

CUENTAS, PERFILES DE USUARIOS Y GRUPOS DE UNA RED DE ÁREA LOCAL

Módulo 8: Recuperación y respaldo de información en redes de área local.



Conectividad y Redes



Objetivos de Aprendizaje de la Especialidad

Módulo 1	<p>OA1 Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI.</p> <p>OA3 Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes.</p> <p>OA7 Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.</p>	Módulo 6	<p>OA9 Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de acuerdo a las especificaciones técnicas del equipo.</p>
Módulo 2	<p>OA2 Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos.</p> <p>OA11 Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.</p>	Módulo 7	<p>OA10 Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.</p>
Módulo 3	<p>OA8 Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.</p>	Módulo 8	<p>OA6 Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.</p>
Módulo 4	<p>OA4 Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.</p>	Módulo 9	<p>No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.</p>
Módulo 5	<p>OA5 Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.</p>		



Perfil de Egreso – Objetivos de Aprendizaje Genéricos

<p>A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.</p>	<p>B- Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.</p>	<p>C- Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.</p>
<p>D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.</p>	<p>E- Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.</p>	<p>F- Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.</p>
<p>G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.</p>	<p>H- Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.</p>	<p>I- Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.</p>
<p>J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.</p>	<p>K- Prevenir situaciones de riesgo y enfermedades ocupacionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.</p>	<p>L- Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.</p>



Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información

1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.

2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas

1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o función.

2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.

3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos

1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.

2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.

3. Identifica y aplica procedimientos y técnicas específicas de una función de acuerdo a parámetros establecidos.

4. Comunicación

4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros

1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía

1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.

2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.

3. Evalúa el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.

4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad

1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.

2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.

3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.

4. Actúa acorde al marco de sus conocimientos, experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos

1. Demuestra conocimientos específicos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.



Metodología seleccionada

Demostración guiada

- Esta presentación les ayudará a poder comprender los conceptos necesarios para el desarrollo de su actividad.

Aprendizaje Esperado

- **AE1.** Gestiona cuentas, perfiles de usuarios y grupos de una red de área local mediante el uso de herramientas de administración del sistema operativo.



¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Reconocer las características de las cuentas de perfiles de usuarios en red local, así como los pasos de configuración de éstas.



Contenidos

01 Cuentas y perfiles de usuarios.

02 Derechos de acceso.

03 Asignación de permisos.

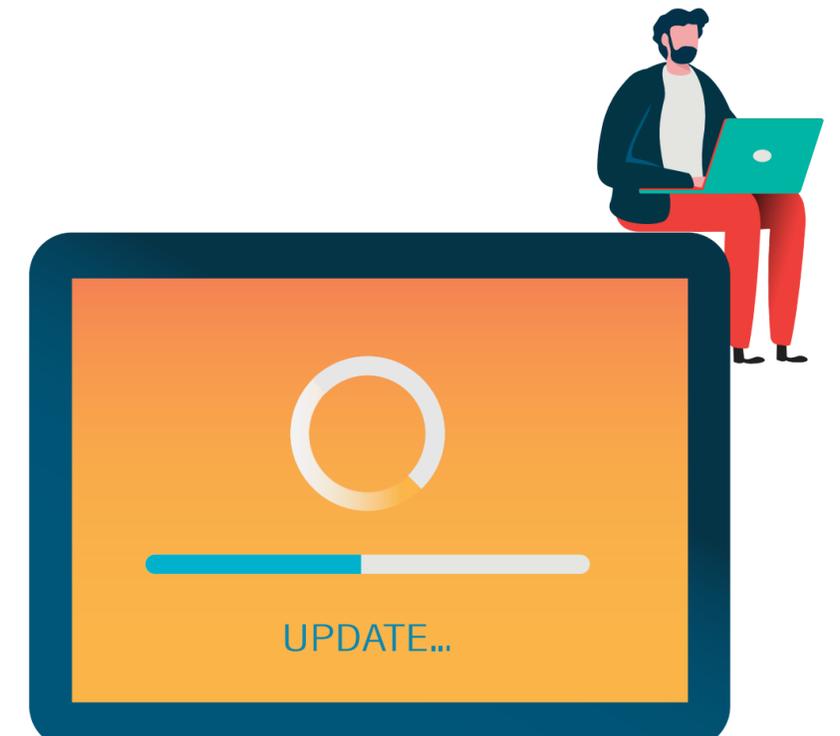
04 Cuentas de grupos.



MOTIVACIÓN CLASE

**A tu juicio, en una red local,
¿debería haber uno o varios
administradores?**

¿Por qué?



Red de área local: Cuentas de usuario

- Las cuentas de usuario son el modo habitual de personalizar el acceso a la red. Así, toda persona que utilice la red con regularidad debe tener una cuenta de acceso.



- Para que el control de este acceso sea suficientemente bueno, las cuentas **deben ser personales**, es decir, dos usuarios no deben compartir la misma cuenta. La cuenta proporciona el acceso a la red y lleva asociadas todas las características y propiedades del usuario útiles en las labores de administración. Las cuentas de usuario suelen tener **parámetros** semejantes a los que a continuación se describen, aunque cada sistema operativo de red tiene los suyos propios.

Red de área local: Cuentas de usuario

- **Nombre de usuario:** Es el nombre único atribuido al usuario y que utiliza para identificarse en la red.
 - Suele ser una cadena de caracteres corta (entre uno y 16 caracteres, normalmente).
- **Contraseña:** Es la cadena de caracteres que codifica una clave secreta de acceso a la red para cada usuario.
 - La contraseña va ligada al nombre de usuario.
 - Proporciona la llave que protege los datos personales del usuario que la posee.



- **Nombre completo del usuario:** Es una cadena de caracteres con el nombre completo del usuario. El nombre de usuario suele ser una abreviatura del nombre completo. En este campo se permite un número mayor de caracteres, incluyendo espacios en blanco, para identificar totalmente al usuario. Algunos examinadores de red muestran este nombre al solicitar una inspección de la red.

- **Nombre completo del usuario:** Es una cadena de caracteres con el nombre completo del usuario. El nombre de usuario suele ser una abreviatura del nombre completo. En este campo se permite un número mayor de caracteres, incluyendo espacios en blanco, para identificar totalmente al usuario. Algunos examinadores de red muestran este nombre al solicitar una inspección de la red.
- **Estaciones de inicio de sesión:** Describe el nombre de los equipos desde los que el usuario puede presentarse en la red.



Cuentas de usuario

- Además, el administrador puede establecer una serie de condiciones por defecto asignadas a cada cuenta y gestionadas mediante políticas (policies), que facilitan su gestión o que mejoran su seguridad. Entre ellas se encuentran las siguientes:

- a. El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- b. El usuario no puede cambiar su contraseña.
- c. La contraseña no caducará nunca.
- d. La cuenta quedará desactivada en un plazo de tiempo.
- e. La cuenta se bloqueará si ocurre un número de fallos de presentación consecutivos previamente fijado.



Cuentas de usuario

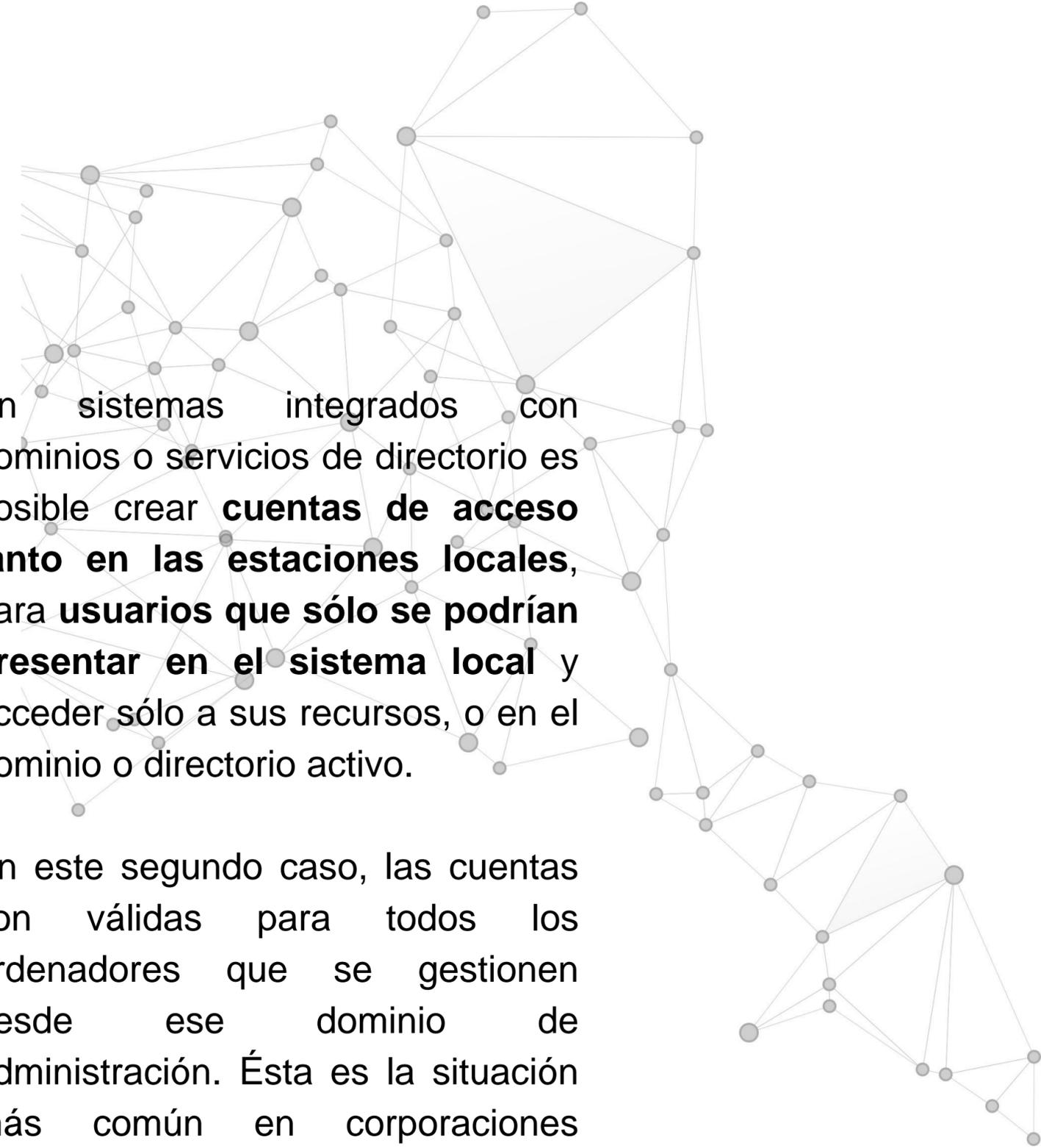
- Además de las cuentas que puede definir el administrador de la red, los sistemas operativos de red poseen unas cuentas por defecto con una funcionalidad específica, que normalmente no se pueden borrar, aunque sí modificar y desactivar. Entre estas cuentas se encuentran:

- a. El supervisor (en Novell), administrador (en Windows), root (en UNIX o Linux), system (en VMS), etc. Es la cuenta privilegiada por excelencia y que suele ser utilizada por el administrador del sistema.**



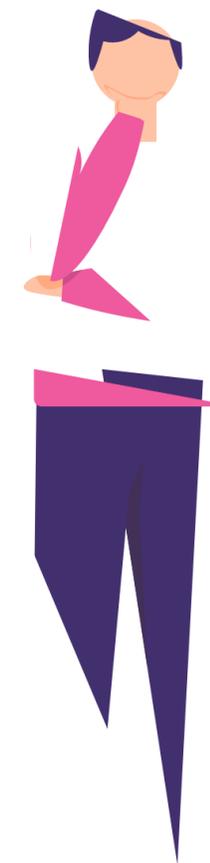
- **Invitado o guest:** Es una cuenta a la que normalmente **no se le asocia contraseña y que carece de privilegios**. Sirve para que aquellos usuarios que no tienen cuenta en el sistema puedan acceder a los servicios mínimos, que define el administrador. Por defecto, **esta cuenta está desactivada al instalar el sistema operativo de red** con objeto de **no generar agujeros de seguridad** sin el consentimiento explícito del administrador, que regulará los derechos y permisos de estos usuarios invitados.

- En sistemas integrados con dominios o servicios de directorio es posible crear **cuentas de acceso tanto en las estaciones locales, para usuarios que sólo se podrían presentar en el sistema local y acceder sólo a sus recursos, o en el dominio o directorio activo.**
- En este segundo caso, las cuentas son válidas para todos los ordenadores que se gestionen desde ese dominio de administración. Ésta es la situación más común en corporaciones grandes y medianas.



Pregunta de reflexión

**¿En qué casos
recomendarías dar solo
permisos de invitados?**



Derechos de acceso

- Una vez que se ha identificado a cada usuario con acceso a la red, se pueden arbitrar sus derechos de acceso. Corresponde al administrador determinar el uso de cada recurso de la red o las operaciones que cada usuario puede realizar en cada estación de trabajo. Ejemplo de estas operaciones son el derecho de acceso a un servidor o a otro equipo a través de la red, forzar el apagado de otro equipo remotamente, reiniciar un equipo, cambiar la hora del sistema, etcétera. Cada recurso, servicio o utilidad tiene, de este modo, una información asociada que le indica quién puede utilizarlos o ejecutarlos y quién carece de privilegios sobre ellos.
- No hay que confundir derechos con permisos:
 1. Un **derecho** autoriza a un usuario o a un grupo de usuarios a realizar determinadas operaciones sobre un servidor o estación de trabajo.
 2. Un **permiso** o **privilegio** es una marca asociada a cada recurso de red: ficheros, directorios, impresoras, etc., que regulan qué usuario tiene acceso y de qué manera.



Derechos de acceso

- De esta forma, los derechos se refieren a operaciones propias del sistema operativo, por ejemplo, el derecho a hacer copias de seguridad. Sin embargo, un permiso se refiere al acceso a los distintos objetos de red, por ejemplo, derecho a leer un fichero concreto. Los derechos prevalecen sobre los permisos.
- **Por ejemplo**, un operador de consola tiene derecho para hacer una copia de seguridad sobre todo un disco; sin embargo, puede tener restringido el acceso a determinados directorios de usuarios porque se lo niega un permiso sobre esos directorios: podrá hacer la copia de seguridad, puesto que el derecho de backup prevalece a la restricción de los permisos.

Asignación de Permisos

- La asignación de permisos en una red se hace en dos fases:
 - a) En primer lugar, se determina el permiso de acceso sobre el servicio de red; por ejemplo, se puede asignar el permiso de poderse conectar a un disco de un ordenador remoto. Esto evita que se puedan abrir unidades remotas de red sobre las que después no se tengan privilegios de acceso a los ficheros que contiene, lo que puede sobrecargar al servidor.
 - b) En segundo lugar, deben configurarse los permisos de los ficheros y directorios (o carpetas) que contiene ese servicio de red.



Asignación de Permisos

- Dependiendo del sistema operativo de red, las marcas asociadas al objeto de red varían, aunque en general podemos encontrar las de lectura, escritura, ejecución, borrado, privilegio de cambio de permisos, etcétera. En redes en las que hay que hacer coexistir sistemas operativos de red de distintos fabricantes, hay que determinar los permisos para cada uno de ellos.



Cuentas de grupo



- Para facilitar las tareas de administración de red, el uso de los servicios o recursos y organizar coherentemente el acceso a la red, existen en los sistemas operativos de red otras entidades de administración denominadas **cuentas de grupo** o simplemente **grupos**.
- Una cuenta de grupo es una colección de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo se le asignan automáticamente todas las propiedades, derechos, características, permisos y privilegios de ese grupo. En este sentido, las cuentas de grupo proporcionan una forma sencilla de configurar los servicios de red para un conjunto de usuarios de características similares.
- Los NOS tienen unos grupos predefinidos que ayudan a la administración de la red según las necesidades más comunes que se suelen presentar: administradores, operadores de copia, operadores de cuentas, operadores de impresión, usuarios avanzados, usuarios comunes, etcétera.



Sistemas globales de acceso



- El crecimiento de las redes (en cuanto al número de nodos se refiere) y su organización en grupos de trabajo (subredes, dominios, etc.), así como la integración de NOS (Sistema Operativo de Red por sus siglas en Inglés) de distintos fabricantes, ha llevado a diseñar un sistema de presentación de los usuarios más globalizador.
- De este modo, el usuario no tiene que presentarse en múltiples sistemas; basta con que se presente en uno de ellos y la red se encarga de facilitarle el acceso a todos los servicios y sistemas de la red en los que tiene derecho de modo automático.
- En las organizaciones en las que el número de nodos es elevado, conviene ordenar todo el conjunto de la red en grupos o dominios. El sistema de cuentas es propio de cada grupo o dominio.



Sistemas globales de acceso

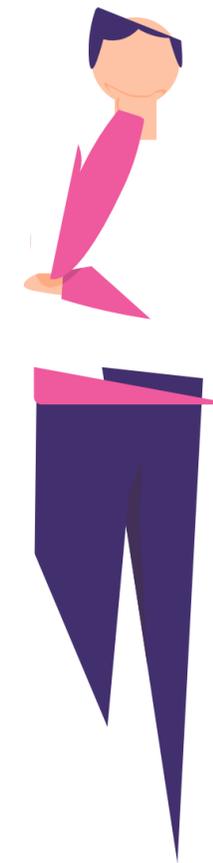


- Una relación de confianza es un vínculo entre grupos o dominios que facilita la utilización de recursos de ambos grupos o dominios, dando lugar a una única unidad administrativa de gestión de red.
- Con el fin de optimizar la organización de la red, es conveniente establecer un dominio maestro centralizador de todas las cuentas de la organización y crear una serie de dominios poseedores de recursos sobre los que establecer las relaciones de confianza necesarias para su utilización.

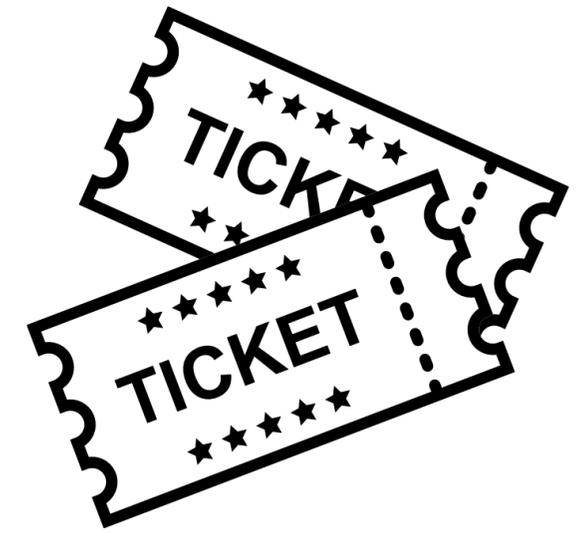


Pregunta de reflexión

¿Qué crees que motivaría a un grupo de usuarios de red local a establecer una relación de confianza?



Ticket de salida



01

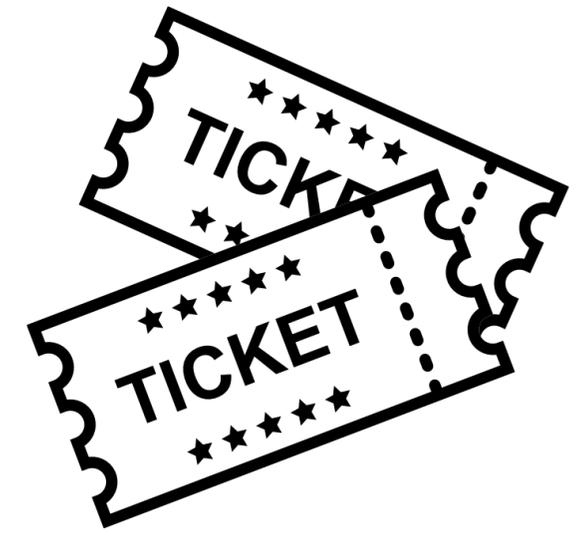
En pares, explica la necesidad de contar con diferentes perfiles en una red local.

02

Si estuvieras asesorando a un administrador de red local, ¿cuáles serían los consejos que le darías para mantenerla segura?



Ticket de salida



03

En tu opinión, ¿qué situaciones pueden generar que se le quiten permisos de administrador a un usuario?

04

Si estuvieras asesorando a un liceo, ¿qué grupos de usuarios recomendarías crear? ¿qué características tendría ese grupo?



Referencias

- **Red de área local. Administración y Gestión**

<http://www.mailxmail.com/curso-red-informatica/red-area-local-sistemas-globales-acceso>

