REE. Plan de seguridad. Acciones a Implementar

Listado de acciones a implementar para el plan:

3. CERTIFICADO

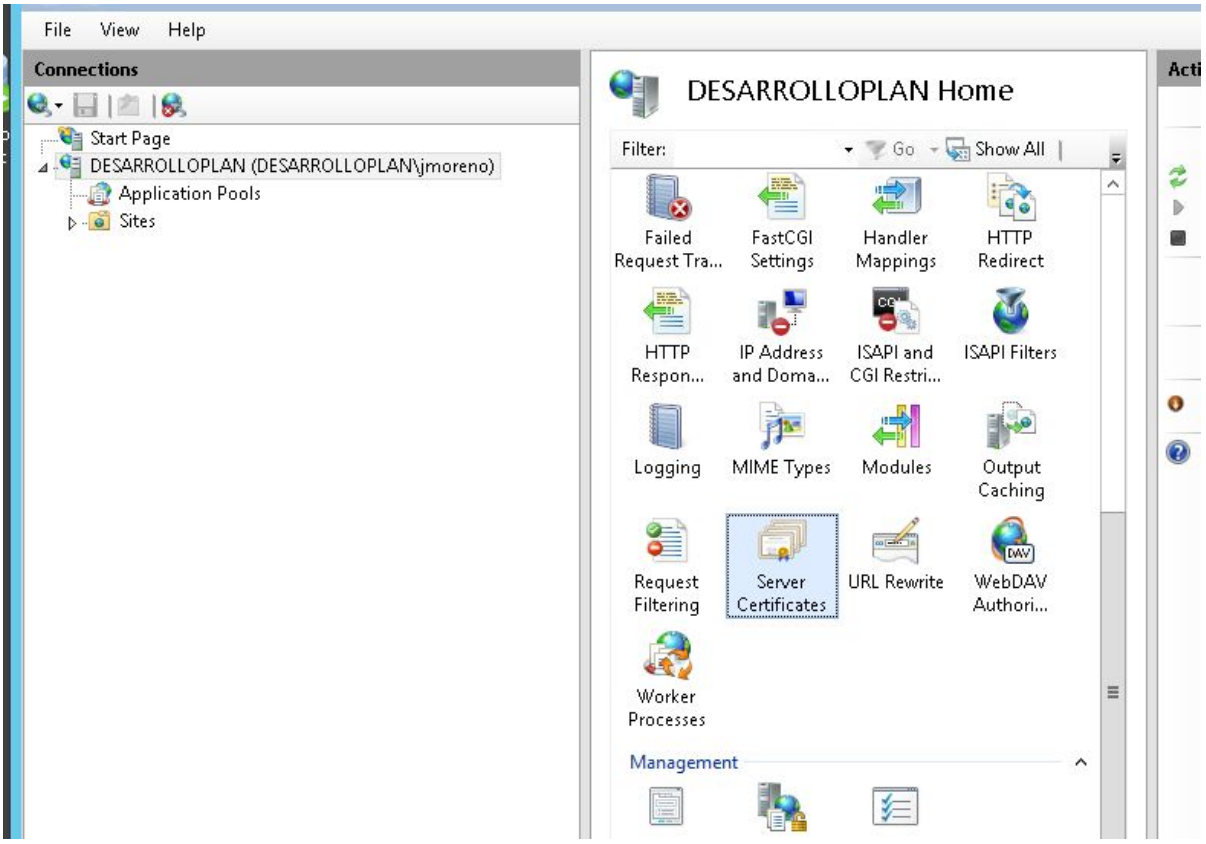
Al ser una aplicación interna de REE y que se ejecuta en sus servidores. Entendemos que tendríamos que usar un certificado propiedad del cliente.

Por lo tanto en este apartado no vamos a entrar en las características del certificado y vamos a centrarnos en los cambios que afecta el servidor de Plan

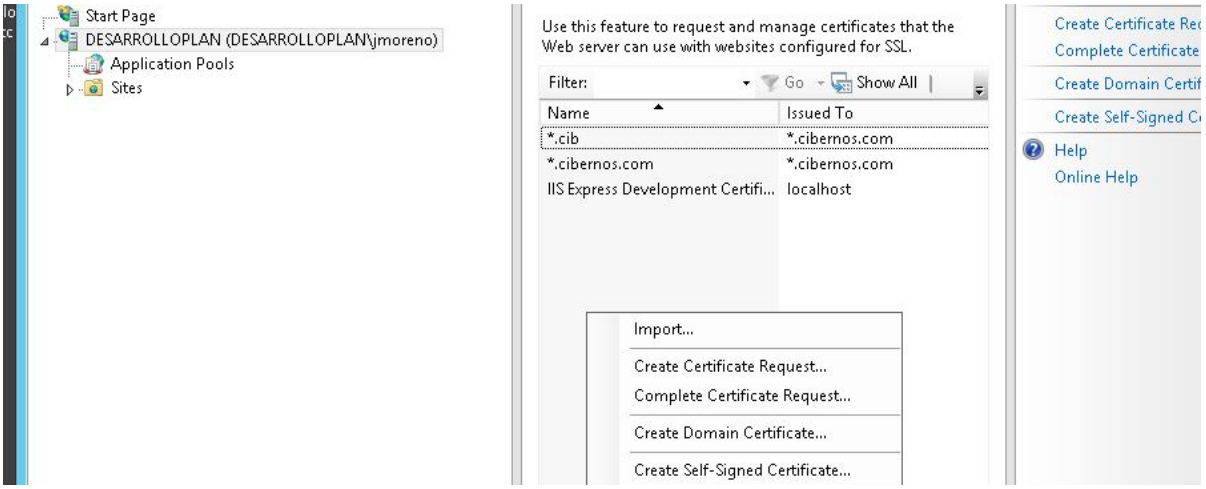
Importar el certificado a IIS

Si hay que cambiar la aplicación para que use SSL. necesitamos que se importe el certificado al servidor donde se ejecuta la aplicación:

Para ello desde el IIS del servidor: Abrir el apartado de certificados de servidor.

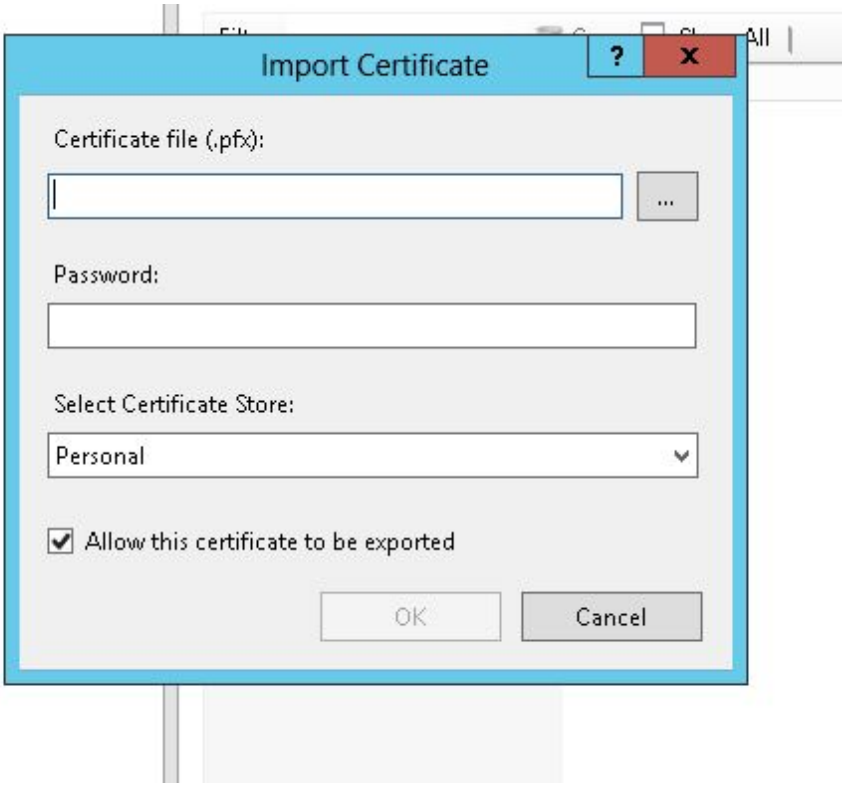


Desde aquí damos a importar certificado:



Se indica la ruta del certificado para importarlo.

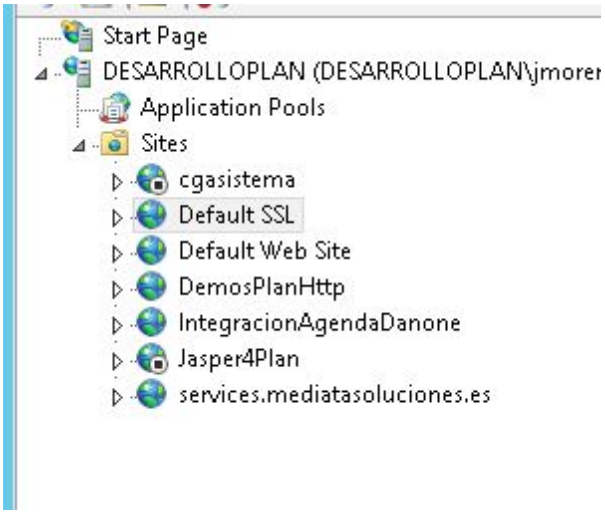
- El certificado tiene que esta en formato .pfx
- La clave para Importarlo



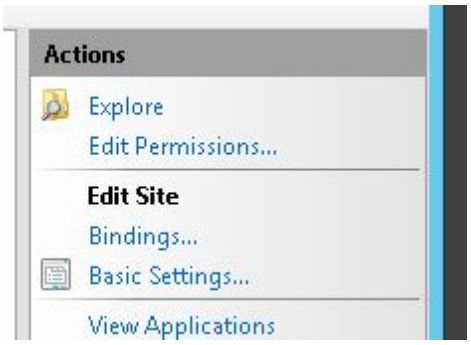
Si el formulario se importa correctamente ya podemos usarlo para publicar cualquier sitio web con SSL

Modificar el sitio web para que use SSL

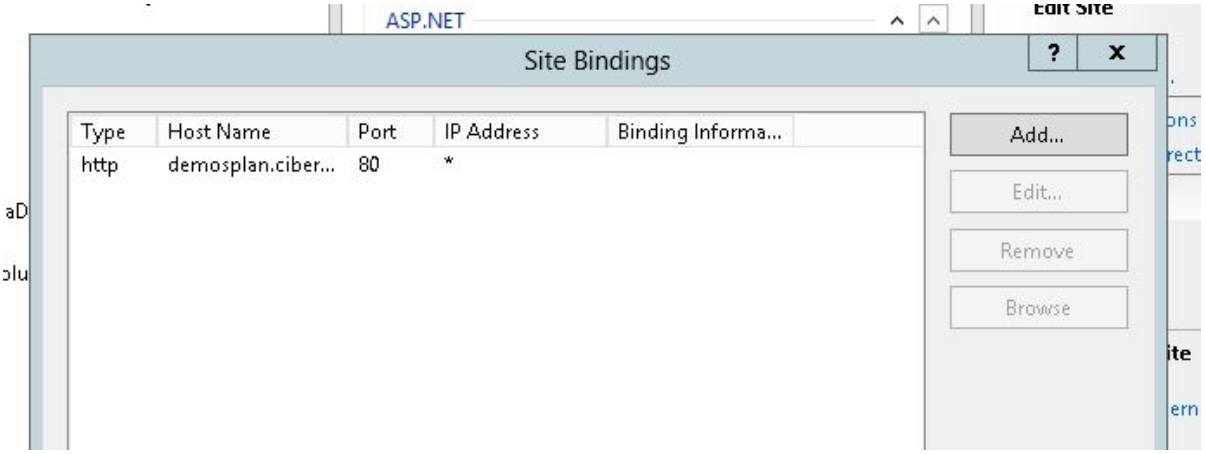
A continuación vamos a las propiedades del sitio web que queremos cambiar a SSL



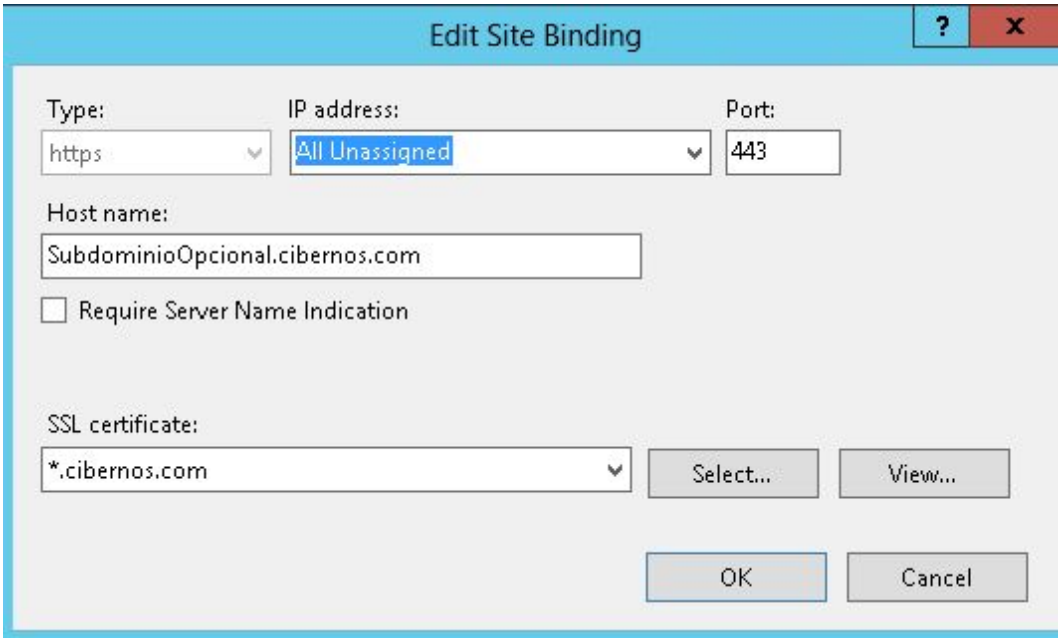
En el menú de la derecha seleccionamos “bindings”



El sitio web con http tendrá este aspecto.
Aquí podemos añadir un nuevo enlace manteniendo el acceso con Http pero lo correcto seria quitar el acceso con http y añadir uno nuevo con https:



Se indica:
El protocolo Https:
El nombre del Host: Si el certificado permite subdominio indicaremos un nombre para el subdominio (por ejemplo prer). si no habrá que usar el nombre del dominio que corresponde al certificado
En el combo de SSL certificate aparecerán todos los certificados que hemos importado a este servidor. se selecciona el certificado que corresponde.

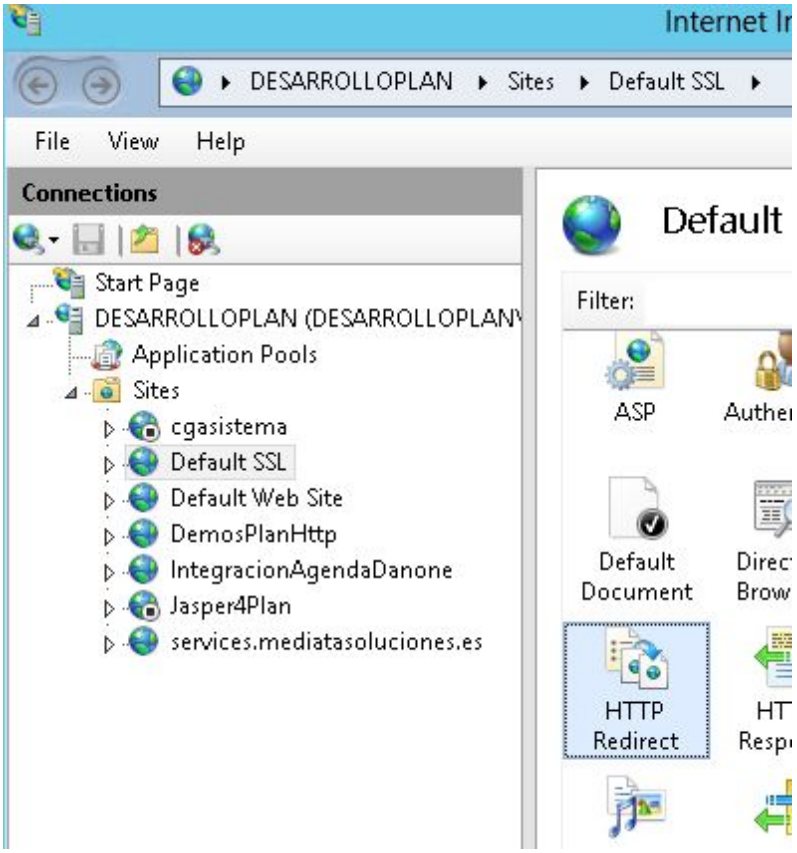


Con esto ya estaría configurado el acceso por https.

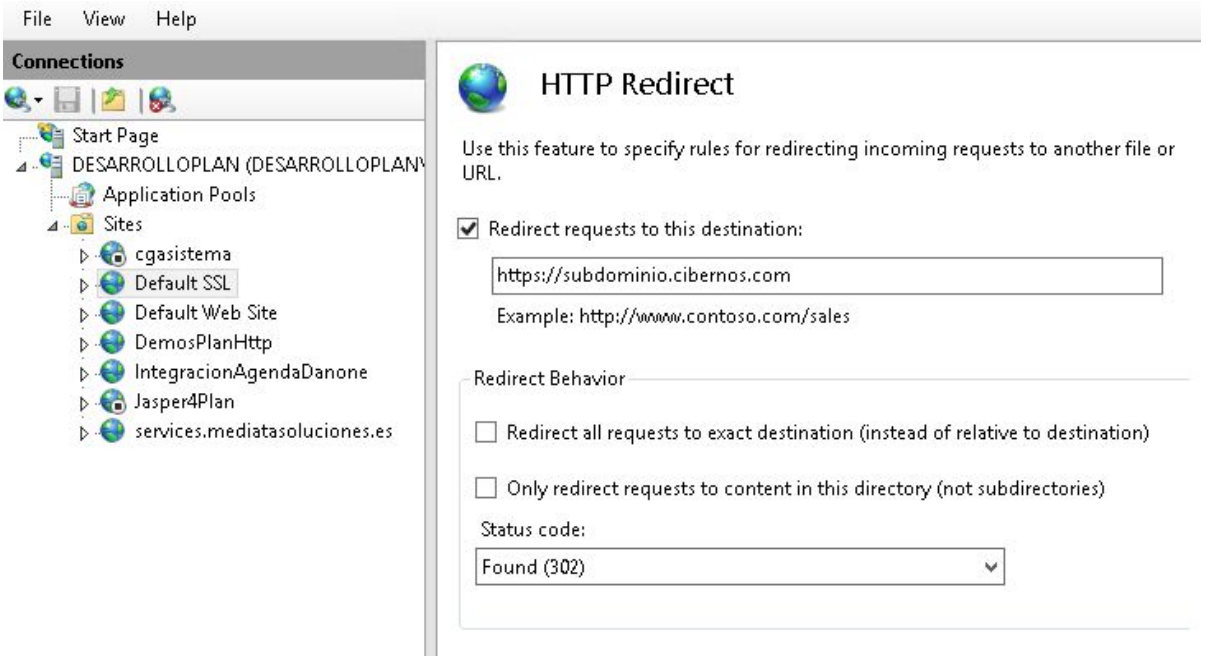
Hacer que las peticiones por http redireccionen al sitio con https:

Para que los usuarios que ya tengan en sus favoritos la URL sin https se requiere que IIS tenga instalada la función de redirección.

En este caso en el sitio web aparecerá la opción de HTTP Redirect.



- Se creará un sitio http vacío con http y las opciones por defecto.
- Sobre en el sitio vacío. abriremos HTTP REdirect e indicaremos la nueva url con https a la que se deben redireccionar las solicitudes a la URL antigua.
-



Habilitar “OCSP Stapling” para retornar el estado de revocación

Solo es posible si el servidor es windows server 2008 o una versión superior.
Las instrucciones en el siguiente enlace:

https://www.digicert.com/ssl-support/windows-enable-ocsp-stapling-on-server.htm

4. PROTOCOLOS

Deshabilitar TSL.1.0

Para deshabilitar TSL.1.0 hay que hacer algunos cambios en el registro del servidor.
Las instrucciones en el siguiente enlace:

https://support.microsoft.com/es-es/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat

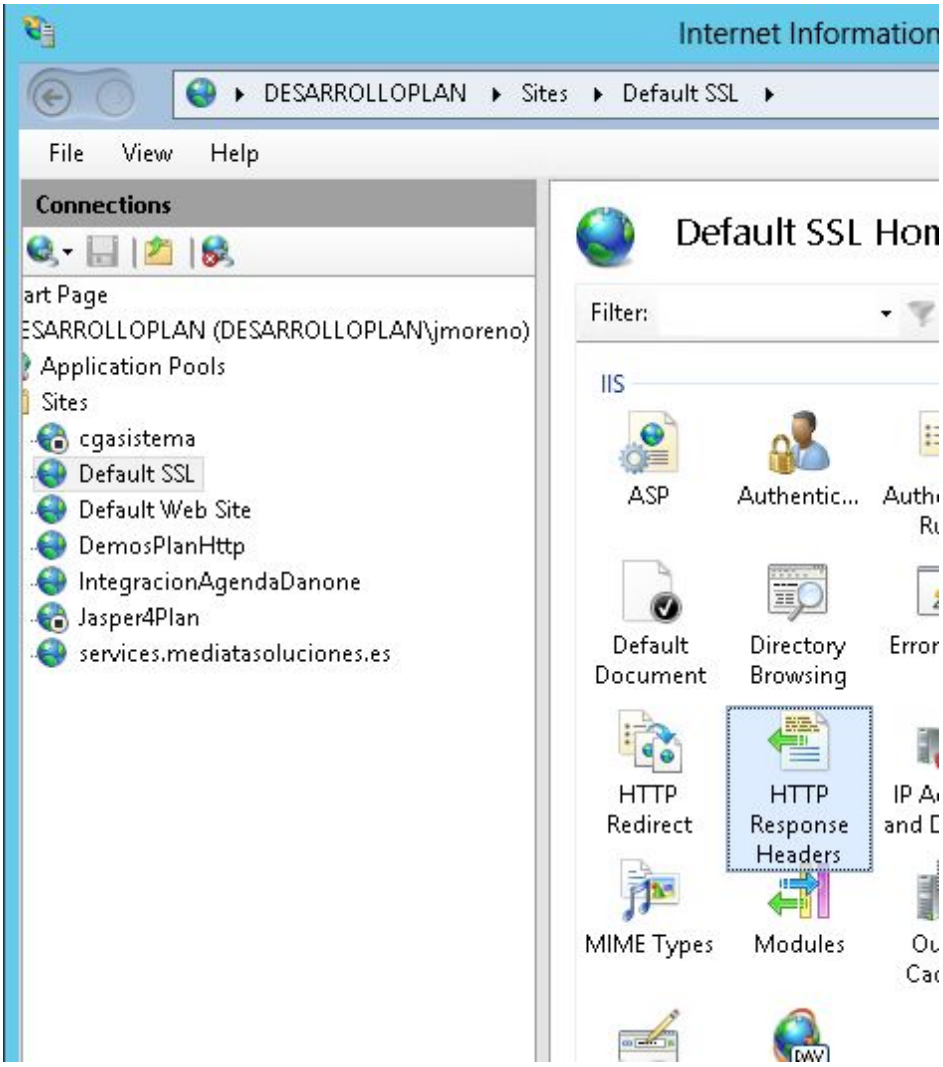
7. CABECERAS DE SEGURIDAD

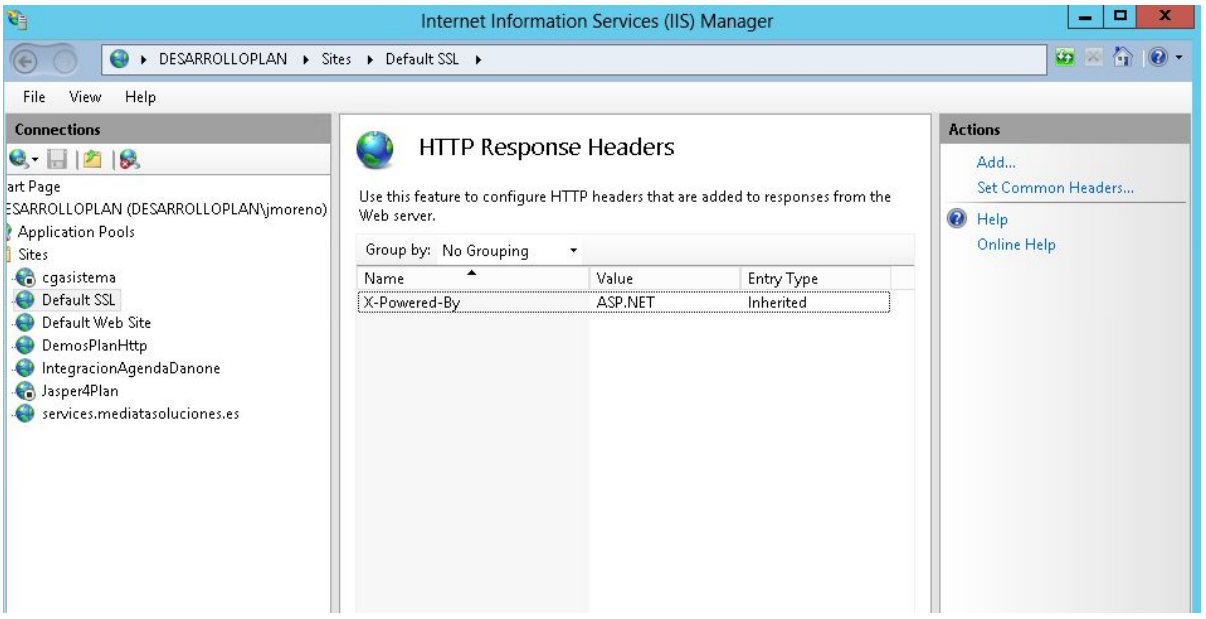
Revisamos las cabeceras de seguridad solicitadas.

Podemos entrar en IIS o alternativamente en el web.config de la aplicación
y añadir o quitar cabeceras

Si es por la consola de IIS nos posicionamos en el sitio web y buscamos HTTP Response Headers.

Desde aquí podemos añadir cabeceras que aplicarán a todas las solicitudes http de la aplicación


Internet Information
DESARROLLOPLAN ▸ Sites ▸ Default SSL ▸
File View Help
Connections
art Page
ESARROLLOPLAN (DESARROLLOPLAN\jmoreno)
Application Pools
Sites
cgasistema
Default SSL
Default Web Site
DemosPlanHttp
IntegracionAgendaDanone
Jasper4Plan
services.mediatasoluciones.es
Default SSL Hom
Filter:
IIS
ASP
Authentic...
Default Document
Directory Browsing
HTTP Redirect
HTTP Response Headers
MIME Types
Modules


Internet Information Services (IIS) Manager
DESARROLLOPLAN ▸ Sites ▸ Default SSL ▸
File View Help
Connections
art Page
ESARROLLOPLAN (DESARROLLOPLAN\jmoreno)
Application Pools
Sites
cgasistema
Default SSL
Default Web Site
DemosPlanHttp
IntegracionAgendaDanone
Jasper4Plan
services.mediatasoluciones.es
HTTP Response Headers
Use this feature to configure HTTP headers that are added to responses from the Web server.
Group by: No Grouping
Name
Value
Entry Type
X-Powered-By
ASP.NET
Inherited
Actions
Add...
Set Common Headers...
Help
Online Help

7.1. Server

Para que no se muestren las páginas de error por defecto
En el web.config de la aplicación comprobaremos que la sección de customErrors esté bien definida y no se encuentre comentada
:

```
<!--<customErrors mode="Off"/>-->
    <customErrors defaultRedirect="./WFinfo.aspx?exception=1" mode="On">
      <error statusCode="400" redirect="./HTMLErr400.htm"/>
      <error statusCode="401" redirect="./HTMLErr401.htm"/>
      <error statusCode="403" redirect="./HTMLErr403.htm"/>
      <error statusCode="404" redirect="./HTMLErr404.htm"/>
      <error statusCode="405" redirect="./HTMLErr405.htm"/>
      <error statusCode="406" redirect="./HTMLErr406.htm"/>
      <error statusCode="408" redirect="./HTMLErr408.htm"/>
      <error statusCode="412" redirect="./HTMLErr412.htm"/>
      <error statusCode="501" redirect="./HTMLErr501.htm"/>
      <error statusCode="502" redirect="./HTMLErr502.htm"/>
      <error statusCode="502" redirect="./HTMLErr502.htm"/>
    </customErrors>
```

7.2 HTTP STRICT TRANSPORT SECURITY (HSTS)

Esta cabecera debe añadirse si tenemos habilitada simultáneamente el acceso http y https en el mismo sitio web. si en el sitio web lo hemos configurado solo por https no aplica

7.3 X-FRAME-OPTIONS

Esta cabecera puede añadirse sin problemas.
Se recomienda usarla con el valor “SAMEORIGIN” ya que plan Si utiliza iframes de forma interna

<add name="X-Frame-Options" value="SAMEORIGIN"/>

7.4 X-XSS-PROTECTION

Esta cabecera puede añadirse sin problemas.

<add name="X-XSS-Protection" value="1; mode=block"/>

7.5 X-CONTENT-TYPE-OPTIONS

Esta cabecera si que puede dar problemas con la versión de Plan que es la que está instalada en Red Eléctrica. Si habilitamos esta cabecera las llamadas ajax dejan de funcionar . Las llamadas Ajax se hacen sin indicar un mime-type y el IIS las da por no válidas.

La solución pasa por cambiar las llamadas ajax que se hacen con el método antiguo y actualizarlas. esto conlleva obligatoriamente un cambio de versión del motor de Plan.

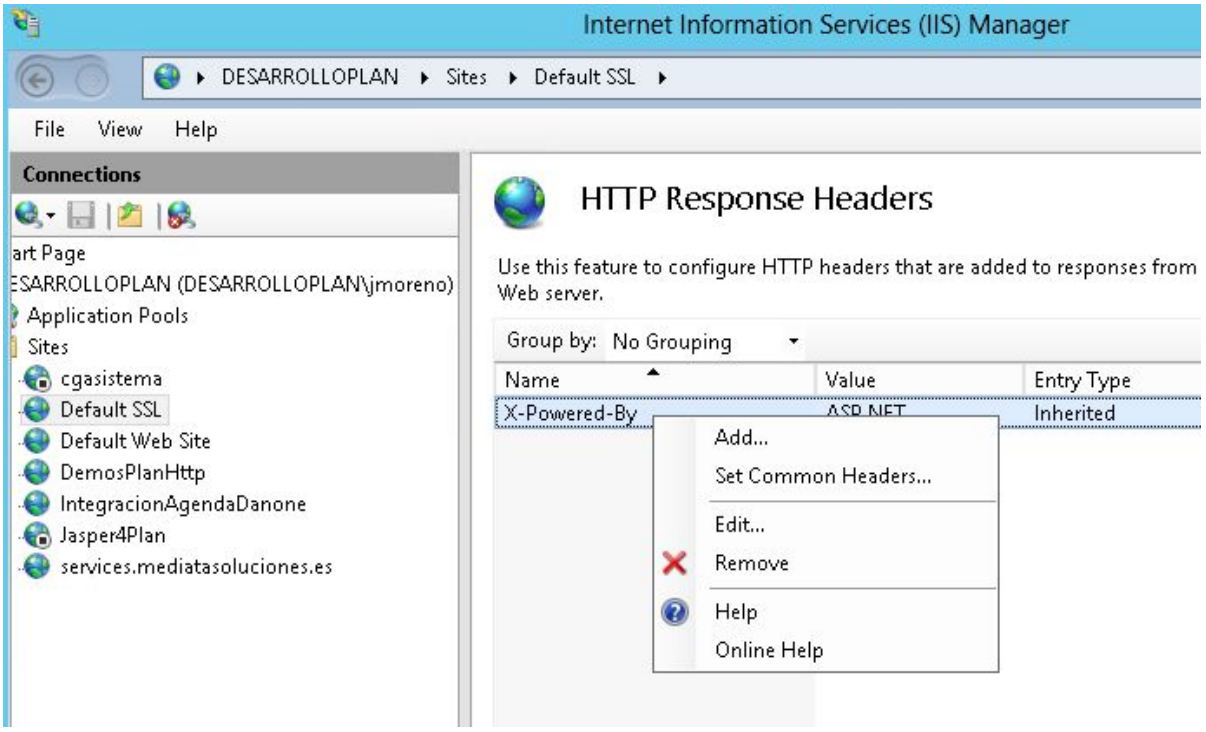
Aunque cambiemos el motor nos obliga a que las funcionalidades antiguas que mantenemos por compatibilidad con la versión 3. también tendríamos que actualizarlas.

7.6 COOKIES

Para añadir HttpOnly a las cookies requiere modificación de Plan. Requiere una modificación del programa.

7.7 X-POWERED-BY

Habría que quitar la cabecera que Windows mete por defecto a las aplicacion aspx.
X-Powered-By

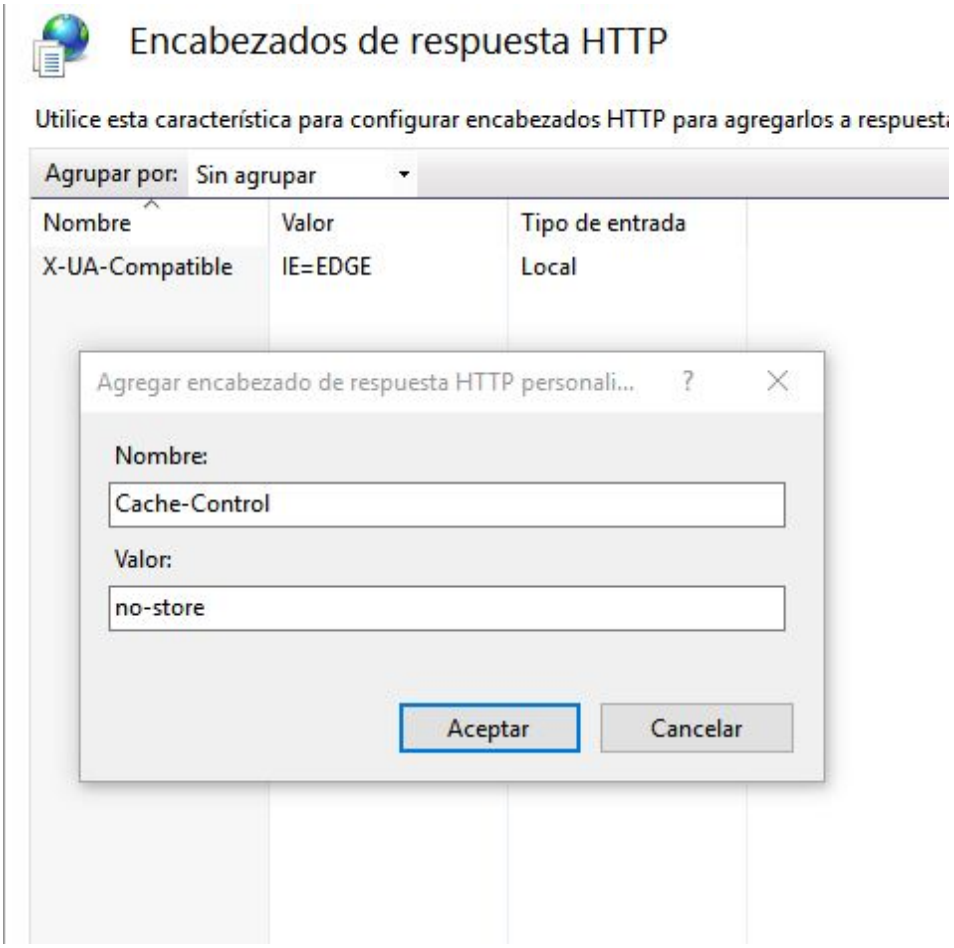


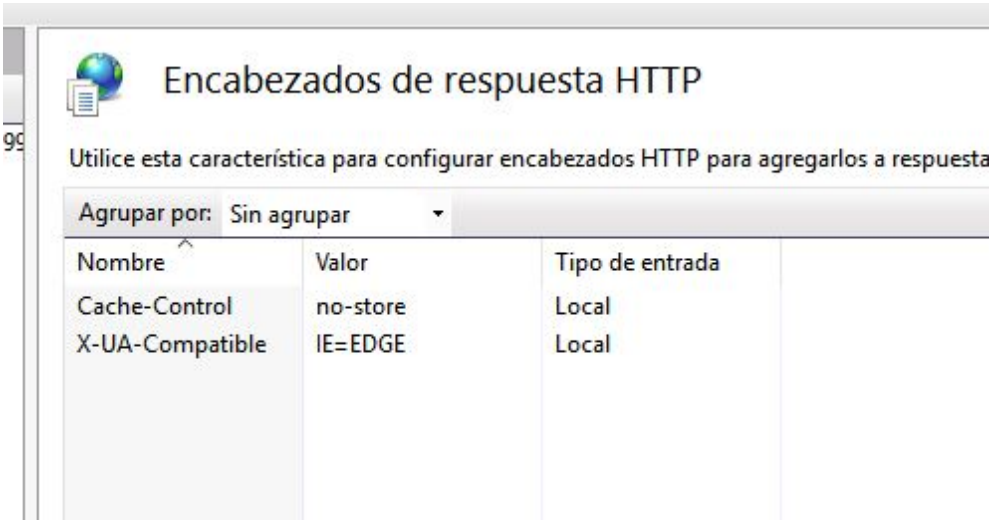
7.8 CACHE

Esta cabecera puede añadirse al IIS . Pero hay que tener en cuenta que conlleva que se ralentice significativamente la carga de la página.

Para hacerlo correctamente habría que añadir la cabecera por programa y requiere una nueva opción de configuración

Alternativamente se puede añadir en IIS las cabeceras. se puede añadir la directiva: Cache-Control: no-store Esto evita que se use la caché del navegador.



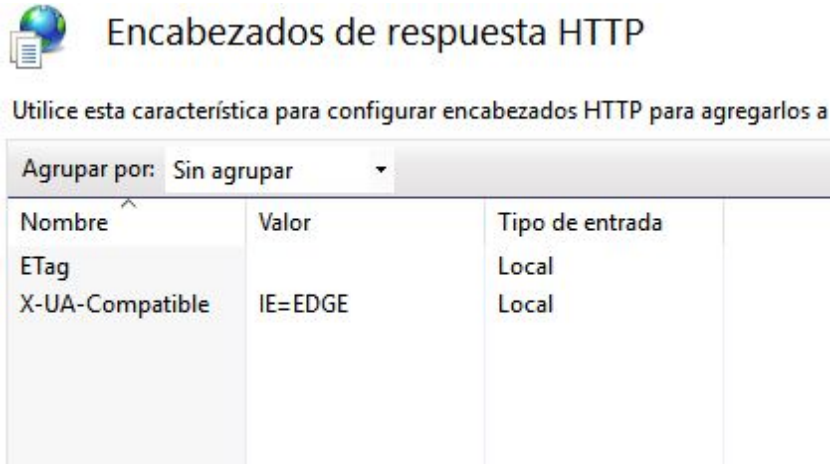


7.9 ETAG

Quitar esta cabera requiere investigación. hay que hacer modificaciones al servidor IIS para que sea efectiva. requiere incluir una regla en el servidor de aplicaciones para reescribir esta cabecera.

Alternativamente se pueden probar otras formas de hacerlo. eliminando directamente las cabeceras en todas las acciones de respuesta de la aplicació. Esto requeriría tocar el código de la aplicación en bastantes puntos.

Un modo más simple que se podría probar antes. es sobre-escribir esta cláusula. no la eliminamos pero podemos poner un valor que no aporte ninguna información real:
En los encabezados de respuesta Http añadir una cláusula Etag con un espacio en blanco.



7.10 HTTP PUBLIC KEY PINNING (HPKP)(Desestimado de momento)

Requiere investigación. es un punto bastante complejo.

7.12 REFERRER-POLICY

Para esta cabecera plan requiere la configuración
Referrer-Policy: same-origin

Si el servidor se configura tal y como indica el documento como
Referrer-Policy: no-referrer. Hay que modificar esta cabecera en Plan con el valor same-origin

8. MÉTODOS Y PROTOCOLOS HTTP

Plan solo utiliza los métodos POST y GET. Se podrían deshabilitar en IIS el uso de otros métodos. Esta es la configuración por defecto de IIS. Tendríamos que verificar que de hecho se encuentre así configurado.

Respecto a deshabilitar páginas HTTP 1.0. Al Ser una versión antigua del motor de Plan. tendríamos que ver si es posible y no da problemas.
Es algo que puede hacerse modificando el web.config o en el IIS de ld servidor.

9. ANEXO: CONFIGURACIÓN DE SERVIDOR APACHE (No aplica)

No Aplica.