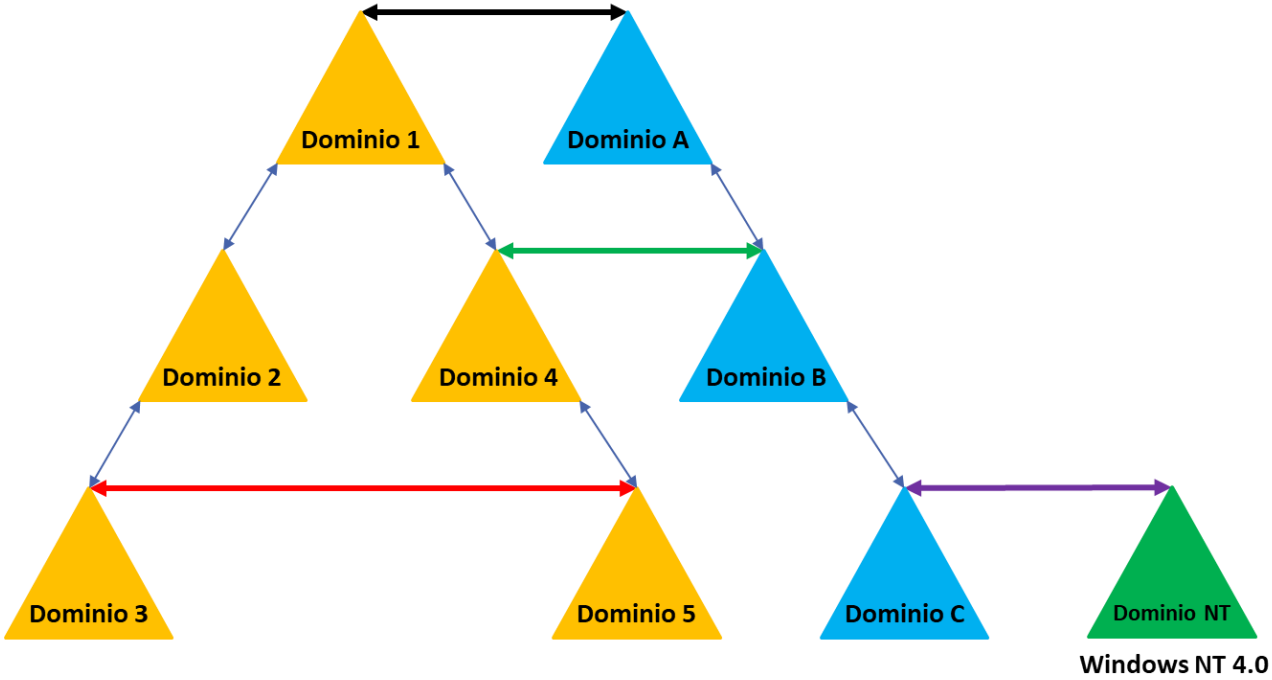
UD03
Relaciones de confianza



Índice

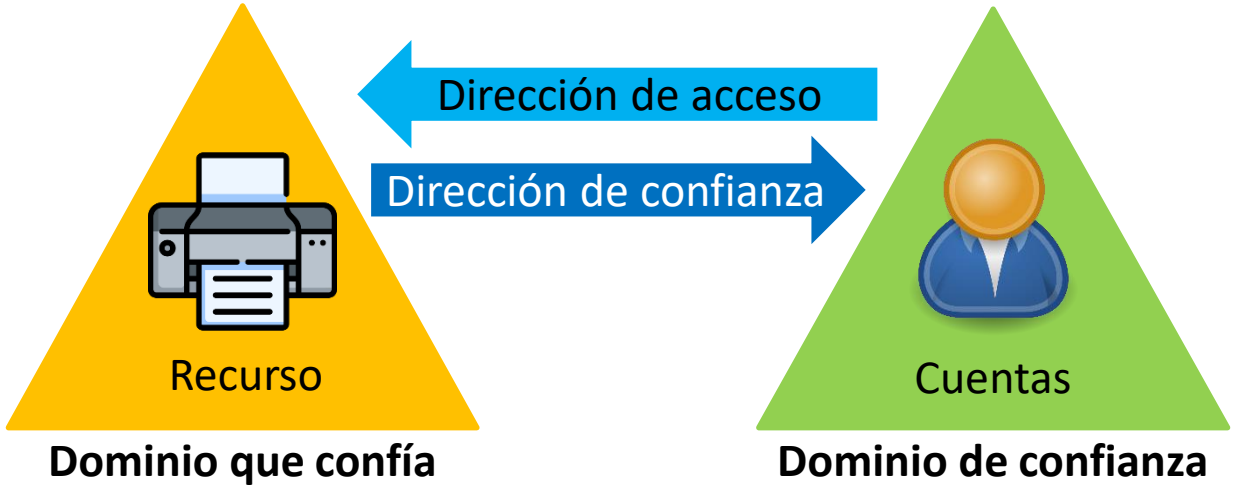
Introducción

Introducción

- Una **Relación de Confianza** es un **característica de Active Directory** que facilita a los usuarios de un Dominio tener **acceso a los recursos de un dominio diferente**, es decir, **un usuario se autentica en un Dominio y puede acceder a los recursos de otro Dominio**.

Introducción

- **Distinguimos**:
  - **Dominio que confía**: aquel que ofrece ciertos recursos.
  - **Dominio de confianza** o en el que se confía: aquel en el que se autentica un usuario que utilizará los recursos del Dominio que confía.

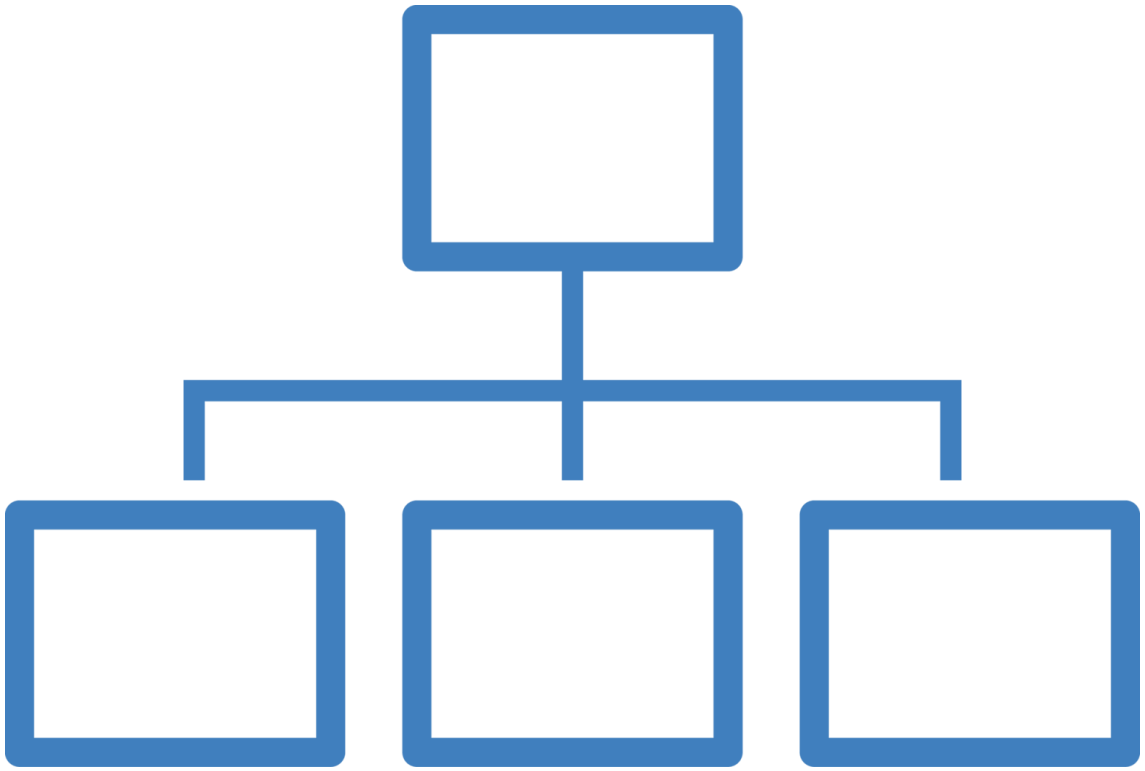


- Por tanto, las **Relaciones de Confianza son un método de comunicación seguro entre dominios, árboles y bosques** en Active Directory.

Introducción

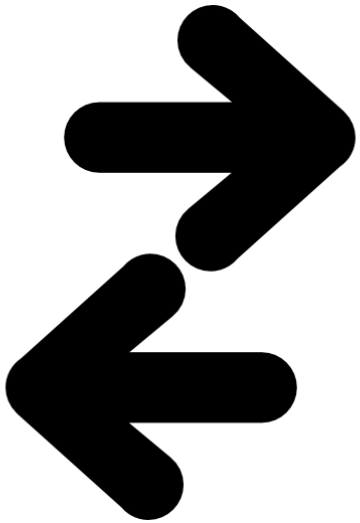
- Al **crear una Relación de Confianza**, habrá que **configurar ambos lados** de la relación, por lo que habrá que disponer de **credenciales válidas** en **ambos Dominios**. Para ello podemos emplear la herramienta "**Dominios y confianza de Active Directory**".
- Este trabajo se **puede hacer de forma independiente**, ejecutando el **Asistente** para nueva confianza **en los dos Dominios** (el que confía y el de confianza), o hacerlo de forma **simultánea**, con lo que ejecutaremos el **Asistente** para nueva confianza **sólo en uno de los dominios**.
- Si lo hacemos de forma **simultánea**, se creará automáticamente una **contraseña de confianza segura**.
- Si lo hacemos por **separado** deberemos asegurarnos de **incluir la misma contraseña de confianza en ambos lados** de la relación.

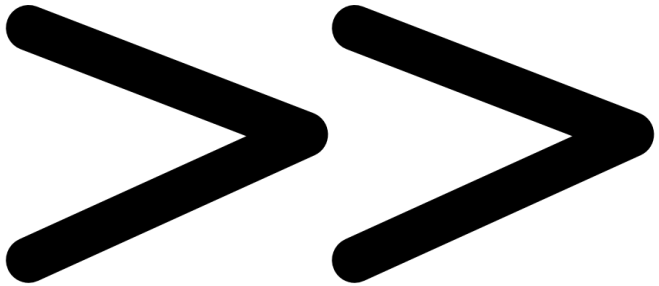
Tipos de relaciones de confianza



Tipos de relaciones de confianza

- Existen **dos criterios para clasificar las relaciones de confianza:**
  - **Direccionalidad.**
  - **Transitividad.**



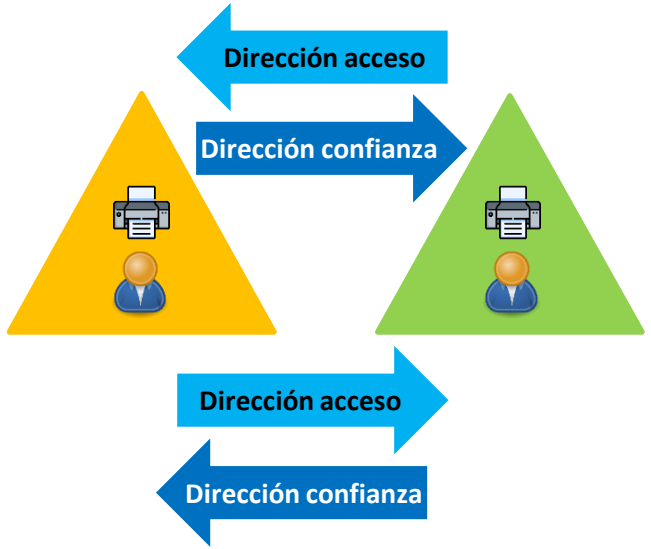


Tipos de relaciones de confianza
Direccionalidad

- En relación a la **direccionalidad**, existen **dos tipos** de Relaciones de Confianza:
  - **Unidireccionales**: entre Dominio A (que confía) y dominio B (de confianza), los **usuarios** que se autentiquen en **dominio B** podrán tener **acceso** a recursos del **dominio B**, pero **NO al revés**.
  - **Bidireccionales**: ambos dominios **confían el uno en el otro**.

Unidireccional

Bidireccional



Tipos de relaciones de confianza

Transitividad

- La **transitividad establece** si una **relación** de confianza se puede **extender más allá** de los dos dominios entre los que se **estableció inicialmente**.
- En relación a la **transitividad**, existen **dos tipos** de Relaciones de Confianza:
  - **Transitivas.**
  - **No transitivas**.

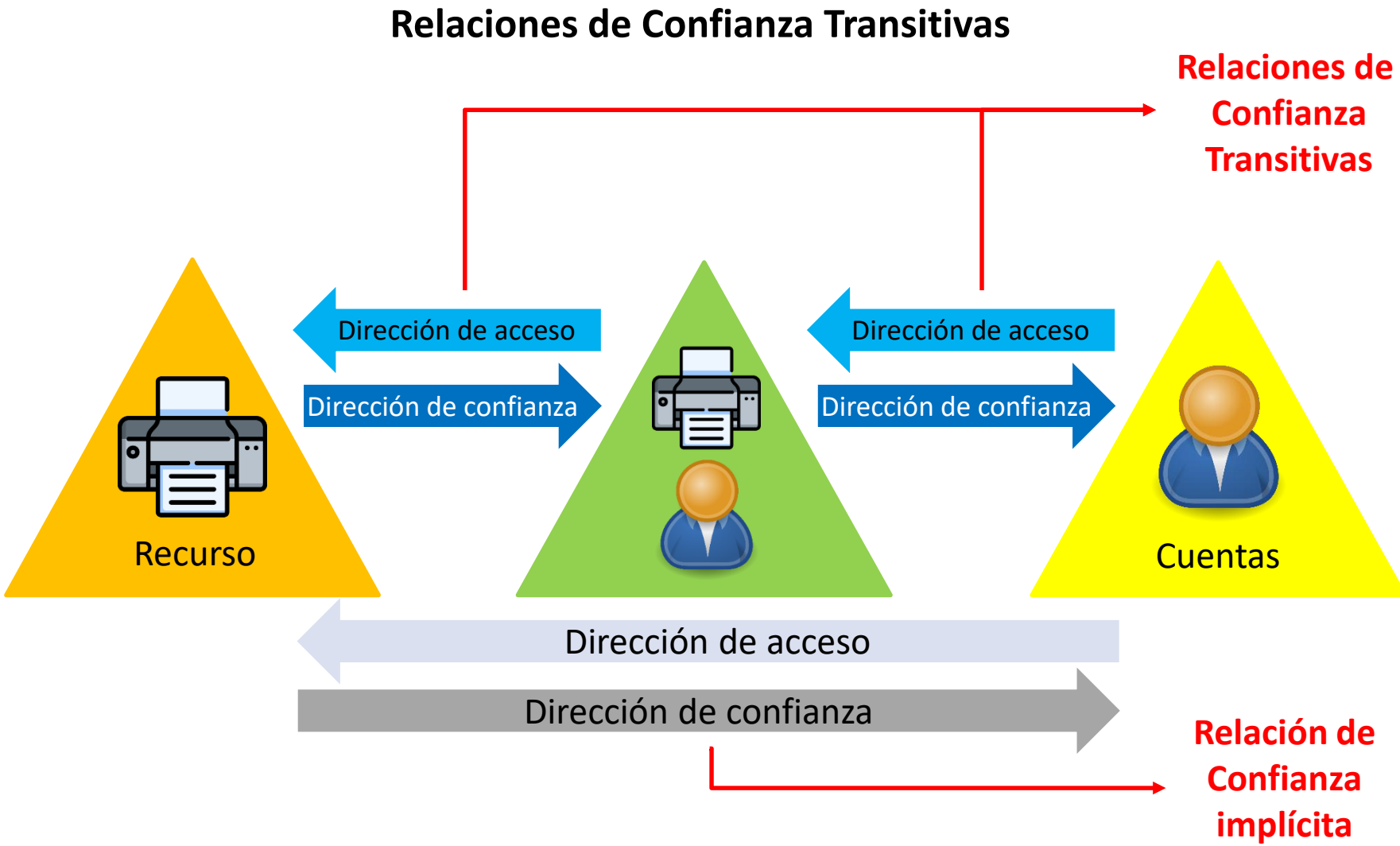
Tipos de relaciones de confianza

Transitividad

- **Transitivas:**
  - Dominio A confía en dominio B y dominio B confía en dominio C, entonces **dominio A confía en dominio C**, y **usuarios** que se autentiquen en **dominio C** podrán **acceder** a **recursos en A**.
  - Si establecemos una **confianza transitiva**, ésta podrá **extenderse a otros dominio**.
  - Estas relaciones de confianza **se amplían de forma automática** cuando se incluya un **nuevo Dominio** en el árbol.
  - Pueden ser **unidireccionales o bidireccionales**.

Tipos de relaciones de confianza

Transitividad

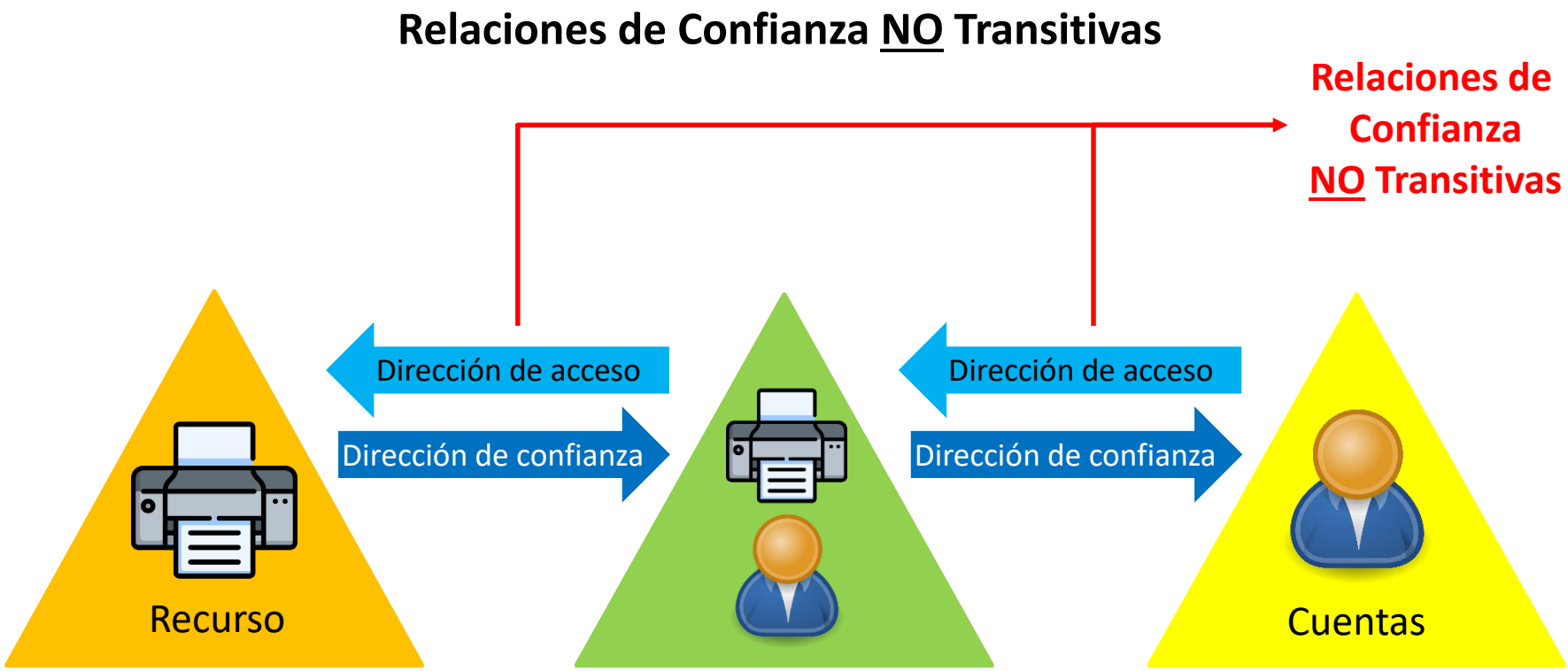


Tipos de relaciones de confianza
Transitividad

- **No transitivas**:
  - Dominio A confía en domino B y dominio B confía en dominio C, pero **dominio A NO confía en dominio C**.
  - Si establecemos una **confianza no transitiva** se verá reducida **únicamente** a los **dominios implicados inicialmente** en la relación (A y B por un lado, B y C por otro lado).
  - Estas relaciones de confianza **no se amplían de forma automática** cuando se incluya un **nuevo Dominio** en el árbol, como sí ocurre con las confianzas transitivas.
  - Las Relación de Confianza no Transitiva es **unidireccional**. Sin embargo, se puede **crear** una Relación de Confianza no Transitiva **bidireccional** a partir de **dos relaciones de confianza unidireccionales**, una en cada sentido de la relación.

Tipos de relaciones de confianza

Transitividad

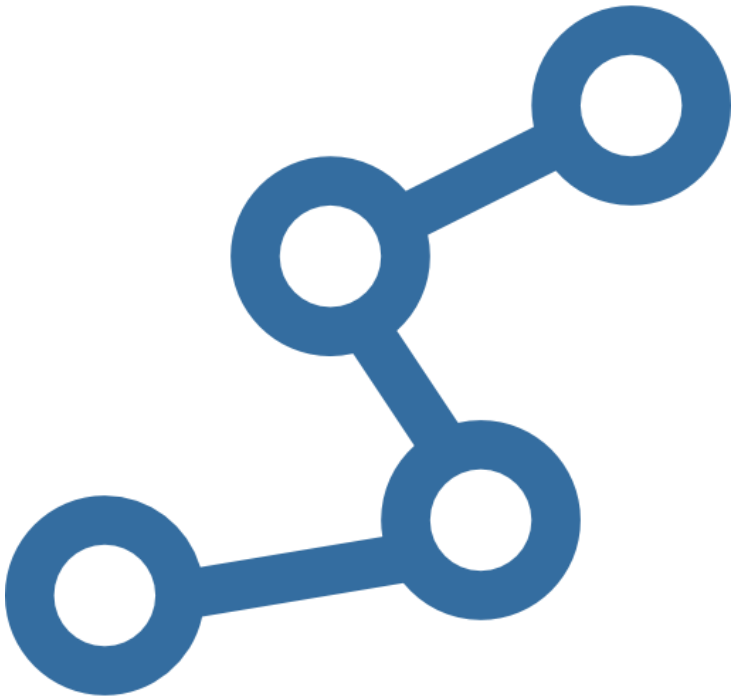


Tipos de relaciones de confianza

Transitividad

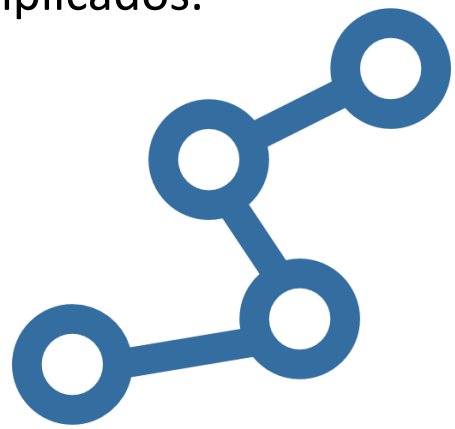
- A **partir de Windows 2000 Server**, para **autenticar** a los **usuarios** se utiliza el protocolo **Kerberos V5, que permite** establecer **relaciones bidireccionales y transitivas**.

Ruta de confianza



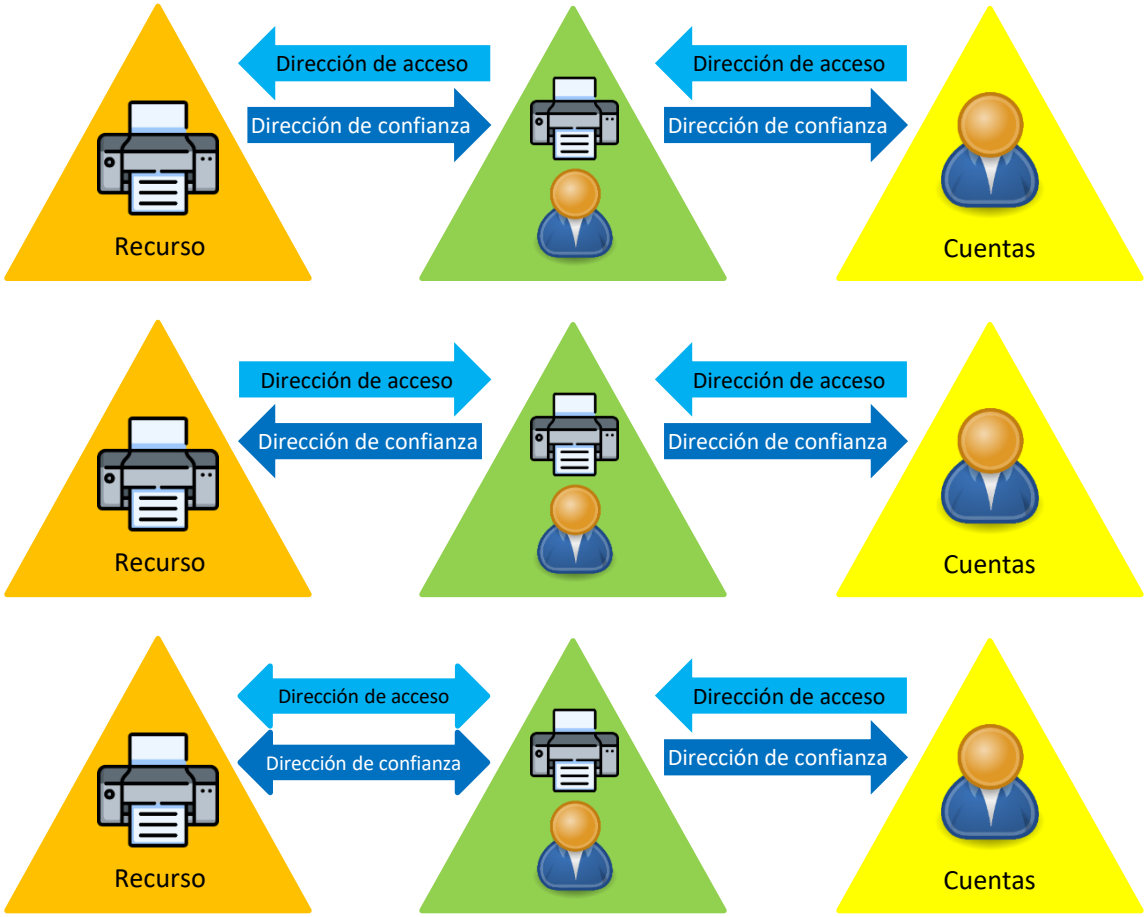
Ruta de confianza

- **Antes** de que un **usuario de un dominio** pueda **utilizar** los **recursos** de **otro dominio,** el sistema de seguridad debe:
  - **Determinar** si el **dominio que confía** (es decir, el que ofrece el recurso) **tiene una relación con el dominio de confianza**, que debe ser el dominio donde el usuario se ha autenticado.
  - **Calcular la ruta de acceso de confianza**, es decir, la ruta de relaciones de confianza **que seguirán las solicitudes de autenticación entre los dominios** implicados.



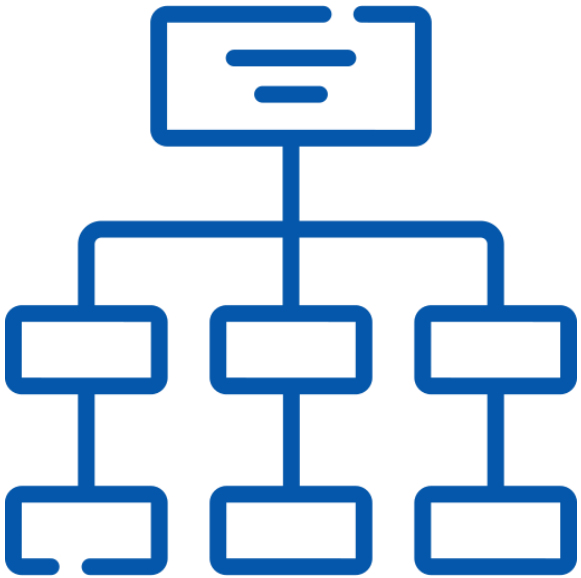
Ruta de confianza

- Para **establecer la ruta** de acceso de confianza, es **imprescindible tener en cuenta la direccionalidad** de cada relación de confianza implicada.



¿Cuál es la ruta de confianza en cada caso?

Relaciones de confianza en Windows Server

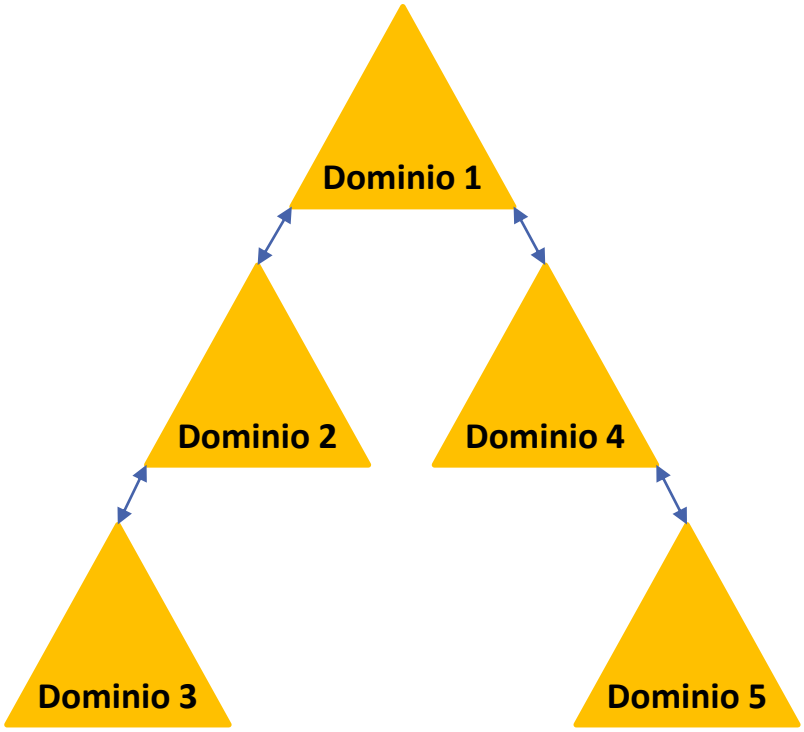


Windows Server

Relaciones de confianza en Windows Server

A partir de **Windows 2000 Server:**

- Cuando creamos un **nuevo Dominio** en un Bosque existente, automáticamente se establece una **Relación de Confianza bidireccional y transitiva** entre el Dominio nuevo y su Dominio padre.



Relaciones **transitivas bidireccionales** creadas automáticamente al crear nuevos dominios en un árbol.

Relaciones de confianza en Windows Server

- Permite **expandir la estructura jerárquica** de Dominios **sin tener que configurar** Relaciones de Confianza **con los otros Dominios** existentes.
- Cualquier **usuario** podrá disponer de una **cuenta en cualquier dominio** del bosque y **autentificarse en cualquier otro**, pudiendo **acceder** desde ahí a cualquier **recurso** sobre el **que tenga permisos** y que esté **compartido en cualquier otro dominio del bosque**.
- En **Windows Server**, **además** de las relaciones **transitivas bidireccionales** que se crean automáticamente al incorporar un **nuevo dominio**, podemos **crear manualmente otras relaciones de confianza**, que vemos a continuación.

Relaciones de confianza en Windows Server

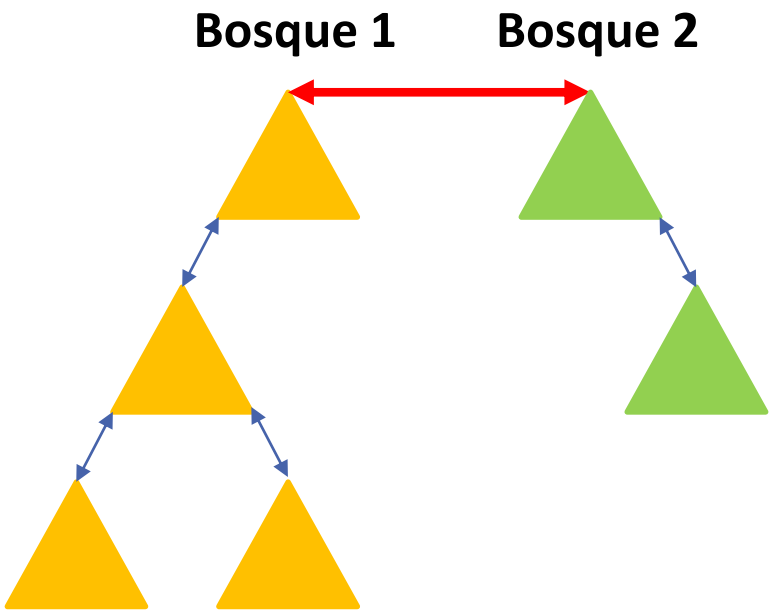
Tipos de relaciones en Windows Server

- **Se distinguen cuatro relaciones de confianza** diferentes que podemos crear **manualmente** utilizando el **Asistente para nueva confianza** o la orden Netdom:
  - Confianza **de bosque**.
  - Confianza **directa**.
  - Confianza **externa**.
  - Confianza **de dominio kerberos**.

Relaciones de confianza en Windows Server

Tipos de relaciones en Windows Server. Confianza de bosque

- **Confianza de bosque**:
  - Se establece **entre los nodos raíz** de dos **bosques**.
  - Permiten **compartir recursos** entre diferentes **bosques**.
  - **Siempre** son **transitivas.**
  - Pueden ser tanto **unidireccionales como bidireccionales**.
  - En el caso de ser **bidireccionales**, las solicitudes de **autenticación** pueden llegar **desde un bosque a otro, y viceversa**.



¿Qué implica que **siempre** sean transitivas?

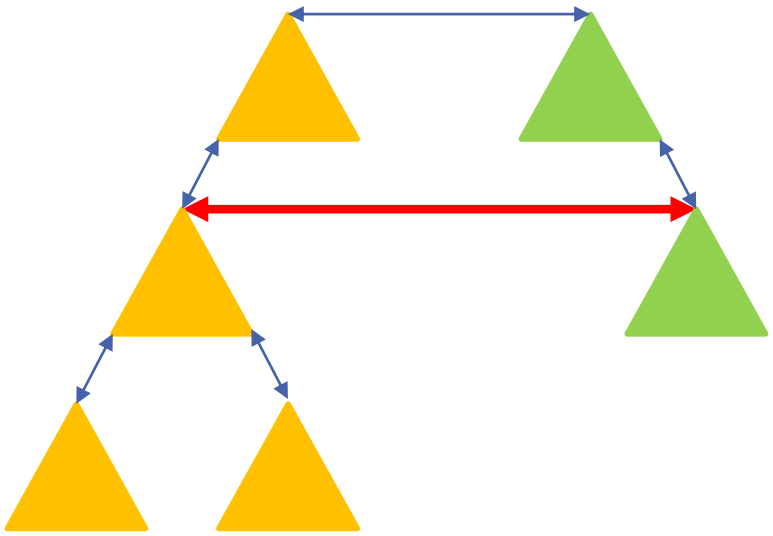
- Permiten el acceso entre los distintos dominios de ambos bosques.
- En caso contrario, sólo se permitiría el acceso a recursos entre los dominios raíz de ambos bosques.

Relaciones de confianza en Windows Server

Tipos de relaciones en Windows Server. Confianza directa

- **Confianza directa**:
  - Entre **dos dominios de árboles distintos en un mismo bosque**, para **abreviar la ruta** de acceso de confianza entre ellos.
  - **Mejora el tiempo** que necesitan los usuarios para **iniciar sesión entre dichos dominios.**
  - **Siempre** son **transitivas.**
  - Pueden ser tanto **unidireccionales como bidireccionales**.

Bosque



¿Qué implica que **siempre** sean transitivas?

- Misma respuesta que anteriormente.

¿Por qué entre árboles distintos?

- Porque dentro de un mismo árbol se respeta la jerarquía padre e hijo (*)

(*) Depende de tipo de Directorio.

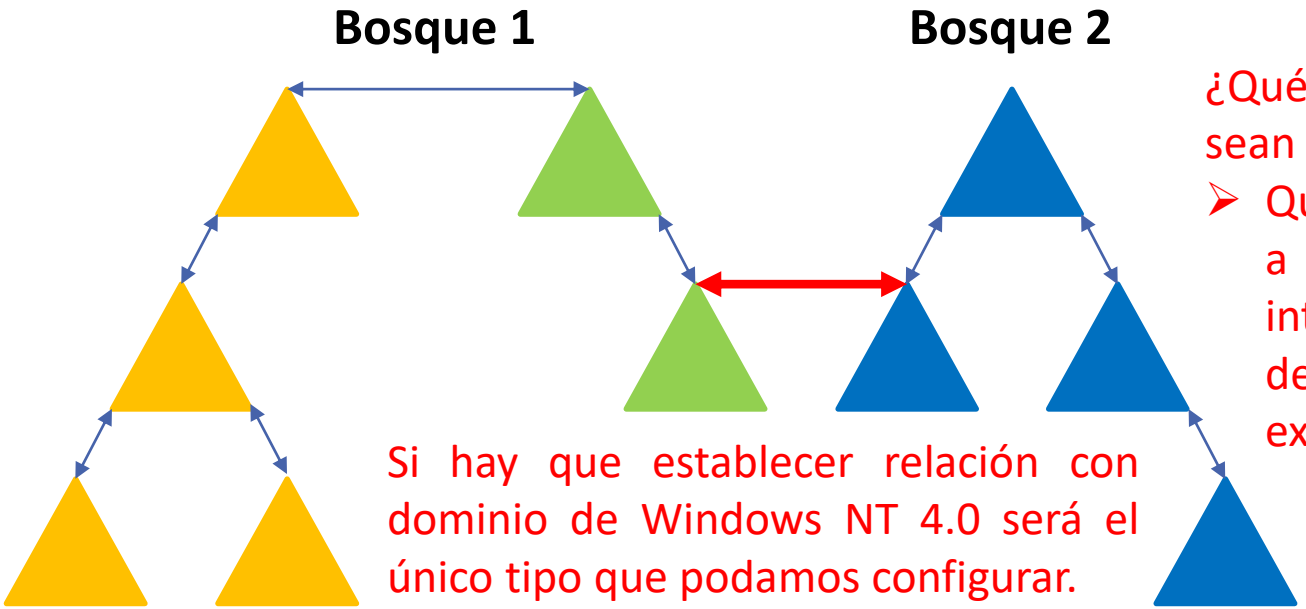
¿Por qué dentro de un mismo bosque?

- Porque si es entre dominios de distintos bosque es otro tipo de relación denominada Externa.

Relaciones de confianza en Windows Server

Tipos de relaciones en Windows Server. Confianza externa

- **Confianza externa**:
  - Facilita el **acceso a recursos** pertenecientes a un **dominio Windows NT 4.0 o** a dominios de **bosques diferentes sin confianza de bosque**.
  - **También con confianza de bosque para reducir tiempo inicio sesión** entre dominios de distintos bosques. **Útil** si este inicio es **habitual**
  - **Siempre** son **NO transitivas**.
  - Pueden ser tanto **unidireccionales como bidireccionales**.



Si hay que establecer relación con dominio de Windows NT 4.0 será el único tipo que podamos configurar.

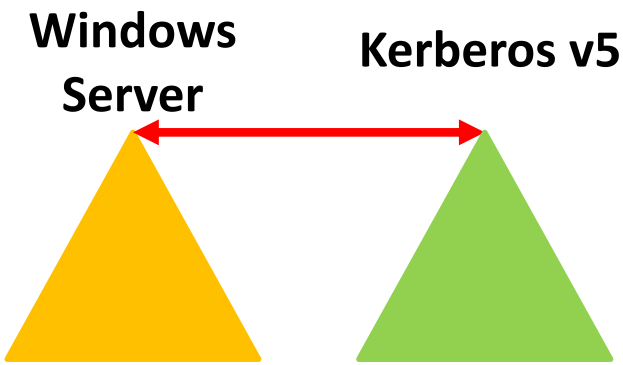
¿Qué implica que **siempre** sean no transitivas?

- Que la relación se reduce a los dos dominios que intervienen en la relación de confianza. No se extiende por los árboles.

Relaciones de confianza en Windows Server

Tipos de relaciones en Windows Server. Confianza Kerberos

- **Confianza de dominio kerberos**:
  - Permiten establecer relaciones de confianza **entre dominios Windows Server** (Active Directory) y dominios que **no sean Windows Server**, pero utilicen el protocolo **kerberos v5** (eDirectory, Unix Directory, …)
  - Pueden ser **relaciones transitivas o no transitivas.**
  - Pueden ser tanto **unidireccionales como bidireccionales**.



Relaciones de confianza en Windows Server

Resumen

Resumen tipos de confianza Windows Server 2019:

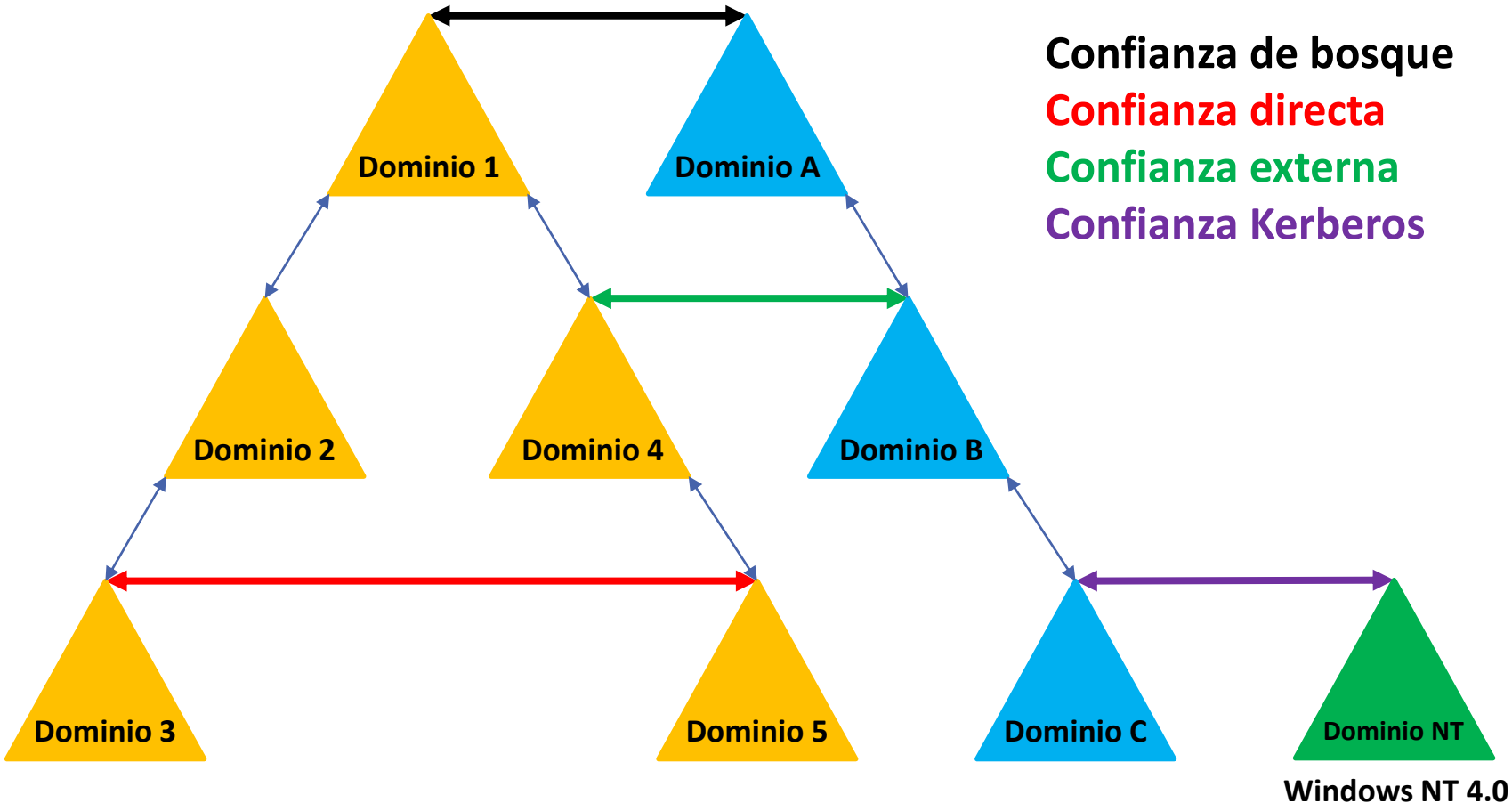
Tipo	Participantes	Transitivas	No Transitivas	Direccionales	Bidireccionales
Bosque	-Entre bosques.	X		X	X
Directa	-Entre dominios de árboles distintos de un bosque.	X		X	X
Externa	-Con bosques Windows NT 4.0. -Entre bosques sin relación de confianza de bosque.		X	X	X
Kerberos	-Con dominios NO Windows Server pero que utilizan protocolo Kerberos V5.	X	X	X	X

¿**Con qué dominios puede establecer relaciones** de confianza Windows Server 2019?

- **Dominios de Windows Server** 2019, 2016, 2012 R2, 2012, 2008, 2008 R2 o 2003 **(dentro del mismos bosque o con otro bosque).**
- Dominios de **Windows NT 4.0**
- Dominios **Kerberos V5**

Relaciones de confianza en Windows Server

Resumen



Objetos del dominio de confianza

Objetos del dominio de confianza

- Cada **relación de confianza** de un dominio se **representa** con un **Objeto de Dominio de Confianza** (TDO, Trusted Domain Object).
- Por lo tanto, cada vez que **se crea una nueva relación**, **se crea un nuevo TDO único** con todos sus **atributos** y se **almacena** en el **contenedor System del dominio**.
- Como mínimo, los **atributos** incluidos en un **TDO** son:
  - La **transitividad.**
  - La **direccionalidad** de la confianza.
  - El **nombre de los dominios** recíprocos.