www.infoPLC.net

BERRIKUNTZA TEKNOLOGIKOA
INNOVACIÓN EN LA TECNOLOGÍA

EUSKO JAURLARITZA GOBIERNO VASCO

Tknika

Actividad 10:

Configuración DCOM para Servidores y Clientes OPC.

1.- Listado de materiales:

- **2 PC´s con Tarjeta de red 3com o similar.**

- **1 PLC Omrom CJ1M – CPU11 – ETN**

Este autómata lleva integrada la tarjeta de comunicaciones ethernet que deberá estar previamente configurada. Sería posible utilizar un autómata de la misma serie añadiéndole una tarjeta de comunicaciones ethernet.
Si el PLC no dispone de tarjeta ethernet, puede realizarse una comunicación serie con el PC que hace de servidor y utilizar la tecnología DCOM para acceder a los datos desde el equipo cliente. Incluirá fuente de alimentación y unidades de entrada y salida.

- **Software Microsoft Windows XP**

- **Software Visual Basic v:6.0 o superior de Microsoft o Microsoft Office Excel.**

- **Software CX-Server OPC y KepServer de KepWare.**

- **Software CX-Programmer ver 5.0 o superior.**

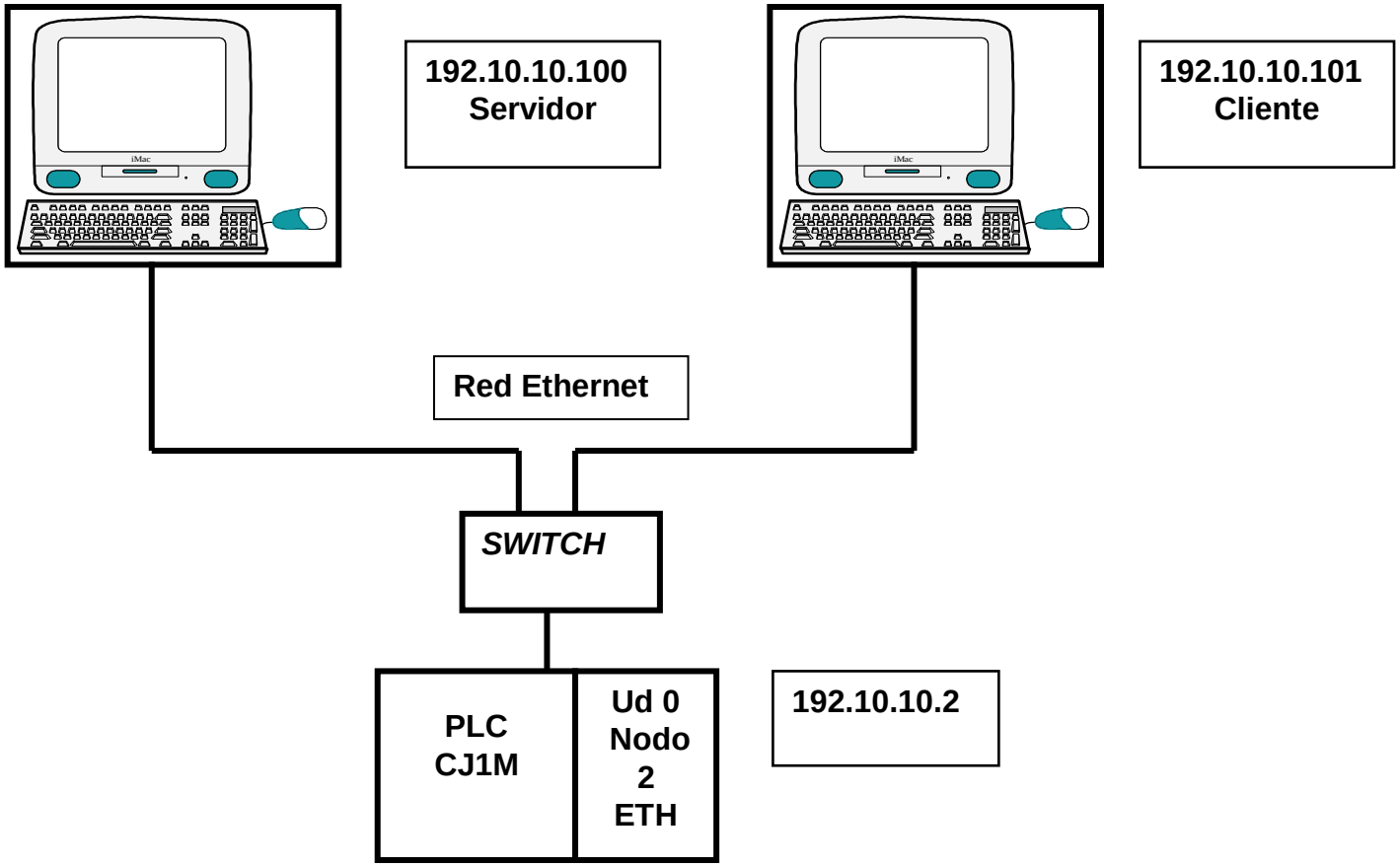
- **1 Switch para conexión Ethernet y 3cables con conector RJ45**

2.- Objetivos de la actividad.

Intercambiar datos entre Visual Basic (o Excel) instalado en un PC cliente y el PLC CJ1M utilizando un servidor de datos OPC instalado en otro PC.

- **Configurar DCOM en un PC que actúa como cliente.**
- **Configurar DCOM en un PC que actúa como servidor.**

Esquema del equipo



Introducción a DCOM.

► **COM es una tecnología desarrollada por Microsoft para favorecer la integración de diferentes componentes dentro de una plataforma Windows. Una variación de esta tecnología es DCOM que, basado en la tecnología COM, proporciona la integración de los componentes, aún estando éstos en distintos ordenadores.**

► **De esta forma, a través de DCOM es posible establecer la comunicación con una aplicación SCADA o VB remota.**

► **En la actividad se muestra la configuración necesaria para establecer una comunicación entre dos nodos, cliente y servidor que se ejecutan en el sistema operativo Microsoft Windows XP.**

► **En la actividad 6 (OPC. Conceptos.) se encuentra más información. Ver anexos al final de esta actividad y de la actividad 6.**

Configuración de los equipos en una red con workgroup o trabajo en grupo.

Configuración DCOM en el equipo servidor para trabajo en grupo.

- **Tendremos que realizar las siguientes operaciones:**
  - **Desactivar el cortafuegos de Windows**
  - **Configurar COM distribuido (DCOM) y Seguridad COM**
  - **Configurar la ejecución DCOM para las aplicaciones usadas**
  - **Reiniciar el equipo**

Servidor: Desactivar el cortafuegos (Firewall) de windows.

► **Es necesario desactivar el cortafuegos y configurar otros antivirus que puedan restringir el intercambio de datos entre servidor y cliente.**

Se accede a través de *Panel de control* → *Firewall de Windows* → "desactivar"

Servidor: Configurar COM distribuído (DCOM).

► **La configuración en este equipo es sencilla. Tenemos que habilitar DCOM (COM Distribuido) en el PC cliente. De esta forma tendrá los permisos para intercambiar objetos con otros equipos de la red.**

► **Para ello tenemos que seleccionar la Configuración del Administrador de Componentes de Windows.**

► **El acceso al menú de esta configuración puede hacerse de dos formas:**

a.- **Desde *Inicio → Panel de control → Herramientas administrativas → Servicios de componentes***

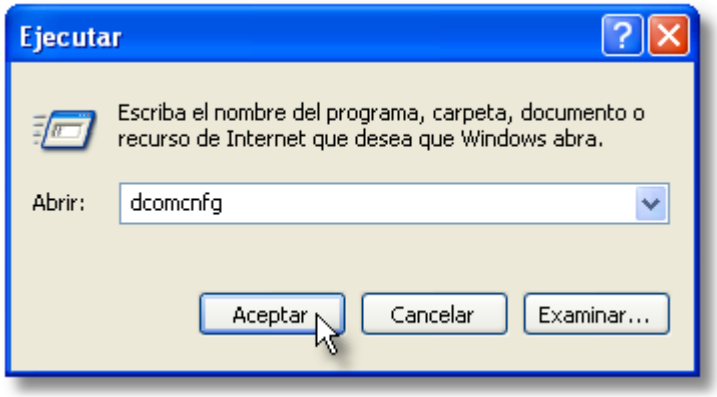
b.- **O bien, ejecutando dcomcnfg (es más rápido)**

Servidor: Configurar COM distribuído (DCOM).

1 Vemos esta segunda opción accediendo al menú de configuración desde Inicio:

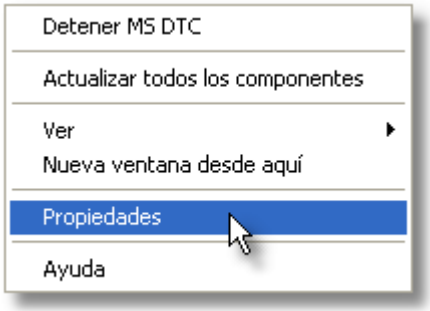
2 Ejecutar:

3 Escribiremos “dcomcnfg”:



Servidor: Configurar COM distribuído (DCOM).

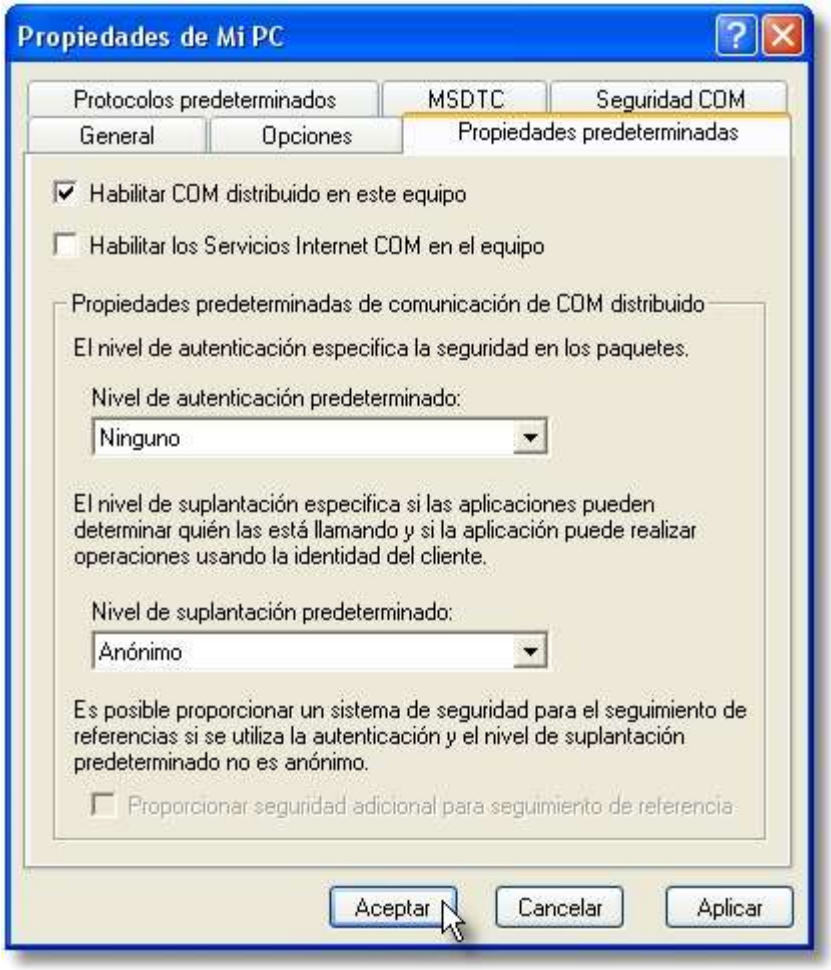
4 Y desde el Administrador de Servicios de Componentes, seleccionaremos *Servicios de Componentes* → *Equipos* → *Mi PC* → pulsar el botón derecho del ratón para seleccionar *propiedades*:



Servidor: Configurar Seguridad COM.

5 En la pestaña *Propiedades Predeterminadas*, validaremos la opción "Habilitar COM distribuido en este equipo" y en los niveles de autenticación y suplantación escogeremos "Ninguno" y "Anonimo".

El nivel de seguridad es nulo y sólo se debe realizar esta operación si trabajamos en una LAN en la que confiemos en los usuarios.



Servidor: Configurar Seguridad COM.

► **En la misma ventana de Propiedades de Mi PC escogemos la opción *Seguridad COM* y añadiremos en *Editar límites* y en *Editar valores predeterminados* tanto de los *Permisos de acceso* como de los *Permisos de inicio y activación* a los usuarios:**

ANONYMOUS LOGON
INTERACTIVE

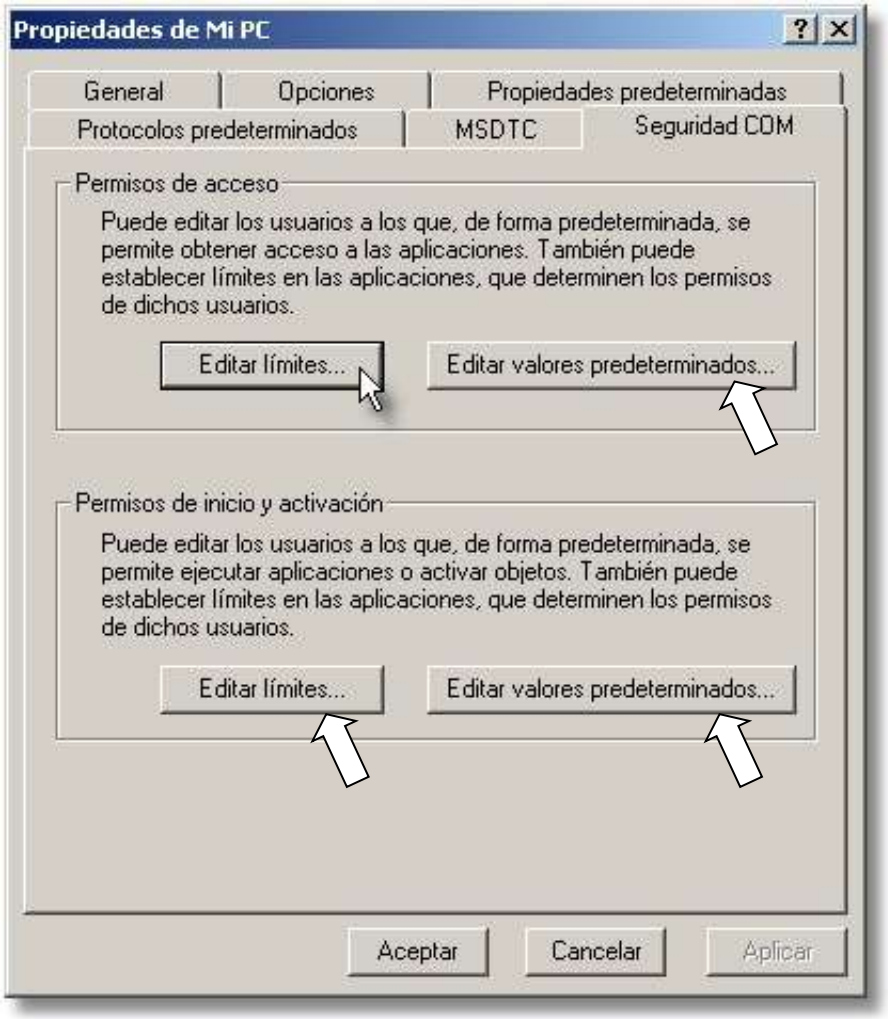
► **Podría ser necesario añadir también a los usuarios *Network y Todos.***

► **Los permisos de *acceso, inicio y activación* serán tanto de *acceso local* como *remoto*.**

► **Con esta operación se permite a cualquier usuario de la red la posibilidad de acceder a las aplicaciones que más adelante configuraremos.**

► **En las siguientes imágenes sólo se indica la forma de añadir a los usuarios en los límites de los permisos de acceso. Esta operación hay que realizarla en el resto de los casos.**

Servidor: Configurar Seguridad COM.

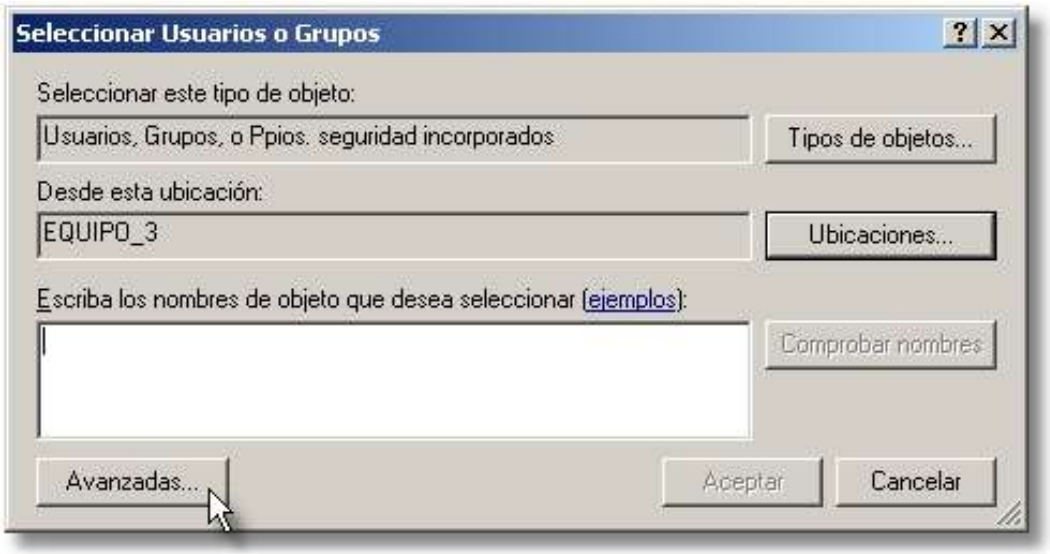


Servidor: Configurar Seguridad COM.

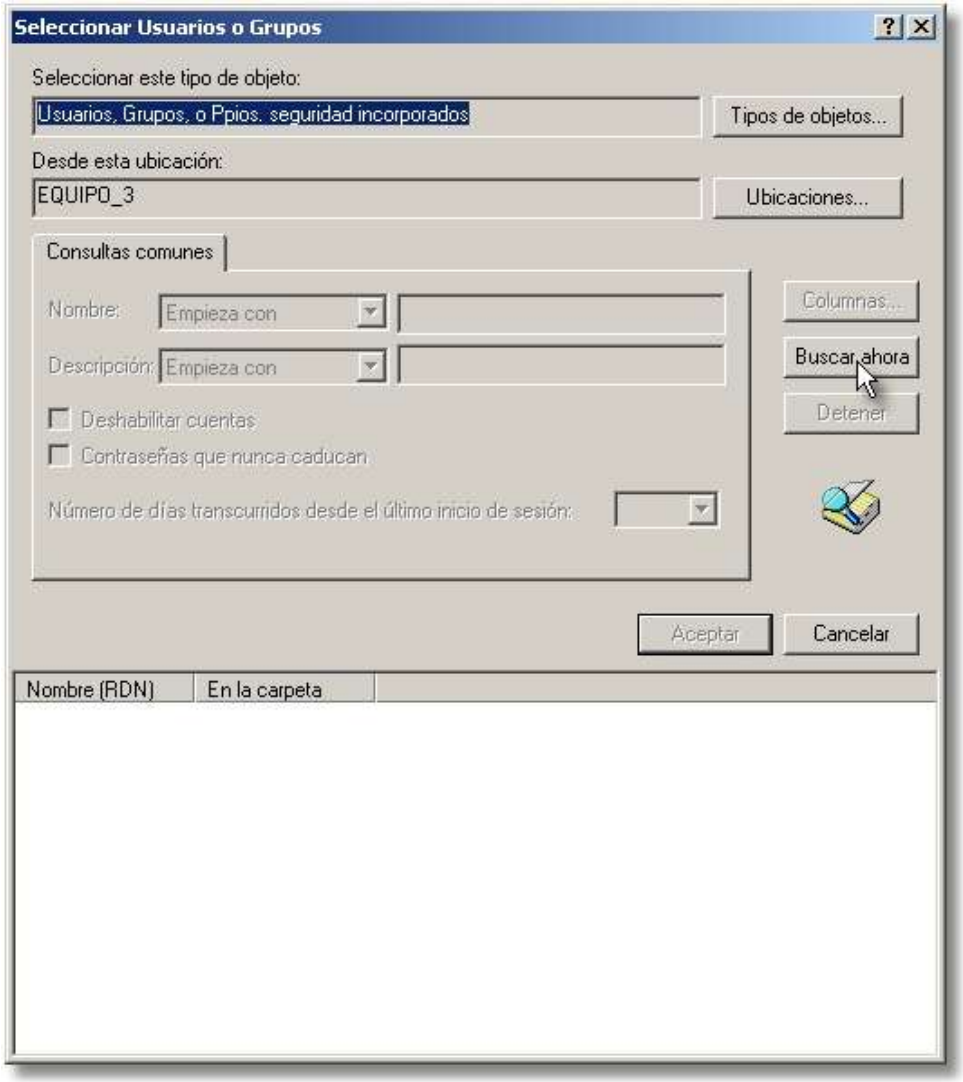
- **Para añadir a los usuarios indicados, se pincha sobre el botón *agregar***

Servidor: Configurar Seguridad COM.

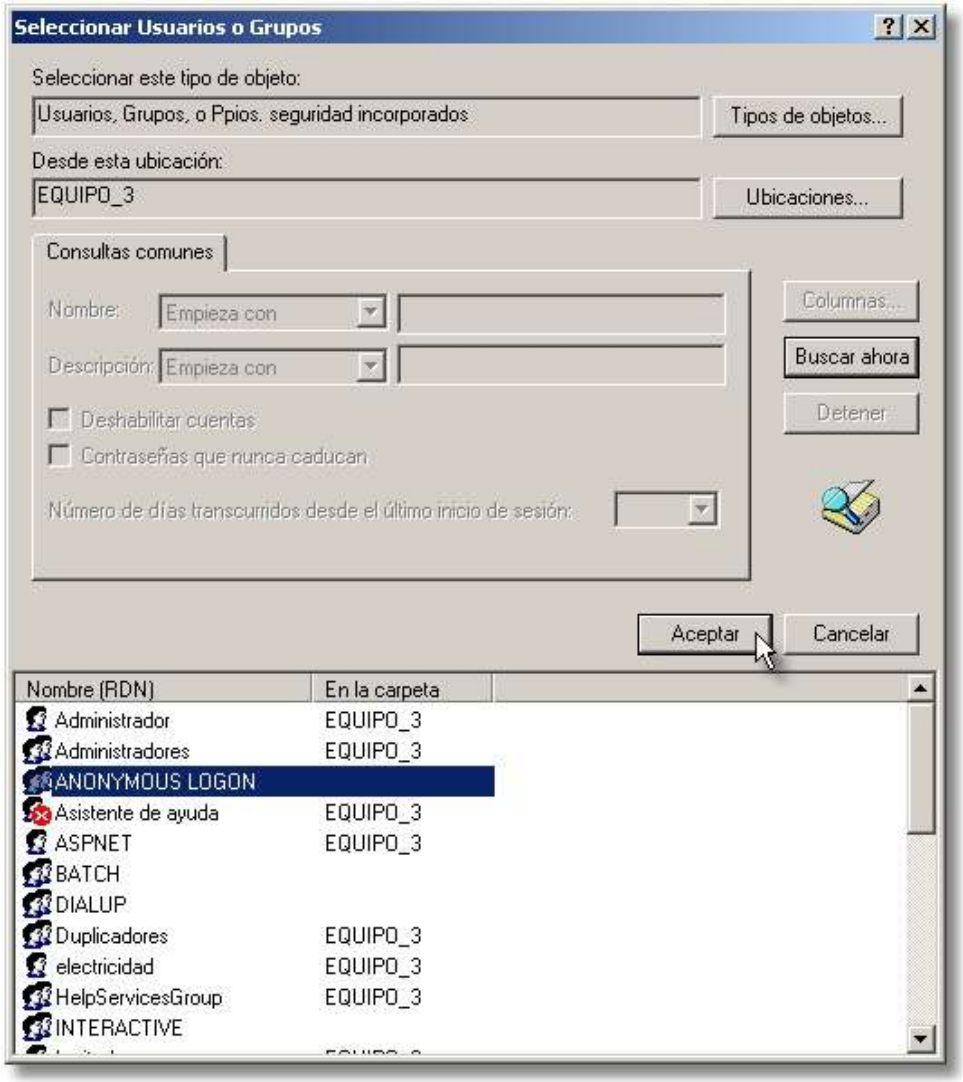
► **Y a continuación, para buscar a los usuarios, escogeremos *Avanzadas y Buscar* ahora desde el equipo en el que estemos (en este caso aparece EQUIPO_3 porque es donde se ha hecho esta imagen),**



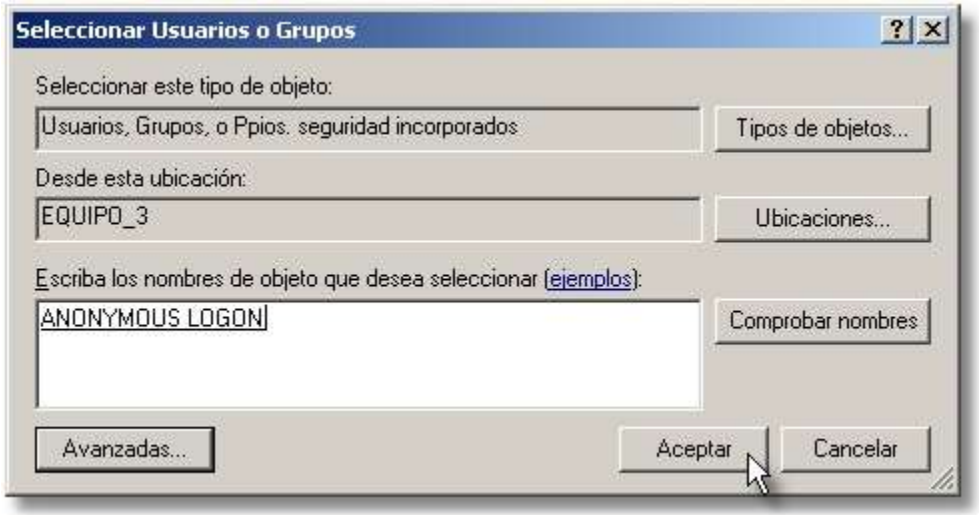
Servidor: Configurar Seguridad COM.



Servidor: Configurar Seguridad COM.



Servidor: Configurar Seguridad COM.

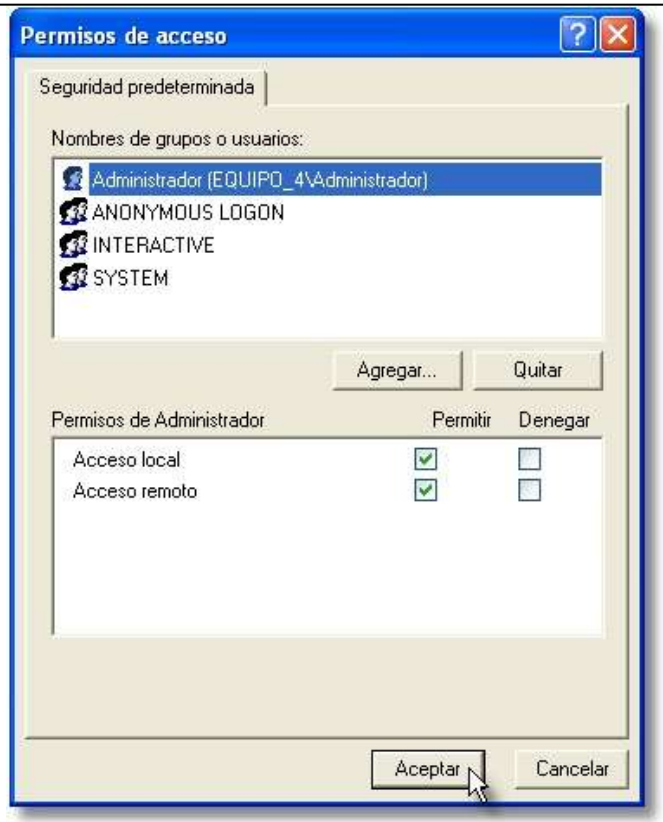


► **Una vez escogidos los usuarios se validan sus permisos local y remoto.**

Servidor: Configurar Seguridad COM.

- Hasta aquí se han configurado los límites para los permisos de acceso.
- Después editaremos el resto de permisos, que quedarán con dichos usuarios:

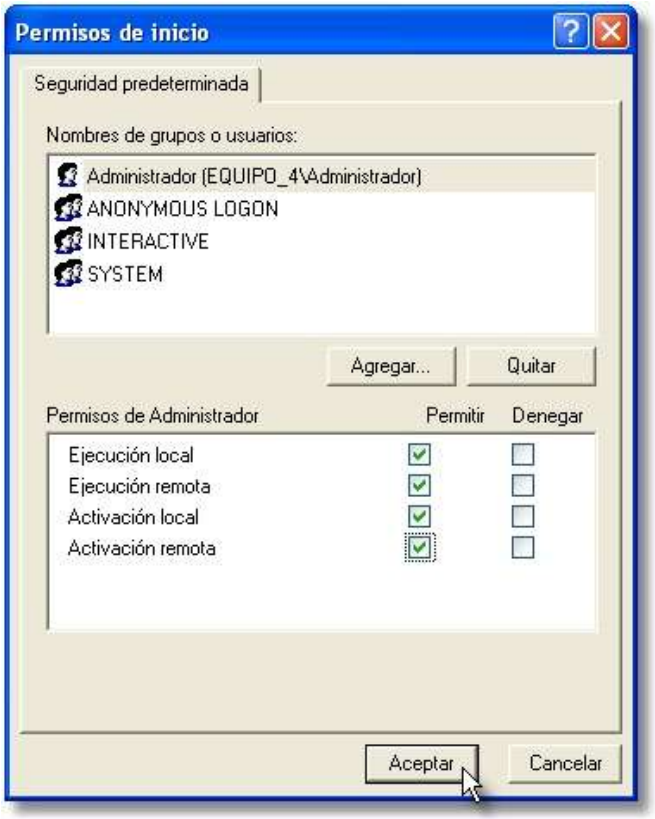
- Permisos de acceso predeterminados :



- Los límites para los permisos de inicio y activación:

Servidor: Configurar Seguridad COM.

► **Y los permisos de inicio y activación predeterminados:**



Servidor: Configurar Seguridad COM.

► **Configurar los propiedades para las aplicaciones usadas:**

► **A continuación es necesario establecer los permisos para que el ordenador remoto o cliente sea capaz de lanzar las aplicaciones *OpcEnum* , *Open Data Server* y *KEPware Enhanced OPC/DDE Server*, así como otros servidores OPC instalados.**

► **OpcEnum es la aplicación que busca en un equipo los servidores OPC instalados.**

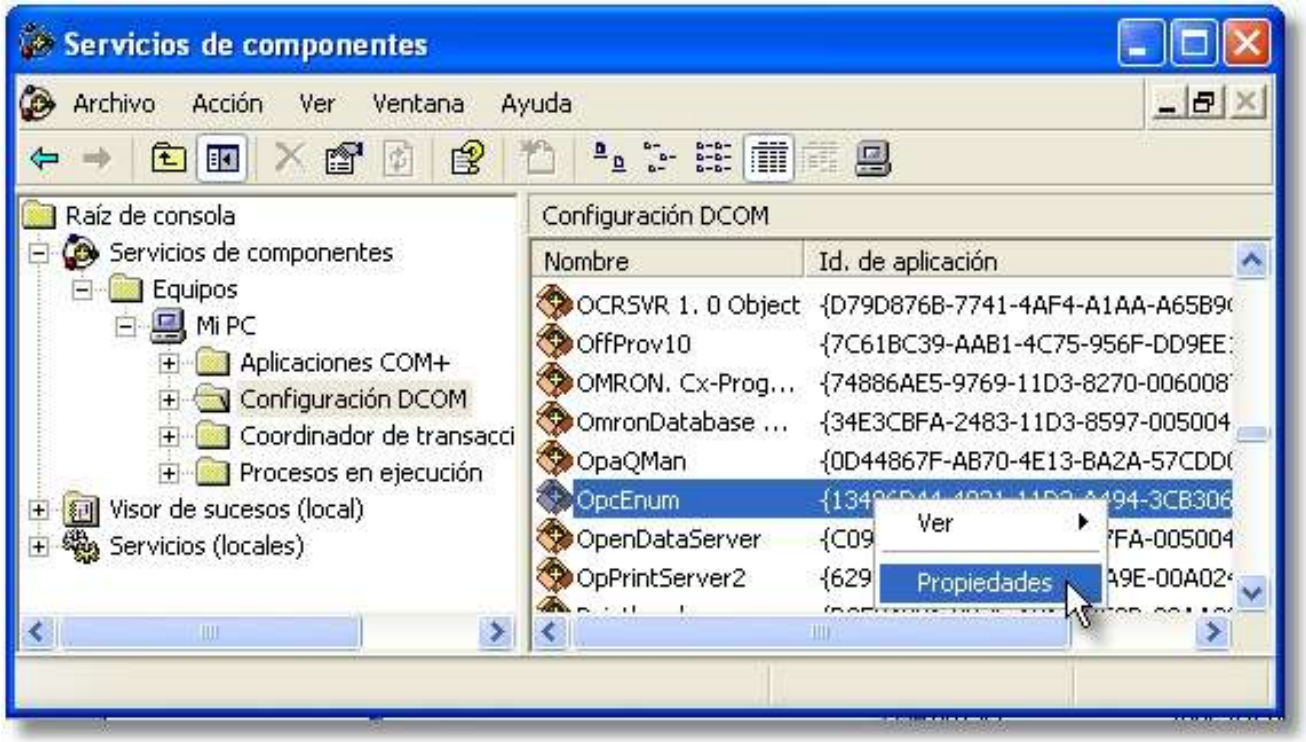
► **Open Data Server es la aplicación que sirve datos OPC de equipos de Omron.**

► **KEPware EnhancedOPC/DDE Server es la aplicación que sirve datos OPC de varios fabricantes.**

► **Si se desea también se puede dar permisos para acceder a otras aplicaciones como un SCADA etc.**

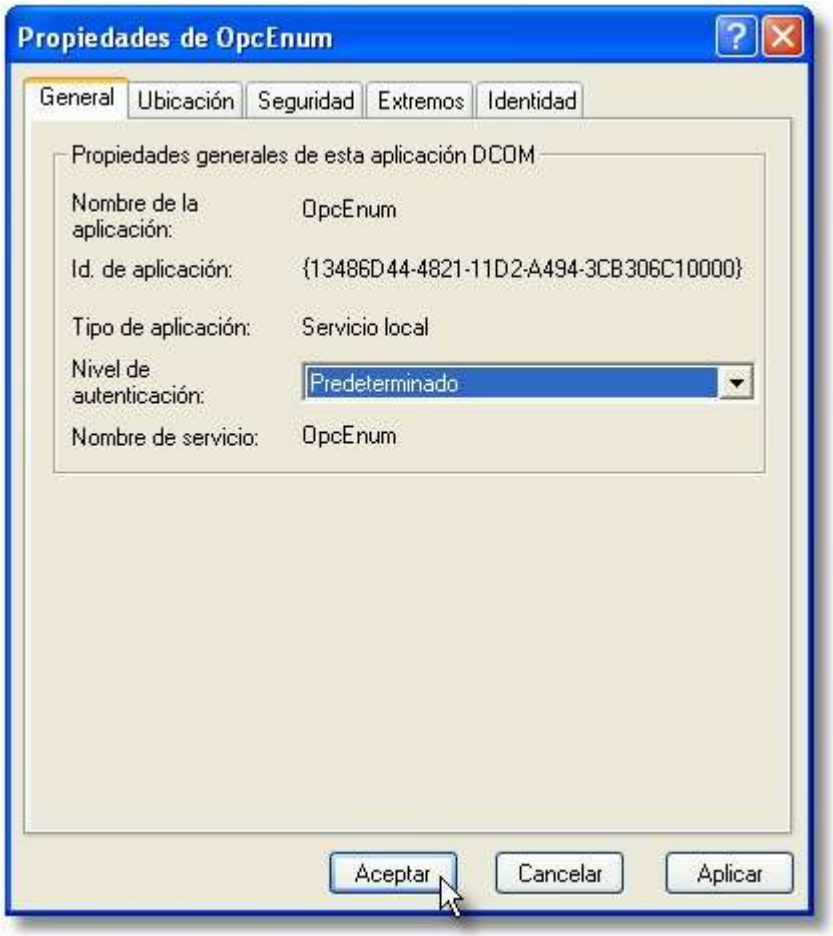
Servidor: Configurar Seguridad COM.

► **Para ello nos situamos de nuevo en la ventana de *Servicios de componentes* para configurar los servicios DCOM específicos que se utilizarán en la conexión. Abrimos el menú *Raíz de consola* → *Servicios de Componentes* → *Equipos* → *Mi PC* → *Configuración DCOM* → *OpcEnum* (pulsamos el botón derecho y seleccionamos propiedades):**



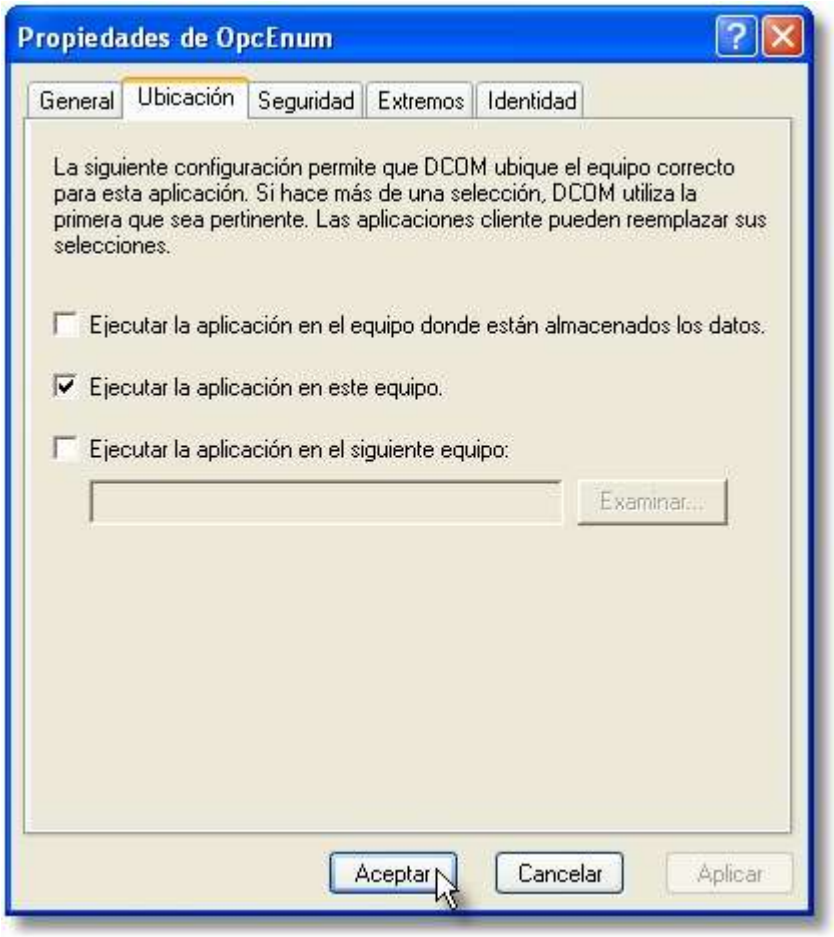
Servidor: Configurar Seguridad COM.

► **En esta ventana de propiedades estableceremos las opciones:**
En la pestaña *General* → *Nivel de autenticación* → *Predeterminado*



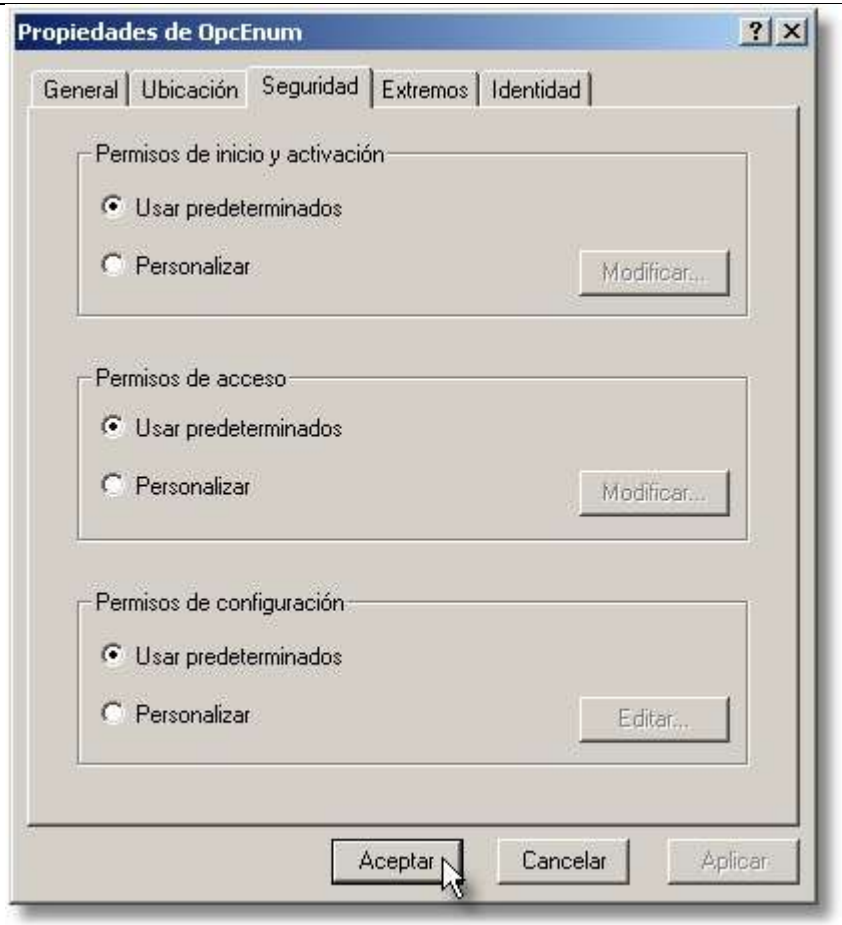
Servidor: Configurar Seguridad COM.

► **En la pestaña *Ubicación* → *Ejecutar la aplicación en este equipo***



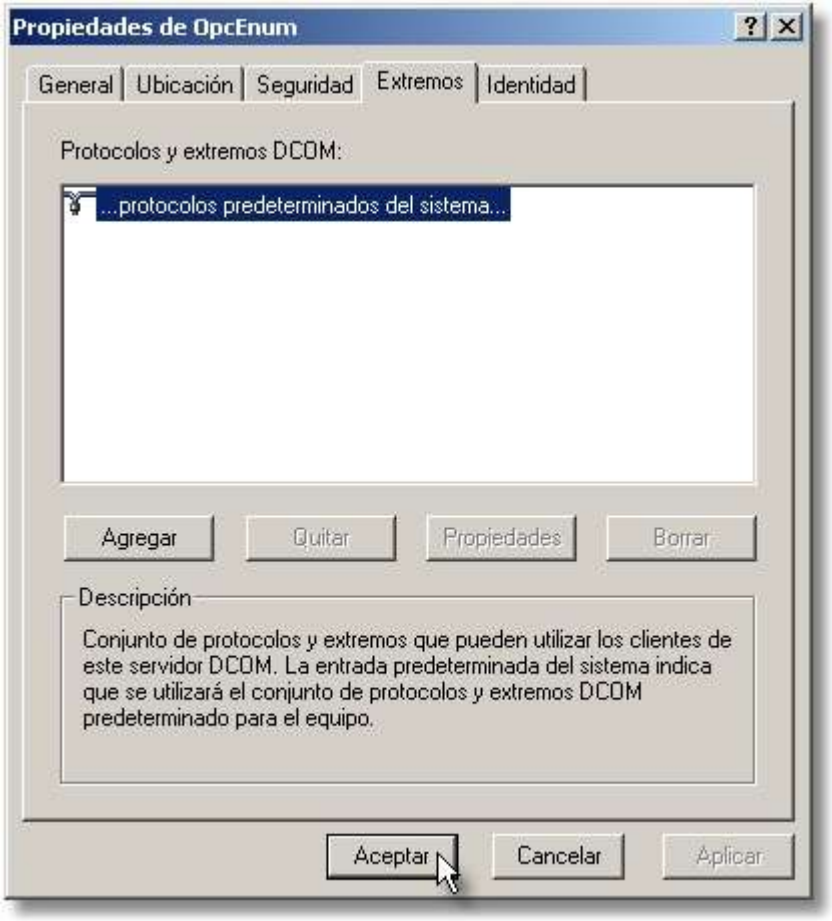
Servidor: Configurar Seguridad COM.

► **En la pestaña *Seguridad* → dejamos los permisos en *predeterminados* ya que anteriormente hemos habilitado como predeterminados a los usuarios anónimo e interactivo para los Permisos de acceso de inicio y activación, permisos de acceso.**



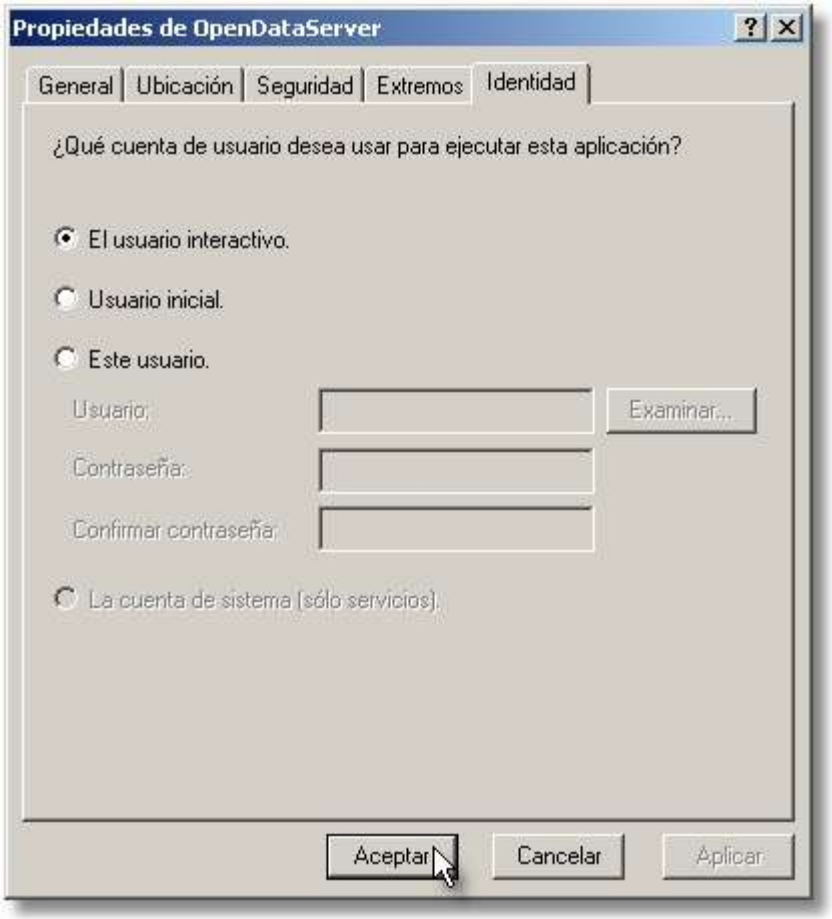
Servidor: Configurar Seguridad COM.

► **En la pestaña *extremos* → dejamos los protocolos determinados del sistema.**



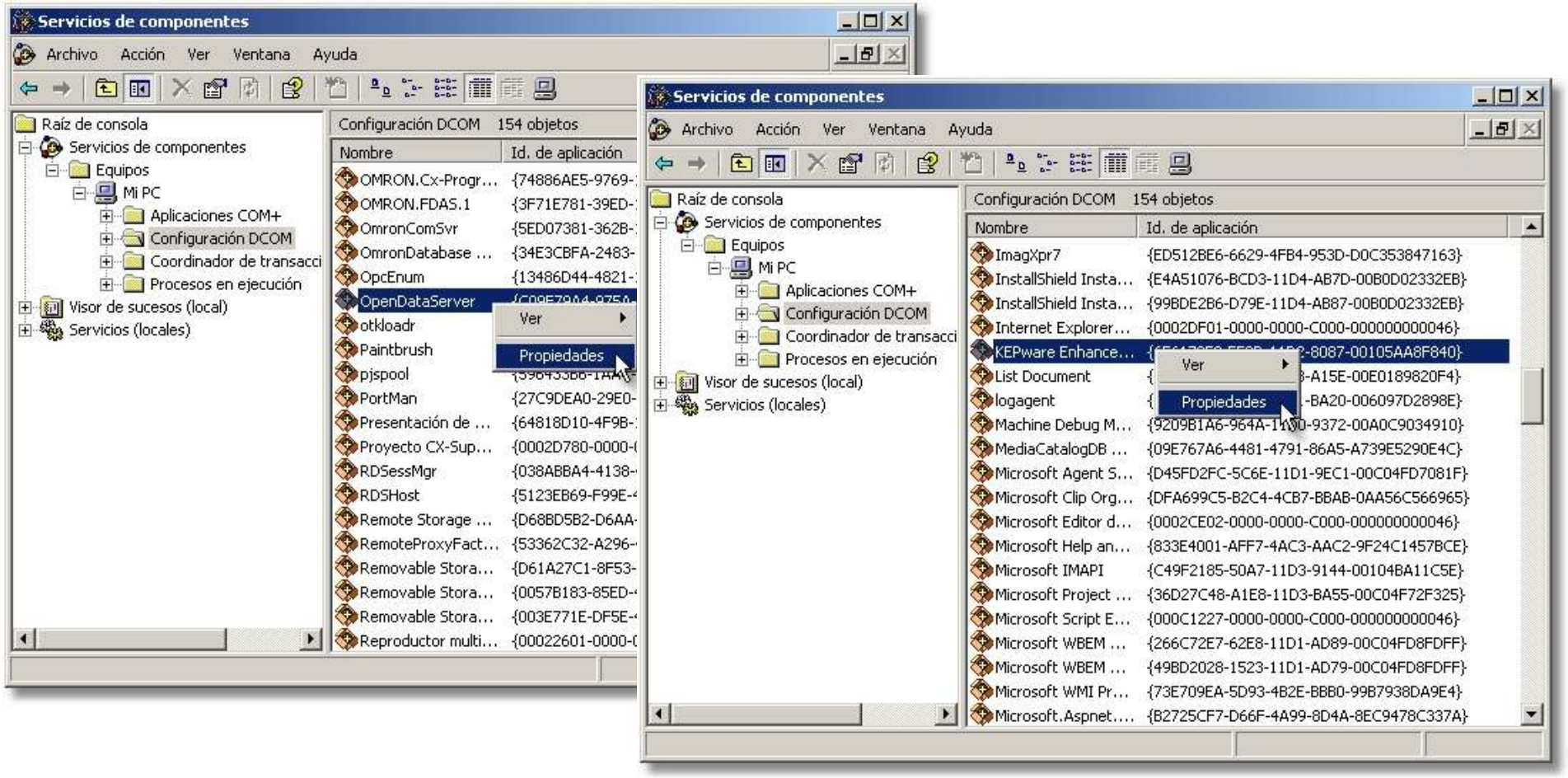
Servidor: Configurar Seguridad COM.

► **En la pestaña *identidad* → dejamos al *usuario interactivo*.**



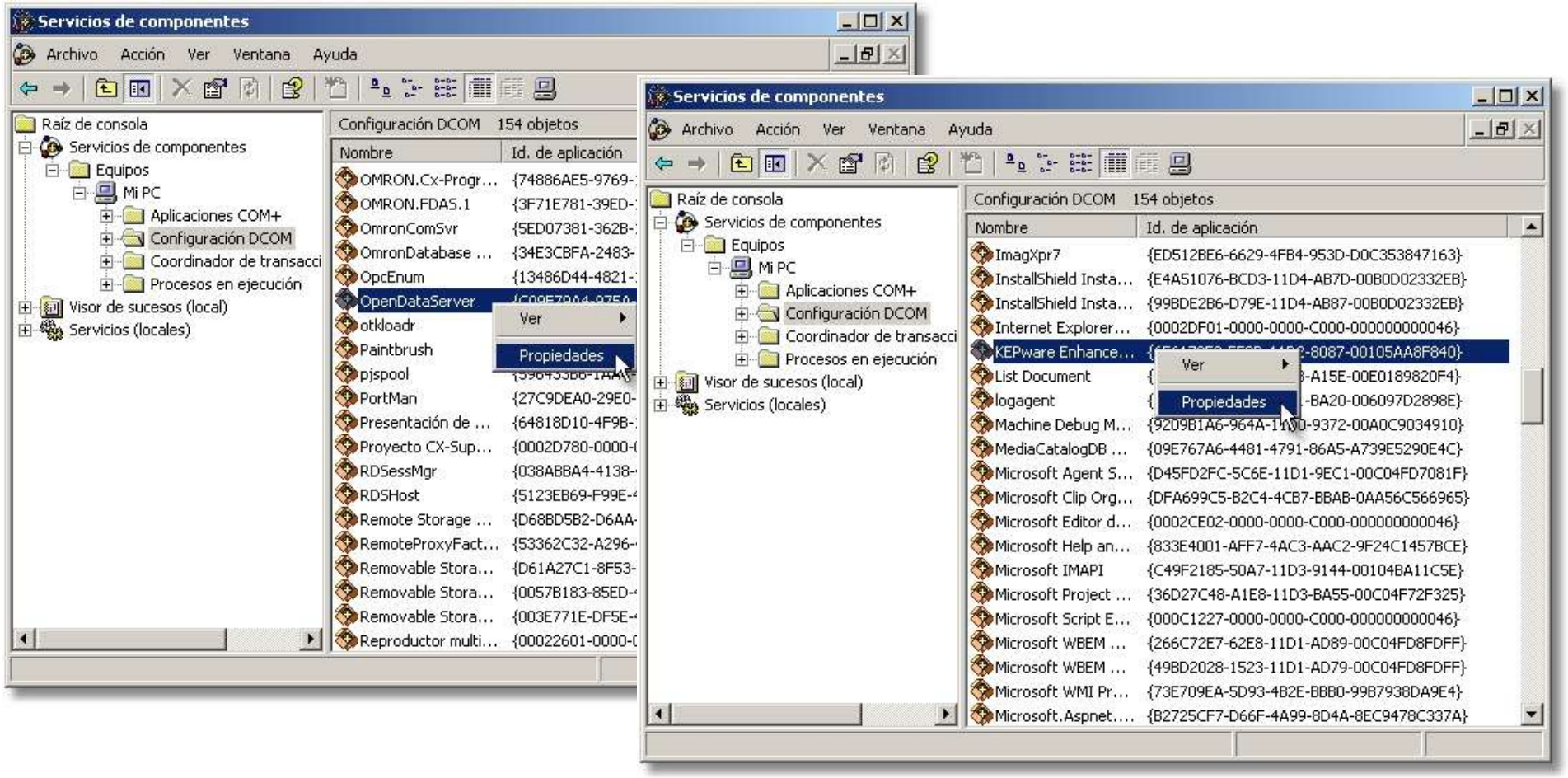
Servidor: Configurar Seguridad COM.

► **Las operaciones realizadas en propiedades de OPCEnum las repetiremos para Open Data Server , KEPware Enhanced OPC/DDE Server y otros servidores:**



Servidor: Configurar Seguridad COM.

► **Las operaciones realizadas en propiedades de OPCEnum las repetiremos para Open Data Server , KEPware Enhanced OPC/DDE Server y otros servidores:**



Servidor: Reiniciar el equipo.

► **Cuando se cambian, como en este caso, la seguridad en las propiedades de comunicación, es necesario reiniciar el equipo.**

► **Con estas configuraciones ya está dispuesto el equipo cliente para solicitar datos de un servidor.**

Configuración de los equipos en una red con workgroup o trabajo en grupo.

Configuración DCOM en el equipo cliente para trabajo en grupo.

- **Tendremos que realizar las siguientes operaciones:**
  - **Desactivar el cortafuegos de Windows**
  - **Configurar COM distribuido (DCOM) y Seguridad COM**
  - **Reiniciar el equipo**

Para ello *seguiremos los mismos pasos realizados en el equipo servidor* salvo la configuración de las aplicaciones. (Aquí no se desarrolla).

Desarrollo de una aplicación cliente.

► **Vamos a crear una aplicación que lea el canal de entradas de un PLC en el display que nos proporciona el conjunto de los objetos OPC de Omron.**

1.- Crear un proyecto en el Servidor OPC.

► **El primer paso es configurar CX-Server OPC o KepServer OPC en el ordenador que hace de servidor.**

► **En nuestro caso crearemos un proyecto con un PLC y un punto otag que será un canal o byte de entradas del mismo.**

► **Para ello seguiremos el proceso que está desarrollado en la actividad 7. (Aquí no se desarrolla).**

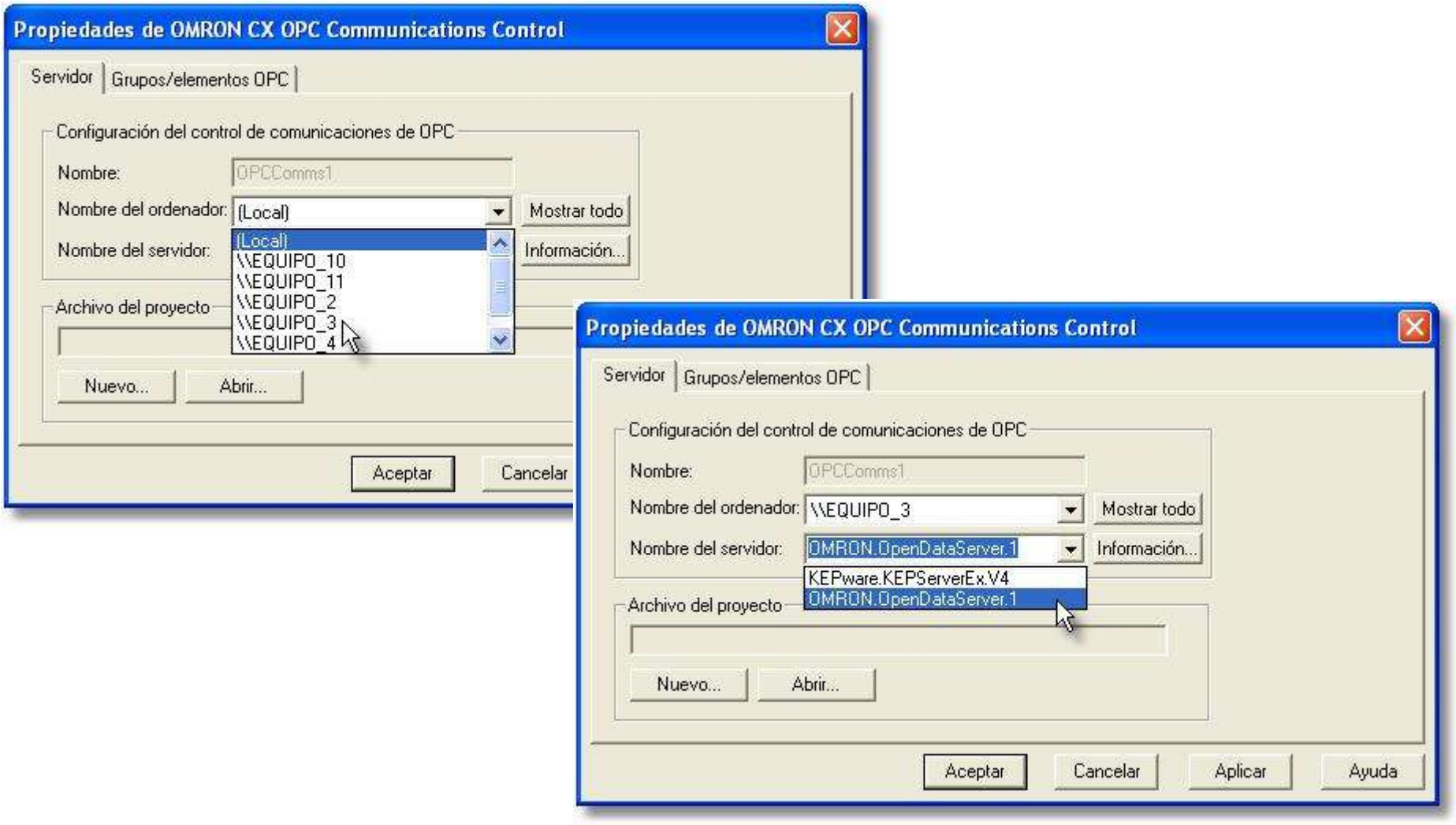
2.- Crear un proyecto en el Cliente.

► **En el ordenador cliente de la red, creamos una aplicación en Excel o Visual Basic como se desarrolló en la actividad 8:**

En *modo diseño* → *insertar* → *Objeto* → *OMRON CX OPC Comunications Control*

► **Con el botón derecho en *Objeto OMRON CX OPC Comunications Control* → *propiedades* → seleccionaremos el *ordenador* de la red que hace de servidor y el *servidor OPC* deseado de la lista que tenga instalados:**

2.- Crear un proyecto en el Cliente.



2.- Crear un proyecto en el Cliente.

► Continuar como en la actividad 8: Crear el proyecto nuevo, añadir un grupo con su frecuencia de actualización y el elemento que nos interesa (canal de IN)

► En este punto se abrirá en el otro PC (servidor) el programa del servidor OPC configurado y en nuestro PC cliente la ventana con los puntos creados en el servidor para escoger los deseados en el cliente.

► A partir de aquí el proceso es el mismo que el que hicimos anteriormente en la actividad 8.

► Si insertamos más de un control de comunicaciones porque hay más de un servidor, que pueden estar en ordenadores diferentes, se generarán OPCComms1, OPCComms2, etc.

► Insertamos el display de Omron o cualquier otro objeto deseado y le asignamos el servidor y el elemento correspondiente.

► Por último ejecutar el programa cliente si estamos en VB o salir del modo diseño si estamos en Excel.

ANEXO : Ayudas de Windows para la configuración DCOM

► **El usuario interactivo es el usuario que está registrado en la cuenta de Windows del equipo en el que se ejecuta la aplicación. El que ha iniciado actualmente la sesión en el equipo.**

► **El usuario Red o Network es el grupo que contiene a todos los usuarios que tienen actualmente acceso al sistema a través de la red.**

► **El usuario anónimo es el que se ha conectado al equipo sin proporcionar un nombre de usuario y una contraseña.**

ANEXO : Permisos de acceso

► **Los permisos de acceso especifican una lista de usuarios a los que se les concede o niega el acceso a aplicaciones COM. Los permisos de acceso a todo el equipo son aplicables a todas las aplicaciones COM que no especifican sus permisos de acceso propios.**

► **Los permisos de acceso se pueden especificar de manera independiente para cada aplicación COM. Los permisos de acceso predeterminados a todo el equipo son aplicables a todas las aplicaciones COM que no especifican sus permisos de acceso propios. La directiva de restricción de todo el equipo limita los permisos de acceso que se otorgan al utilizar un escenario.**

► **Los permisos de acceso se dividen en permisos de acceso local y de acceso remoto. Los usuarios con permisos de acceso local pueden tener acceso a una aplicación COM ejecutándose en el mismo equipo que el cliente de llamada. Los usuarios con permiso de acceso remoto pueden tener acceso a una aplicación COM desde otros equipos a través de una conexión de red.**

ANEXO : Permisos de acceso

► **Mediante la herramienta administrativa Servicios de componentes, se pueden agregar o quitar cuentas de usuario o grupos a las listas de usuarios que tienen permisos de acceso. Esto no afecta a las aplicaciones COM+.**

► **La directiva de restricción de todo el equipo limita los permisos de acceso que se otorgan para una aplicación COM. El Administrador puede utilizar los límites de la directiva de restricción de todo el equipo para suplantar un nivel de la aplicación menos restrictivo o los permisos predeterminados de todo el equipo. De forma predeterminada, la directiva de restricción de todo el equipo posibilita permisos de acceso local y remoto a los miembros del grupo Todos, y permiso de acceso local otorgado tanto a los miembros del grupo Todos como al de usuario Anónimo. Si la directiva del sistema excluye al " usuario Anónimo" del grupo Todos, el cliente anónimo no puede tener acceso remoto a aplicaciones COM.**

► **Para obtener instrucciones paso a paso sobre cómo modificar estos valores de configuración, consulte en las ayudas de windows: Establecer los permisos de acceso de todo el equipo o Establecer permisos de acceso específicos de la aplicación**

ANEXO : Permisos de inicio y activación

► **Los permisos de inicio y activación especifican una lista de usuarios a los que se les otorga o deniega el permiso para lanzar o activar aplicaciones COM. Es necesario el permiso de inicio para iniciar una nueva aplicación COM. El permiso de activación se requiere para que un nuevo cliente utilice una aplicación COM, aunque ésta haya sido ya iniciada.**

► **Los permisos de inicio y activación se pueden especificar de manera independiente para cada aplicación COM. Los permisos de inicio y activación predeterminados para todo el equipo son aplicables a todas las aplicaciones COM que no especifican sus permisos de inicio propios. La directiva de restricción de todo el equipo limita los permisos de inicio y activación que se otorgan al utilizar un escenario.**

► **Los permisos de inicio y activación se dividen en locales y remotos. Los usuarios con permiso de inicio y activación local puede iniciar o utilizar una aplicación COM ejecutándose en el mismo equipo que el cliente de llamada. Los usuarios con permiso de inicio y activación remoto puede iniciar o utilizar una aplicación COM desde otros equipos a través de una conexión de red.**

ANEXO : Permisos de inicio y activación

► **La directiva de restricción de todo el equipo limita los permisos de inicio y activación que se otorgan para una aplicación COM. El Administrador puede utilizar los límites de la directiva de restricción de todo el equipo para suplantar un nivel de la aplicación menos restrictivo o los permisos de inicio y activación de todo el equipo. De forma predeterminada, la directiva de restricción de todo el equipo posibilita permisos de inicio y activación local y remoto a los miembros del grupo Administradores, y permiso de inicio y activación local otorgado al grupo. Si la directiva del sistema excluye al " usuario Anónimo" del grupo Todos, el cliente anónimo no puede iniciar o activar aplicaciones COM.**

► **Para obtener instrucciones paso a paso sobre cómo modificar estos valores de configuración, consulte Establecer los permisos inicio y activación de todo el equipo o Establecer permisos de inicio y activación específicos de la aplicación.**

► **En Permisos de inicio y activación, haga clic en el botón Editar límites... o en el botón Modificar predeterminados... según se desee modificar o bien la directiva de restricción de todo el equipo, o bien la configuración predeterminada. Aparecerá el cuadro de diálogo Permisos de inicio.**

ANEXO : Directiva de restricción de software

► **Si se utiliza adecuadamente, la directiva de restricción de software puede hacer que su compañía sea más ágil ya que proporciona una estructura dinámica para prevenir problemas, en vez de una estructura que funcione por reacción y que esté basada en la costosa alternativa que representa restaurar un sistema si se ha producido un problema. La directiva de restricción de software fue creada para proteger los sistemas contra código desconocido y posiblemente peligroso, y proporciona un mecanismo en virtud del cual sólo el código de confianza tiene acceso sin restricciones a los permisos del usuario.**

► **Al utilizar la directiva de restricción de software, se permite que el código desconocido, que puede contener virus o código que entre en conflicto con programas instalados actualmente, se ejecute sólo en un entorno restringido (a menudo denominado un *recinto de seguridad*) en el no tiene acceso a ningún permiso de usuario que ponga en peligro la seguridad. Por ejemplo, un archivo adjunto de correo electrónico que contiene un gusano no podría tener acceso a la libreta de direcciones y, por lo tanto, no se podría propagar. Si el archivo adjunto del correo electrónico contuviera un virus, la directiva de restricción de software restringiría su capacidad para dañar el sistema, porque sólo se le permitiría ejecutarse en un entorno restringido.**

ANEXO : Directiva de restricción de software

► **La directiva de restricción de software depende de la asignación de niveles de confianza para el código que puede ejecutarse en un sistema. Actualmente, existen dos niveles de confianza: sin restricciones y no permitido. Al código que tiene el nivel de confianza sin restricciones se le otorga acceso sin límite a los permisos del usuario, por lo que este nivel de confianza sólo debe ser aplicado al código totalmente confiable. Al código con un nivel de confianza no permitido no se le permite el acceso a ningún permiso de usuario que sea importante para la seguridad y sólo puede ejecutarse en un recinto de seguridad, por lo que el código sin restricciones no puede cargar el código no permitido en su espacio de direcciones.**

► **La configuración de la directiva de restricción de software para un sistema se realiza mediante la herramienta administrativa Directiva de seguridad local, mientras que la configuración de la directiva de restricción de aplicaciones COM+ individuales se realiza mediante programación o a través de la herramienta administrativa Servicios de componentes. Si el nivel de confianza de la directiva de restricción no se especifica para una aplicación COM+, la configuración de todo el sistema se utiliza para determinar el nivel de confianza de la aplicación.**

► **Se debe coordinar cuidadosamente la configuración de la directiva de restricción de software COM+ con la configuración de todo el sistema, porque una aplicación COM+ que tiene un nivel de confianza sin restricciones sólo puede cargar componentes con un nivel de confianza sin restricciones, mientras que una aplicación COM+ con el nivel no permitido puede cargar componentes con cualquier nivel de confianza pero no puede tener acceso a ningún permiso de usuario importante para la seguridad.**

ANEXO : Configurar la directiva de restricción de software

► **Cuando configure explícitamente los niveles de confianza de la restricción de software de una aplicación COM+, suplantará la configuración predeterminada en todo el sistema para la directiva de restricción de software. A menudo es necesario hacerlo para las aplicaciones de servidor COM+ ya que la directiva de restricción de software del sistema es la misma para todas las aplicaciones de servidor (debido a que todas se ejecutan en el mismo archivo, dllhost.exe).**

► **Nota Cuando configure el nivel de confianza de una aplicación de biblioteca COM+, afectará a la directiva de restricción de software del sistema para esa aplicación. Para ver información general acerca de cómo utilizar la directiva de restricción de software en COM+, consulte Directiva de restricción de software.**

ANEXO : Para configurar la directiva de restricción de software

1.- Haga clic con el botón secundario del *mouse* (ratón) en la aplicación COM+ para la que va a establecer la directiva de restricción y, después, haga clic en **Propiedades**.

2.- En el cuadro de diálogo de propiedades de la aplicación, haga clic en la ficha **Seguridad**.

3.- En **Directiva de restricción de software**, active la casilla de verificación **Aplicar directiva de restricción de software** para habilitar la configuración del nivel de confianza; si desactiva la casilla de verificación, hará que COM+ utilice la directiva de restricción de software del sistema para la aplicación.

4.- En el cuadro Nivel de restricción, seleccione el nivel adecuado. Los niveles, de la menor confianza a la mayor, son los siguientes:

- **No permitido** No se permite a la aplicación utilizar todos los privilegios del usuario. Se pueden cargar los componentes que tengan algún nivel de confianza de la directiva de restricción.
- **Sin restricciones** La aplicación tiene acceso sin restricciones a los privilegios del usuario. Sólo se pueden cargar componentes que tengan un nivel de confianza Sin restricciones.

5.- Haga clic en **Aceptar**.

El nivel de confianza seleccionado surtirá efecto la próxima vez que se **inicie la aplicación**.

ANEXO : Configurar COM distribuido

- El protocolo de cableado COM distribuido (DCOM) administra toda la comunicación de red entre los componentes COM que se ejecutan en equipos distintos. Debe habilitar DCOM en cada equipo que disponga de componentes COM y se comunique con otros a través de la red. Deshabilitar DCOM no influye en la comunicación entre componentes del mismo equipo, pero sí deshabilita la comunicación entre componentes de equipos distintos. Para obtener instrucciones acerca de cómo habilitar la comunicación entre componentes de distintos equipos, consulte Habilitar o deshabilitar COM distribuido.

ANEXO : Hacer que los equipos sean visibles para los Servicios de componentes

- Debe agregar al árbol de la consola de la herramienta administrativa Servicios de componentes cualquier equipo que desee administrar con dicha herramienta. A menos que un equipo sea visible con la herramienta administrativa Servicios de componentes, no se puede establecer la seguridad ni instalar aplicaciones. Para obtener instrucciones acerca de cómo agregar equipos a Servicios de componentes, consulte Hacer que los equipos sean visibles para los Servicios de componentes.

ANEXO : Nuevo sistema de seguridad (D)COM

- **Windows XP SP2 incluye un nuevo sistema de seguridad para aplicaciones (D)COM. El nuevo sistema de seguridad facilita reducir la accesibilidad de los usuarios no autorizados a las aplicaciones COM.**

Además de los permisos de inicio y de acceso anteriores para aplicaciones COM, el nuevo sistema incluye un permiso de activación independiente. Los usuarios que dispongan del permiso de activación, pero no del permiso de inicio, pueden crear un cliente proxy para una aplicación COM, siempre y cuando ésta se esté ejecutando ya en el servidor. Todavía se requiere el permiso de acceso para utilizar el proxy, por lo tanto todos los usuarios con permiso de activación deberían tener permiso de acceso.

Los permisos de acceso, inicio y activación se dividen ahora en permisos locales y remotos independientes. Los usuarios con permiso local para una aplicación COM pueden realizar la acción permitida sólo en el equipo local (el equipo en el que se ejecuta la aplicación.). Para realizar la acción desde un equipo diferente a través de una red, el usuario debe tener un permiso remoto.

El nuevo sistema de seguridad también incluye una nueva directiva de restricción de todo el equipo. Esta directiva limita en algún aspecto los permisos que se pueden conceder (como el uso de la API CoInitializeSecurity). Por ejemplo, se puede desautorizar el acceso remoto a cualquier aplicación COM, denegando los permisos de activación, de inicio y remoto a todos los usuarios en la directiva de restricción de todo el equipo.

ANEXO : Nuevo sistema de seguridad (D)COM

- La siguiente tabla resume la directiva de restricción predeterminada de todo el equipo.

Permiso	Administradores	Todos	Anónimo
Acceso	Local, remoto	Local, remoto	Local
Activación	Local, remoto	Local	Sin permisos
Inicio	Local, remoto	Local	Sin permisos

- Tenga en cuenta que el usuario anónimo no tiene permisos remotos, y los usuarios que no son administradores no tienen permisos de inicio o de activación. Esta configuración predeterminada puede hacer que los escenarios existentes funcionen mal. Para obtener más información, consulte DCOM en MSDN.

Para obtener más información acerca del nuevo sistema de seguridad COM, incluyendo instrucciones específicas sobre cómo establecer los permisos, consulte Permisos de acceso y Permisos de inicio y activación.

ANEXO : Configuración de la seguridad COM

- **Las aplicaciones COM, por ejemplo Microsoft® Word, utilizan una serie de propiedades de configuración de seguridad: nivel de autenticación, nivel de representación, permisos de acceso, permisos de inicio, y permisos de configuración. Estas propiedades tienen valores que afectan a todo el equipo y que una aplicación puede utilizar de manera predeterminada. Alternativamente, las propiedades de seguridad COM, se pueden configurar específicamente para cualquier aplicación determinada. Si una aplicación no tiene una configuración de seguridad específica, utilizará la configuración de seguridad de todo el equipo. Una directiva de restricción de todo el equipo especifica un nivel mínimo de seguridad que no puede ser suplantado por la configuración de seguridad de todo el equipo, o por la específica de la aplicación.**

- **Aunque, por lo general, no es necesario cambiar ningún valor de configuración, los requisitos de seguridad para aplicaciones determinadas o sistemas determinados pueden exigir que lo haga. Se puede cambiar la configuración de seguridad para una aplicación COM determinada, la configuración de seguridad de todo el equipo y la directiva de restricción de todo el equipo con la herramienta administrativa Servicios de componentes.**

ANEXO : Configuración de seguridad de todo el equipo

- **Para cada propiedad de seguridad COM, una aplicación COM puede utilizar la configuración de todo el equipo o utilizar una configuración personalizada. Cuando una aplicación tiene una configuración de seguridad personalizada, la configuración de todo el equipo se descarta; sin embargo, una aplicación que no tiene su propia configuración utilizará la configuración de todo el equipo.**

- **Si los valores predeterminados no cumplen los requisitos de seguridad de las aplicaciones en el sistema, se puede modificar la configuración de seguridad de todo el equipo mediante la herramienta administrativa Servicios de componentes. Sin embargo, no olvide que el hecho de cambiar la configuración de todo el equipo afecta a todas las aplicaciones COM que no tengan una configuración personalizada.**

- **Si se desea utilizar la configuración predeterminada de todo el equipo, no necesita hacer nada. COM utiliza los siguientes valores predeterminados automáticamente para la configuración de seguridad de todo el equipo:**
  Un nivel de autenticación de Conexión.
  - **Un nivel de representación de Identificación.**
  - **Los permisos de acceso conceden permisos a la identidad del servidor y al sistema local.**
  - **Un nombre principal basado en el nombre de usuario y la contraseña.**
  - **COM determina un proveedor de servicio de seguridad para que sea el mejor para el entorno. En Microsoft Windows® 2000, Windows XP y Windows Server 2003, es Kerberos o NTLMSSP.**

ANEXO : Configuración de seguridad de todo el equipo

► **Consulte los temas que se describen en la siguiente tabla para obtener información de tareas y general acerca de cómo establecer niveles de seguridad en COM.**

Tema	Descripción
Nivel de autenticación	Proporciona información general acerca de los niveles en los cuales el cliente comprueba la identidad del servidor y viceversa mediante credenciales, a partir de la cual ambos comprueban y cifran datos que se envían mutuamente.
Nivel de representación	Presenta los niveles a través de los cuales un servidor realiza una llamada en nombre de un cliente y presenta la identidad del cliente y las credenciales en su lugar cuando se hace la llamada.
Permisos de acceso	Presenta los permisos que especifican una lista de usuarios a los que se les concede o niega el acceso a aplicaciones COM.
Permisos de inicio y activación	Proporciona una visión general de los permisos que especifican una lista de los usuarios a los que se otorgan o niegan los permisos para iniciar o utilizar las aplicaciones COM.
Seguimiento de referencias	Presenta una tecnología a través de la cual COM llevará a cabo comprobaciones de seguridad adicionales para autenticar llamadas de número de referencias y realizará un seguimiento de la información adicional para impedir que un objeto esté disponible demasiado pronto, accidental o malintencionadamente.