Tema 2

Windows NT

Grupos de trabajo y dominios

Microsoft con su **Windows 3.11 para trabajo en grupo** introdujo el concepto de grupo de trabajo (workgroup). Un grupo de trabajo era un conjunto de ordenadores conectados entre sí con el fin de compartir sus recursos. Todos los ordenadores del grupo de trabajo, son iguales desde un punto de visto organizativo. Es decir, no existe un ordenador central en el que se concentren los recursos y realice tareas de control de seguridad. Cada usuario del grupo de trabajo realizaba la administración de su propio ordenador, es decir, decidía que recursos compartía y quienes de los usuarios del grupo de trabajo podían acceder a esos recursos. Es decir, estabamos ante una red de igual a igual. Este tipo de organización es muy sencillo de instalar, pero su eficiencia se reduce a medida que el tamaño de la red crece. Al incrementarse el número de usuarios y recursos compartidos, resulta más difícil localizar un determinado recurso en esa red. Sin embargo, el principal problema de estas redes es la seguridad. A medida que el sistema crece, el número de passwords que los usuarios necesitan aumentan, los usuarios precisarán de diferentes password para acceder a distintos recursos. Se tiende a usar password fáciles de recordar y, por tanto, fáciles de averiguar. Todo esto hace que las redes igual a igual, no sean adecuadas para redes de gran tamaño o para redes que precisan de un control centralizado.

Por todo ello, Microsoft necesitaba un SO que le permitiera crear una red basada en un servidor central, salvando con ello todo los problemas de eficiencia y seguridad de las redes igual a igual. Y esto es lo que nos ofrece NT, un SO en red que permite una gestión centralizada de todos los equipos que componen tu red. El conjunto de todos esos equipos es lo que NT denomina **dominio** y que no es otra cosa más que un conjunto de ordenadores que comparten la misma información de seguridad. La estructura en dominios, en la que se basa Windows NT Server, ofrece una flexibilidad mayor y una administración más simple. Se adapta perfectamente a redes de gran tamaño o con una estructura compleja. De dominios y de sus componentes es de lo que vamos a hablar a continuación.

Dominios

Un dominio es una agrupación lógica de servidores y otras estaciones que comparten una información común de seguridad y de cuentas de usuario. Un usuario registrado en un dominio con un nombre de usuario y una palabra de paso, automáticamente es capaz de acceder a todos los equipos que forman dicho dominio utilizando el mismo nombre y la misma palabra de paso. Esto supone una gran ventaja frente a los grupos de trabajo, en los que un usuario podía precisar de más de una palabra de paso para el acceso a todos los recursos que necesitaba.

Para constituir un dominio simplemente hace falta contar con un servidor (un servidor será un equipo que ejecute Windows NT Server) que actúe como **controlador primario de dominio** (ya veremos más adelante que es esto) y asignarle un nombre, ese nombre será el **nombre del dominio** y debe ser único. En este servidor primario es donde se crearán las cuentas de los usuarios que serán comunes para todos los equipos del dominio. Simplemente con un servidor instalado como controlador primario ya tienes un dominio creado, aunque no tiene sentido que tu dominio esté formado únicamente por un equipo. El objetivo de un dominio es que varios equipos compartan las mismas cuentas de usuario y por tanto, una información común de seguridad, luego a parte del controlador primario es lógico que haya otros equipos dentro del dominio. Resumiendo, los pasos para crear un dominio son dos:

- instalar un servidor NT que actúe como controlador primario de dominio
- dar un nombre único a ese dominio

Se podría decir que un dominio es un grupo de trabajo que incluye un servidor central. El objetivo sigue siendo el mismo, permitir a los usuarios de una red compartir recursos. El dominio incluye un servidor, es decir, un punto central y único para el control y la administración.

Elementos de un dominio

Una estructura de dominio típica estará constituida por una mezcla de servidores, estaciones y sistemas operativos. Se puede observar un ejemplo en la figura siguiente:

Controlador Primario de Dominio (PDC)

El PDC (**Primary Domain Controller**) será el ordenador más importante dentro del dominio. En cada dominio solamente puede existir un controlador primario. Se encargará de las tareas de seguridad y contendrá la base de datos que recoge toda la información sobre el dominio. Esta información se guarda en una base de datos llamada **SAM** (Security Account Manager). La SAM contiene básicamente dos cosas:

- las cuentas de usuario, y
- la información sobre los equipos del dominio.

La principal misión de los PDC será la de mantener esta base de datos y, por tanto, se encargará de gestionar y validar todas las conexiones de los usuarios desde los equipos del dominio, permitiendo entrar a los usuarios con cuenta y denegando el acceso a los usuarios que no dispongan de una cuenta.

Los cambios en la base de datos de cuentas de usuario se hacen sobre los datos almacenados en el PDC. Cuando te conectas como administrador y empleas la herramienta para la administración de cuentas de usuario (Administrador de usuarios para dominios) no se elige un servidor, sino el dominio que se quiere administrar. Este es una de las diferencias con otros sistemas operativos en red. Por ejemplo, en NetWare cada servidor tiene sus propias cuentas, con NT varios servidores pueden emplear las mismas cuentas, todos los que formen parte del mismo dominio. El **PDC se encarga de copiar la base de datos de usuarios a todos los BDCs** (mirar apartado siguiente) de su dominio de manera periódica.

El PDC también puede ser el punto central donde se almacenen otros recursos compartidos: aplicaciones de los usuarios, impresoras, espacio en disco... Si estamos en una pequeña red, esto puede ser aceptable. Sin embargo, en dominios con varios servidores no es muy aconsejable. En esos casos, es mejor distribuir los recursos (disco, impresoras) en otros servidores pertenecientes al dominio.

En el caso de la red de nuestra escuela el PDC es Othello.

Controlador secundario de dominio (BDC)

Si tenemos un dominio formado solamente por un PDC y varias estaciones, el dominio dependería en exceso de la disponibilidad del controlador primario. ¿Qué pasaría, si por cualquier motivo, el PDC dejará de funcionar? ¿Podrían los usuarios seguir entrando desde las estaciones conectadas al dominio? La respuesta es evidente, si el elemento que valida los login (entradas al sistema) de los usuarios es el PDC y éste deja de funcionar, automáticamente ningún usuario podría conectarse al dominio desde su estación de trabajo. Para salvar esa posible eventualidad es para lo que sirven los BDCs, es decir, su misión es permitir el acceso al dominio a los usuarios del mismo siempre que por cualquier causa el PDC deje de funcionar.

Para cumplir este objetivo, cada BDC (**Backup Domain Controller**) contiene una copia de la base de datos de las cuentas de los usuarios (SAM). Mientras en un dominio puede haber un solo PDC, BDCs puede haber varios, tantos como se quieran. Tienen una misión de respaldo, si el PDC del dominio no está activo, los usuarios podrán entrar en el sistema gracias a un BDC, siempre y cuando alguno de ellos esté funcionando. Es recomendable tener al menos un BDC, ya que en caso de un fallo en el PDC se pueden seguir validando los login de los usuarios. A través de los BDC se consigue que nuestro dominio tolere fallos en el PDC sin resentirse. Es fundamental que estos sistemas sean capaces de sobreponerse a cualquier error que se produzca, proporcionando mecanismos que hagan que los usuarios no vean entorpecido su trabajo por esos errores.

Cuando el PDC no está activo se puede seguir entrando al sistema, pero no se pueden modificar las cuentas de usuario ya que las bases de datos de usuarios de los BDC son de **solo lectura**. Un BDC puede cambiarse para que actúe como PDC, ese proceso se llama **promoción**, ya que el BDC sube de categoría y se convierte en PDC. Cuando el PDC "vuelva a la vida" se habrá convertido en un BDC. La promoción de un BDC (solamente se puede promocionar uno de los BDCs) se suele realizar cuando el PDC no está activo y necesitamos crear un cuenta de usuario o dar de alta un equipo dentro del dominio. Recordemos que la base de datos de los BDC es de solo lectura, y en cualquiera de las dos tareas antes citadas necesitaríamos escribir en la base de datos (SAM) del dominio. Tiene sentido realizar la promoción cuando la avería en el PDC es importante.

En redes pequeñas, de pocos usuarios, no es absolutamente esencial, pero es una buena idea contar con un BDC. Si sólo está el PDC, toda la red se vendrá abajo si ese servidor no está disponible. Para que un ordenador actúe como PDC o BDC debe utilizar como sistema operativo Windows NT Server. Al instalar NT Server se elige si se quiere que el servidor actúe como PDC, BDC o servidor sin más.

Los BDC podrán contener, además, recursos o copias de recursos críticos contenidos en otros servidores, aunque ya decimos que en redes grandes hay que tratar de distribuir las tareas (validación de entradas, servidores de respaldo, servidores de ficheros o impresoras) entre los servidores con que cuente nuestro dominio.

En nuestra dominio de Informatica, el BDC es Shamal.

Servidores

Todos los servidores de un dominio no tienen porque ser PDC ó BDC. Un servidor puede no ser ninguna de las dos cosas. Es muy normal tener un dominio con un PDC, un BDC y otros servidores para almacenar ficheros y compartir impresoras. A estos servidores se les denomina servidores miembro o simplemente servidores. Obviamente necesitan tener instalado una copia de Windows NT Server e indicar que se desea que el equipo trabaje como servidor solamente.

Hay que indicar que estos servidores disponen también de su propia base de datos de usuarios, su SAM. Esto es así, ya que cuando un usuario se conecta desde estos equipos puede elegir a donde quiere conectarse, bien al dominio del que forma parte el servidor, o bien a ese servidor localmente. En el segundo caso el usuario solamente podrá acceder a los recursos locales de ese servidor. El acceso a los recursos del dominio no sería de forma directa[1]. De todas formas, si se incluye un servidor dentro de un dominio, es para usar las cuentas de usuario de todo el dominio, por lo que no tiene sentido definir cuentas de usuario locales (salvo las imprescindibles).

Estaciones de trabajo

Los usuarios del sistema no trabajarán desde ninguno del los equipos indicados anteriormente. Dado que los requerimientos de su trabajo son mucho menores y que además disponen de los recursos proporcionados por los servidores del dominio, es habitual que a los puestos de trabajo de los usuarios se les asignen equipos con menos recursos. Al ser equipos peores, trabajan con sistemas operativos más simples.

Los dominios NT vienen preparados con los protocolos adecuados para soportar diversos tipos de clientes o estaciones: MS-DOS, Windows para Trabajo en Grupo, OS/2, Windows 95/98, Windows NT Workstation, UNIX y Macintosh OS. El que más se suele emplear es Windows 95/98, ya que tiene unos requerimientos menores que los de NT Workstation. Las estaciones con NT Workstation, Windows 95/98 y Windows 3.11 para trabajo en grupo pueden configurarse para participar en un dominio o en un grupo de trabajo. Al configurar una estación para su funcionamiento en red hay que indicar **un nombre para el equipo** y el **nombre del dominio** o grupo de trabajo en el que va a participar. Si el nombre coincide con el nombre de un dominio, el equipo aparecerá en la lista de examen del dominio cuando vemos nuestro Entorno de Red. Para determinar si el equipo participará de un dominio o

[1] Esto es una verdad a medias. En el caso de que el nombre de usuario y la password fueran idénticos en la cuenta del dominio y en la del servidor, el acceso sería directo. Si no es así, al intentar la conexión se le solicita al usuario su cuenta dentro del dominio y su palabra de paso.

grupo de trabajo, en la instalación se indicara si ese equipo va a iniciar la sesión en un dominio o grupo de trabajo.

En el caso de una estación con NT Workstation, sirven los mismos comentarios que se han hecho anteriormente para los servidores NT. Las estaciones NT disponen también de su propia base de datos de usuarios, su SAM. El usuario al entrar en sesión puede elegir o entrar en sesión en el dominio (con el consiguiente acceso a los recursos) o entrar en sesión localmente (con acceso solamente a los recursos locales).

¿Cómo establecer el rol de un servidor NT?

Como se ha visto en el punto anterior, un equipo con NT Server instalado puede realizar tres funciones: ser controlador primario, ser controlador secundario o, simplemente, ser un servidor del dominio sin almacenar las cuentas de usuarios del dominio y no desempeñar labores relacionadas con la seguridad del dominio. En principio, el papel de un equipo se determina durante el **proceso de instalación**. Cuando se instala NT Server, en un momento dado se nos pregunta qué papel va a ejercer el equipo. En el caso de que se configure como controlador primario, habrá que indicar el nombre del dominio, **un nombre que debe ser único,** ya que no puede ocurrir que dos dominios tengan el mismo nombre. Si se instala como controlador reserva, el proceso de instalación nos solicitará la contraseña de la cuenta Administrador (véase apartado Cuentas de Usuario), que se define durante la instalación del controlador primario. En el caso de los servidores miembro, se nos solicitará la contraseña para la cuenta Administrador de ese equipo que no tiene nada que ver con la cuenta Administrador del dominio, son diferentes. Además, el programa de instalación nos pedirá si deseamos añadir el equipo a un dominio existente o un grupo de trabajo. En el caso de la primera opción, tendremos que proporcionar una cuenta que tenga el derecho para Agregar equipos al dominio (véase apartado Derechos de Usuarios). Un cuenta con ese derecho es la cuenta de Administrador, ojo se refiere a la cuenta del dominio, no la del servidor.

Figura 1 Administrador de Servidores

Promoción de un BDC

En el caso de los PDCs y BDCs sus papeles son intercambiables y se pueden cambiar en cualquier momento. Para ello se emplea la herramienta Administrador de Servidores que se encuentra dentro del grupo Herramientas Administrativas del Menú Inicio. Con esa herramienta tenemos la posibilidad de promocionar un BDC para que se convierta en PDC (comando Promover a controlador principal de dominio, véase Figura 1). Normalmente esto se hace porque el PDC tiene algún tipo de avería y necesitamos cambiar o definir cuentas de usuario. Con la promoción el BDC se convierte en PDC y al revés[2].

[2] Después de hacer la promoción, es habitual que el Administrador de Servidores nos indique que existen dos controladores primarios, cuando realmente nuestro PDC inicial ya ejerce labores de BDC y al revés. Para evitar esa

Relaciones de confianza

Cuando se instala una red NT en una empresa, si ésta es medianamente grande, es lógico que cada departamento tenga su propio dominio, un dominio que agrupe a los usuarios de ese departamento y a los recursos que necesitan. En una red con dos o más dominios, cada dominio actúa como una red independiente, con sus propias cuentas de usuario. Pero incluso en la empresa u organización con la estructura más rígida que podamos imaginar, siempre existirán proyectos o trabajos que impliquen a gente de distintos departamentos. Esos usuarios necesitarán compartir datos, datos que se almacenarán en uno solo de los dominios de la empresa (almacenarlos en varios sitios, podría ocasionarnos problemas de duplicidad de versiones). Es decir, nos encontramos con una situación en la que un usuario de un dominio precisa de los recursos de otro dominio dentro de la organización. Evidentemente este usuario podría tener una cuenta en cada uno de los dominios. Sin embargo esta no es la mejor solución. El problema de esta idea es que los usuarios necesitan acceder a los recursos de ambos dominios simultáneamente, lo que es imposible con esta solución (bueno se puede hacer siempre que el nombre de usuario y la contraseña sea idéntica en los dos dominios). El usuario tendrá que hacer login de un dominio a otro. Esto es ineficiente y muy frustrante.

Una red lo suficientemente grande para necesitar más de un dominio tendrá muchos usuarios y muchos de ellos tendrían cuentas en más de un dominio. Cada vez que se necesite cambiar una password o modificar los permisos de acceso a unos ficheros, el administrador tendría que entrar en cada uno de los dominios y hacer esos cambios. Esta solución se convertirá en una pesadilla para el administrador.

NT proporciona un método para que un dominio permita el acceso a sus recursos a los usuarios de otro dominio. Este método son las **relaciones de confianza (trust)**. Una relación de confianza es un vínculo que combina dos dominios para formar una unidad administrativa por la que los usuarios de un dominio pueden acceder a los recursos de otro dominio. Es decir, un dominio aporta los recursos y el otro los usuarios.

Se dice que un **dominio A confía en otro B**, o que hay establecida una relación de confianza desde A hacia B, cuando cualquier usuario perteneciente en el dominio B puede entrar sin más en el dominio A.

Existen dos tipos de relaciones de confianza: unidireccionales y bidireccionales.

Relación de confianza unidireccional

En una relación de confianza unidireccional un dominio confía en los usuarios del otro dominio, permitiéndoles utilizar sus recursos. Más específicamente, un dominio confía en que los controladores del otro domino (PDC o BDC) validen las cuentas de usuario para que utilicen sus recursos. Los recursos que pasan a estar disponibles se encuentran en el dominio "que confía" y las cuentas de usuario que pueden usarlos se encuentran en el dominio "en el que se confía".

Como Pepe tiene cuenta en el dominio Marketing y Medios de Pago confía en Marketing. Pepe podrá acceder al dominio Medios de Pago. Eso no quiere decir que tenga acceso automático a los recursos de Medios de Pago. El administrador de este dominio tendrá que darle esos permisos dentro del dominio Medios de Pago.

Por otra parte, los usuarios de Medios de Pago no tendrán acceso al dominio Marketing. Para permitir esto tendríamos que establecer una relación de confianza bidireccional.

Relación de confianza bidireccional

Las relaciones de confianza bidireccionales se aproximan más a las necesidades de los usuarios. Es una configuración más flexible y hace la administración de la red más simple. En una relación de confianza bidireccional un usuario que puede acceder a cualquiera de los dominios tendrá acceso al otro. Las relaciones bidireccionales se crean mediante dos

---

anomalía visual, hay que Degradar el PDC, seleccionándolo y utilizando un comando proporcionado en la misma herramienta.

relaciones unidireccionales, una en cada dirección. Medios de Pago confía en Marketing y Marketing en Medios de Pago.

La mayor ventaja de las relaciones bidireccionales es que las cuentas de usuario se crean sólo una vez, en el dominio al que pertenece al usuario. Ese usuario podrá acceder al resto de dominios de la empresa si entre ellos se establecen relaciones bidireccionales. Esto hace la administración de la red más simple pero complica su control.

Con las relaciones de confianza no se cumple la propiedad transitiva. El departamento de Bolsa confía en el de Medios de Pago y éste en el de Marketing. Ello no implica que el dominio de Bolsa confíe en el de Marketing. Es decir, cada relación de confianza que se desee se debe establecer separadamente. Si se desea que un usuario del dominio Bolsa acceda al dominio Marketing se debe establecer esa relación entre ambos dominios.

Establecer una relación de confianza

Para hacer relaciones de confianza entre dominios se emplea el Administrador de Usuarios para dominios. Cada relación de confianza unidireccional consta de dos pasos: primero el dominio en el que se va a confiar permite al otro confiar en él y después este último confía. La ventana donde se realizan cuenta con dos listas, la de arriba para indicar los dominios en los que confiamos y la de abajo, los dominios a los que permitimos confiar en nosotros.

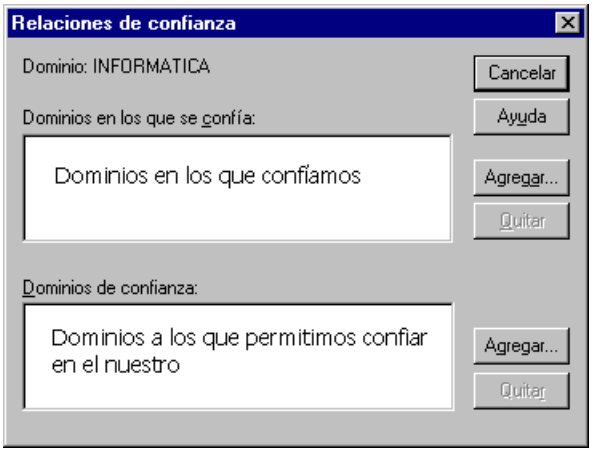

Figura 2 Relaciones de confianza

Supongamos que queremos establecer una relación de confianza de forma que el dominio INFORMATICA confíe en el dominio AIC. Lo primero que hay que hacer es irnos al dominio AIC e incluir el dominio de INFORMATICA dentro del grupo de dominios a los que permitimos confiar en AIC. Para ello se pulsa sobre el botón de Agregar inferior. Nos aparece la ventana de la Figura 3, donde tenemos que indicar el nombre del dominio al que vamos a dejar confiar (INFORMATICA) y una contraseña. Esta contraseña no tiene nada que ver con la del Administrador y sólo se utiliza para establecer la relación definitivamente desde INFORMATICA.

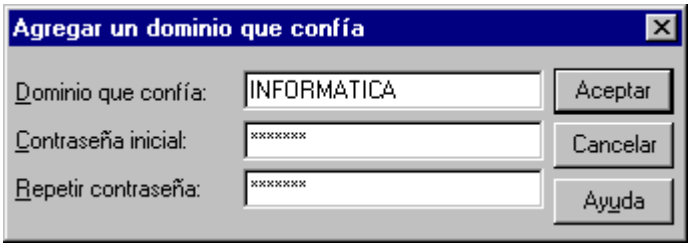

Figura 3 Permitir a un dominio confiar

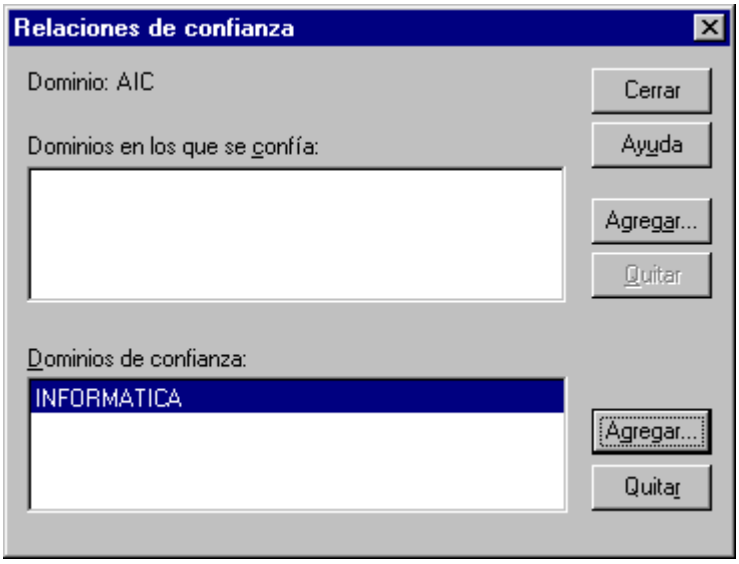

Figura 4 El dominio INFORMATICA puede confiar en AIC

Como se puede ver, el dominio INFORMATICA se ha añadido a los dominios a los que permitimos confiar en AIC. Ahora falta por hacer el segundo paso. Nos vamos al dominio de INFORMATICA e indicamos que queremos confiar en AIC. Para ello, pulsamos el botón Agregar superior (ojo, estamos en el dominio INFORMATICA no en el de AIC) y aparecerá la ventana de la Figura 5. En esa ventana tendremos que introducir el dominio en que queremos confiar (AIC) y la contraseña para establecer la relación, esto es, la que se metió en el dominio AIC en el paso anterior.

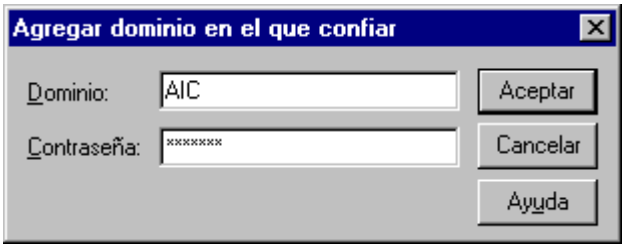

Figura 5 Introducimos la contraseña para confiar en AIC

El sistema nos indicará que la relación se ha establecido con éxito y veremos aparecer el dominio AIC entre los dominios en los que confía INFORMATICA (Figura 6).

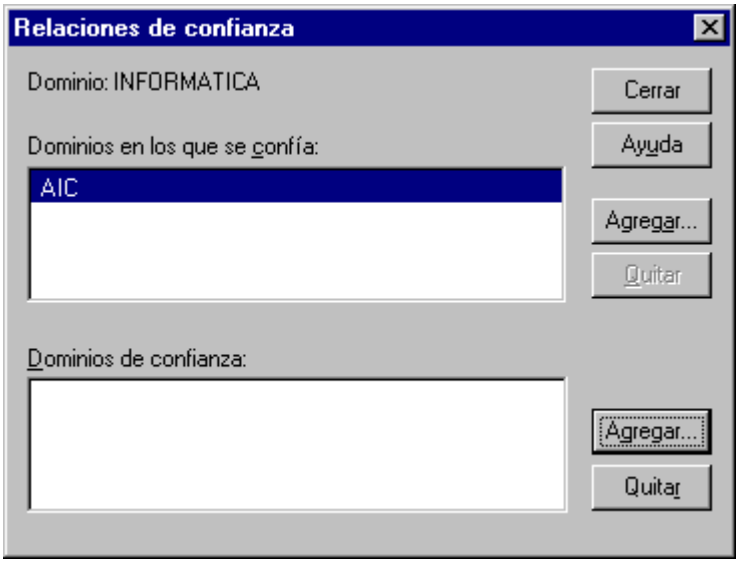

Figura 6 INFORMATICA confía en AIC

Si la relación fuera bidireccional habría que repetir los mismos pasos pero a la inversa. Como se ha dicho en párrafos anteriores, una relación bidireccional está formada por dos unidireccionales establecidas independientemente.

Modelos de dominio

Siempre que se establece una nueva red es necesario realizar una planificación previa. La principal estrategia que hay que decidir es el tipo de modelo de dominio que se va a seguir. Por modelo de dominio se entiende la forma en la que los equipos de nuestra organización se agruparán, esto es, en cuantos dominios dividiremos nuestra red y cual será la relación entre esos dominios. Existen cuatro modelos de dominio distintos que se pueden emplear:

- Modelo de dominio único
- Modelo de dominio maestro único
- Modelo de dominio maestro múltiple
- Modelo de dominio maestro múltiple con confianza total

Modelo de dominio único

Es el modelo de dominio más simple. La red sólo tiene un dominio. Todos los servidores y las estaciones pertenecen a ese dominio único. En el se crean todos los usuarios y grupos globales. Al haber un solo dominio no hay relaciones de confianza. Todos los administradores podrán controlar todos los servidores. Al dividir la red en dominios se permite tener administradores que sólo puedan controlar algunos de los servidores, por ejemplo los de su departamento.

El modelo de dominio único es aceptable cuando no existen muchos recursos o usuarios. ¿Cuántos son muchos? Difícil de contestar. No se debe emplear este modelo cuando:

- Existen distintos grupos de usuarios que acceden a distintos recursos.
- La empresa va a incluir otro edificio o localización separada.
- La búsqueda de los recursos en la red consumen demasiado tiempo.

Ventajas	Inconvenientes
Administración simple	No existen grupos por departamentos
Control central de las cuentas de usuario	El rendimiento decrece al aumentar los recursos
No hay relaciones de confianza	Las búsquedas se hacen más lentas al aumentar el número de servidores
Los grupos locales se definen una vez	No existen grupos lógicos de recursos

Tabla 1 Ventajas e inconvenientes del Modelo de Dominio Único

Modelo de dominio maestro único

Si el número de recursos es excesivo en un dominio único quizá deberíamos pensar en utilizar un dominio maestro. Este tipo de estructura proporciona administración central de usuarios junto con una agrupación lógica de los recursos departamentales. En este modelo se incluye un dominio por cada departamento (dominio secundario). Los dominios secundarios tendrán una relación de confianza unidireccional respecto del dominio maestro. El dominio maestro actúa como unidad administrativa central para las cuentas de usuario y de grupo. Todos los dominios secundarios confían en el dominio maestro, es decir, reconoce los usuarios y grupos globales definidos en él. Cada dominio secundario tendrá definidos sus grupos locales.

Dado que el domino maestro realiza las tareas de administración central es necesario que disponga de un BDC. La idea consiste en definir en él todas las cuentas de usuario, cuentas

que después se emplearán desde los dominios secundarios. En estos últimos se distribuirán los recursos, que serán accesibles desde toda la red y administrados localmente. Los usuarios de los dominios secundarios verán inicialmente los recursos de su dominio simplificándose su búsqueda.

Suele ser normal pasar de un modelo de dominio único a uno de dominio maestro único. El original dominio único pasa a ser dominio maestro y los recursos se distribuyen entre los demás dominios.

En resumen, tendremos una administración centralizada de las cuentas y una administración descentralizada de los recursos. Se emplea cuando es necesario dividir la red en dominios por motivos organizativos y el número de usuarios y grupos es pequeño.

Ventajas	Inconvenientes
Control central de las cuentas de usuario	Rendimiento decrece al aumentar el número de usuarios y grupos
Grupos globales sólo se definen una vez	Punto central de fallos
Administración de recursos a nivel de departamento	Es necesario definir grupos locales en cada dominio secundario
Sólo se precisa una relación de confianza por cada dominio secundario	

Tabla 2 Ventajas e inconvenientes del Modelo de Dominio Maestro Único

Modelo de dominio maestro múltiple

Se emplea cuando el número de usuarios hace que el modelo de dominio maestro único no ofrezca un buen rendimiento pero se desea seguir manteniendo un control centralizado de las cuentas de usuario y descentralizado de los recursos. Ideal para una organización con muchos usuarios y estructura administrativa centralizada. Proporciona administración central a través de dos o más dominios y los recursos distribuidos a través de dominios secundarios.

Todos los dominios maestros mantienen relaciones de confianza bidireccionales. Las cuentas de usuario estarán distribuidas entre ellos. Cada usuario sólo tendrá cuenta en un dominio maestro. Cada dominio secundario confía en todos los dominios maestros. Los recursos, como ficheros e impresoras, se proporcionan y administran a nivel de dominio secundario.

Habrá que decidir como se distribuirán las cuentas de usuario a través de los dominios maestros. Se pueden distribuir por grupos lógicos de usuarios o por criterios arbitrarios (pe. alfabético). Los usuarios tendrán que iniciar la sesión en el dominio que contiene su cuenta. Los dominios maestros tendrán que tener un PDC y un BDC.

Ventajas	Inconvenientes
Control central de las cuentas de usuario.	No existe un punto central de administración.
Administración de recursos a nivel de departamento.	Necesario definir los grupos globales y locales más de una vez y hay que modificarlos en más de un sitio.
Fácilmente escalable.	Se amplían las relaciones de confianza.
Agrupación lógica de los recursos.	

Tabla 3 Ventajas e inconvenientes del Modelo de Dominio Maestro Múltiple

Modelo de dominio con confianza total

Tiene sentido si se prefiere una administración distribuida tanto de recursos como de usuarios. Cada dominio tiene establecida una relación de confianza bidireccional con todos los demás. El número de relaciones de confianza que hay que establecer para N dominios será de N*(N-1). Personalmente me parece un poco caótica.

Ventajas	Inconvenientes
Fácilmente escalable.	No existe administración central de usuarios y grupos.
	Muy complejas relaciones de confianza.
	Necesarios definir los grupos locales y globales más de una vez y se modifican en más de un sitio.

Tabla 4 Ventajas e inconvenientes del Modelo de Dominio con confianza total