**Informe IIS**

**Servidor Web avanzado**



Daniel Escaño Hernández 2º ASIR

# **1. Índice:**

[**1. Índice:**](#_rzuyw1wdho0p) **2**

[**2. Carpetas Seguras**](#_xop5ocazssen) **3**

[2.1 Captura de la creación del sitio web:](#_ri1wk99oeqvx) 3

[2.2 Capturas de la creación del certificado autofirmado y la configuración de pagos para ser accedido vía https:](#_8e2g95rtmt8w) 4

[2.3 Captura del acceso a pagos vía https desde Windows Server:](#_mk0jmefw287m) 4

[2.4 Capturas de la solicitud de un certificado para nuestro servidor:](#_sk9z6r3si5jq) 5

[2.5 Capturas de la creación del certificado para nuestro servidor con OpenSSL:](#_vlud7fw53as4) 6

[2.6 Captura del acceso a tienda vía https desde Windows Server:](#_amq3483nmn8f) 9

[2.7 Capturas de los accesos vía https desde Windows Cliente:](#_g85949oa821) 10

[**3. Carpetas Privadas**](#_o6mrizcdmxwu) **12**

[3.1 Captura de la estructura del nuevo sitio web:](#_352lqiy9g9hk) 12

[3.2 Captura de la activación de la Autenticación Básica y deshabilitación del acceso anónimo:](#_xhn08a6h8f3v) 12

[3.3 Captura de los usuarios y grupo creados:](#_jyj05listn5d) 13

[3.4 Capturas de las configuraciones de permisos:](#_zb6214gnmmka) 14

[3.5 Capturas de los accesos vía https desde Windows Server:](#_v4m2gddiji70) 16

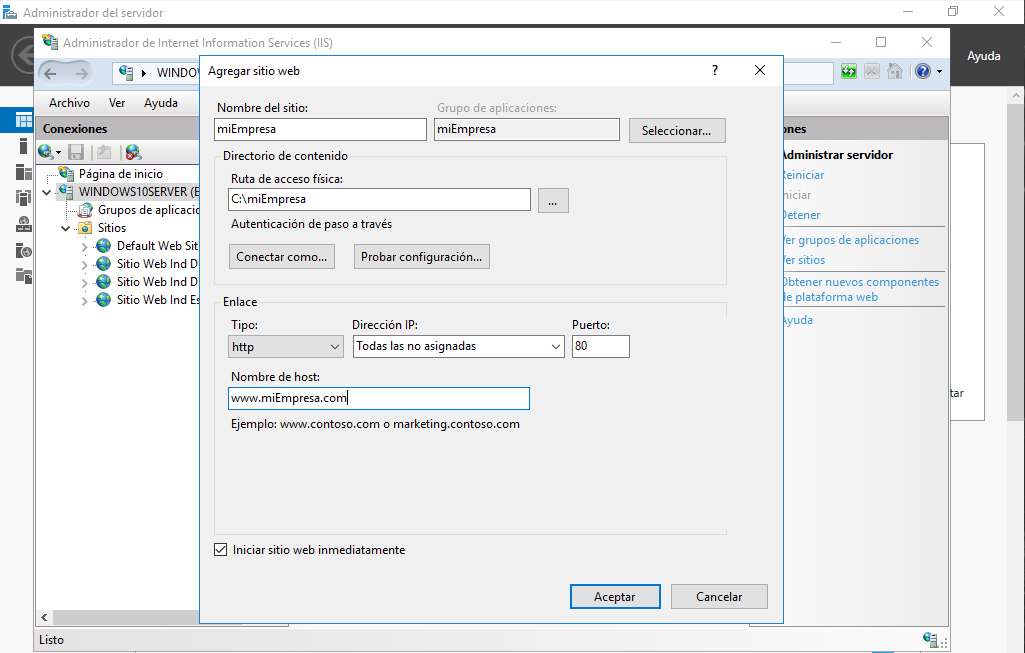
[3.6 Capturas de los accesos vía https desde Windows Cliente:](#_p5kh2rdty2vj) 18

# **2. Carpetas Seguras**

Crea una nueva zona de búsqueda directa en los servicios DNS asociado al dominio miEmpresa. Crea también una carpeta miEmpresa en C:\ y una subcarpeta ‘principal’.

Crea un nuevo sitio web denominado miEmpresa en IIS asociado a la subcarpeta anterior y con acceso a través de la dirección www.miEmpresa.com. Actualiza DNS adecuadamente.

### **2.1 Captura de la creación del sitio web:**

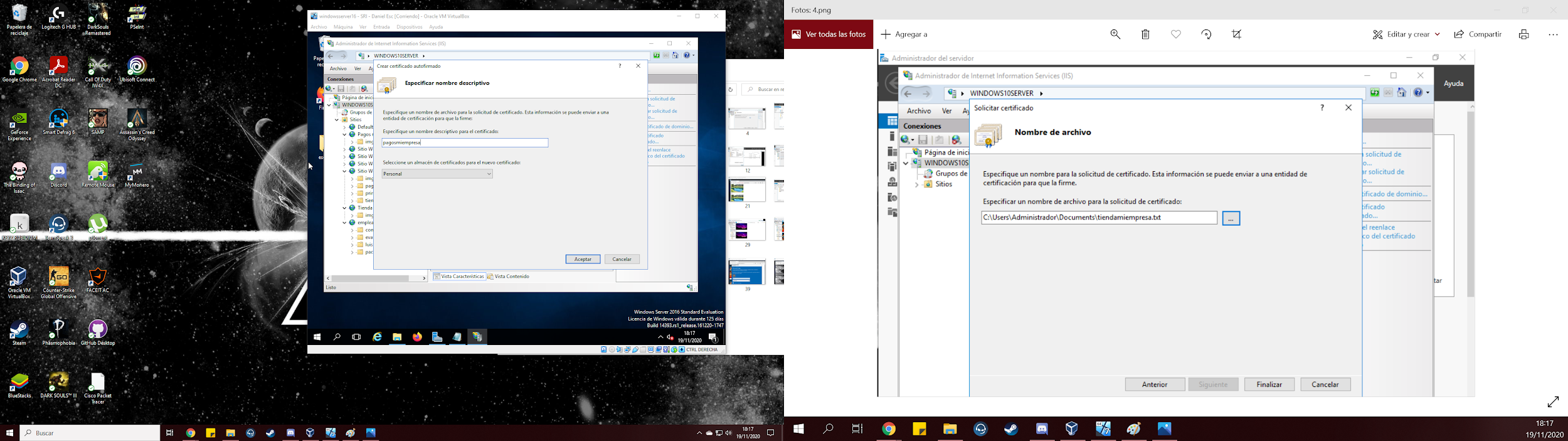


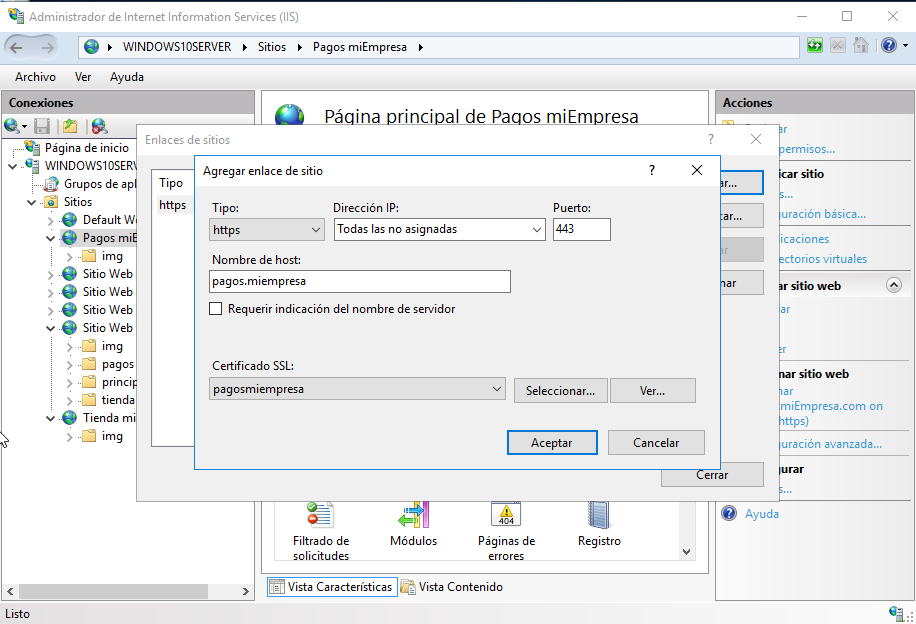
Crea un nuevo sitio web (denominado ‘pagos’) como subdominio de miEmpresa (pagos.miEmpresa.com) y configura este último para ser accedido de forma segura

Crea el sitio web, asociado a una carpeta (miEmpresa\pagos) y con la configuración adecuada en IIS y en los servicios DNS. Comprueba el acceso (aún vía ‘http’) con un navegador desde el propio servidor y desde un cliente W7.

Configuración A: Configura el nuevo sitio para que se pueda acceder (sólo) como sitio web seguro (https) con un Certificado Autofirmado.

### **2.2 Capturas de la creación del certificado autofirmado y la configuración de pagos para ser accedido vía https:**



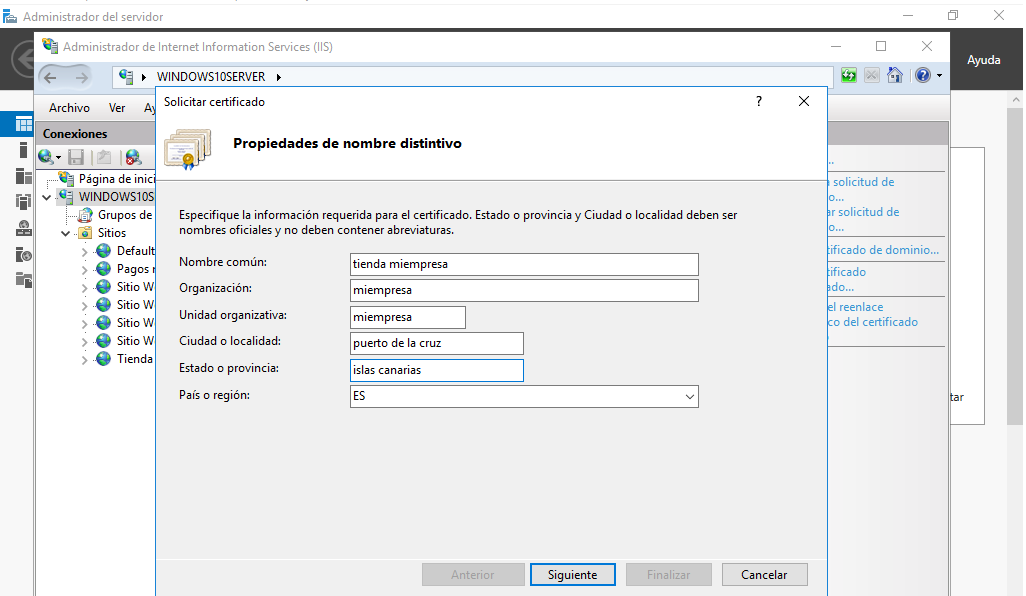


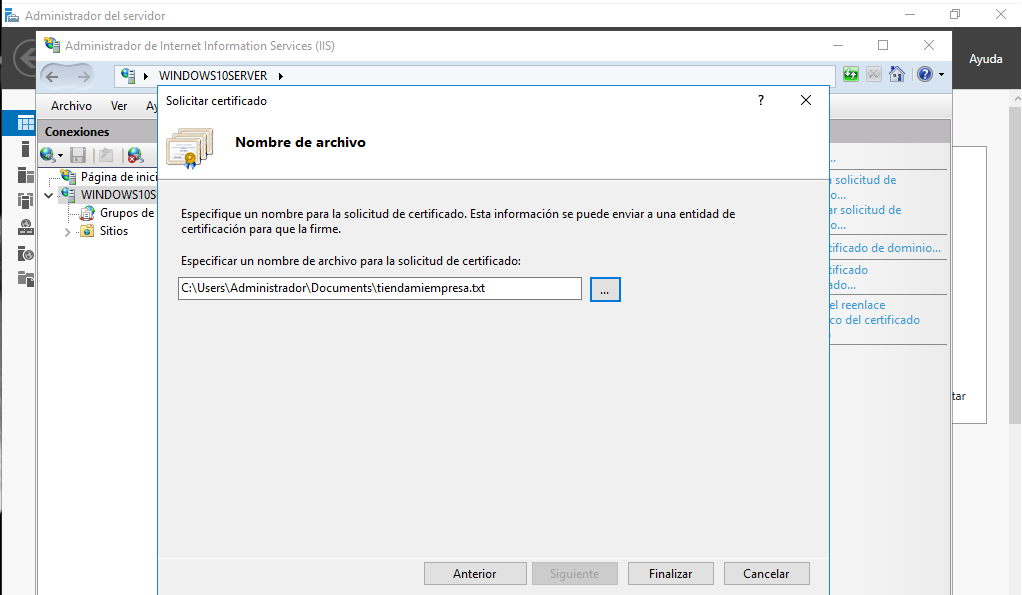
### **2.3 Captura del acceso a pagos vía https desde Windows Server:**

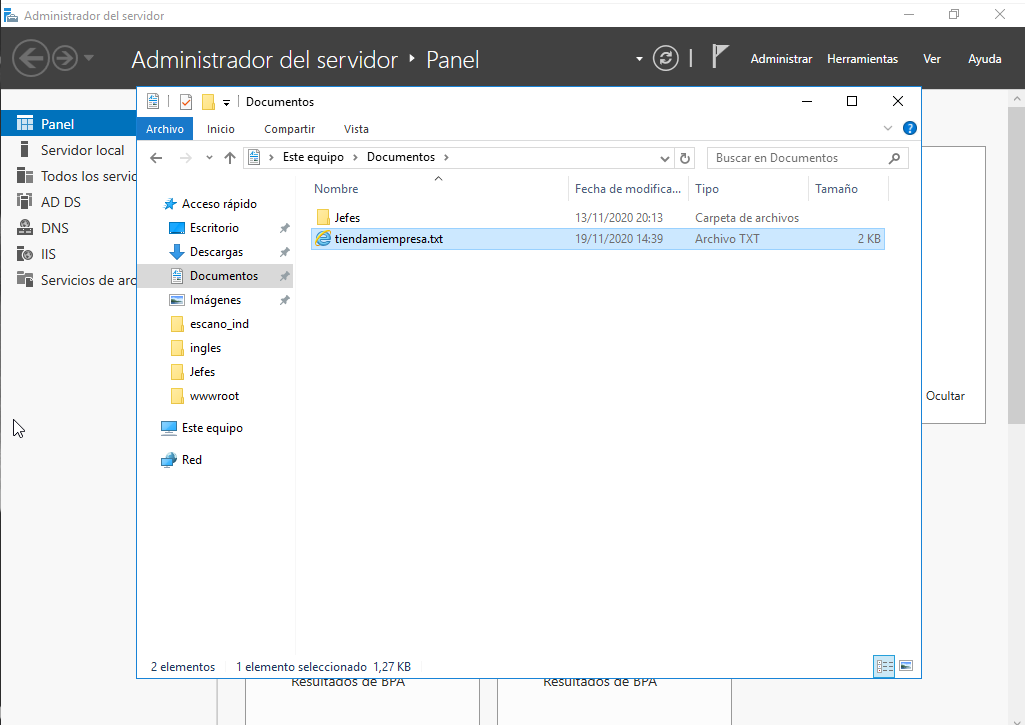


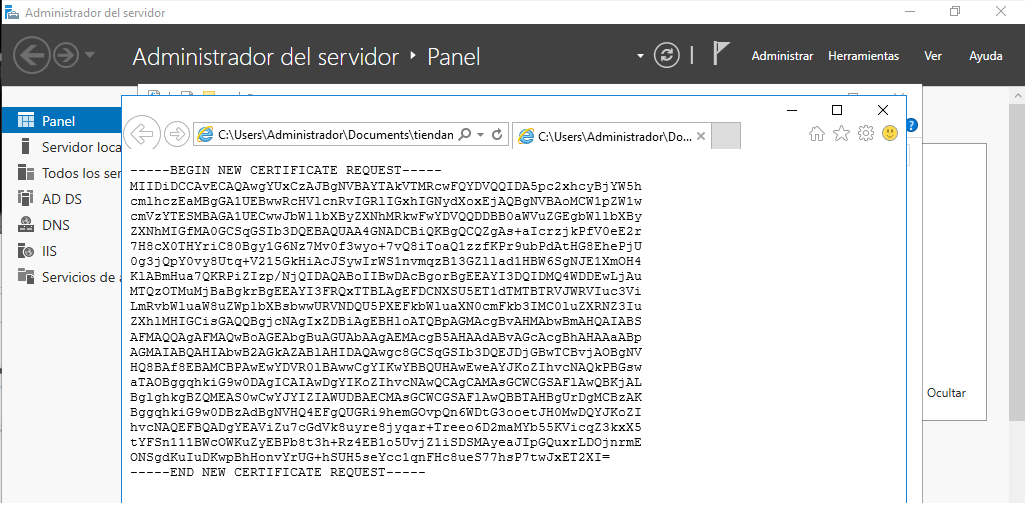
Configuración B: Crearemos un nuevo sitio seguro (tienda.miempresa.com) con la generación de un Certificado Digital a través de la aplicación OpenSSL. Para empezar, realizaremos la solicitud de un nuevo certificado de servidor para nuestro sitio seguro (crear fichero certreq.txt).

### **2.4 Capturas de la solicitud de un certificado para nuestro servidor:**







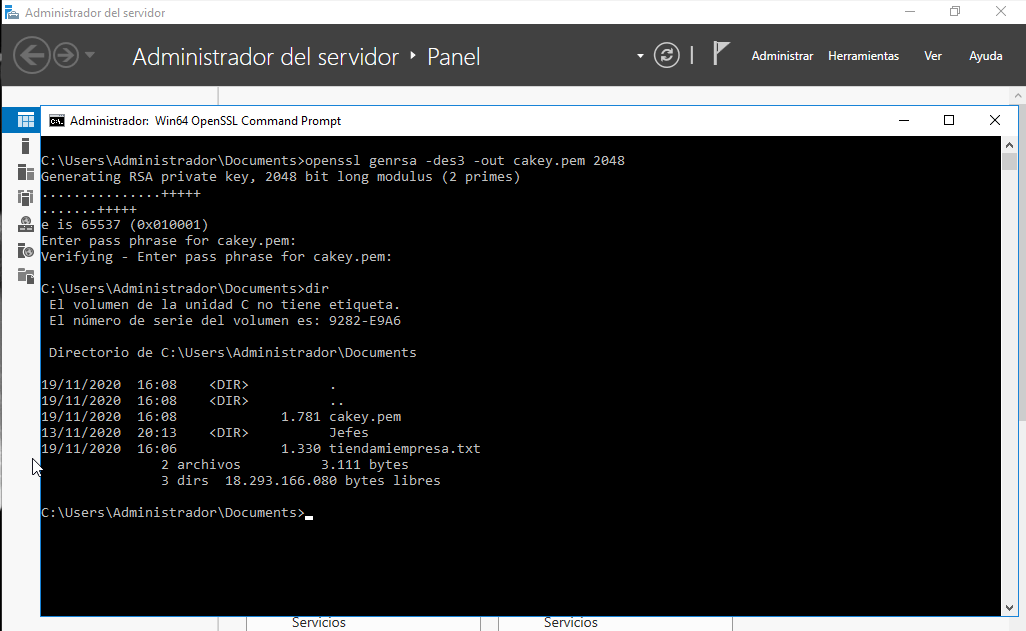


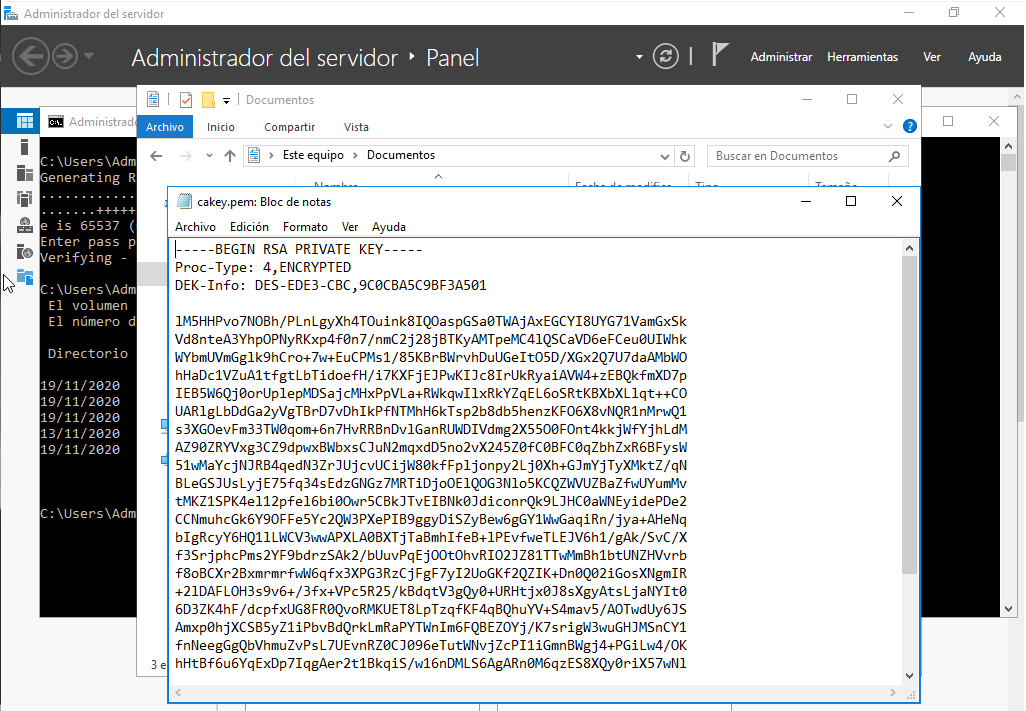
Descargar e instalar OpenSSL para Windows.

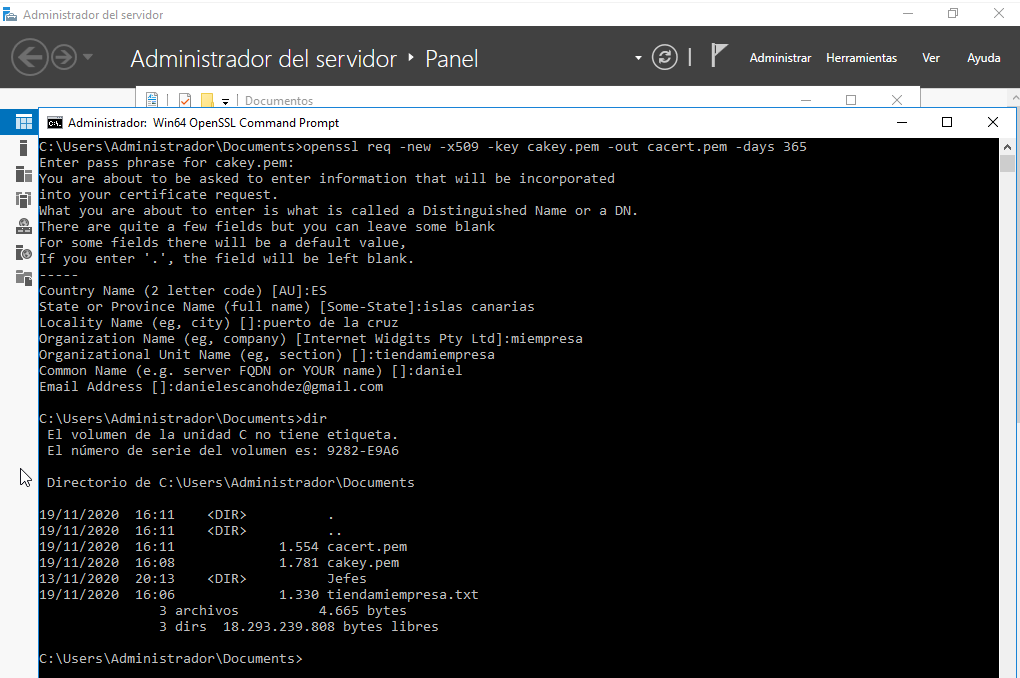
A través de OpenSSL genera un nuevo certificado de servidor, siguiendo los pasos que se detallan en tutorial web (y comprobando los ficheros generados en cada paso): generar una clave privada de la entidad certificadora, crear un certificado digital de la entidad certificadora y, finalmente, crear un certificado digital de nuestra web.

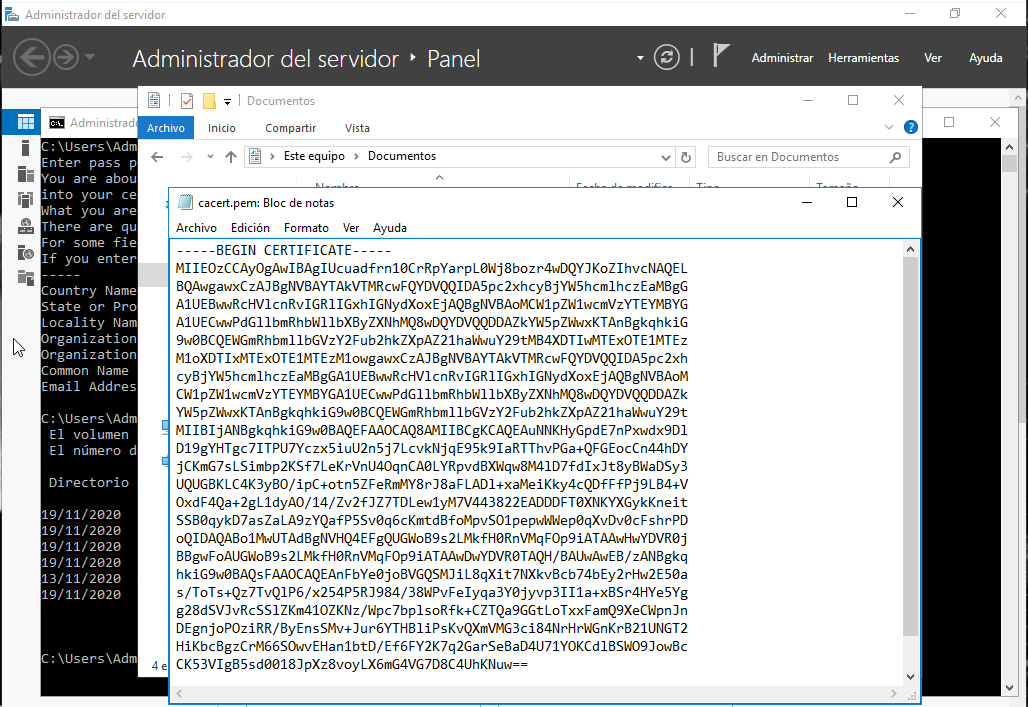
Importar el nuevo certificado de servidor creado para completar la petición pendiente en nuestro sitio seguro ‘pagos’.

### **2.5 Capturas de la creación del certificado para nuestro servidor con OpenSSL:**

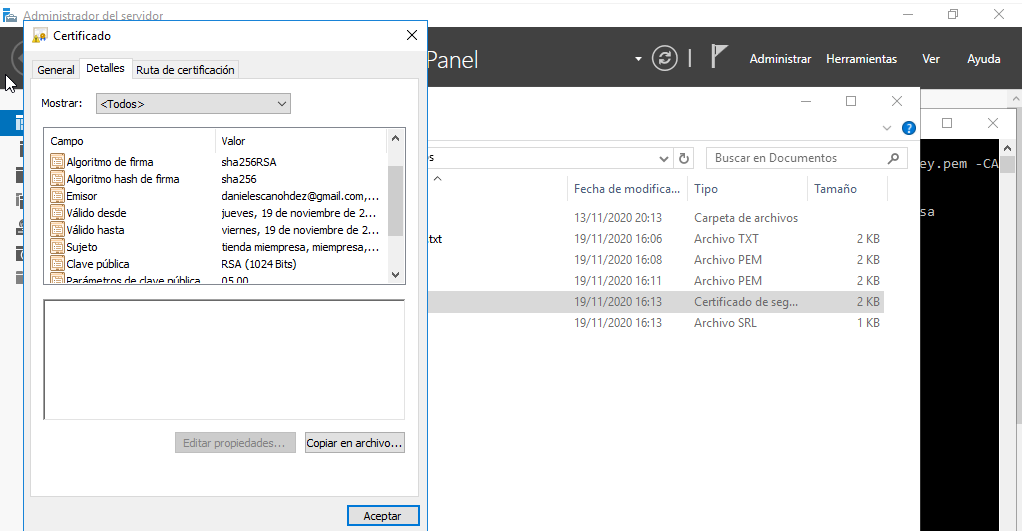


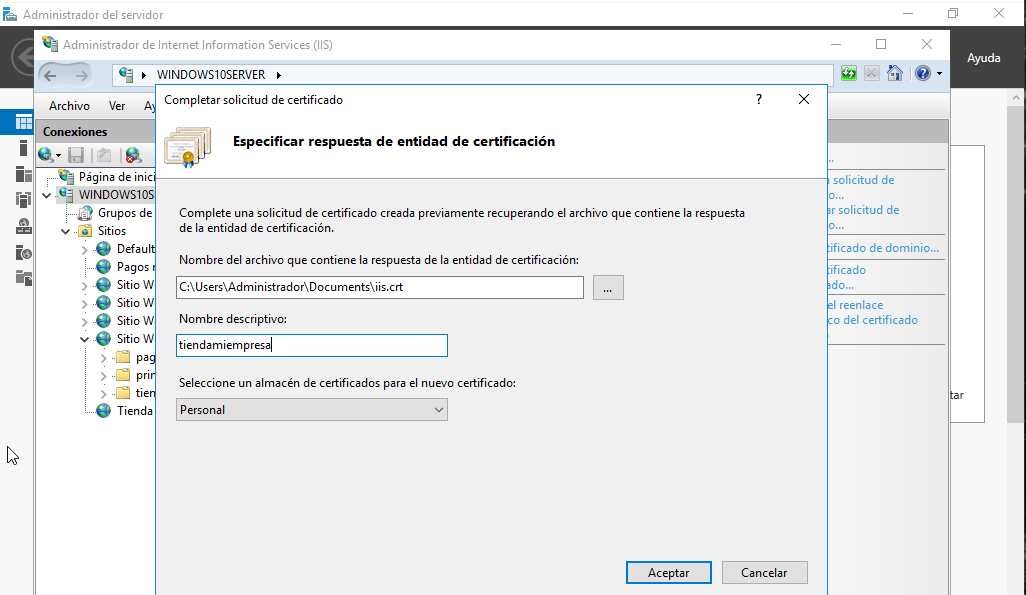


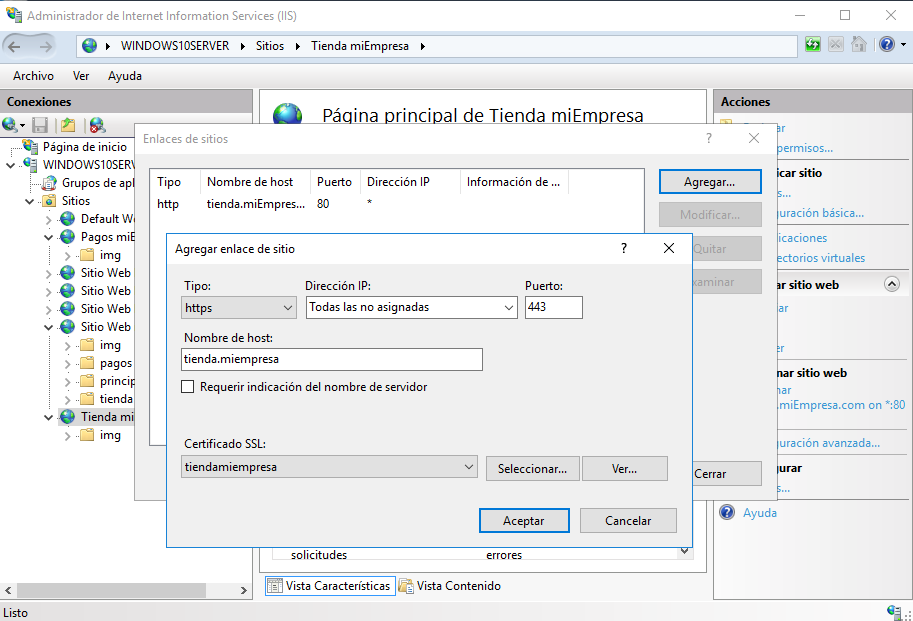




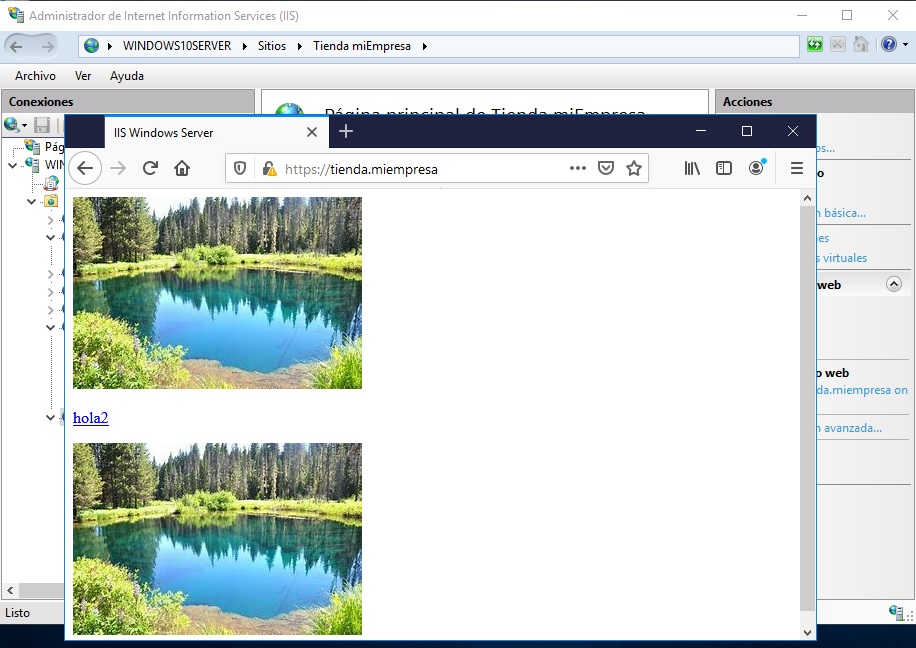








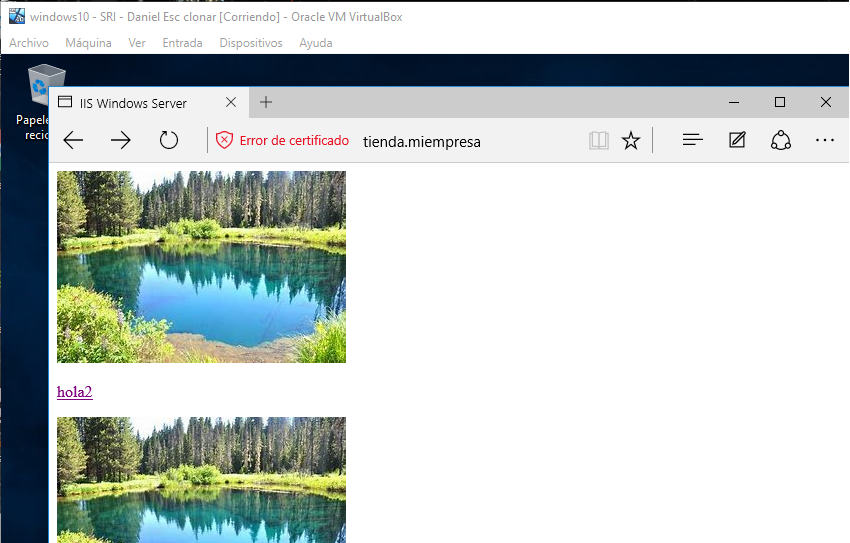
### **2.6 Captura del acceso a tienda vía https desde Windows Server:**



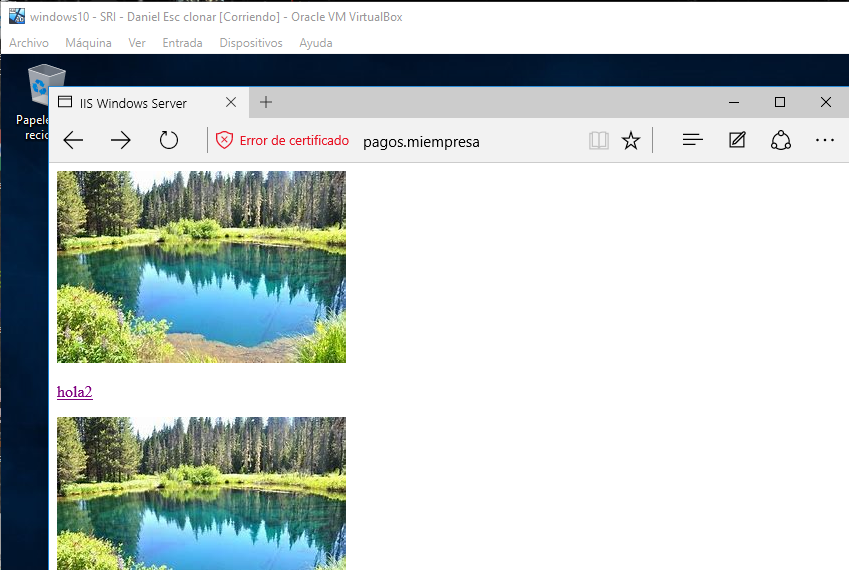
Finalmente, acceder mediante http y mediante https a los sitios seguros desde el propio servidor y desde un cliente W7, aceptando los posibles problemas con la entidad certificadora.

### **2.7 Capturas de los accesos vía https desde Windows Cliente:**









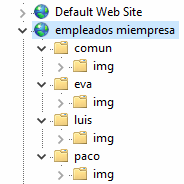
# **3. Carpetas Privadas**

Necesitamos crear una carpeta empleados (dentro de miEmpresa) y, dentro de esta, tres o cuatro subcarpetas personales con nombres de empleados y una, denominada común, a la que tendrán acceso todos los empleados, pero no otros usuarios sin identificar.

Crearemos el nuevo sitio web, como subdominio de nuestro dominio principal, asociado a la carpeta genérica empleados.

Colocar un fichero index.html diferente en cada una de las carpetas creadas, con el objetivo de poder comprobar el acceso desde un navegador.

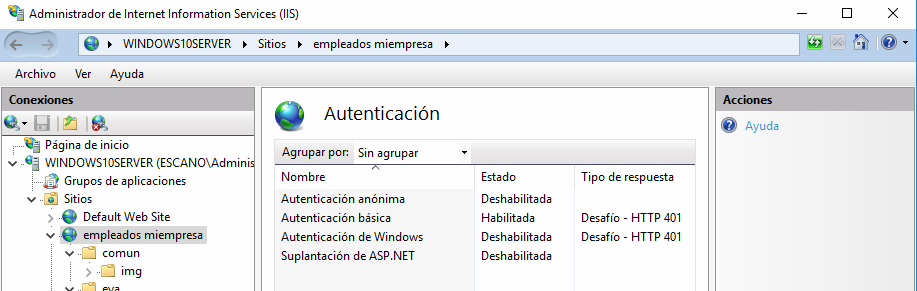
### **3.1 Captura de la estructura del nuevo sitio web:**



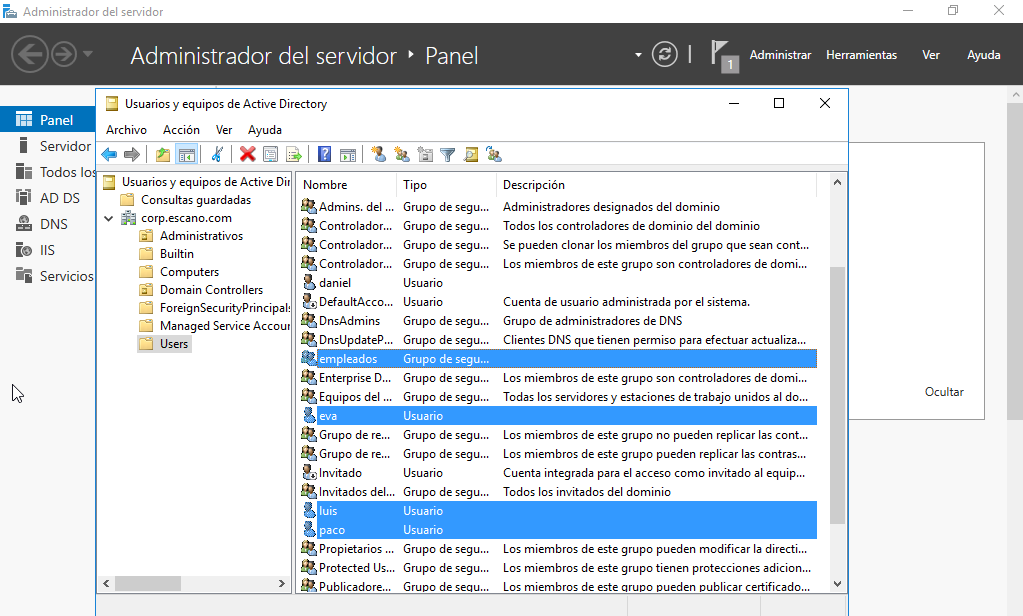
Para el sitio web creado y para cada una de sus carpetas, deshabilitamos el acceso anónimo y agregar función de Autenticación Básica a nuestro Servicio de IIS a través de la Administración del Servidor.

### **3.2 Captura de la activación de la Autenticación Básica y deshabilitación del acceso anónimo:**

En Active Directory, crearemos un usuario para cada empleado (tantos como carpetas personales) y un grupo Empleados que los incluya a todos.



### **3.3 Captura de los usuarios y grupo creados:**

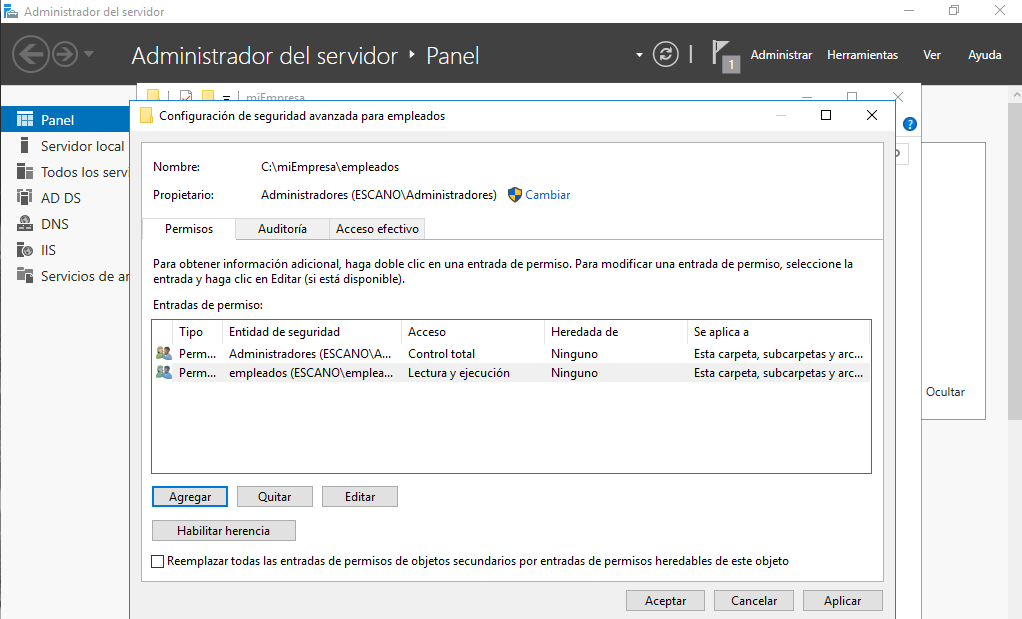


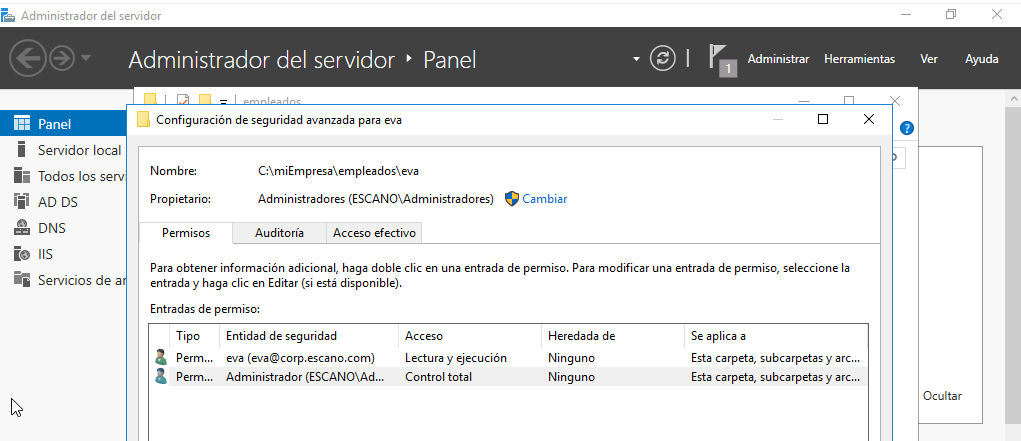
Desactivamos, para la carpeta empleados, los permisos heredables a través de las opciones avanzadas en la ficha de seguridad. Añadimos grupo de Administradores con Control Total y grupo Empleados con Lectura y Ejecución+ Mostrar Carpeta+Leer.

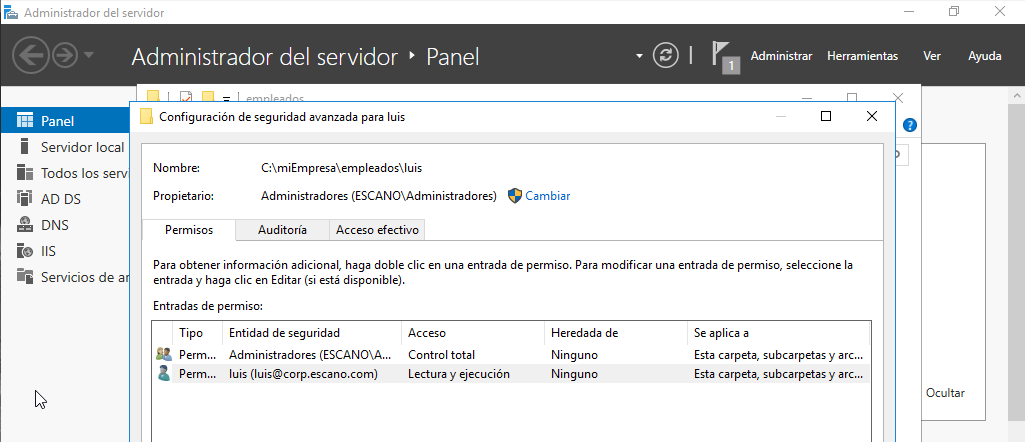
Realizamos el mismo procedimiento para cada una de las carpetas personales de los empleados, colocando como usuarios autorizados el Grupo de Administradores (Control Total) y el empleado propietario de cada carpeta (con los permisos que creas convenientes).

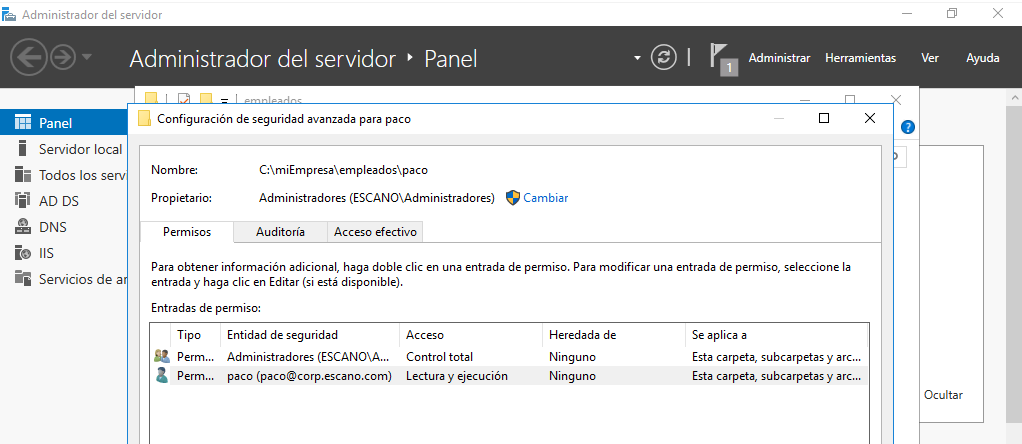
Realizamos el mismo procedimiento para la carpeta ‘común’, colocando como usuarios autorizados el Grupo de Administradores (Control Total) y el grupo Empleados (con los permisos que creas convenientes).

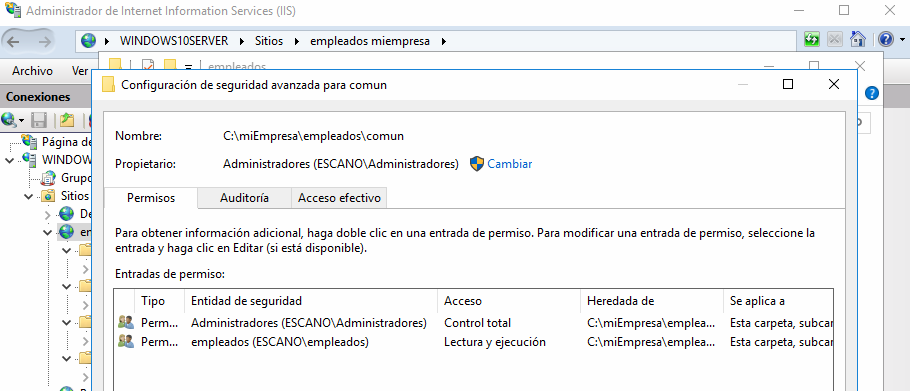
### **3.4 Capturas de las configuraciones de permisos para cada carpeta:**









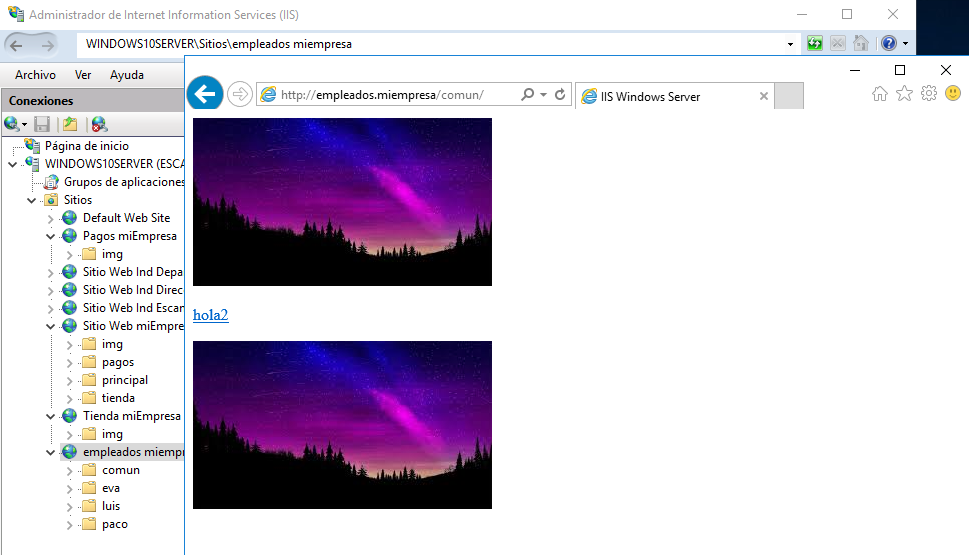


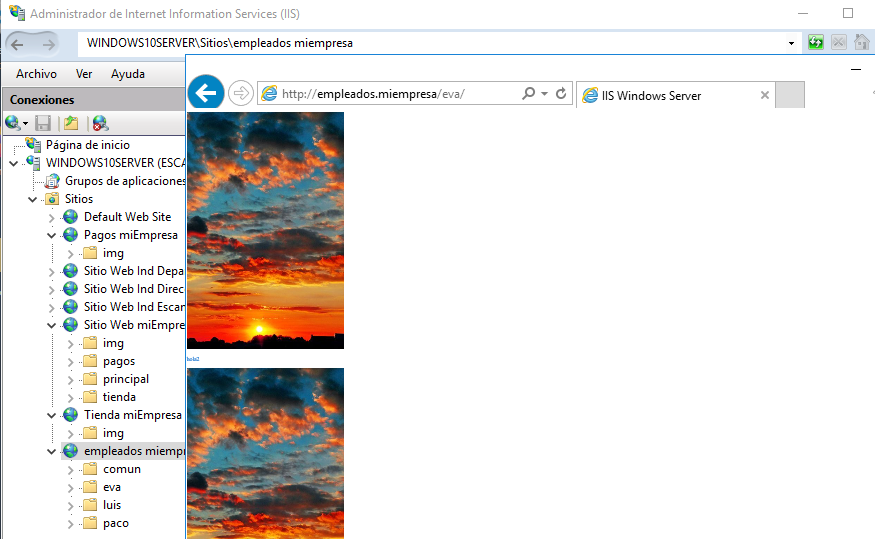
Comprobamos el acceso, tanto desde el servidor como desde el cliente W7, a las diferentes carpetas con distintos usuarios.

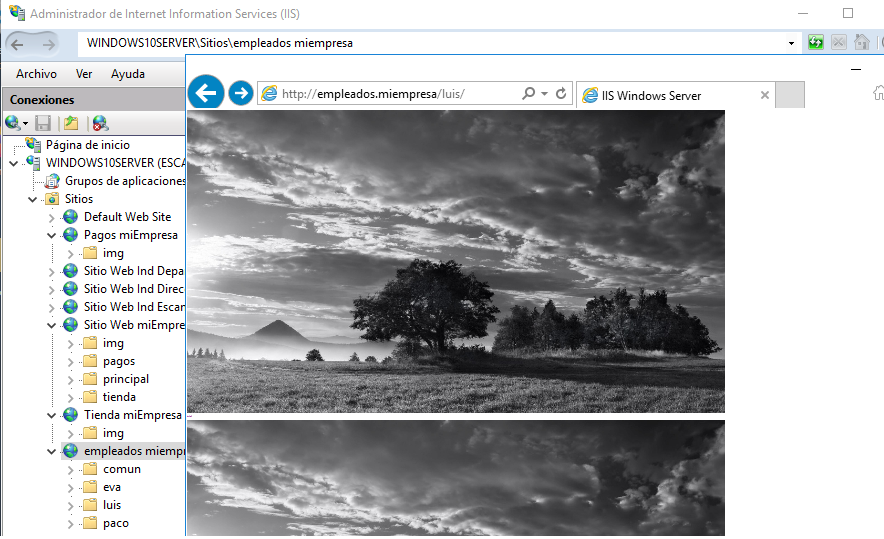
### **3.5 Capturas de los accesos vía https desde Windows Server:**

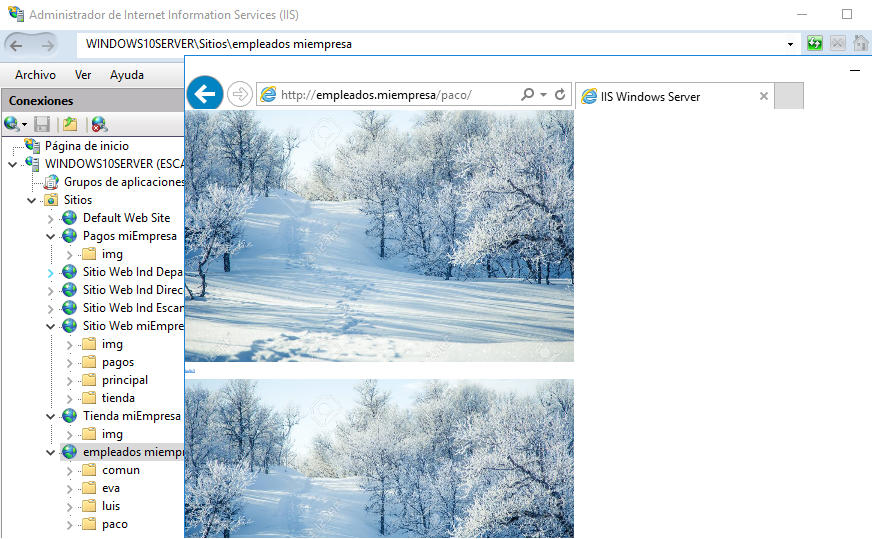
### 

En el Windows Server utilice la cuenta de Administrador por eso no vuelve a pedir autenticación al tener permisos en todas las carpetas.









### **3.6 Capturas de los accesos vía https desde Windows Cliente:**

