Eliminando el blindaje de seguridad de .NET Framework ante aplicaciones rebeldes

Luis Miguel Blanco Ancos

La plataforma .NET Framework proporciona un contexto de seguridad basado en el código a ejecutar de las aplicaciones denominado CAS (Code Access Security), que permite limitar el que un programa sin permisos pueda acceder a recursos sensibles del sistema.

En condiciones normales, cuando desarrollamos una aplicación no nos percatamos de esta capa de seguridad hasta que la ejecutamos en una máquina con un entorno de ejecución de características “particulares”.

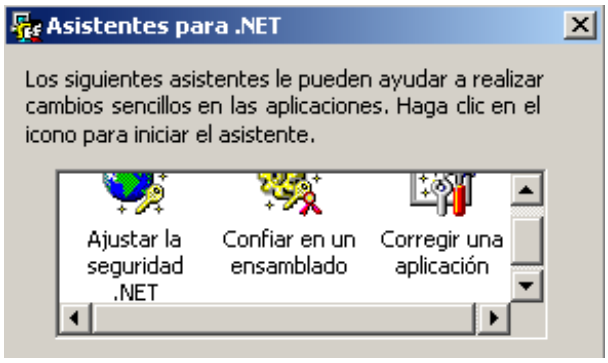
Al hablar de ejecución en una máquina con características especiales nos referimos a servidores que proporcionan acceso a las aplicaciones que hospedan a través de un entorno cliente basado en un terminal virtual, al cual nos conectamos mediante una aplicación cliente que se ejecuta mediante un interfaz Windows o Web.

A efectos del sistema de seguridad de código de la plataforma .NET, la ejecución de la aplicación se realizaría en un contexto similar al de una intranet local o Internet. ¿Qué tiene de particular esta situación?, pues que la configuración por defecto de seguridad del código en .NET, con toda probabilidad, nos impedirá ejecutar el programa si vamos a acceder a recursos tales como el sistema de archivos, devolviéndonos una hilera de errores como la que se muestra a continuación:

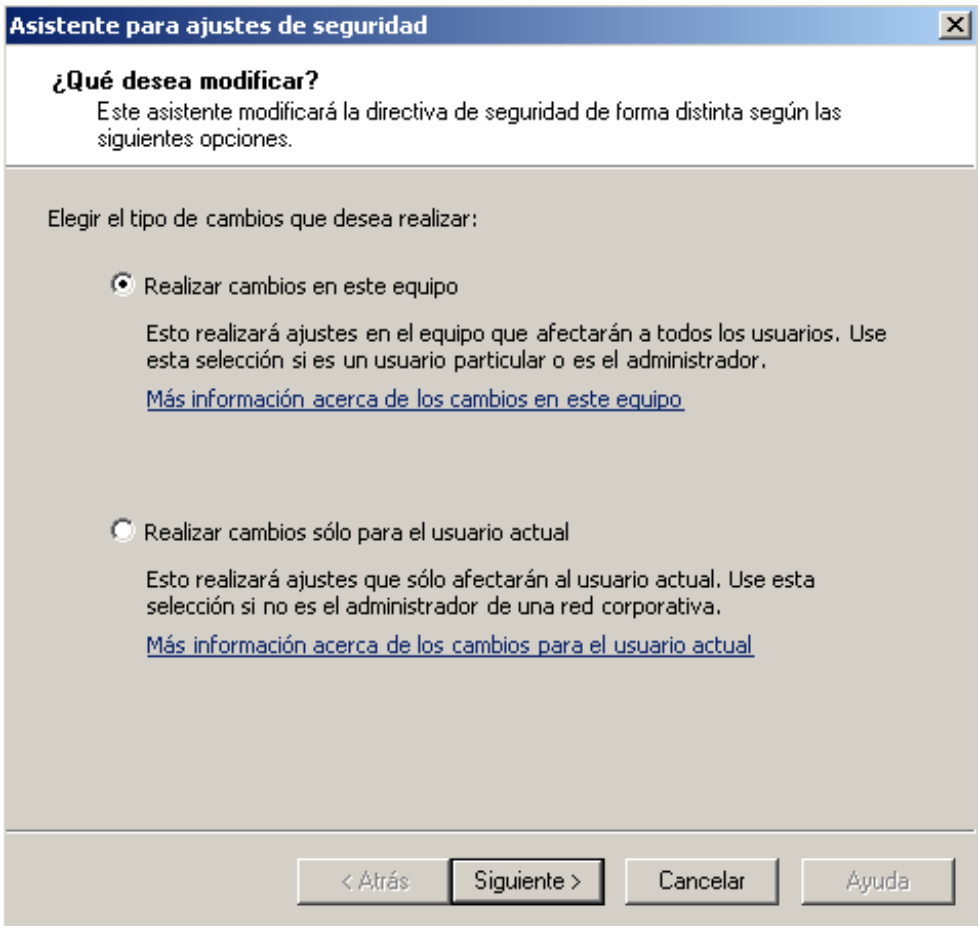
```
Unhandled Exception: System.Security.SecurityException: Request failed.
   at ObtencionDatosBD.Module1.Main()

The granted set of the failing assembly was:
<PermissionSet class="System.Security.PermissionSet"
               version="1">
   <IPermission class="System.Security.Permissions.EnvironmentPermission, mscorl
ib, Version=1.0.5000.0, Culture=neutral, PublicKeyToken=xr7atr56ngf34e089"
                version="1"
                Read="USERNAME"/>
   <IPermission class="System.Security.Permissions.FileDialogPermission, mscorli
b, Version=1.0.5000.0, Culture=neutral, PublicKeyToken=de7w5cxx1965enb9"
                version="1"
                Unrestricted="true"/>
   <IPermission class="System.Security.Permissions.FileIOPermission, mscorlib, V
ersion=1.0.5000.0, Culture=neutral, PublicKeyToken=kj7a876619fd3067"
                version="1"
                Read="C:\GEST\ObtenerDatos\"
                PathDiscovery="C:\GEST\ObtenerDatos\"/>
```

Este error, del cual reproducimos un fragmento, se ha obtenido al ejecutar una aplicación en modo consola que intenta escribir un archivo en un directorio del servidor.

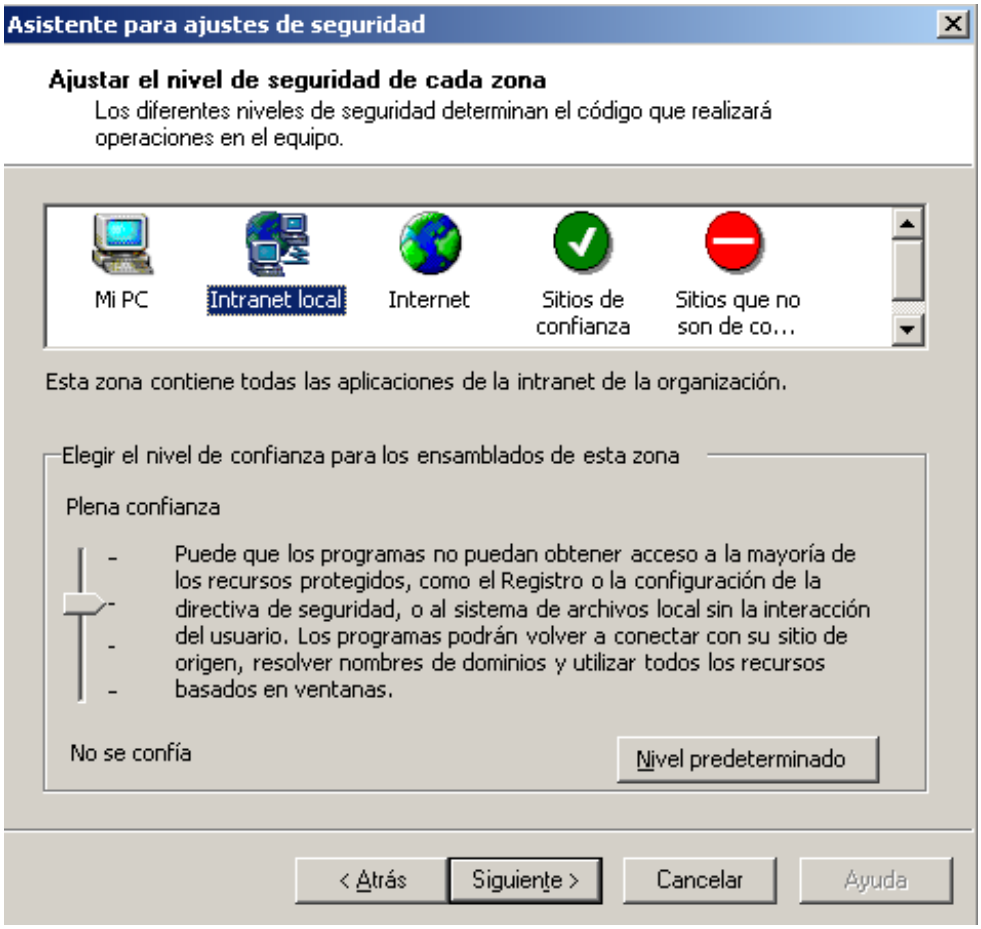
Si nos encontramos en pleno proceso de pruebas de la aplicación en desarrollo, podemos pasar temporalmente por alto este sistema de seguridad de un modo sencillo, ejecutando la herramienta “Asistentes de .NET Framework 1.1”, que vemos en la siguiente figura, y que se encuentra entre las herramientas administrativas de Windows.



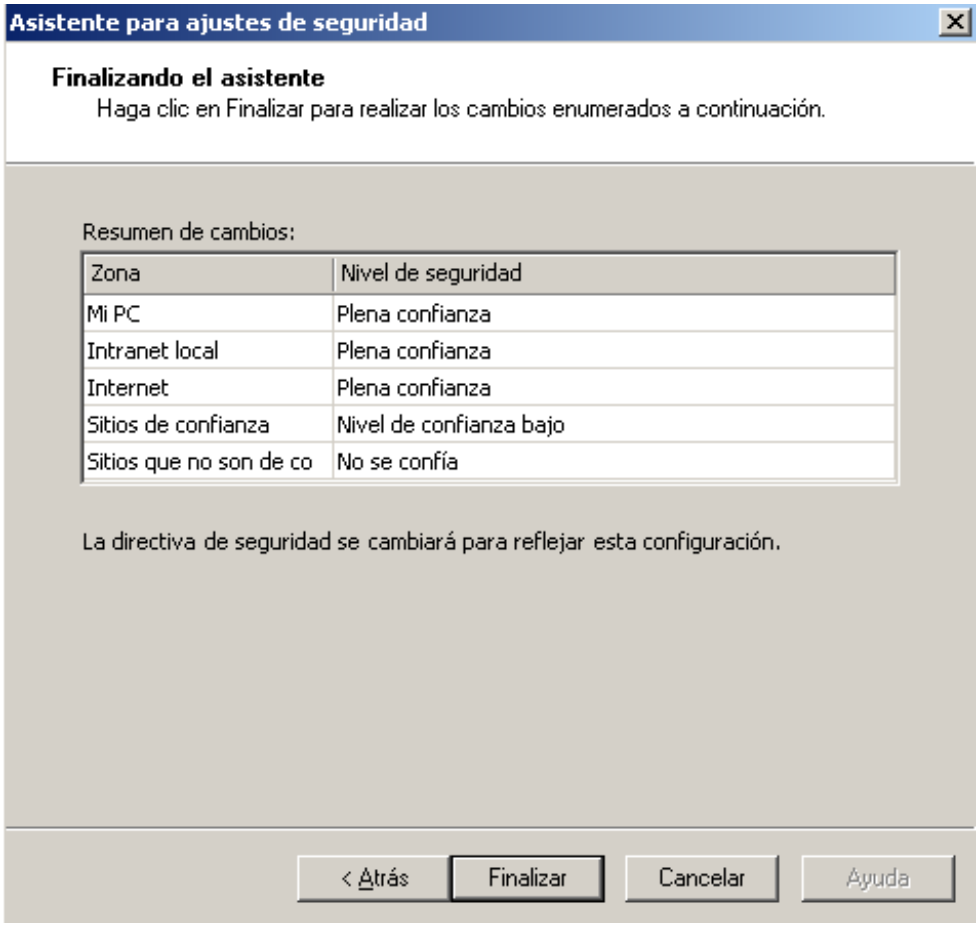
A continuación haremos clic en el elemento “Ajustar la seguridad .NET”, que ejecutará un asistente que nos permitirá variar la configuración de seguridad de .NET.



Pulsando Siguiente podemos observar que para cada zona de ejecución de código es posible establecer unos niveles de seguridad. La zona que corresponde al equipo local ya tiene establecido un nivel de plena confianza, pero como no estamos ejecutando en este contexto, sino como hemos dicho en un entorno similar al de una intranet o Internet, y estos tienen establecidos niveles de confianza media o baja, aumentamos el indicador de estas zonas a plena confianza.



Al llegar al último paso del asistente se mostrará la configuración que hemos establecido, donde pulsaremos Finalizar para grabar los cambios.



Finalmente debemos volver a ejecutar la aplicación problemática, y con toda probabilidad, el error que nos aparecía ya no se producirá.

Como puede deducir el lector, esta configuración de seguridad tiene un alto riesgo ante código inseguro, por lo que sólo debe hacerse en muy determinadas condiciones, tales como fases de prueba de la aplicación, debiendo establecer un ajuste de seguridad adecuado al finalizar el desarrollo del programa.