

# Práctica 3.3

## HTTP Redireccionamiento y Páginas de error

**Alejandro Almendras Nina**

### ÍNDICE DE CONTENIDO

<b>1. Ubuntu Server.....</b>	<b>2</b>
1.1 Apertura de puertos.....	2
1.2 Configurar un nuevo sitio con certificado SSL, con autenticación y con página de error personalizada.....	2
1.3 Configurar redirección.....	3
1.4 Configuración DNS.....	3
1.5 Reinicio de servicios y comprobación en el cliente.....	3
<b>2. Windows Server.....</b>	<b>5</b>
2.1 Apertura de puertos.....	5
2.2 Configurar un nuevo sitio seguro.....	5
2.3 Configurar autenticación.....	6
2.4 Configurar página de error personalizada.....	7
2.5 Configurar redirección.....	8
2.6 Configuración DNS.....	8
2.7 Comprobación en el cliente.....	9

# 1. Ubuntu Server

## 1.1 Apertura de puertos

Este nuevo sitio usará el puerto 445 y el 85 lo usaremos para la página falsa que redireccionará a la segura así que vamos a abrir dichos puertos.

```
GNU nano 4.8 /etc/apache2/ports.conf
Listen 80
Listen 85
Listen 82
Listen 83
<IfModule ssl_module>
    Listen 443
    Listen 444
    Listen 445
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

## 1.2 Configurar un nuevo sitio con certificado SSL, con autenticación y con página de error personalizada

Además será un sitio que use certificado, pida autenticación y tenga un documento de error. Procedemos a visualizar el archivo de configuración de este nuevo sitio además de los contenidos de la página principal y de error.

```
GNU nano 4.8 /etc/apache2/sites-available/web1.conf
<IfModule mod_ssl.c>
    <VirtualHost web1.dominio204.local:445>
        ServerName web1.dominio204.local
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/avanzado204

        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/204cert.pem
        ErrorDocument 404 /error404.html

        <Directory /var/www/avanzado204>
            DirectoryIndex web1.php
            AuthType Basic
            AuthName "Private Access Folder"
            AuthUserFile /etc/apache2/passwd/.htpasswd
            Require user web1
        </Directory>
    </VirtualHost>
</IfModule>

GNU nano 4.8 /var/www/avanzado204/web1.php
<?php
echo '<style>body{color:#190B28;font-family:sans-serif;background-color:#645DD7;';
echo ' margin:20; } a{color:#F4FAFF} </style>';

echo '<h1>Hola, éste sitio es seguro, autenticado, y fue redireccionado</h1>';
echo '<p>Si desea ir a una página inexistente para que le de error, pulse '
echo '<a href="./h.html">aquí</a></p>';
?>

GNU nano 4.8 /var/www/avanzado204/error404.html
<!DOCTYPE html>
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
<title>ERROR 404</title>
<style>body {color: #454851; font-family:sans-serif; background-color:#EE6352; margin:20;}</style>
</head><body><h1>ERROR 404: Página no encontrada &#128546</h1></body></html>
```

### 1.3 Configurar redirección

Configuraremos además una redirección cuando intenten acceder al sitio de manera no segura con el puerto antes mencionado.

```
GNU nano 4.8 /etc/apache2/sites-available/web1red.conf
<VirtualHost web1.dominio204.local:85>
    ServerName web1.dominio204.local
    ServerAdmin webmaster@localhost
    Redirect / https://web1.dominio204.local:445
</VirtualHost>
```

### 1.4 Configuración DNS

Por otro lado nos tenemos que asegurar que el servidor DNS resuelva la consulta de web1 con su IP, pues es el equipo que la sirve también.

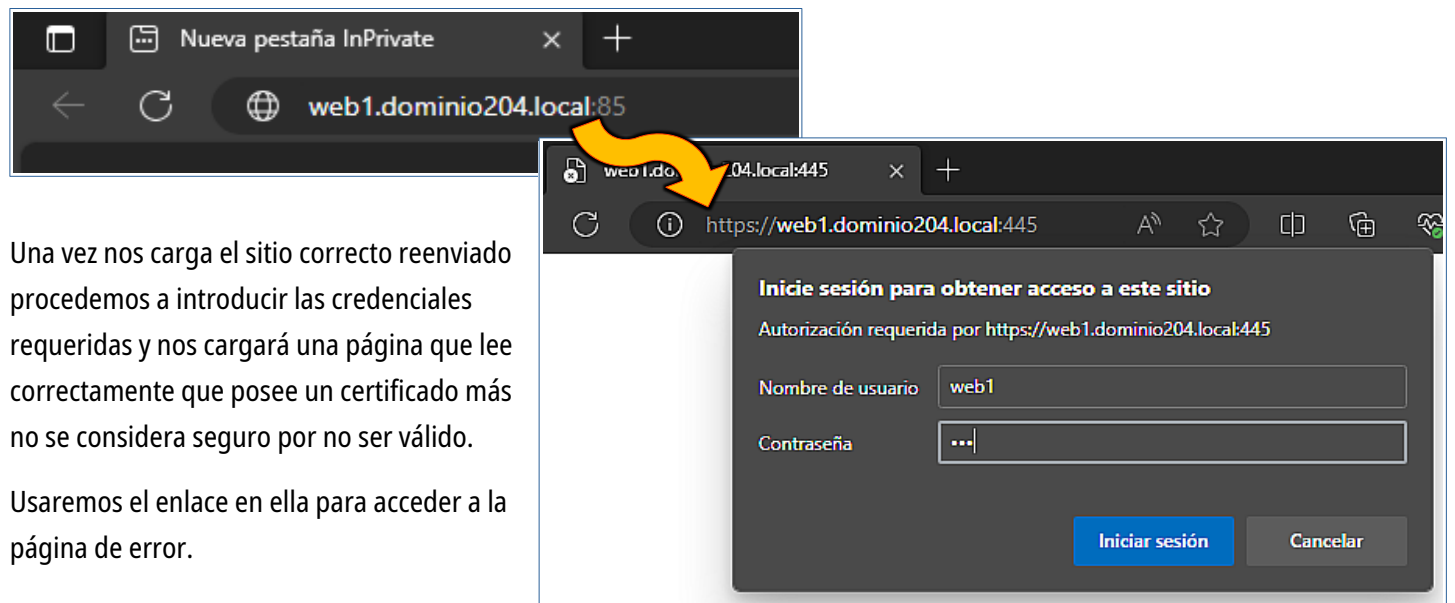
```
GNU nano 4.8 /var/cache/bind/dominio204.local.db
www                A      172.16.204.202
www1               A      172.16.204.205
web1               A      172.16.204.202
```

### 1.5 Reinicio de servicios y comprobación en el cliente

Finalmente habilitamos la configuración de los sitios nuevos (el falso-inseguro y el correcto-seguro), reiniciamos también los servicios de DNS y Apache, y comprobamos el estado de los sitios servidos.

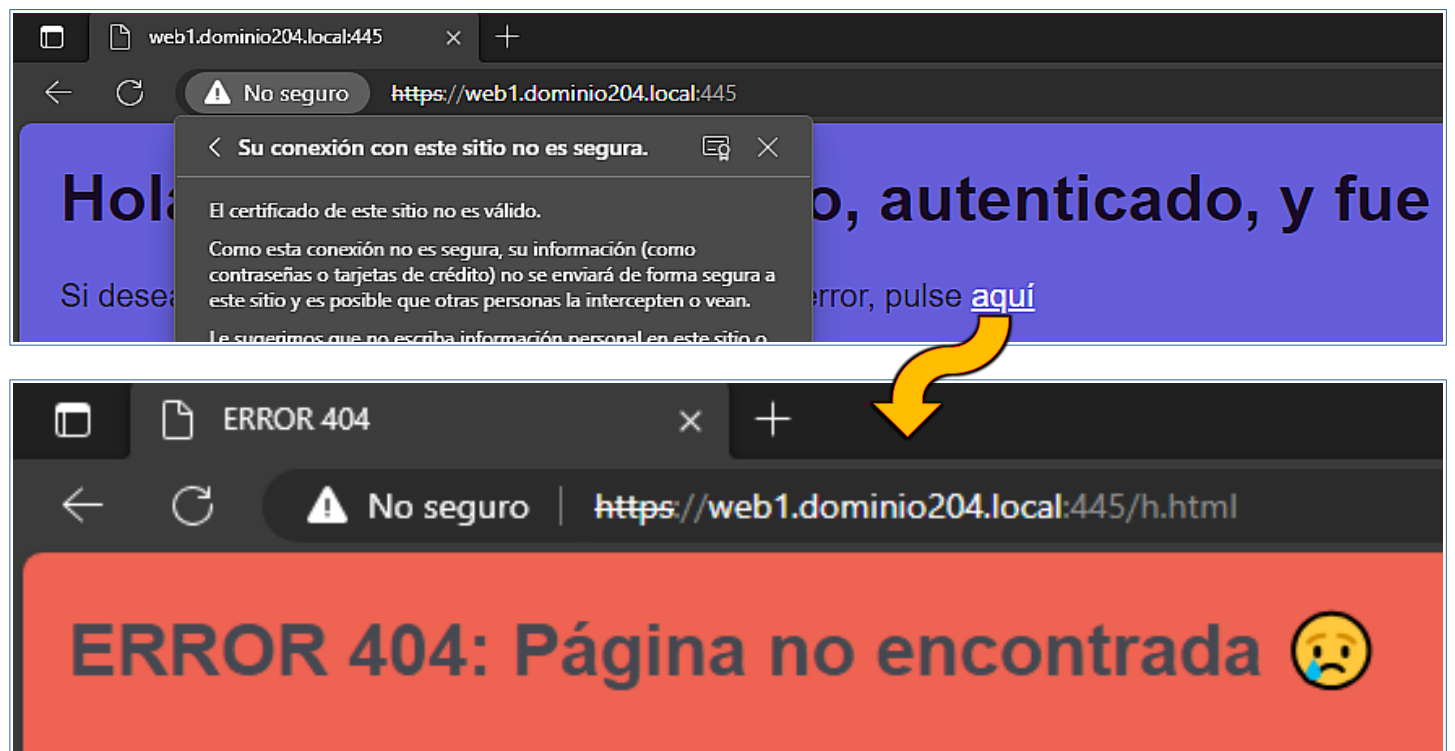
```
administrador-204@ubuntu-204:~$ sudo a2ensite web1.conf
Site web1 already enabled
administrador-204@ubuntu-204:~$ sudo a2ensite web1red.conf
Site web1red already enabled
administrador-204@ubuntu-204:~$ sudo systemctl restart bind9
administrador-204@ubuntu-204:~$ sudo systemctl restart apache2
administrador-204@ubuntu-204:~$ sudo apache2ctl -S
VirtualHost configuration:
172.16.204.202:80       www.dominio204.local (/etc/apache2/sites-enabled/204.conf:1)
172.16.204.202:82       www.dominio204.local (/etc/apache2/sites-enabled/privado.conf:1)
172.16.204.202:444      www.dominio204.local (/etc/apache2/sites-enabled/seguro.conf:2)
172.16.204.202:445      web1.dominio204.local (/etc/apache2/sites-enabled/web1.conf:2)
172.16.204.202:85       web1.dominio204.local (/etc/apache2/sites-enabled/web1red.conf:1)
*:80                   127.0.0.1 (/etc/apache2/sites-enabled/000-default.conf:1)
ServerRoot: "/etc/apache2"
Main DocumentRoot: "/var/www/html"
Main ErrorLog: "/var/log/apache2/error.log"
Mutex watchdog-callback: using_defaults
Mutex ssl-stapling-refresh: using_defaults
Mutex ssl-stapling: using_defaults
Mutex ssl-cache: using_defaults
Mutex default: dir="/var/run/apache2/" mechanism=default
Mutex mpm-accept: using_defaults
PidFile: "/var/run/apache2/apache2.pid"
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="www-data" id=33
Group: name="www-data" id=33
```

Procederemos entonces ahora a comprobar esta configuración desde el cliente. Dado que la redirección es instantánea no hay una manera efectiva de capturar su correcto funcionamiento para éste informe, igualmente la dirección introducida es la de la izquierda y nos carga la imagen de la derecha.



Una vez nos carga el sitio correcto reenviado procedemos a introducir las credenciales requeridas y nos cargará una página que lee correctamente que posee un certificado más no se considera seguro por no ser válido.

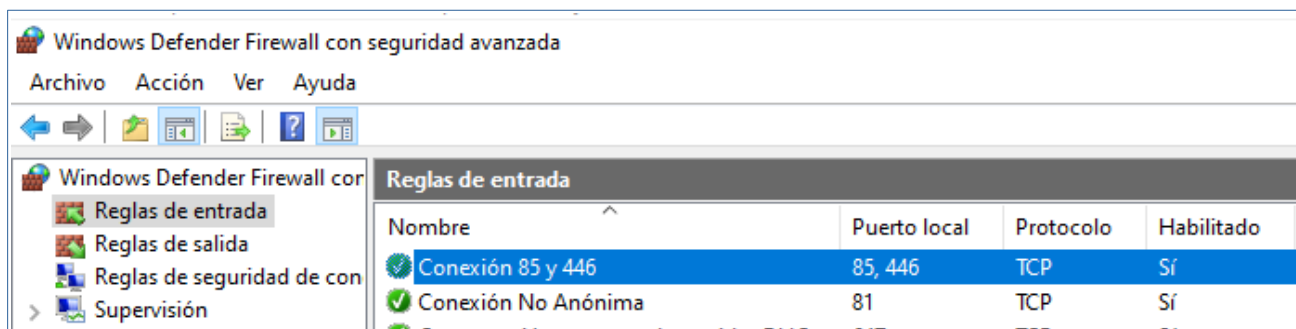
Usaremos el enlace en ella para acceder a la página de error.



## 2. Windows Server

### 2.1 Apertura de puertos

Al igual que hicimos con Ubuntu Server vamos a abrir 2 puertos más de escucha, 85 y 446, y esto lo haremos creando una nueva regla en el panel de seguridad avanzada de Windows Defender Firewall.



### 2.2 Configurar un nuevo sitio seguro

Para crear y configurar los sitios virtuales nos vamos al panel de Administración de Internet Information Services, y en el menú lateral izquierdo, le damos clic derecho a Sitios > Agregar sitio web. En este caso crearemos uno con la siguiente configuración, con el certificado autofirmado que habíamos creado anteriormente:

Agregar sitio web

Nombre del sitio: avanzado204 Grupo de aplicaciones: avanzado204 [Seleccionar...]

Directorio de contenido

Ruta de acceso física: C:\inetpub\empresa204\avanzado [...]

Autenticación de paso a través

[Conectar como...] [Probar configuración...]

Enlace

Tipo: https Dirección IP: Todas las no asignadas Puerto: 446

Nombre de host: web1.empresa204.local

☐ Requerir indicación del nombre de servidor

☐ Deshabilitar TLS 1.3 a través de TCP ☐ Deshabilitar QUIC

☐ Deshabilitar TLS heredada ☐ Deshabilitar HTTP/2

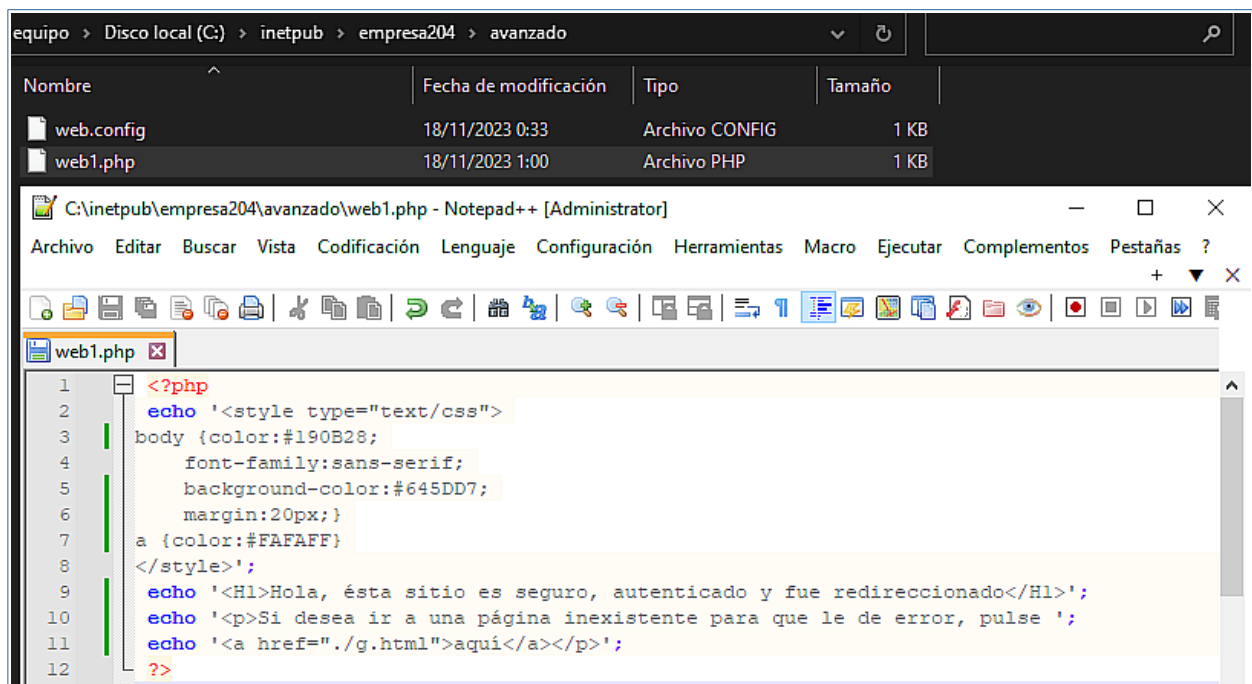
☐ Deshabilitar asociación de OCSP

Certificado SSL: cert\_seguro [Seleccionar...] [Ver...]

☒ Iniciar sitio web inmediatamente

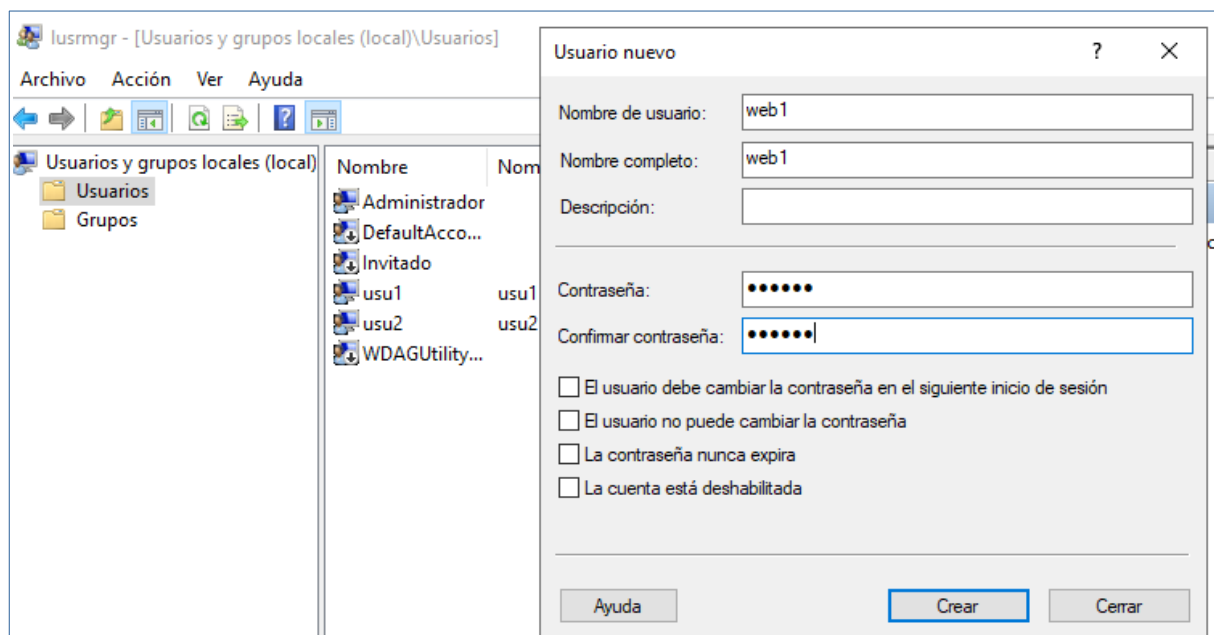
[Aceptar] [Cancelar]

En la carpeta de la ruta de acceso física creamos un documento llamado web1.php el cual tendría su contenido de la siguiente manera, con el documento escrito como se ve abajo.

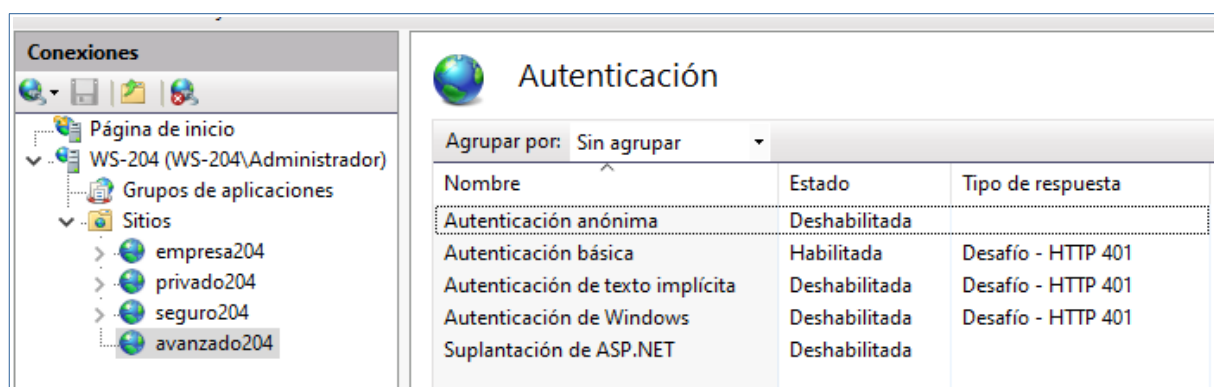


## 2.3 Configurar autenticación

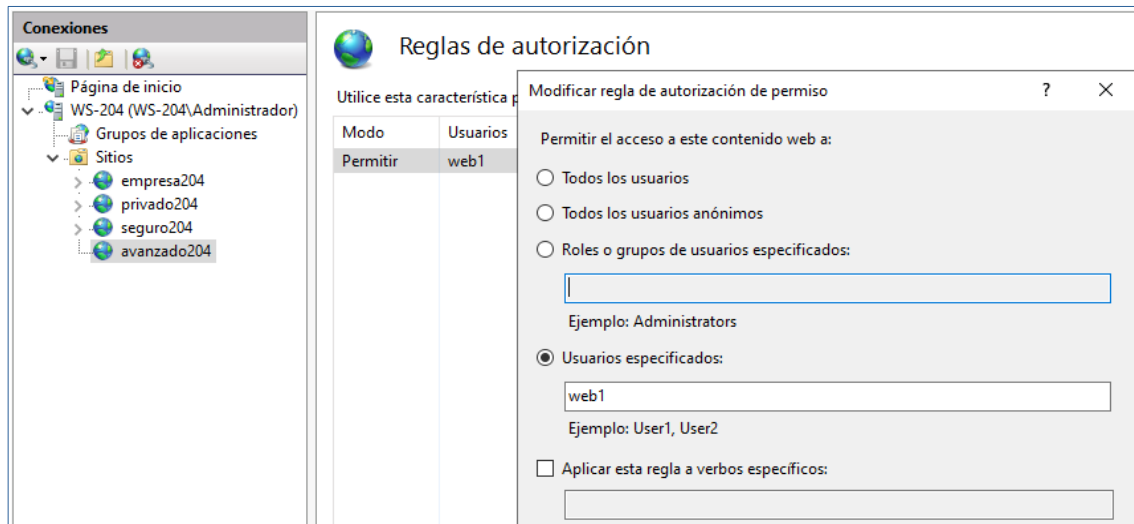
Primeramente creamos un nuevo usuario, desde el Administrador de Grupos y Usuarios, o desde el Panel de Control.



En la configuración del sitio, en el apartado de Autenticación lo configuramos como Básica y quitamos la Anónima.

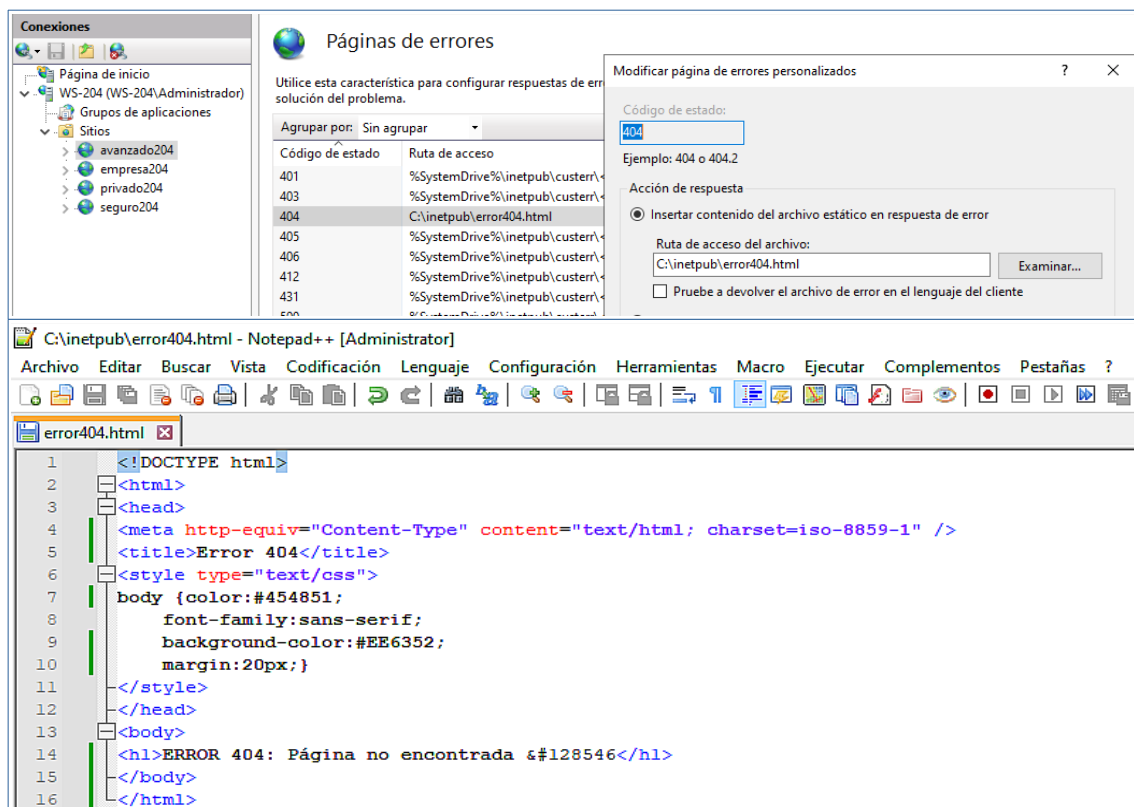


Y en el apartado de Reglas de Autorización configuramos nuestro usuario creado.

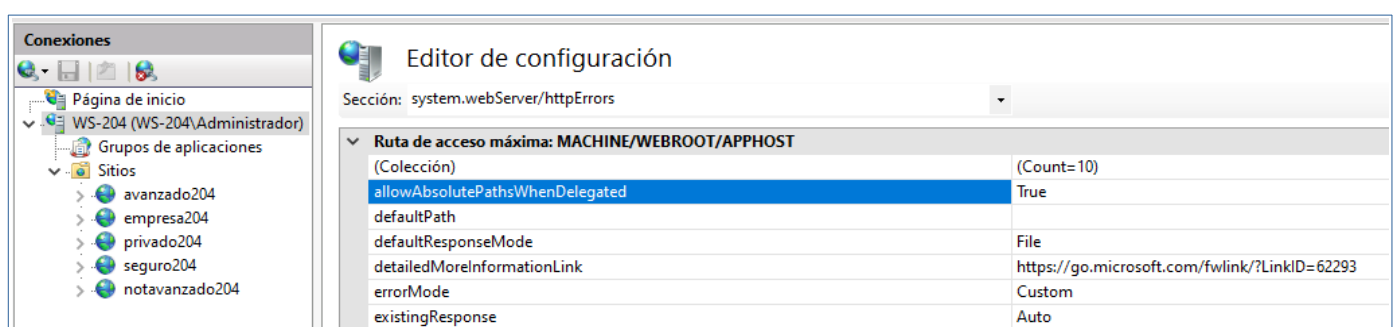


## 2.4 Configurar página de error personalizada

En las configuraciones del sitio nos dirigimos a Páginas de errores, y al del error 404 lo modificamos y establecemos una ruta con nuestra página personalizada.



En caso de que nos aparezca un error respecto a usar una ruta absoluta, lo habilitamos en el Editor de Configuración del servidor en el Administrador de IIS.



## 2.5 Configurar redirección

Queremos que un sitio fallido-inseguro redirija al nuestro correcto-seguro, para ello debemos crear entonces el sitio que redireccionará al ya creado. El cual lo crearemos con la siguiente configuración.

The 'Agregar sitio web' dialog box is shown with the following configuration:

- Nombre del sitio:** notavanzado204
- Grupo de aplicaciones:** notavanzado204
- Directorio de contenido:**
  - Ruta de acceso física:** C:\inetpub\empresa204\notavanzado
  - Autenticación de paso a través:** (empty)
- Enlace:**
  - Tipo:** http
  - Dirección IP:** Todas las no asignadas
  - Puerto:** 85
  - Nombre de host:** web1.empresa204.local

Ejemplo: www.contoso.com o marketing.contoso.com

Y configuramos el apartado de Redirección HTTP de este nuevo sitio.

The 'Redirección HTTP' configuration is shown with the following settings:

- Utilice esta característica para especificar reglas para redirigir solicitudes entrantes a otro archivo o dirección URL.**
- ☒ **Redirigir las solicitudes a este destino:**
  - Destino:** https://web1.empresa204.local:446
  - Ejemplo:** https://www.contoso.com/sales
- Comportamiento de redirección:**
  - ☐ **Redirigir todas las solicitudes al destino exacto (en lugar de al destino relativo)**

## 2.6 Configuración DNS

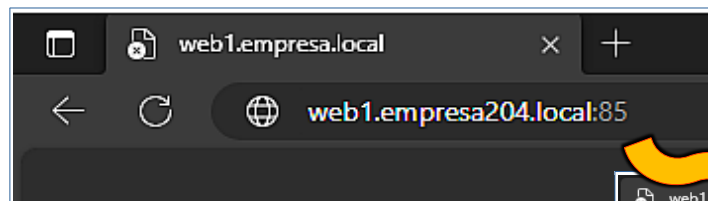
Por último recordemos que para que el cliente acceda a la web, el servidor debe resolver esa petición para que lo redirija a su misma IP dado que es él también el que sirve la página.

Administrador de DNS			
Archivo Acción Ver Ayuda			
DNS			
WS-204			
Zonas de búsqueda directa			
dominio204.local			
empresa204.local			
Zonas de búsqueda inversa			
16.172.in-addr.arpa			
Nombre	Tipo	Datos	
www	Host (A)	172.16.204.201	
WS-204	Host (A)	172.16.204.201	
web1	Host (A)	172.16.204.201	
mail	Host (A)	172.16.204.201	
ftp	Alias (CNAME)	www.empresa204.local.	



## 2.7 Comprobación en el cliente

Procederemos entonces ahora a comprobar esta configuración desde el cliente. Dado que la redirección es instantánea no hay una manera efectiva de capturar su correcto funcionamiento para éste informe, igualmente la dirección introducida es la de la izquierda y nos carga la imagen de la derecha.



Una vez nos carga el sitio correcto reenviado procedemos a introducir las credenciales requeridas y nos cargará una página que lee correctamente que posee un certificado más no se considera seguro por no ser válido.

Usaremos el enlace en ella para acceder a la página de error.

