:

1. Abrir la *Consola de administración de Exchange/Configuración de destinatarios.*
2. Aparece una ventana. En su parte central, botón secundario para seleccionar la opción *Buzón nuevo* del menú contextual.

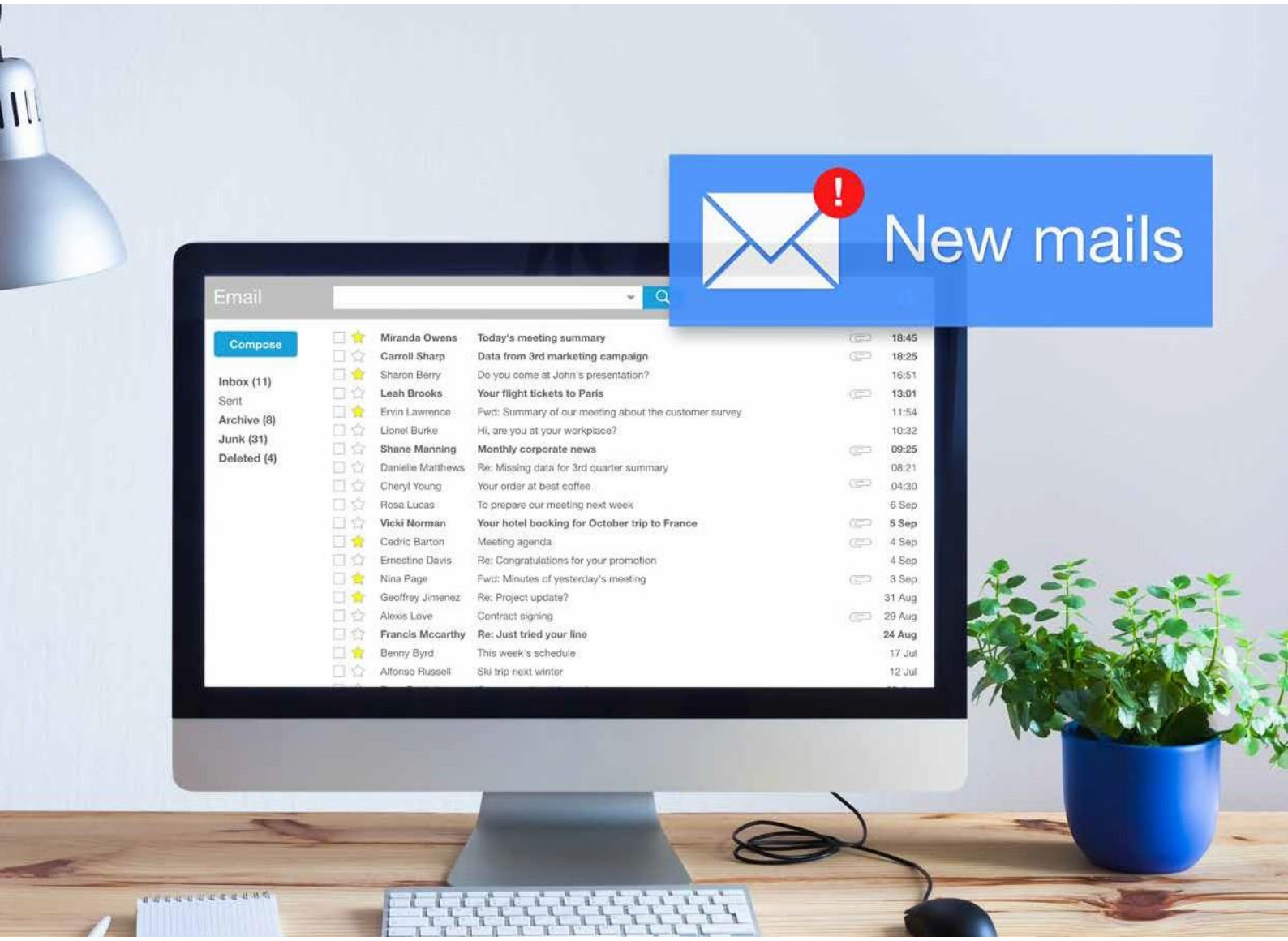
3. Se inicia el asistente para crear un buzón de correo nuevo. Seleccionar *Buzón de usuario*. Clic en *Siguiente.*
4. Se muestra la ventana *Tipo de usuario* y:
   - Seleccionar *Usuarios existentes.* Clic en *Agregar.*
   - En la ventana que aparece, seleccionar el usuario para el que estamos creando el buzón. En este caso, *Prueba*. Clic en *Aceptar.*
   - A continuación, debemos comprobar que aparece el usuario prueba. Clic en *Siguiente.*
5. En la ventana *Configuración del buzón:*
   - En *Alias*, dejar el nombre de prueba.
   - Clic en *Examinar* y seleccionar la ruta *Mailbox Database* y *Aceptar.*
   - Seguimos avanzando haciendo clic en *Siguiente.*
   - Ahora aparece un cuadro resumen con los pasos que se han ido dando hasta el momento. Comprobar si todo es correcto y hacer clic en *Nuevo.*
   - Esperar el tiempo que corresponda. A continuación, clic en *Finalizar.*

4.7. realización de documentación adecuada para apoyar al usuario

Para finalizar el proceso de instalación y configuración del correo electrónico en nuestro servidor, es recomendable realizar un documento que englobe todo el procedimiento. Las ventajas de realizar este documento es que se deja constancia de todos los pasos previos a la instalación; es decir, a las condiciones en las que se encontró el equipo: *hardware* y *software* instalados, particiones de partida, *drivers* instalados y usuarios configurados.

En el proceso de configuración es posible dejar constancia de las opciones seleccionadas y de las razones que nos han llevado a tomar tal decisión. Este documento debe ser una guía de consulta para futuras ampliaciones o posibles incidencias ocasionadas. Con referencia a las características del correo, se pueden detallar sus especificaciones, funcionamiento, protocolos de descarga, cuentas de correo.

Otros posibles administradores pueden utilizar este tutorial como ayuda y explicación de todo el proceso, así como del estado en el que se encuentra el servidor y toda la red de comunicaciones.



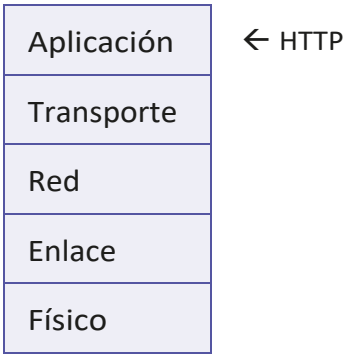
Cuando hay incidencias en el correo electrónico, este documento puede ser útil para buscar una solución y, si el proyecto está totalmente actualizado, podemos ver como se solucionaron algunos incidentes parecidos ocurridos anteriormente.

Este documento se puede elaborar mediante una aplicación informática que facilite la recogida de las incidencias.

Muchas de estas incidencias se pueden resolver *in situ*; por tanto, se actúa directamente. Para problemas no tan importantes se gestiona de forma remota.

Otra vía para solventar los problemas es mediante el soporte técnico en línea que posee Microsoft en su centro TechNet. Esta ayuda es posible gracias a contar con un producto con licencia que permite estos privilegios. En el caso de un *software* libre, solo tendrá la ayuda de los foros no oficiales. Estos pueden ser útiles también, pero sabiendo que no son oficiales.

HTTP *(hipertext transfer protocol):* protocolo de transferencia de hipertexto. Es otro protocolo de la capa de aplicación que comparte y distribuye aquella información entre distintos sistemas a través de las páginas web.



HTTP en el modelo TCP/IP

Protocolo desarrollado por sir **Timothy Berners-Lee** y su equipo, que fueron capaces de crear el lenguaje de etiquetas de hipertexto o HTML junto con un sistema de localización de objetos en la web o URL.

Fue a partir de los años 90 cuando HTTP se fue convirtiendo en el protocolo de la **world wide web (www)** que es la red global mundial, creada también por Timothy y basada, principalmente, en unir el hipertexto con internet.

Hoy en día, la versión que se utiliza es la **HTTP v1.1** aunque no se deja de trabajar sobre siguientes versiones que permitirán, el día que consigan salir a la luz, una mayor velocidad y conexión a través de los dispositivos móviles.

Localizador URL (Localizador uniforme de recursos)

Una URL es un conjunto de caracteres que permiten denominar de forma única los recursos en internet, de esta forma facilita el acceso a ellos.

El formato de una URL es el siguiente:

protocolo://máquina:puerto/ruta_fichero

Si es necesario identificación para acceder a ese recurso, el usuario y contraseña se deben indicar delante de la máquina, de forma que la URL quedaría:

protocolo://usuario:contraseña@máquina:puerto/ruta_fichero

Donde:

- **Protocolo:** conjunto de reglas de comunicación que se va a utilizar en cada documento, como HTTP, HTTPS, FTP, etc.

- **Usuario:** debe ir seguido de los dos puntos (:) e indica el usuario.
- **Contraseña**: va seguida de la arroba (@) y hace referencia a la contraseña del usuario.
- **Máquina**: nombre del equipo donde se encuentra la información almacenada, como FQDN, dirección IP, nombre dominio.
- **Puerto**: puerto disponible para escuchar la información. Se sitúa detrás de los dos puntos (:).
- **Ruta_fichero**: ruta que especifica el nombre del archivo que contiene al recurso.

No todos los campos que dispone tienen por qué aparecer obligatoriamente.

Esquema	Usuario	Contraseña	Máquina	Puerto	Directorio	Archivo
http://			ilerna.com			/recurso/html
http://	Alumno	1234abc	192.168.100.1	:80	/mario	/a.html

Aunque no aparezcan todos los campos, algunos ejemplos podrían quedar de la siguiente forma:

http://ejemplo.com/recurso/html

http://alumno:1234abc@192.168.100.1:80/mario/a.html

Dos conceptos que están estrictamente relacionados con el protocolo URL son URN y URI. A continuación, vamos a detallar cada uno de ellos.

URN *(uniform resource name)*

Este **nombre de recurso uniforma** se encarga de identificar los diferentes recursos en internet. Es parecido a URL, aunque en este caso no se indica la forma de poder acceder a ellos. Un ejemplo de URN podría ser el **ISBN** de un libro. Mediante este código, se puede identificar la obra, pero no indica en qué librerías disponen de él.

URI *(uniform resource identifier)*

El identificador de nombre de recurso permite añadir, de forma opcional, los campos de pregunta y fragmento al final de la URL.

- **Pregunta:** una o varias variables separadas por ";". Van precedidas por el separador "?". Mediante el separador "=" se puede indicar el valor de una variable determinada.
- **Fragmento:** parte final del documento que va precedida por el separador "#".

El URI puede ser considerado como un localizador, nombre o ambos, incluso; por lo que es más recomendable que URL y URN.

5.1. Sistema criPtográfico

El sistema criptográfico hace referencia al conjunto de operaciones que permiten transmitir información de una forma privada y segura entre el emisor y el receptor de un mensaje.

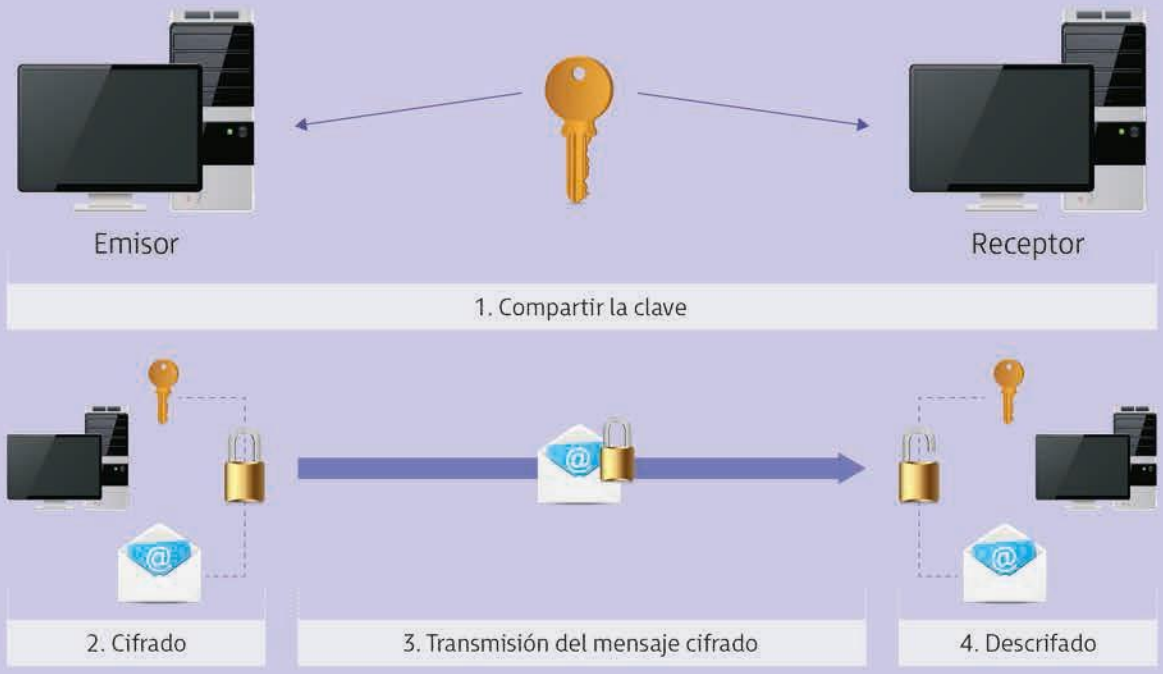
El proceso de cifrado consiste en utilizar un algoritmo sobre un texto de tal forma que se obtenga otro diferente (formado por letras y símbolos) que solo puede ser leído por el receptor del mensaje.

Los dos métodos de cifrado más importantes que se detallan en este apartado utilizan una **clave simétrica** o **asimétrica**.

Clave simétrica

Se refiere al uso de una única clave para cifrar y para descifrar un mensaje. Lo primero que hay que hacer es compartir la clave entre emisor y receptor.

Esta forma de trabajar presenta una ventaja muy importante: la **velocidad** a la hora de transmitir mensajes. Aunque como inconveniente es posible que la clave sea **interceptada** por terceros.



Clave asimétrica

La clave asimétrica resuelve el problema anterior de que la clave pueda ser interceptada, mediante el uso de dos claves:

- Una **pública**: que permite enviar a todos los usuarios.
- Una **privada**: que el propietario tiene que mantener en secreto.

Estas claves son complementarias; es decir, lo que se cifra con una, solo lo puede descifrar la otra, y viceversa.

Como ventaja cabe resaltar que, dado que la clave pública es la única que transmite, aunque sea interceptada, **no perjudica** a las transmisiones seguras. Pero como inconveniente, conviene señalar que es un proceso **más lento** ya que se debe comprobar que la clave pública realmente pertenece a su dueño. Por esto, es imprescindible que en este sistema de cifrado se utilice el certificado digital y la firma electrónica.

5.2. Funcionamiento y arquitectura web. Funcionamiento del protocolo HTTP

Como el protocolo HTTP consiste en un protocolo de pregunta/respuesta, basado en el modelo cliente/servidor, su funcionamiento se lleva a cabo de la siguiente forma:

1. El navegador web envía un mensaje de petición al servidor web.
2. El servidor que almacena la información envía un mensaje de respuesta.

Mensajes HTTP

Los mensajes contienen el estado de la solicitud y pueden añadir cualquier tipo de información que solicite el cliente. Presentan un formato estandarizado (RFC 822) pudiendo:

- **Mensaje de petición**

  El cliente comunica qué acción desea realizar, el recurso sobre el cual se desea realizar esa acción y otros datos necesarios que pueda necesitar el servidor para poder atender la petición.

- **Mensaje de respuesta**

  El servidor añade al paquete la información necesaria para que el protocolo consiga funcionar de forma correcta.

Sesión HTTP

Hace referencia a las diferentes transacciones de red entre cliente y servidor.

1. El **cliente realiza la petición** estableciendo una conexión TCP a través del puerto 80 del servidor que permanece a la escucha.
2. **El servidor procesa la información** y, posteriormente, transmite la respuesta mediante un mensaje de estado con el recurso solicitado.
3. **HTTP v1.0: inicia la conexión** cuando el cliente se comunica con el servidor. Cuando el servidor ofrece respuesta, se cierra.
4. **HTTP v1.1: permite varias transacciones a través de una misma conexión** consiguiendo de esta forma aumentar la velocidad de transmisión.

Métodos de petición

Hacen referencia a las diferentes funciones que solicitan realizar una operación con el recurso. Existen ocho métodos diferentes, aunque los más utilizados son:

- ***GET**:* solicita un recurso al servidor a través de URL.
- ***POST**:* es utilizado, sobre todo, en formularios. Avisa al servidor de que le va a llegar una información.
- ***HEAD**:* parecido al *GET*, aunque en este caso, el servidor no devuelve el cuerpo principal del mensaje, solamente la línea del principio con las cabeceras.

Códigos de estado

Son un conjunto de tres dígitos que indican si una petición ha sido aceptada o no. Si no se ha aceptado, también se debe indicar. A continuación, se puede ver una tabla con los diferentes grupos de códigos de estado:

Código	Definición
1XX	Informa
2XX	Indica que ha tenido éxito
3XX	Redirección. Debe realizar más operaciones para completar la acción
4XX	Error en cliente
5XX	Error en servidor

Gestión del estado de conexiones (Cookies)

Como el protocolo HTTP no tiene memoria, no puede guardar ninguna información referente a las transacciones que se han realizado con anterioridad. Por este motivo, debemos utilizar una serie de *cookies* que van a actuar como si fuera un sistema externo.

Las cookies son un conjunto de datos que puede recibir el cliente y que además almacenan la petición del servidor web en concreto. La empresa **Netscape** fue la primera que las desarrolló en 1994.

Las *cookies* ayudan al servidor a saber si un cliente ha sido validado o no y, de esta forma, puede ofrecerle diferentes servicios específicos de los usuarios registrados.

Los dos tipos de *cookies* que podemos diferenciar son:

- **Origen:** aquellas que se habilitan por el sitio que estamos visitando.
- ***Third-Party cookies (cookies a terceros)*:** producidas por anuncios o causas externas al sitio que estamos visitando.

Los usuarios tienen opción de ver las diferentes *cookies* que se han almacenado por el UA y también tienen la posibilidad de eliminarlas.

Arquitectura de aplicaciones web

Las distintas aplicaciones web son aquellas que se pueden descargar de forma total o parcial directamente desde la web. Algunos ejemplos de estas aplicaciones son Google, Wikipedia, eBay, entre otras. Estas aplicaciones utilizan la estructura cliente- servidor tanto desde internet como a través de la intranet.

Ejecución de código en el cliente

Este tipo de ejecución se refiere a que el cliente puede mostrar por pantalla el documento que se genera a partir de un código HTML y se hace responsable de los ***scripts*** (programas) que tienen el código de los mismos.

Su funcionamiento es el siguiente:

1. El navegador solicita una petición al servidor web.
2. Este servidor envía un documento en formato HTML junto con todas las sentencias que incorpore.
3. El navegador llama a los programas que están situados

al lado del cliente, solicitándole que traduzcan los *scripts* en tiempo de ejecución.

4. Cuando el código consigue ser interpretado, se le devuelve al navegador.
5. Por último, el navegador ya puede generar el documento y mostrarlo en pantalla.

Ejecución de código en el servidor

En este caso, los programas situados al lado del servidor son los que deben interpretar y ejecutar los *scripts* para, posteriormente, el código HTML resultante. Por último, lo enviarán al navegador web.

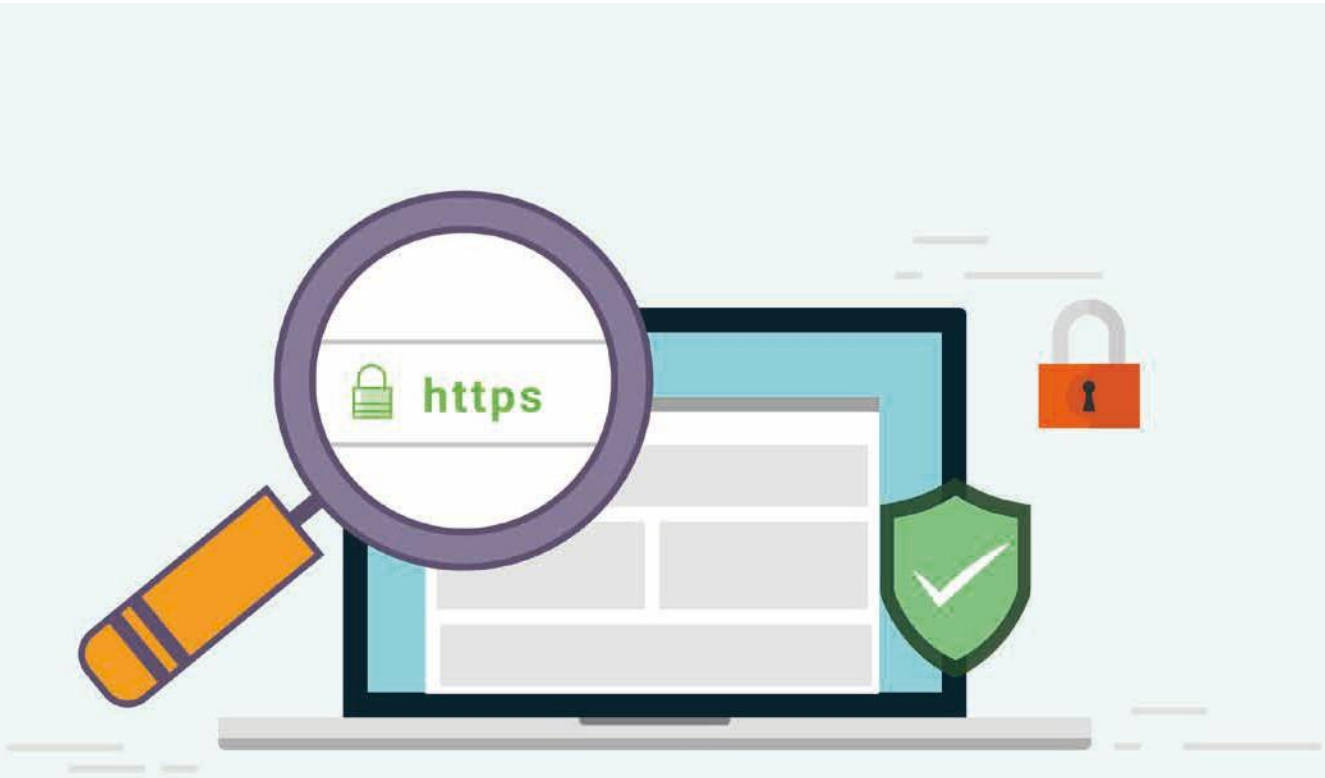
5.3. Funcionamiento HTTPS

Su función principal es establecer conexiones de forma segura entre cliente y servidor.

Como el proceso de cifrado a través de claves asimétricas es bastante lento, no se utiliza para cifrar páginas web. Por tanto, en su lugar, se utiliza una combinación de los algoritmos de **clave asimétrica** (**SSL**) junto con los de **clave simétrica** (**TLS**).

Este protocolo **HTTPS** autentifica al servidor frente al cliente haciendo uso del certificado digital. El cliente lo lleva a cabo mediante un usuario y una contraseña, tomando en cuenta el procedimiento a continuación:

1. Cuando el cliente contacta con el servidor por primera vez, este le envía la clave pública mediante su certificado.
2. Una vez que el cliente acepta la clave, ya puede generar otra simétrica (aleatoria).
3. El cliente cifra el nombre del usuario junto con su contraseña para acceder al sitio web gracias a la clave simétrica que ha generado.
4. Ahora, el cliente puede cifrar la clave simétrica mediante la clave pública del servidor haciendo uso de criptografía asimétrica.
5. Al servidor se le transmiten el usuario y contraseña cifrados.
6. El servidor ya puede descifrar la clave simétrica gracias a su clave privada.
7. La clave simétrica permite descifrar tanto el nombre de usuario como la contraseña correspondiente.
8. El servidor ya solo tiene que comprobar si el usuario puede acceder al servicio web. A partir de este momen-

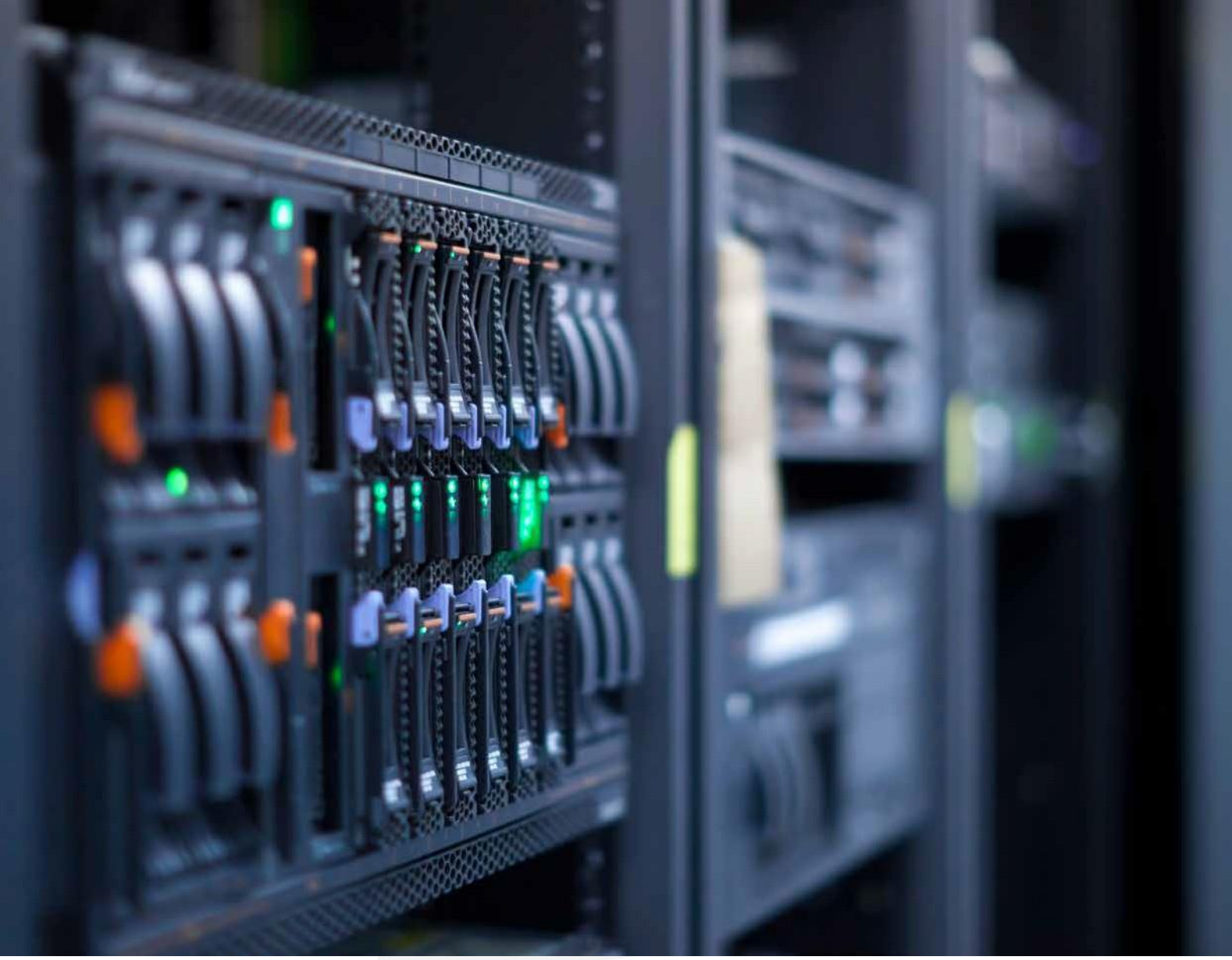


to, debe cifrar las páginas web con la clave simétrica antes de que se le transmitan al cliente. Este, una vez que las reciba, tendrá que descifrarlas utilizando esa misma clave.

Es un protocolo bastante rápido y seguro debido a que, gracias al cifrado asimétrico, se transmite la clave simétrica entre cliente y servidor sin poner en peligro su confidencialidad.

5.4. ServiDores virtuales. nombre De encabezamiento De orDenaDor central. iDentificaDor De un serviDor virtual

Mediante el alojamiento virtual se ofrece la posibilidad de almacenar una serie de sitios web en el mismo servidor de páginas web. A estos sitios se les denomina **servidor virtual**.



Al crear un servidor virtual, hay que seguir los siguientes pasos:

Alojamiento basado en dirección IP

Para crear este servidor, es necesario que cada servidor virtual tenga asignada una dirección IP distinta.

Presenta, entre otras, las siguientes desventajas:

- Que se terminen las direcciones IP disponibles.
- La asignación de direcciones IP en un servidor web.
- Conseguir administrar las direcciones ante organismos oficiales.

Alojamiento basado en número de puerto TCP (no estándar)

Asigna a cada servidor virtual un puerto distinto. No es uno de los más utilizados porque el usuario debe saber el puerto en el que escucha el servidor web.

Alojamiento basado en nombre de dominio

En este último método, es conveniente que cada servidor virtual tenga su propio nombre de dominio asignado. Este método es el que más se utiliza y ofrece la posibilidad de ser utilizado con un grupo de servidores de red utilizando una única dirección IP.

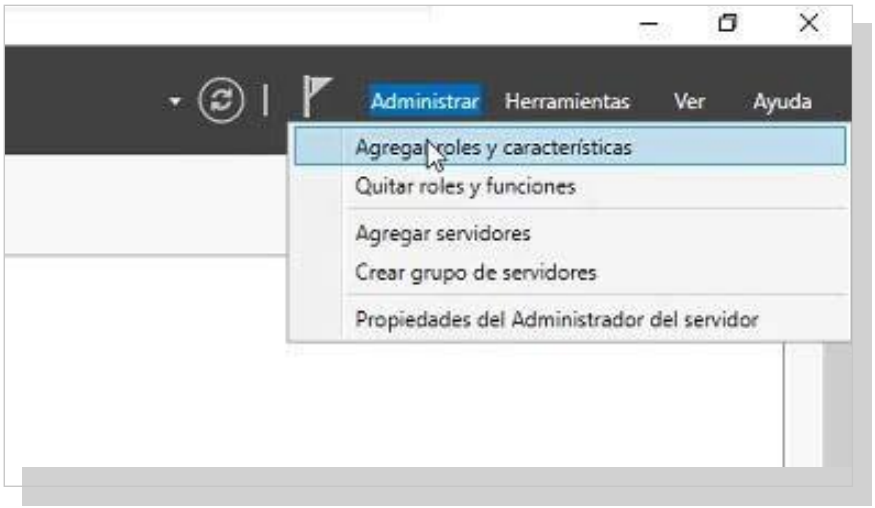
Cuando hay que implementar el alojamiento del servidor virtual basado en el nombre de dominio, es conveniente que:

- El servidor web deba configurarse para que pueda identificar los diferentes nombres de los servidores virtuales.
- El navegador web deba rellenar el campo *host* con el nombre de un sitio web que tiene que pertenecer a la cabecera del mensaje HTTP y, después realizar la petición. Estos factores permiten que el servidor web reconozca a qué servidor virtual se dirige la solicitud.
- Es conveniente que los nombres de *host* se registren en el servidor DNS para que se resuelva la dirección IP del servidor web.

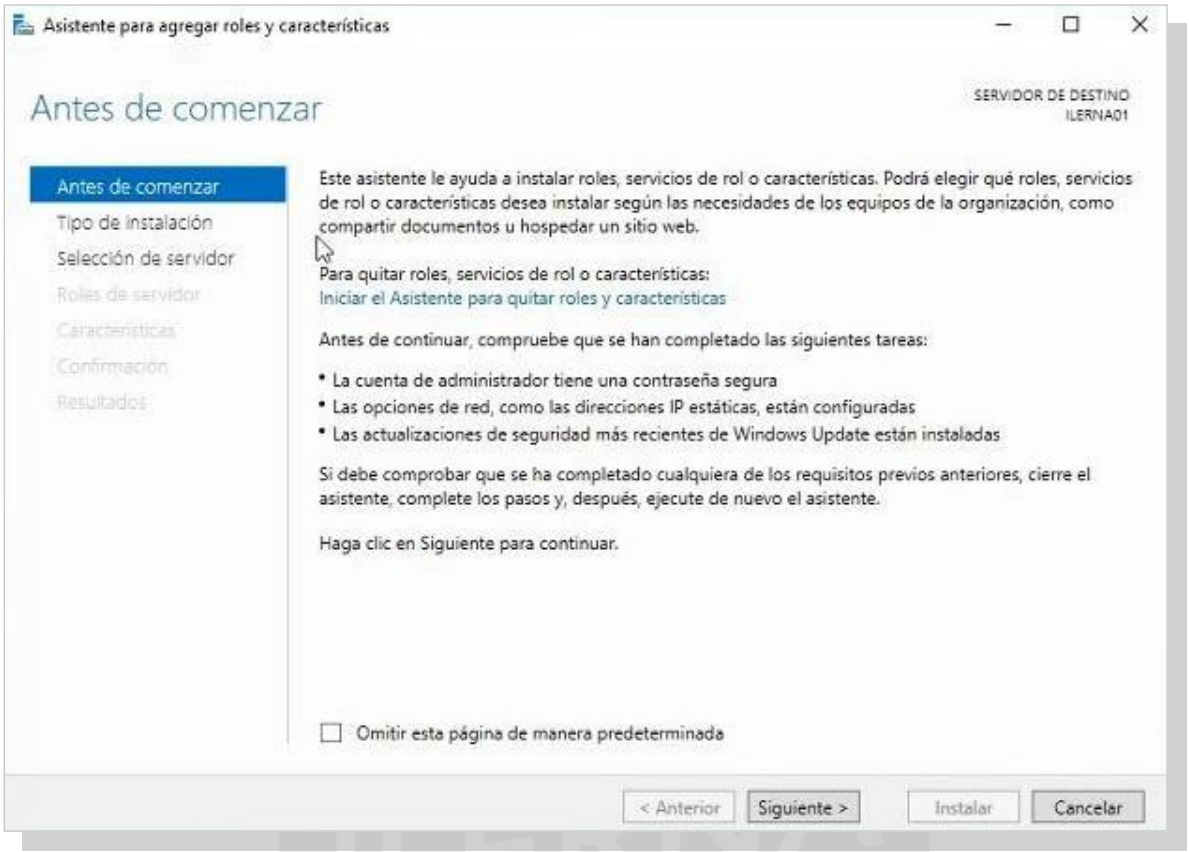
5.5. Instalación De un serviDor web

A la hora de instalar un servidor IIS, se siguen los siguientes pasos:

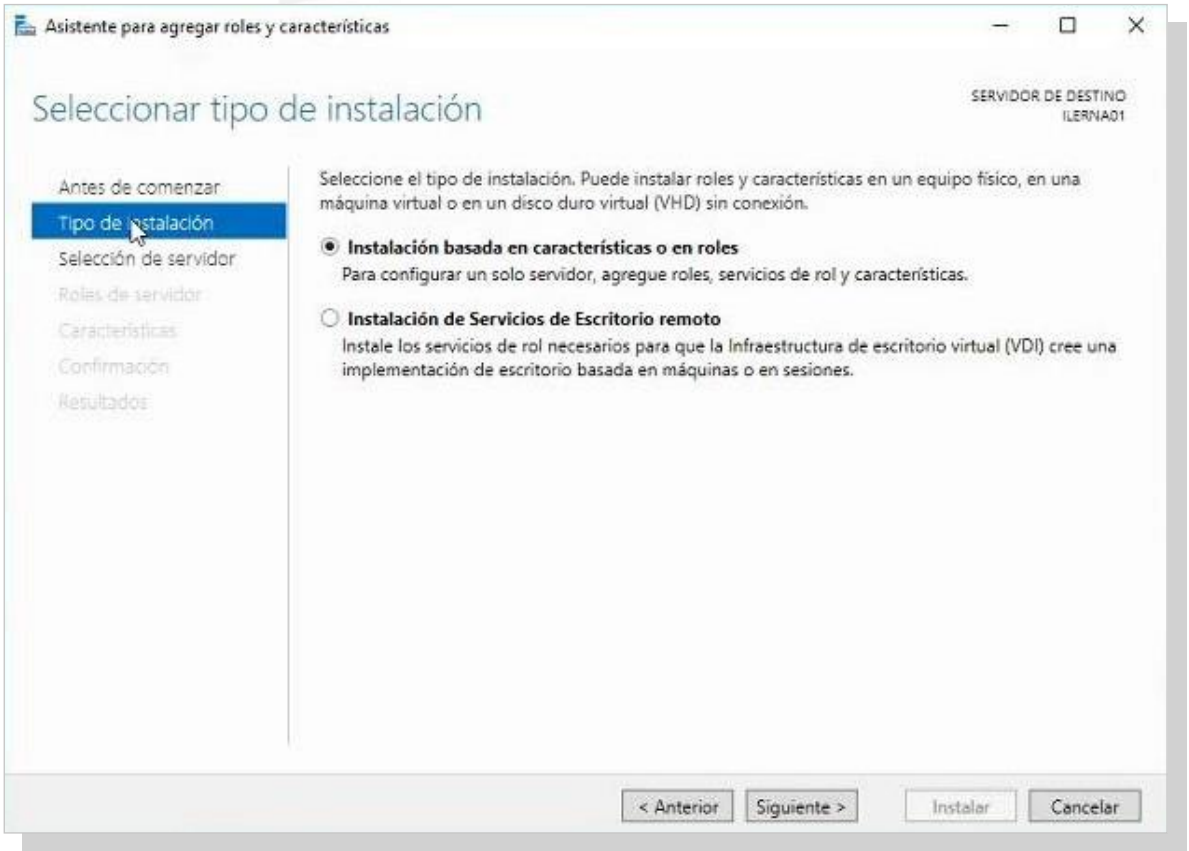
1. Clic en *Inicio* para seleccionar la opción *Administrador del servidor.*

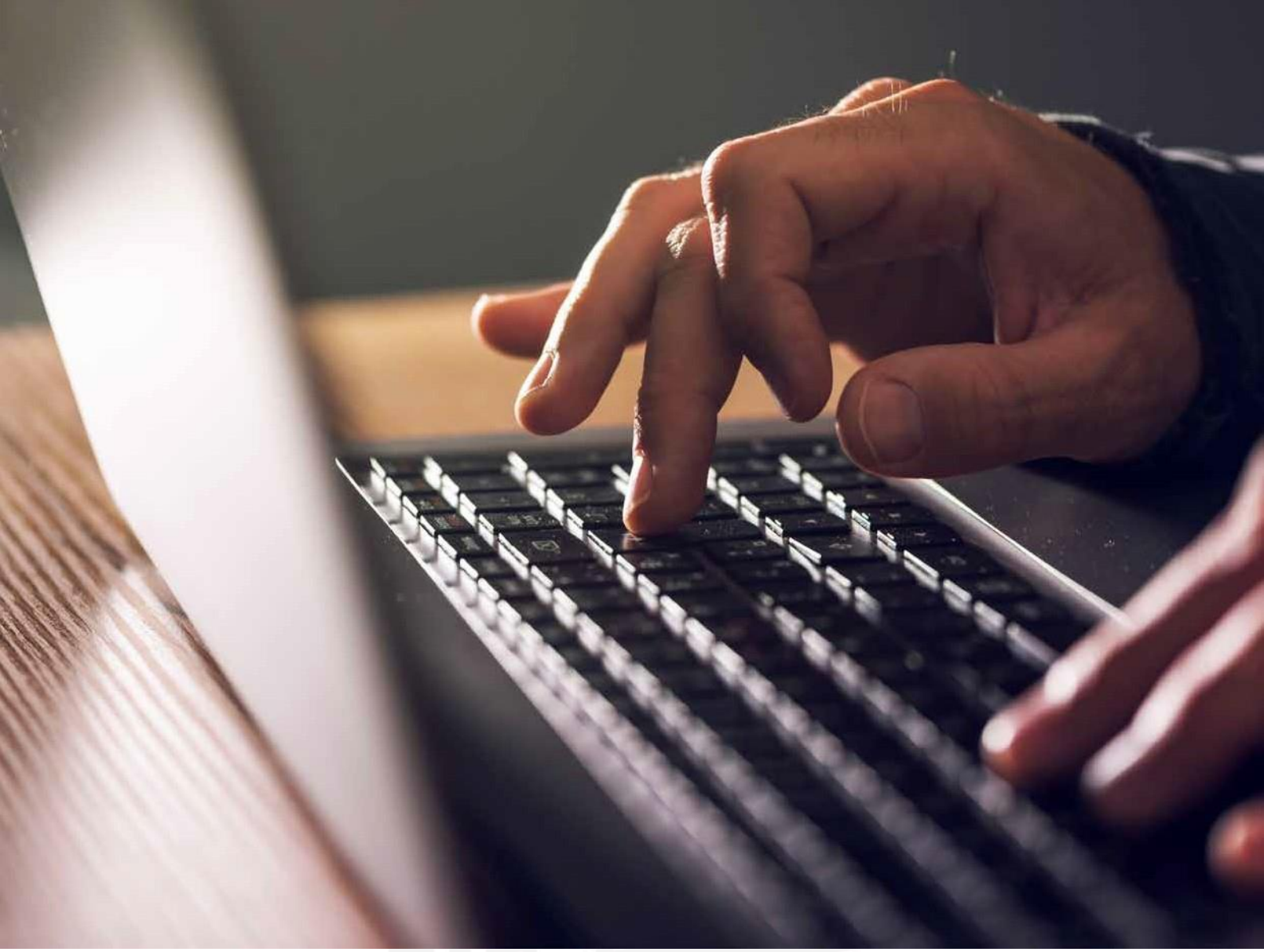


2. Aparece el asistente para agregar roles. Leer detenidamente. Para continuar, elegir la opción *Siguiente*.

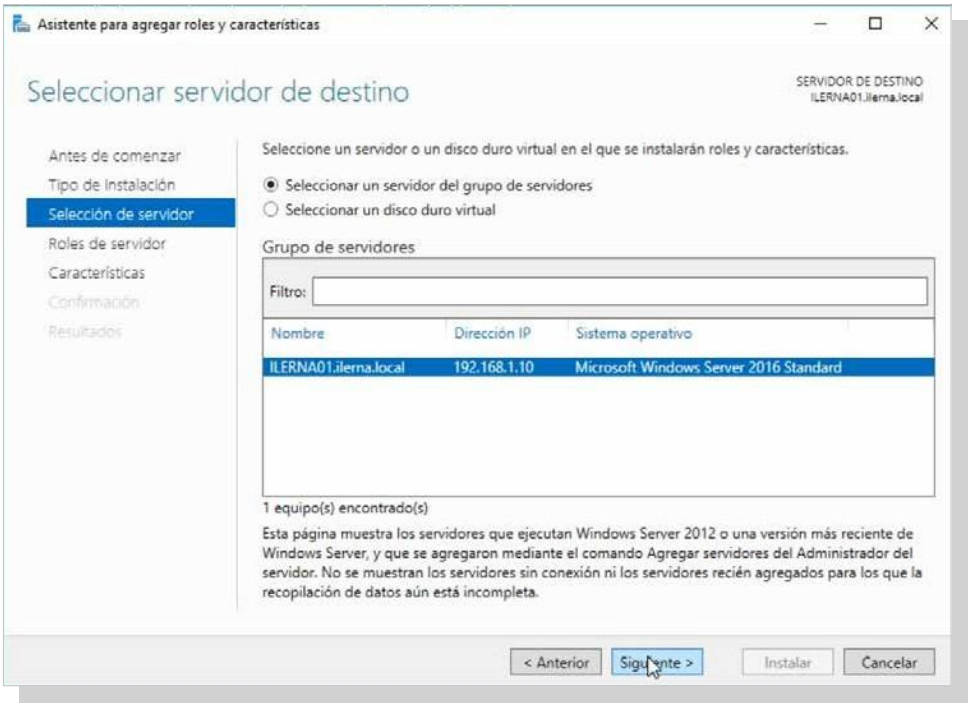


3. Elegir la instalación basada en roles, ya que estos ejemplos se verán de forma práctica en un servidor virtual.

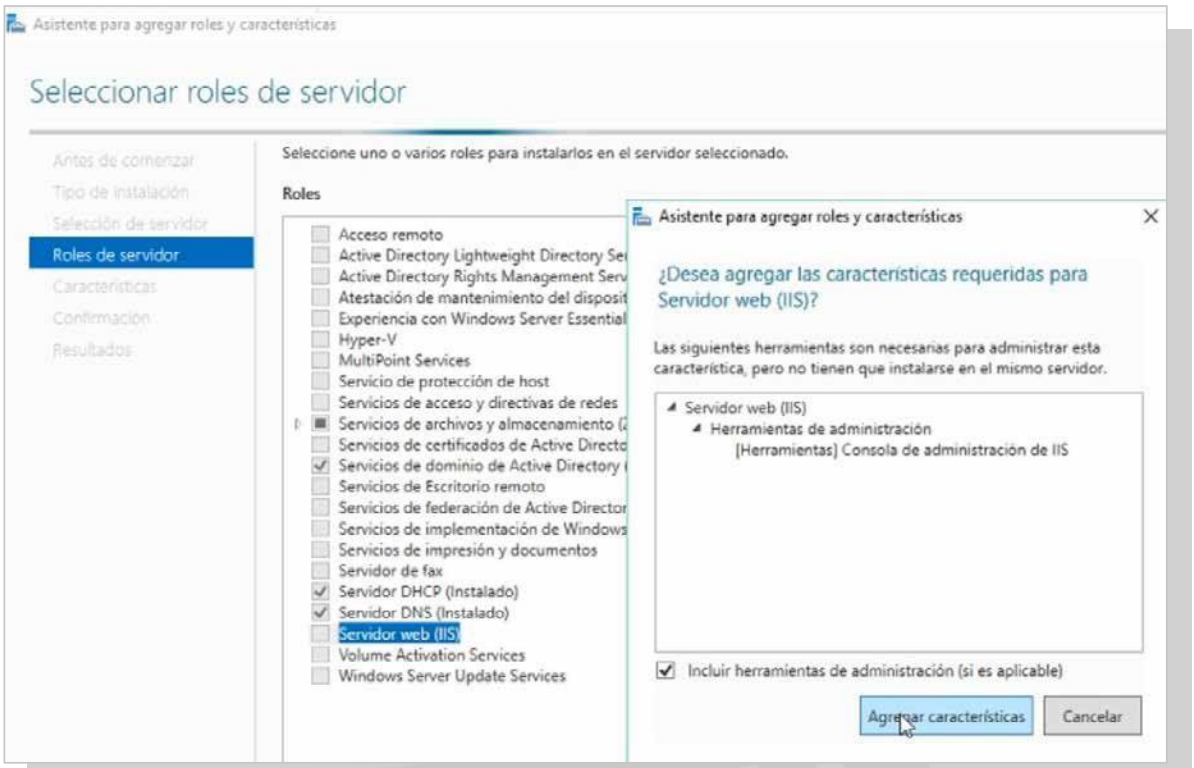


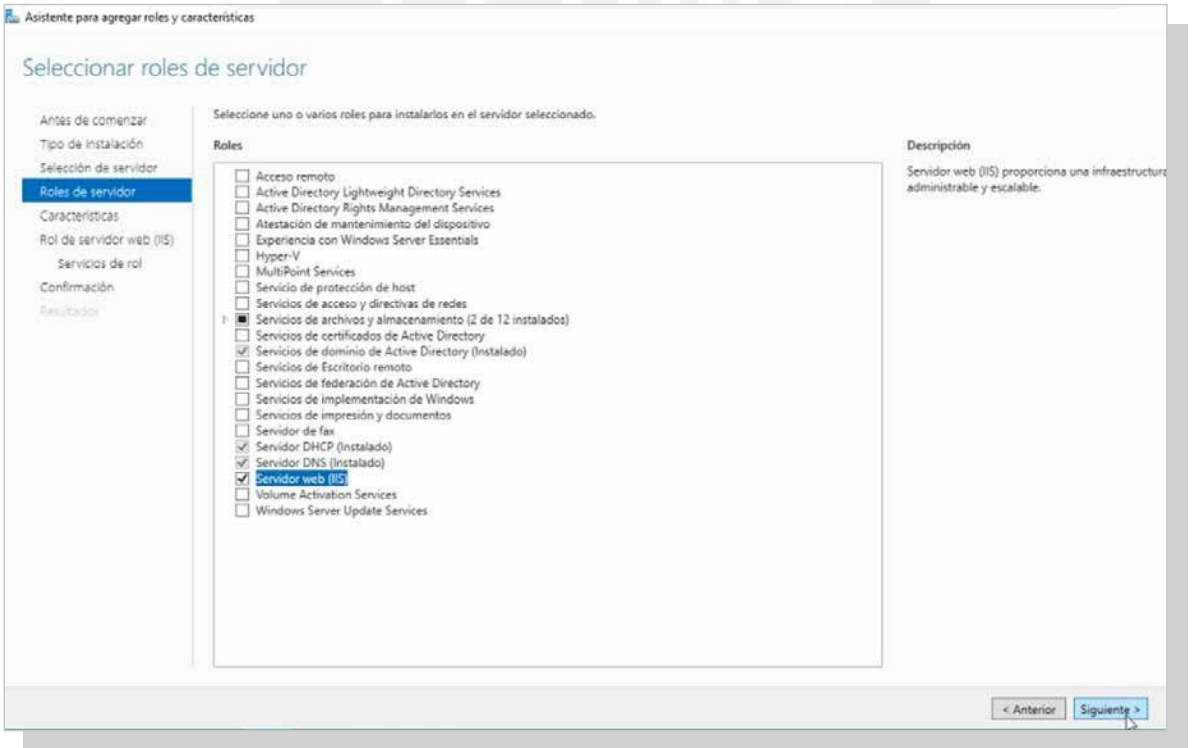


4. Elegir la dirección IP que corresponda al servidor y hacer clic en *Siguiente*.

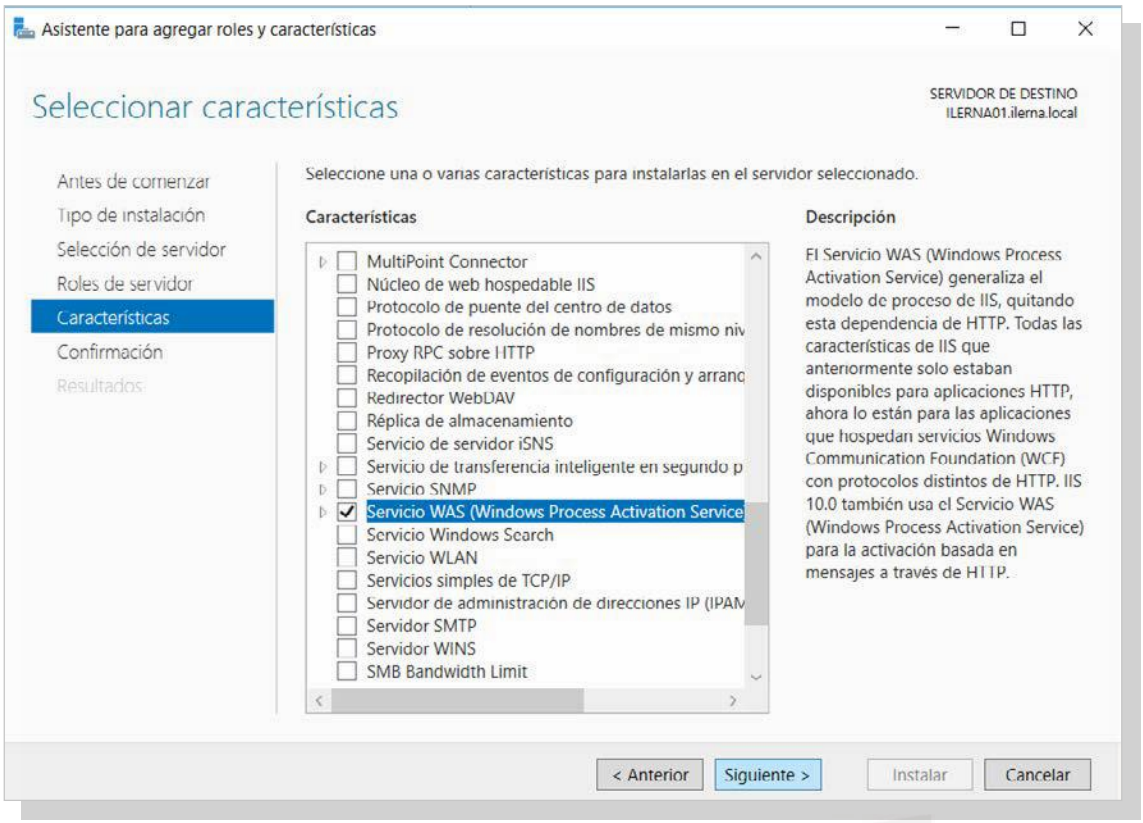


5. Aparece una nueva ventana. Hacer clic en *Servidor web (IIS)*, leer las características que se van a añadir con el nuevo servicio.

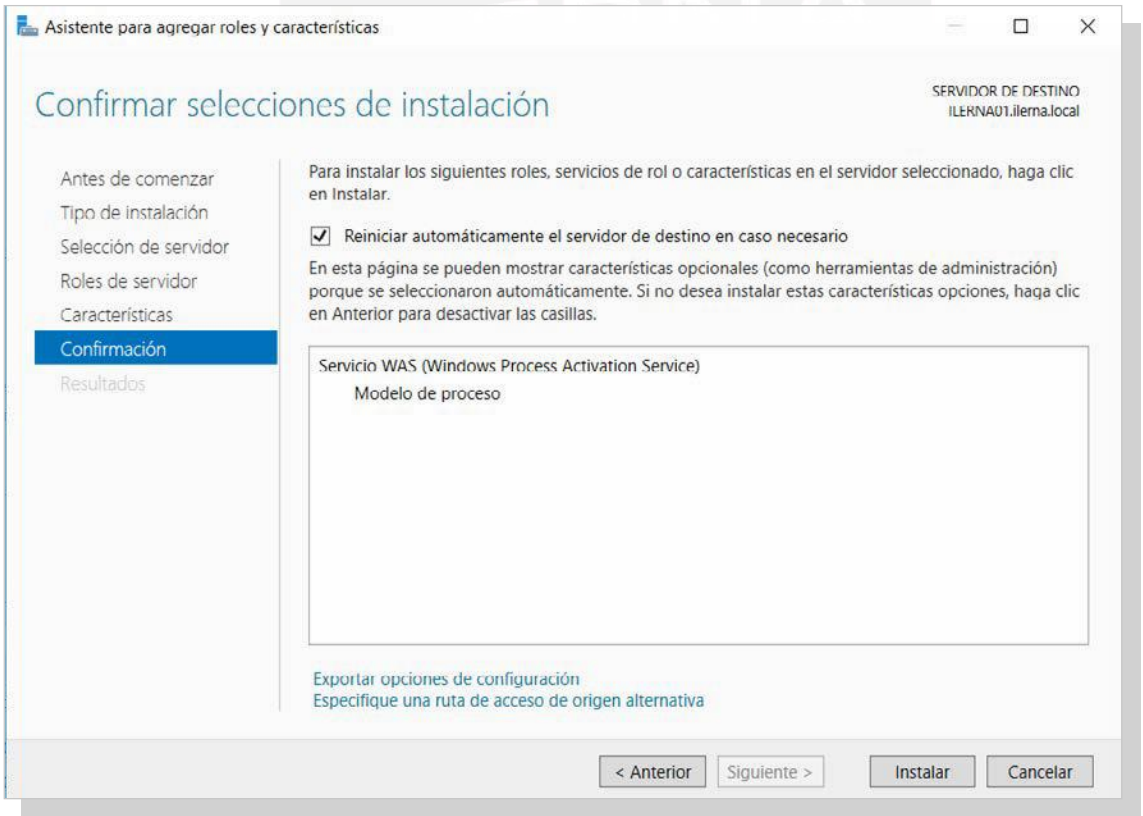




6. Al instalar IIs, es necesario instalar otros servicios que también están incluidos en el servicio WAS (Windows Process Activation Service). Seleccionamos la opción *Agregar características requeridas.*



7. La instalación comenzará al hacer clic en *Instalar.*



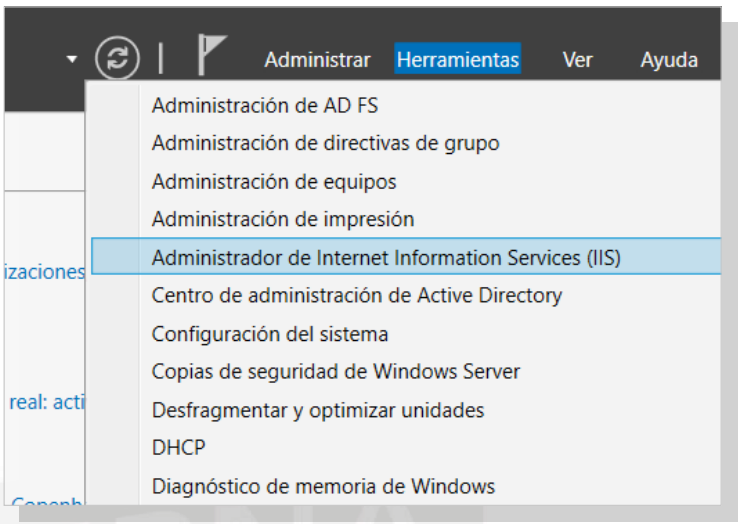
8. Transcurrido el tiempo necesario para concluir el proceso de instalación del servidor, si todo es correcto, hacer clic en *Cerrar* para finalizar este proceso.

5.6. Creación De sitios virtuales

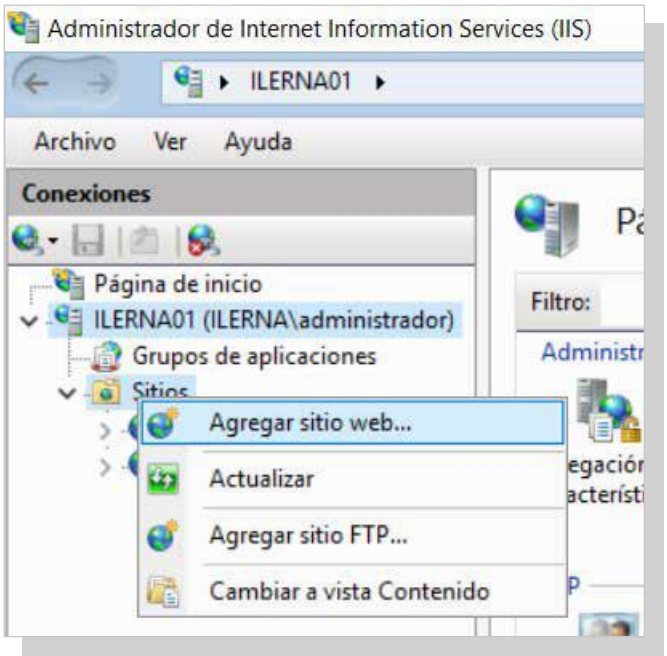
Creación de un sitio web

Es conveniente crear un sitio web para poder publicar en la web de la intranet empresarial.

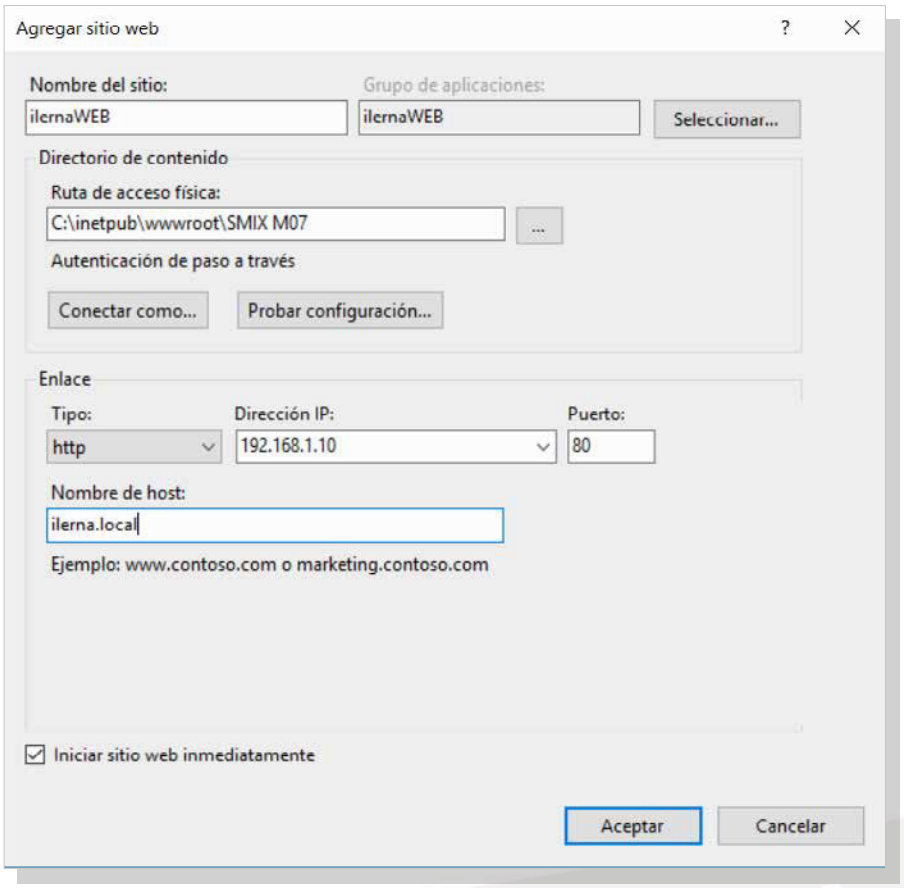
- Crear un archivo *c:\SitiosWeb\www\index.html* que tiene formato HTML.
- A continuación, *abrir el administrador de IIS.*



- Mediante el botón secundario, hacer clic en *SERVIDOR* y elegir la opción *Agregar sitio web.*



- Aparece un cuadro de diálogo *Agregar sitio web* en el que se debe rellenar una serie de campos. Luego, *Aceptar.*

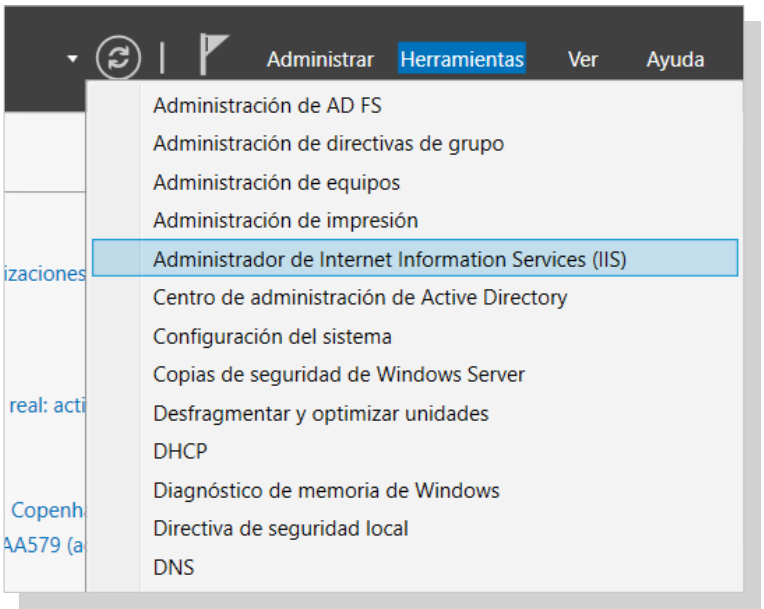


Una vez finalizados los pasos, debe aparecer una lista desplegable *Sitios* denominada *www.*

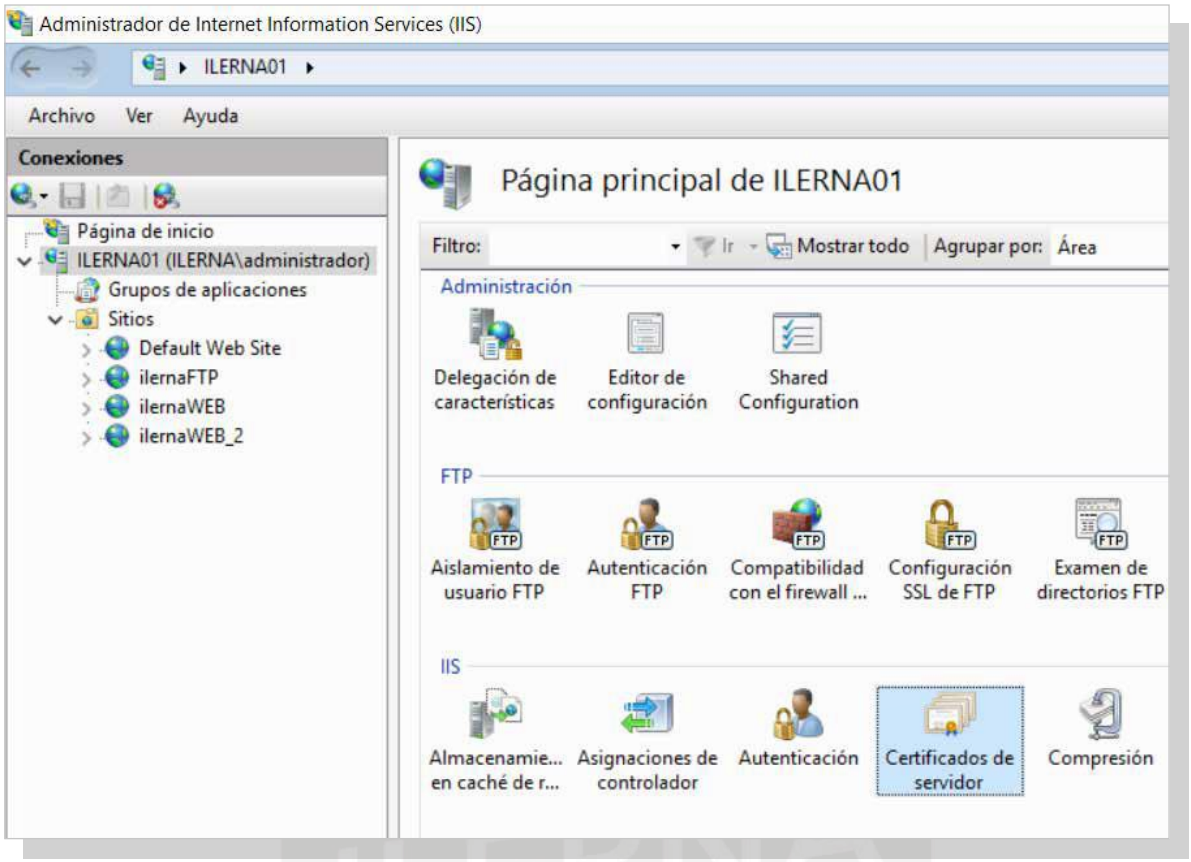
Creación de un certificado

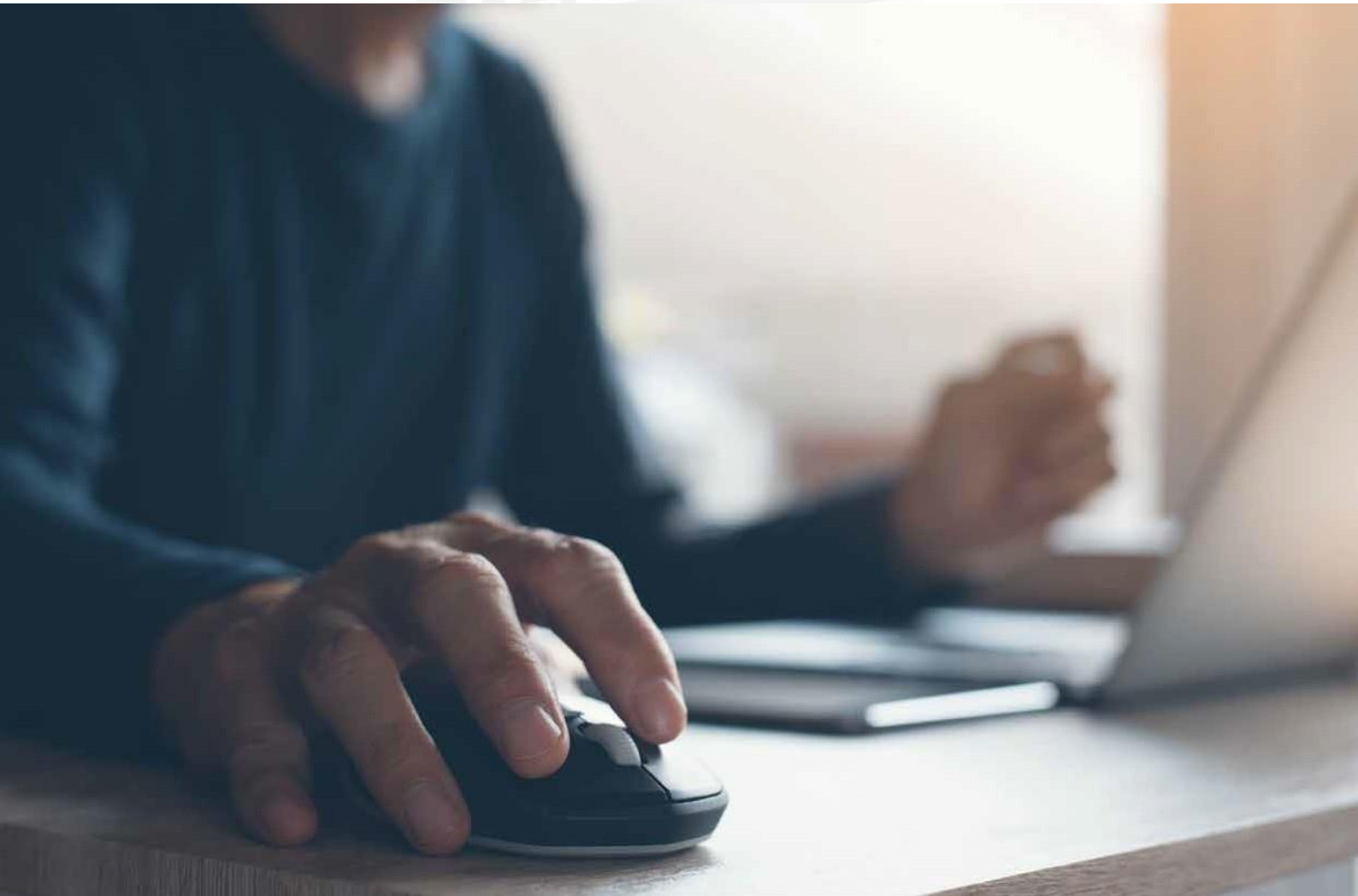
Para crear un certificado (tipo autofirmado), ya que es necesario a la hora de configurar un sitio web seguro, hay que seguir los siguientes pasos:

- Abrir el *administrador de IIS.*

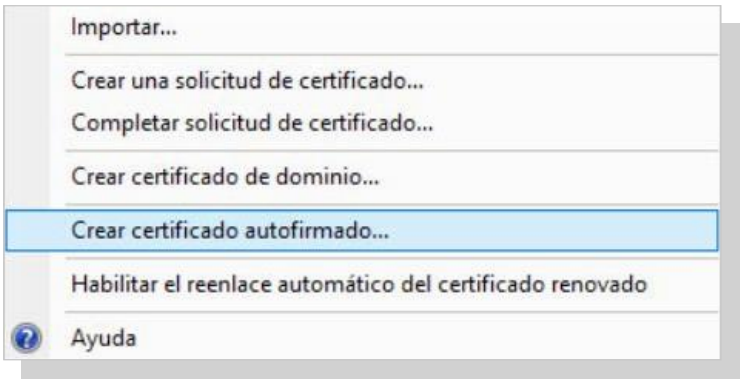


- Hacer doble clic en *Certificados del servidor* y seleccionar *SERVIDOR.*

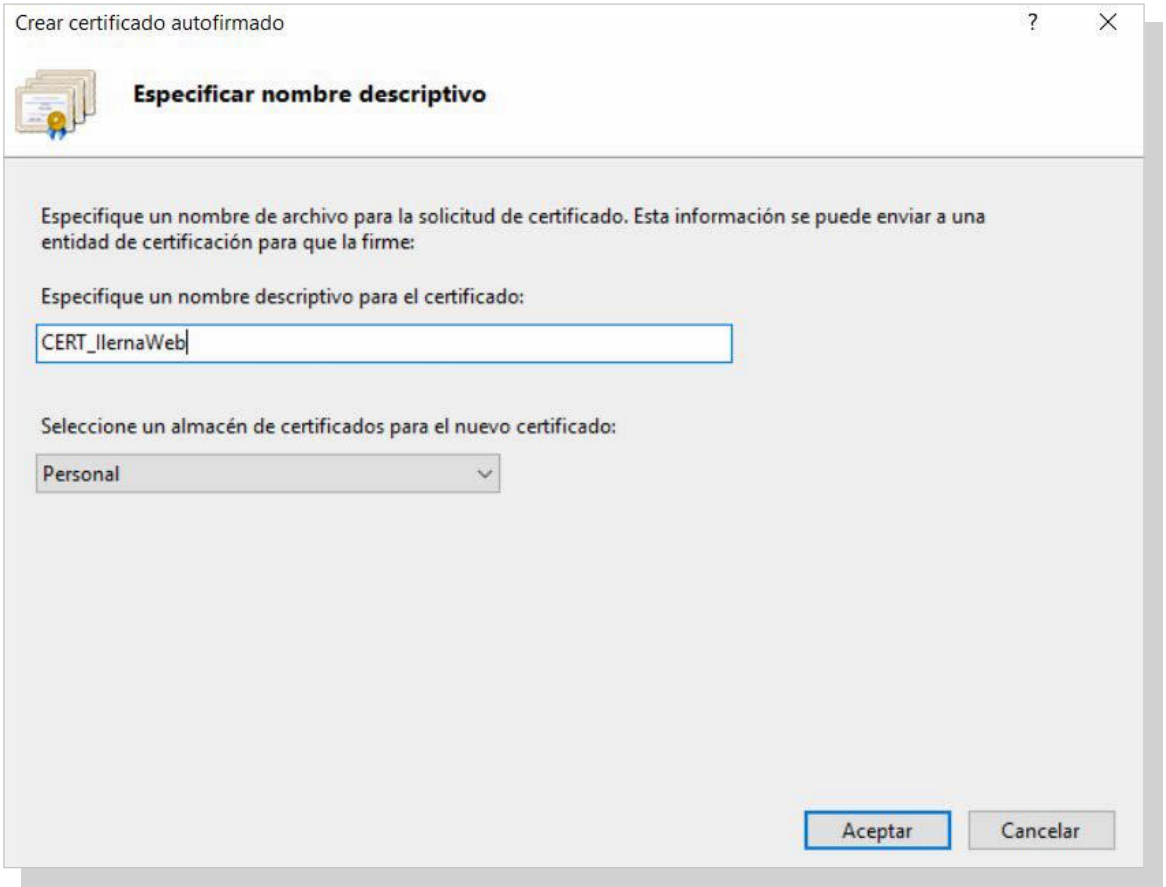




- En el apartado *Acciones*, seleccionar la opción *Crear certificado autofirmado.*



- Aparece la ventana *Crear certificado autofirmado*, en la que se debe escribir un nombre para este certificado. Clic en *Aceptar.*



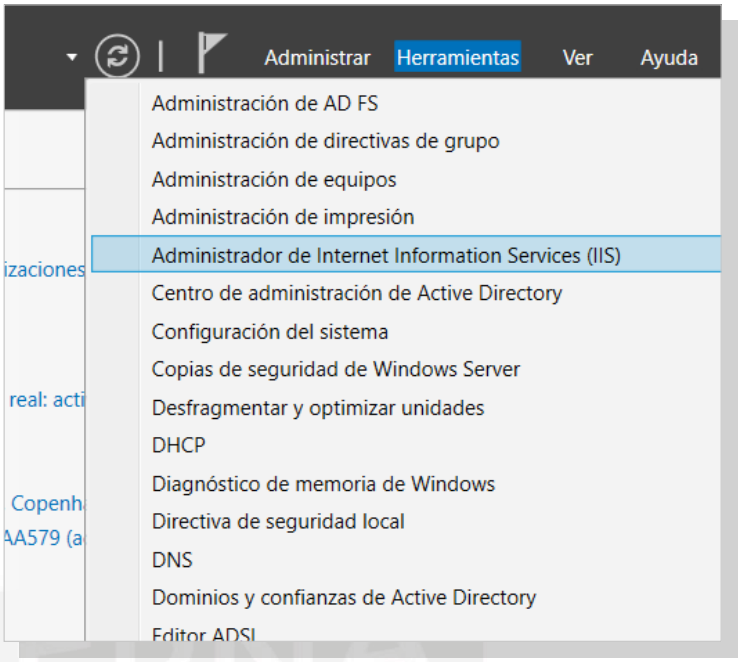
Cuando finalicen los pasos, debe aparecer la lista de *Certificados de servidor.*

Creación de un sitio web seguro https

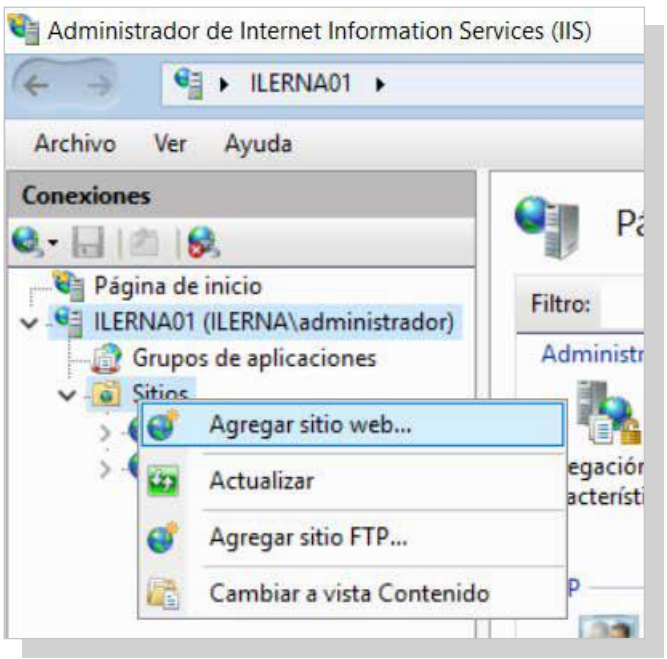
Una vez listo el certificado autofirmado, es el momento de crear y configurar el nuevo sitio web seguro bajo protocolo

HTTPS que se utilizará si se quiere publicar una aplicación web de la intranet empresarial. Para lo cual, hay que seguir los pasos:

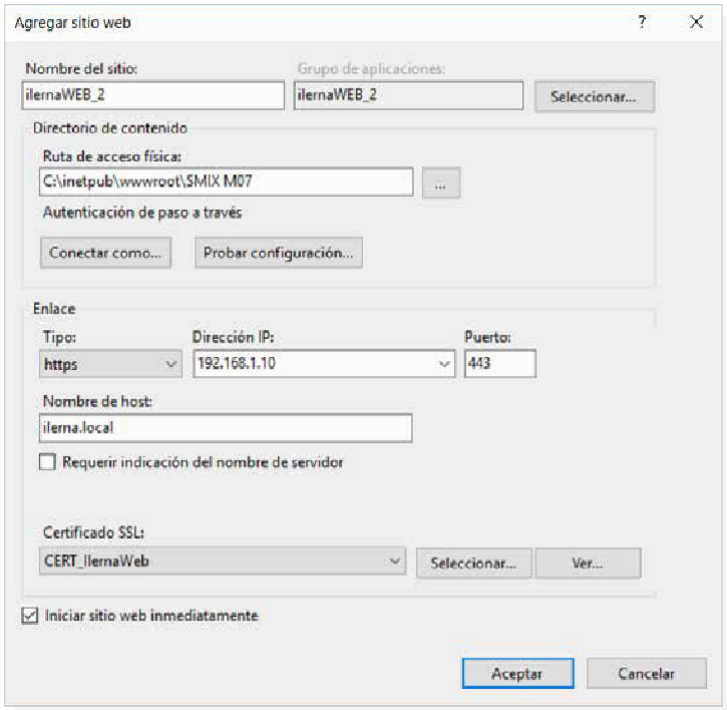
- Se debe crear el archivo *c:\SitiosWeb\webapp\index.html* con formato HTML.
- Abrir el *Administrador de IIS.*



- Con el botón secundario, hacer clic en *SERVIDOR* y seleccionar la opción *Agregar sitio web.*



- En la ventana *Agregar sitio web*, rellenar los campos necesarios y al finalizar, clic en *Aceptar.*

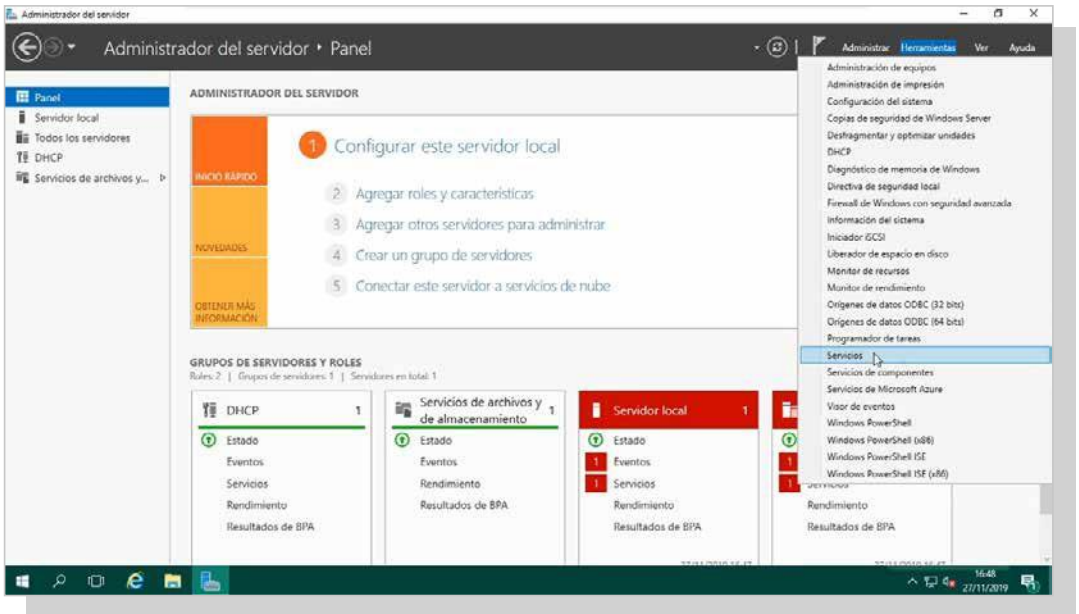


5.7. ComProbación

Siempre es conveniente ir realizando diferentes comprobaciones tanto en el servidor como en el cliente. En el caso del servidor, se debe verificar cómo se encuentra el proceso; el cliente, por su parte debe confirmar si es posible acceder a los distintos sitios web.

Verificación del estado del servicio

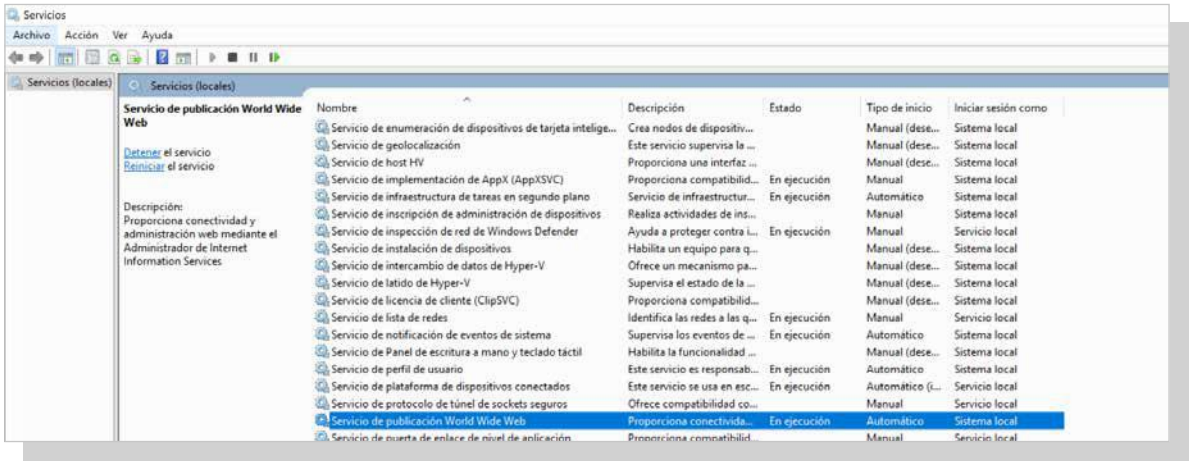
1. Para comprobar el estado del servidor, se sigue la ruta *Inicio/Herramientas administrativas.* Una vez en el sitio, clic en *Servicios.*



2. En la ventana que se muestra, buscar *Servicio de publicación www.*

   —Si el campo *Estado* tiene valor *Iniciado.*

   —Y el dato *Tipo de inicio* tiene valor *Automático.*

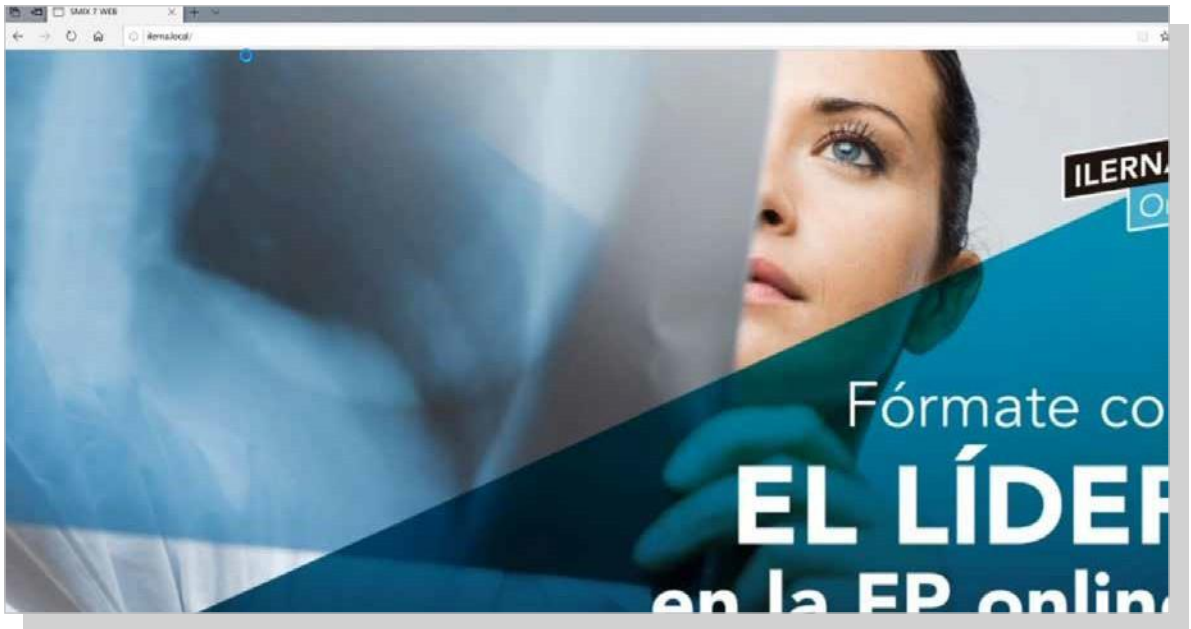


3. Estos datos indican que el servidor web está funcionando y que se iniciará automáticamente cada vez que el equipo se arranque.

Verificación del acceso anónimo al servicio con HTTP

Para hacer la comprobación de que la URL se ha abierto de forma correcta y que funciona sobre el protocolo HTTP:

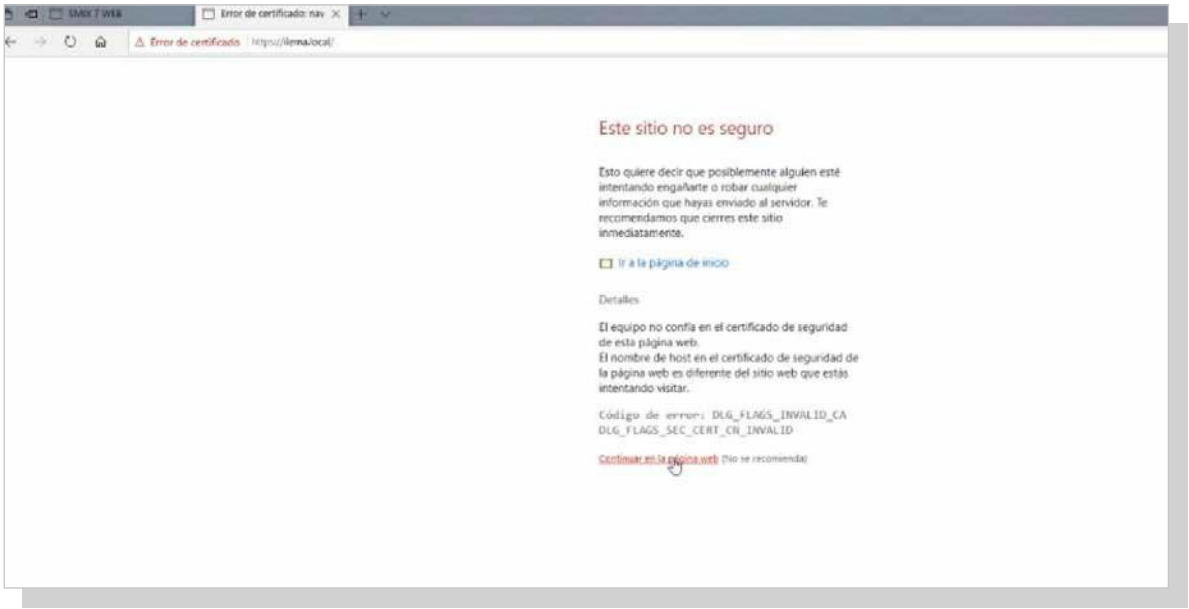
1. El equipo del cliente debe abrir el programa Internet Explorer en *Inicio/ Todos los programas.*
2. A continuación, escribir la dirección URL correspondiente del navegador web y pulsar *Intro.*



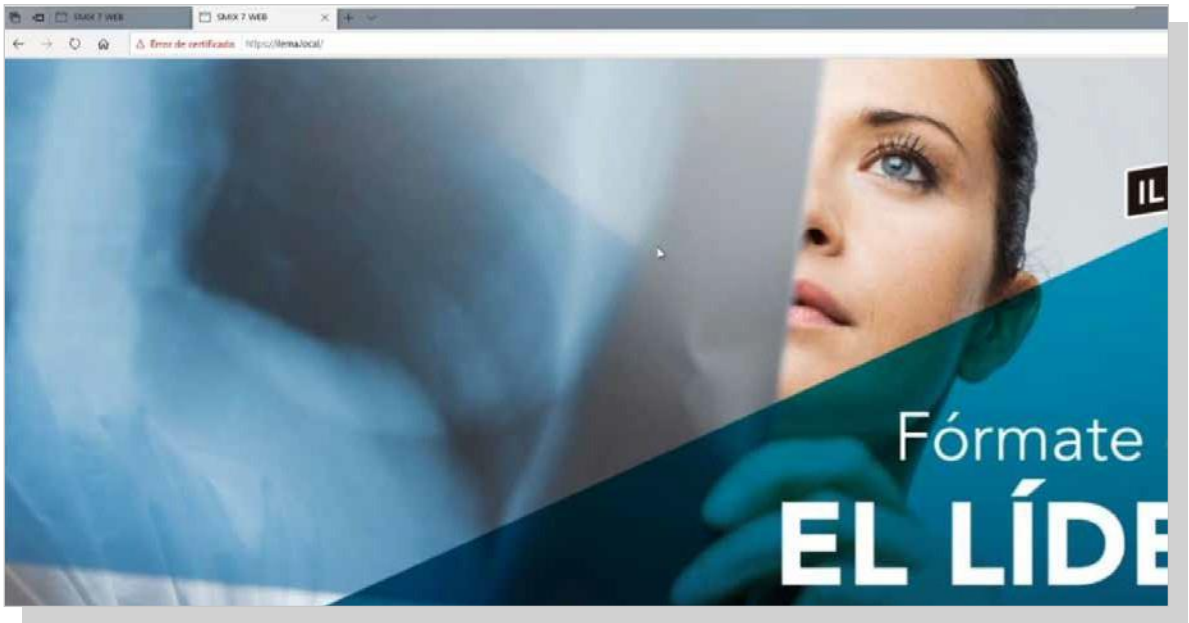
Verificación del acceso anónimo al servicio con HTTPS

Para hacer la comprobación de que la URL se ha abierto de forma correcta y que funciona sobre el protocolo HTTPS:

1. El equipo del cliente debe abrir el programa Internet Explorer en *Inicio / Todos los programas.*
2. A continuación, escribir la dirección URL correspondiente del navegador web y pulsar Intro.
3. Aparece un aviso informando de que el certificado creado no está firmado por ninguna CA, sino autofirmado (por nosotros mismos). Hacer clic en *Vaya a este sitio web (no recomendado)*.



4. Si el servicio HTTPS funciona de forma correcta, debe aparecer la página de aplicación web.



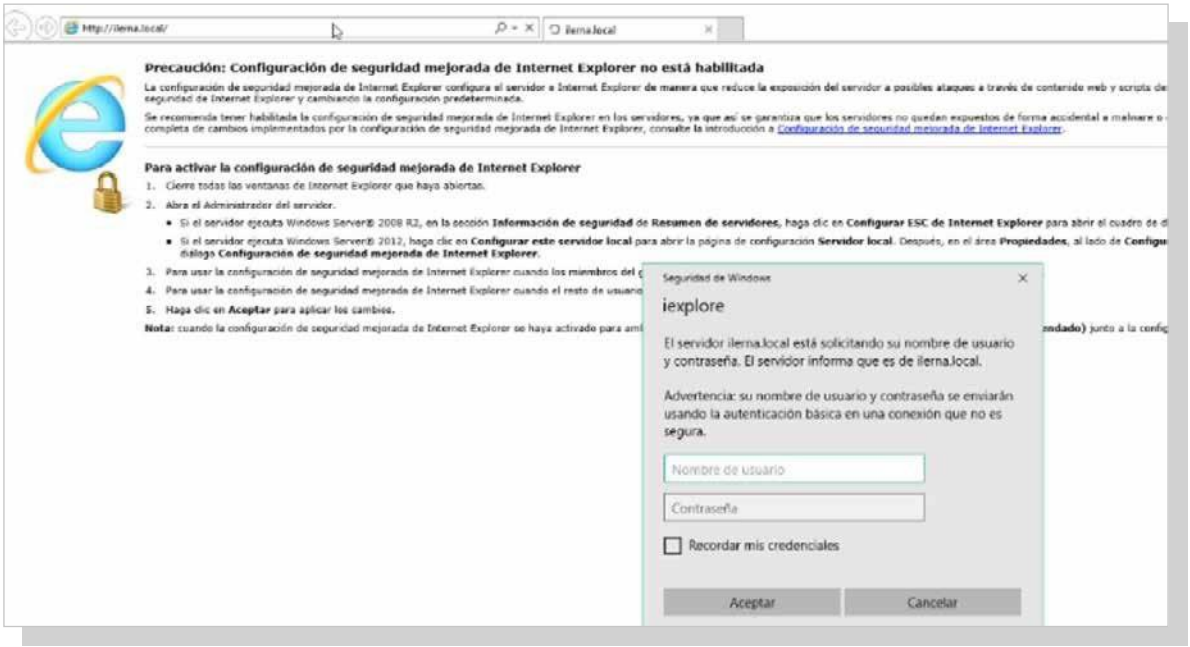
Antes de empezar con las verificaciones de autenticación al servicio web, se tiene que habilitar la autenticación básica (anteriormente instalada) y deshabilitar la autenticación anónima.

Para realizar esta operación tenemos que realizar los pasos que se indican en el punto 1.9 Configuración de comunicaciones seguras.

Verificación del acceso autenticado al servicio con HTTP

Para hacer la comprobación de que la URL se ha abierto de forma correcta y que funciona sobre el protocolo HTTP:

1. El equipo del cliente debe abrir el programa Internet Explorer en *Inicio/ Todos los programas.*
2. A continuación, escribir la dirección URL correspondiente del navegador web y pulsar *Intro.*
3. En la ventana que aparece, introducir el nombre de usuario y la contraseña.

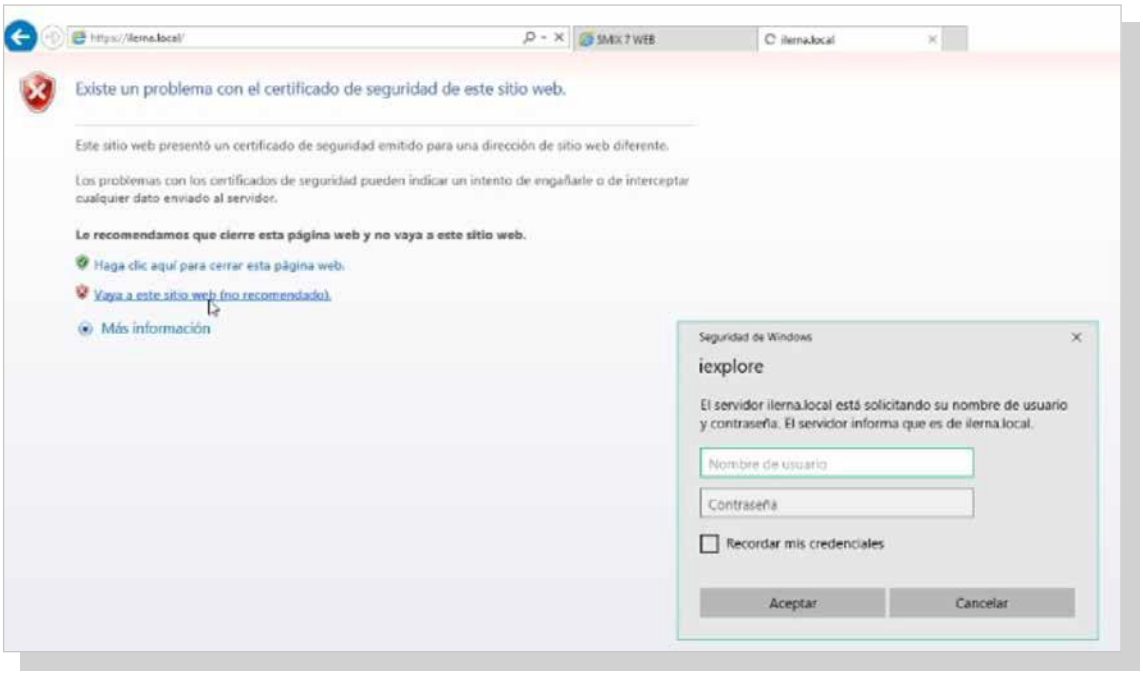


Verificación del acceso autenticado al servicio con HTTPS

Para comprobar que el funcionamiento del URL funciona con el protocolo HTTP seguro sobre HTTPS:

1. Abrir el programa Internet Explorer.
2. En URL escribir la dirección correspondiente y pulsar *Intro.*
3. Se muestra un aviso informando que el certificado creado no está firmado por ninguna CA, sino autofirmado

(por nosotros mismos). Clicar en *Vaya a este sitio web (no recomendado).*

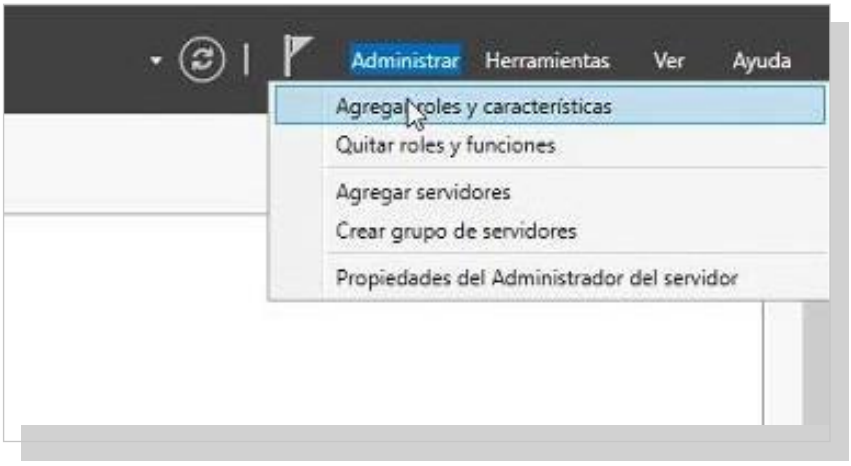


4. En la ventana que aparece, introducir el nombre de usuario y la contraseña.
5. Si el servicio HTTPS funciona de forma correcta, debe aparecer la página de aplicación web.

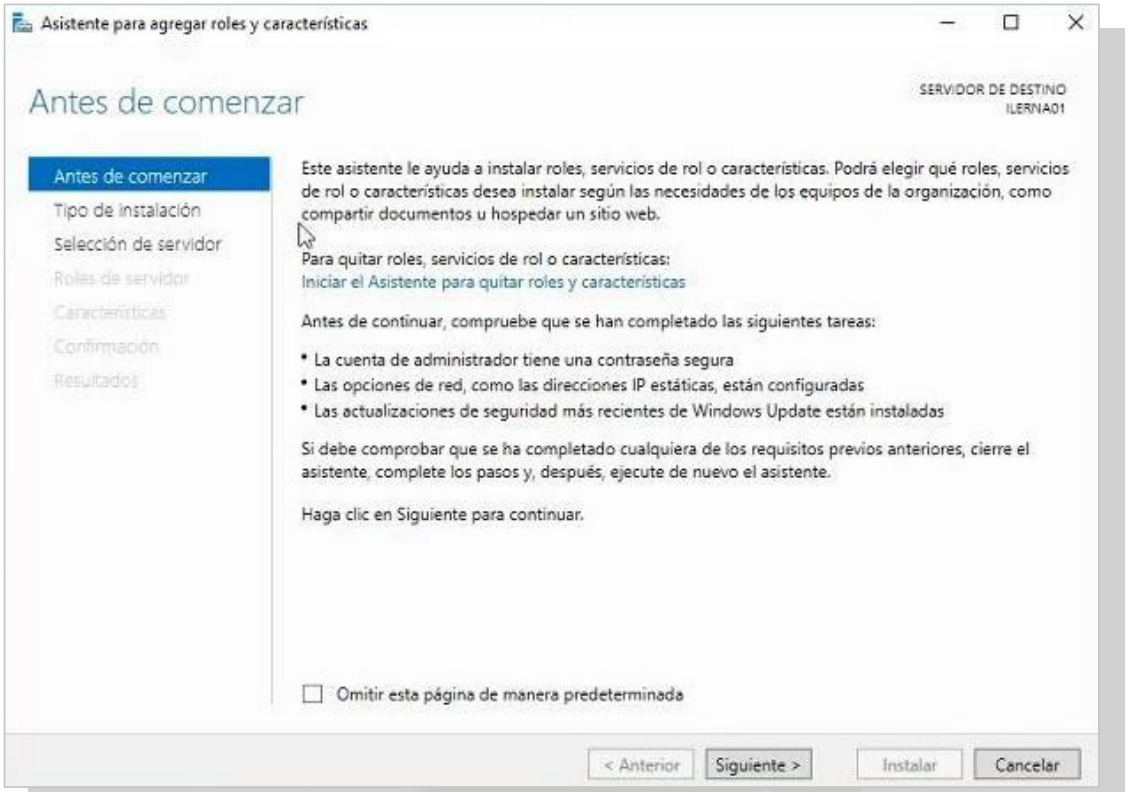
5.8. Instalación De nuevos móDulos

Para instalar nuevos módulos de autenticación básica, se deben seguir los siguientes pasos:

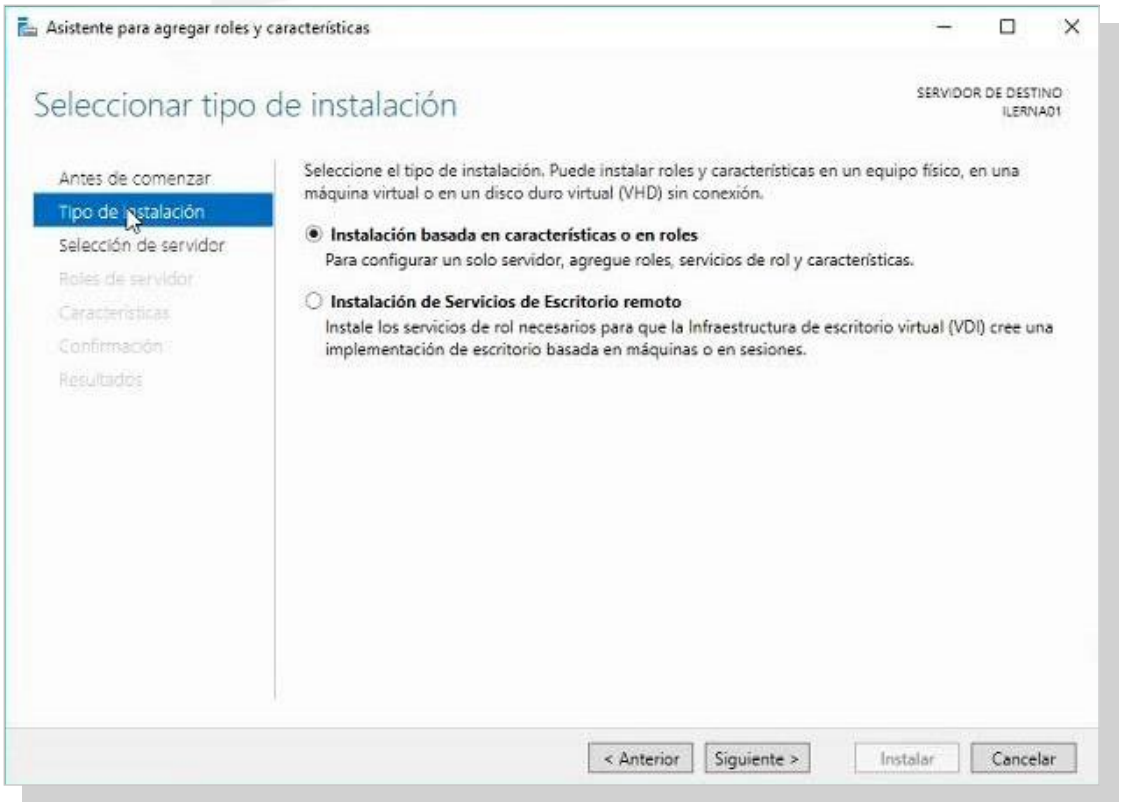
1. Abrir el administrador del servidor.



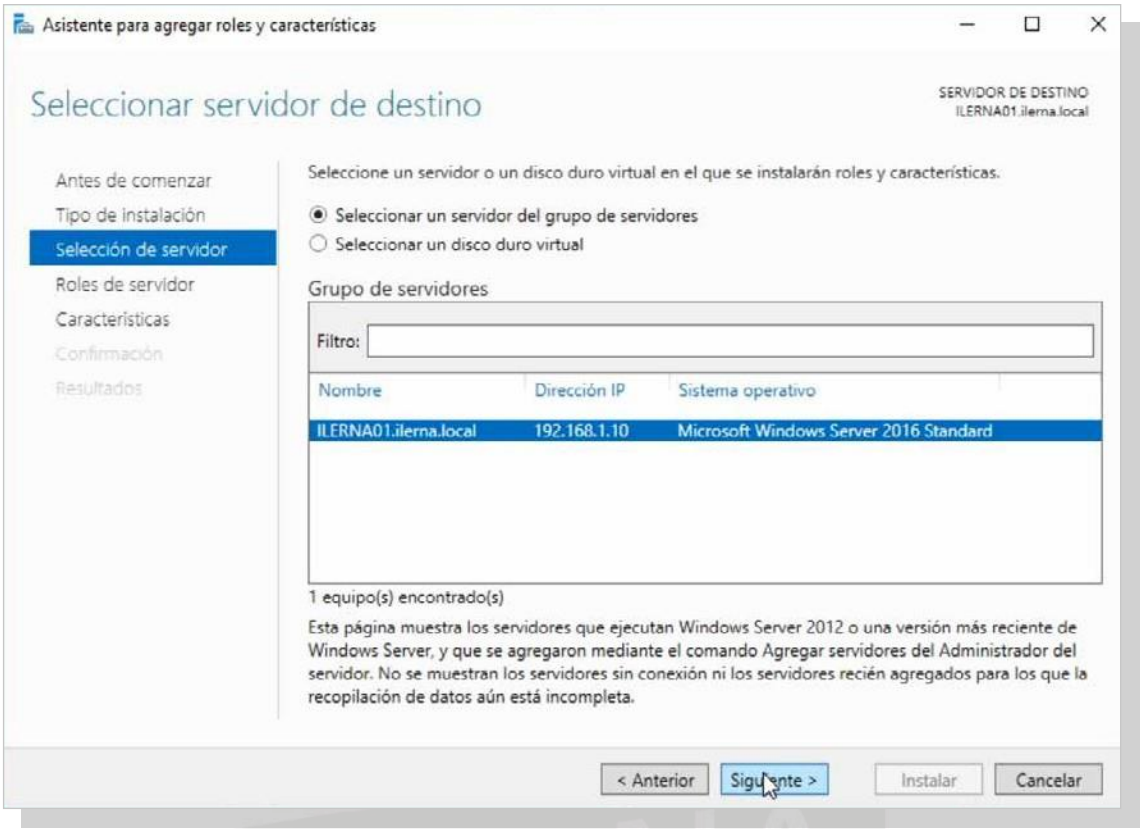
2. Aparece el asistente para agregar roles. Leer detenidamente. Para continuar, elegir la opción *Siguiente*.



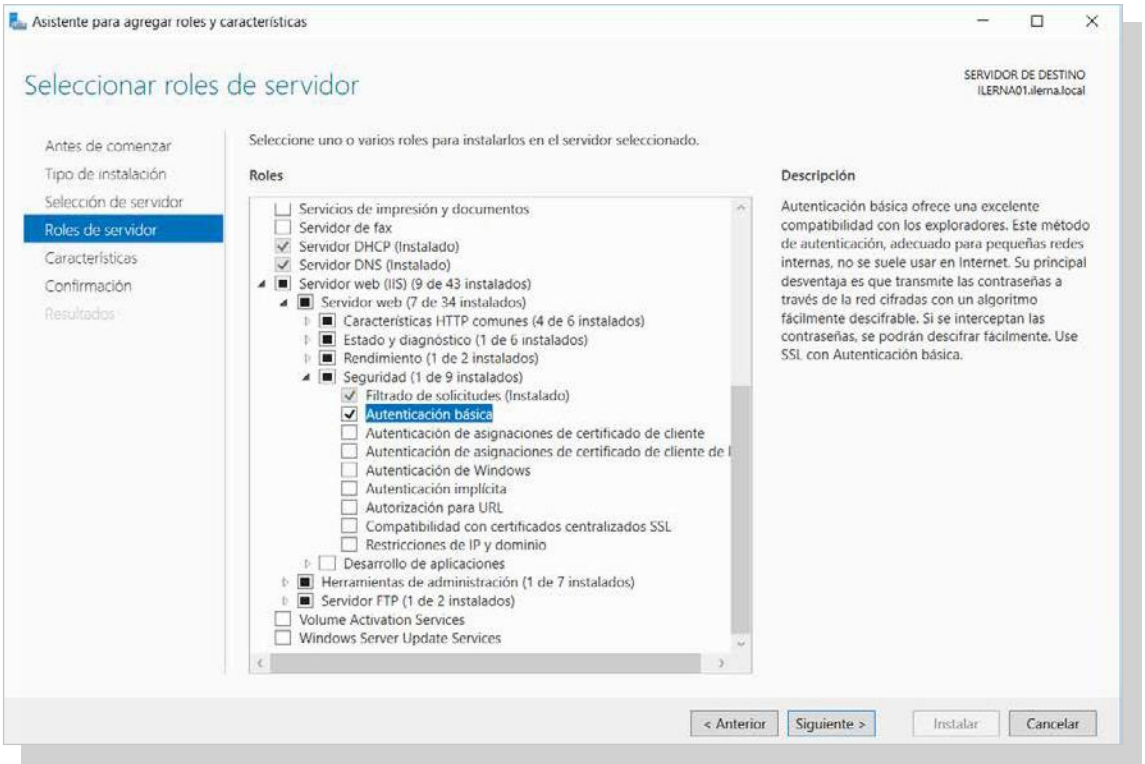
3. Elegir la instalación basada en roles, ya que estos ejemplos los veremos de forma práctica en un servidor virtual.



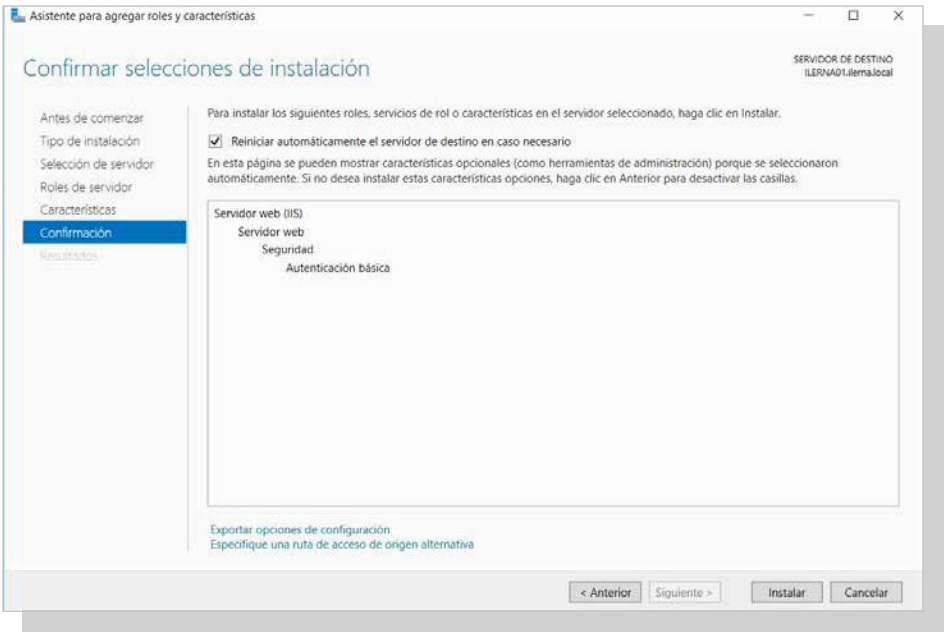
4. Elegir la dirección IP que corresponda a nuestro servidor y hacer clic en *Siguiente*.



5. En la ventana que aparece *Seleccionar servicios de función*, seleccionar la casilla de verificación *Autenticación básica* que se encuentra dentro de *Seguridad*, y hacer clic en *Siguiente.*



6. Seleccionar *Instalar* para iniciar la instalación.

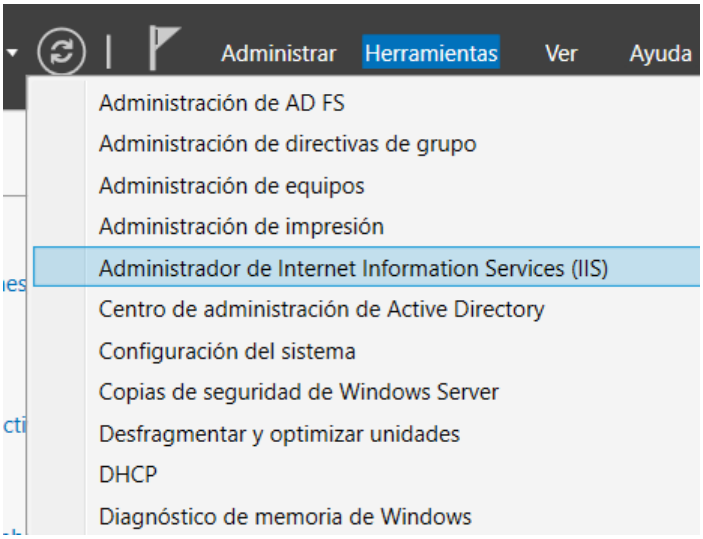


7. Transcurrido el tiempo necesario para la instalación, hacer clic en *Cerrar.*

5.9. Configuración De comunicaciones seguras

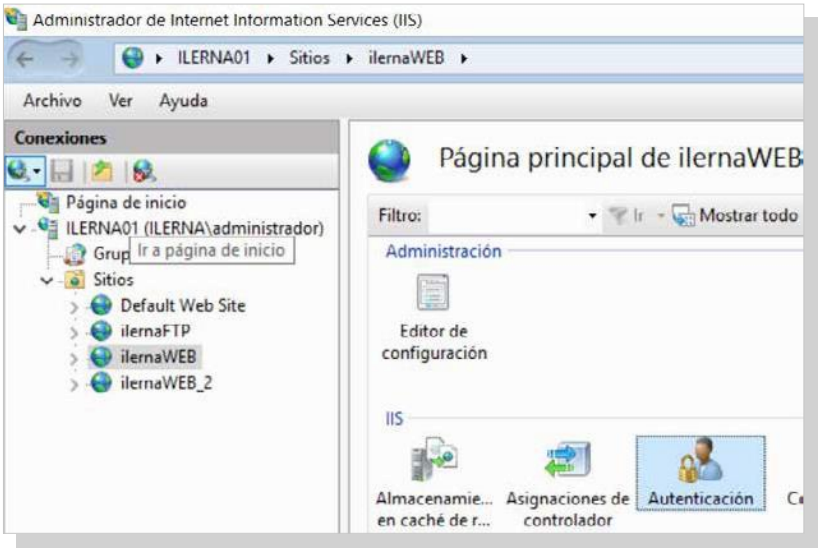
Cuando se necesita configurar un sitio para que pueda ser accesible mediante usuario y contraseña, se siguen los pasos a continuación:

1. Abrir el *Administrador de IIS.*

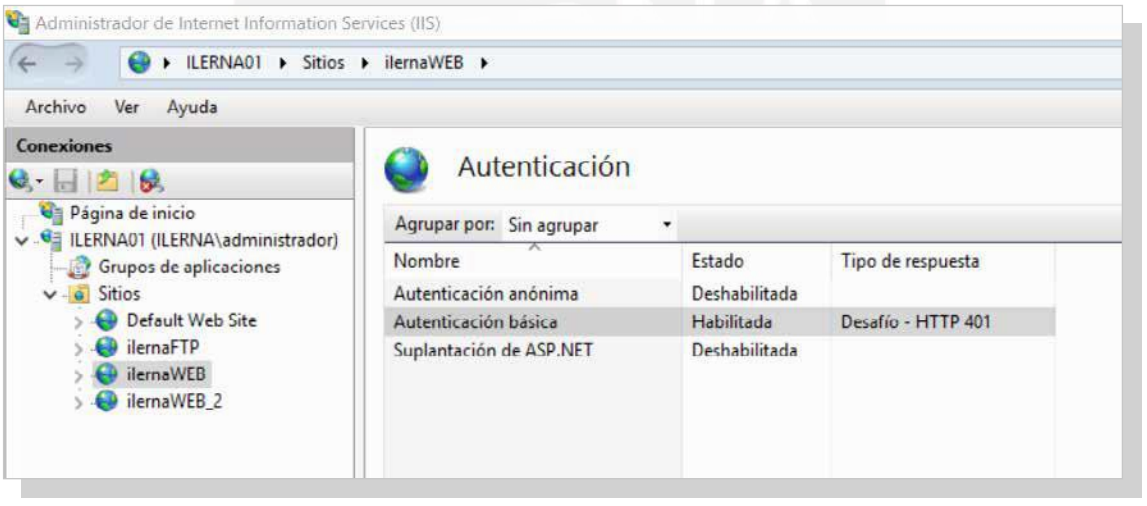


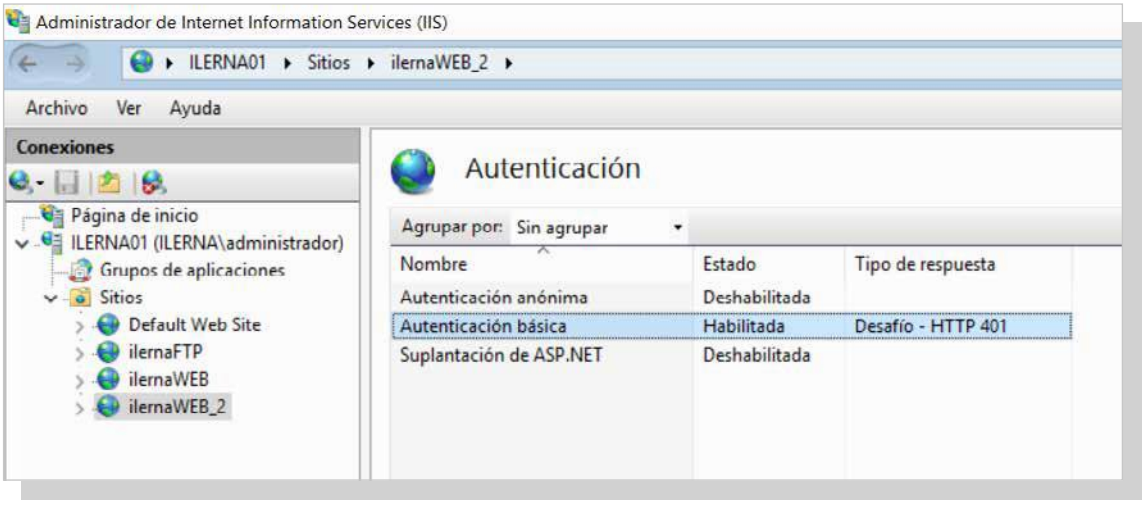
2. Seleccionar el sitio *SERVIDOR/Sitios/web App* y hacer doble clic en *Autenticación.*

3. Con el botón secundario, seleccionar *Autenticación básica* y hacer clic en *Habilitar* en el menú contextual.



4. A pesar de que la autenticación básica ya está activada, el sitio también tiene habilitada la autenticación anónima, por lo que puede ser accesible por más usuarios. Es necesario desactivar este tipo de acceso haciendo clic en *Autenticación anónima* y seleccionando la opción *Deshabilitar.*





5.10. Realización De Documentación aDecuaDa Para aPoyar al usuario

Para finalizar el proceso de instalación y configuración del servidor web en nuestro servidor, es recomendable elaborar un documento que englobe todo el procedimiento. Las ventajas de realizar este documento es que se deja constancia de todos los pasos previos a la instalación; es decir, a las condiciones en las que se encontró el equipo: *hardware* y *software* instalados, particiones de partida, *drivers* instalados y usuarios configurados.

En el proceso de configuración se puede dejar constancia de las opciones seleccionadas y de las razones para haber tomado tal decisión. Este documento debe ser una guía de consulta para futuras ampliaciones o posibles incidencias ocasionadas. Con referencia a las características del correo, se pueden detallar sus especificaciones, funcionamiento, protocolos de descarga, protocolos seguros.

Otros administradores pueden utilizar este tutorial como posible ayuda y explicación de todo el proceso, así como del estado en el que se encuentra el servidor y toda la red de comunicaciones.

Cuando aparecen incidencias en el servidor web, este documento puede ser útil para buscar una solución. Si el proyecto está totalmente actualizado, se puede ver cómo se solucionaron algunos incidentes parecidos ocurridos anteriormente.

La elaboración de este documento se puede hacer mediante una aplicación informática que facilite la recogida de incidencias.

Muchas de estas incidencias se pueden resolver *in situ* y, por tanto, se actúa directamente. Para problemas no tan importantes se gestiona de forma remota.

Otra vía para solventar los problemas es mediante el soporte técnico en línea que posee Microsoft en su centro **TechNet**. Esta ayuda es posible gracias a contar con un producto con licencia que permite estos privilegios. En el caso de un *software* libre, solo tendrá la ayuda que los foros no oficiales. Estos foros también pueden ser considerados en este caso, pero sabiendo que no son oficiales.