

Unión Internacional de Telecomunicaciones

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.500**

(08/2005)

SERIE X: REDES DE DATOS, COMUNICACIONES DE  
SISTEMAS ABIERTOS Y SEGURIDAD

Directorio

---

**Tecnología de la información – Interconexión  
de sistemas abiertos – El directorio: Visión de  
conjunto de conceptos, modelos y servicios**

Recomendación UIT-T X.500

UIT-T



RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.379
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
<b>DIRECTORIO</b>	<b>X.500–X.599</b>
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.889
Aplicaciones genéricas de la notación de sintaxis abstracta uno	X.890–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	X.1000–

Para más información, véase la Lista de Recomendaciones del UIT-T.

**Tecnología de la información – Interconexión de sistemas abiertos –  
El directorio: Visión de conjunto de conceptos, modelos y servicios**

**Resumen**

La presente Recomendación | Norma Internacional presenta los conceptos de directorio y de la base de información de directorio (DIB) y expone los servicios y capacidades que proporcionan.

**Orígenes**

La Recomendación UIT-T X.500 fue aprobada el 29 de agosto de 2005 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. Se publica también un texto idéntico como Norma Internacional ISO/CEI 9594-1.

## PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2006

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

*Página*

1	Alcance .....	1
2	Referencias normativas .....	1
2.1	Recomendaciones   Norma Internacionales idénticas .....	1
3	Definiciones .....	2
3.1	Definiciones relativas al modelo de comunicación .....	2
3.2	Definiciones relativas al modelo de directorio .....	2
3.3	Definiciones relativas a la operación distribuida .....	3
3.4	Definiciones relativas a la replicación .....	3
3.5	Definiciones básicas relativas al directorio .....	3
4	Abreviaturas .....	3
5	Convenios .....	4
6	Descripción general del directorio .....	4
7	La base de información de directorio (DIB) .....	6
8	El servicio de directorio .....	7
8.1	Introducción .....	7
8.2	Calificación del servicio .....	7
8.2.1	Controles de servicio .....	7
8.2.2	Parámetros de seguridad .....	8
8.2.3	Filtros .....	8
8.3	Interrogación de directorio .....	8
8.3.1	Lectura .....	8
8.3.2	Comparación .....	8
8.3.3	Listado .....	8
8.3.4	Búsqueda .....	8
8.3.5	Abandono .....	8
8.4	Modificación de directorio .....	8
8.4.1	Adición de inserción .....	8
8.4.2	Supresión de inserción .....	9
8.4.3	Modificación de inserción .....	9
8.4.4	Modificación de nombre distinguido .....	9
8.5	Otros resultados .....	9
8.5.1	Errores .....	9
8.5.2	Remisiones .....	9
9	El directorio distribuido .....	9
9.1	Modelo funcional .....	9
9.2	Modelo de organización .....	10
9.3	Funcionamiento del modelo .....	10
10	Control de acceso en el directorio .....	14
11	Administración de servicios .....	15
12	Replicación en el directorio .....	15
12.1	Introducción .....	15
12.2	Formas de replicación de directorio .....	16
12.3	Replicación y congruencia de información de directorio .....	17
12.4	Enfoques de la replicación .....	17
12.4.1	Enfoque del usuario de directorio .....	17
12.4.2	Enfoque del usuario administrativo .....	18
12.4.3	Enfoque del DSA .....	18
12.5	Replicación y control de acceso .....	18
13	Protocolos de directorio .....	18
14	Gestión de sistemas de directorio .....	18
14.1	Introducción .....	18
14.2	Gestión del dominio DIT .....	19

	<i>Página</i>
14.3 Gestión de componentes de directorio .....	19
Anexo A – Aplicación de directorio .....	20
A.1 El entorno de directorio .....	20
A.2 Características del servicio de directorio .....	20
A.3 Patrones de utilización de directorio .....	20
A.3.1 Introducción .....	20
A.3.2 Consulta .....	20
A.3.3 Denominación cómoda para el usuario .....	21
A.3.4 Examen rápido ("hojeado") .....	21
A.3.5 Páginas amarillas .....	21
A.3.6 Restricciones y facilitación de búsquedas .....	21
A.3.7 Grupos .....	22
A.3.8 Autenticación .....	22
A.3.9 Ubicación basada en los atributos .....	22
A.4 Aplicaciones genéricas .....	22
A.4.1 Introducción .....	22
A.4.2 Comunicaciones interpersonales .....	23
A.4.3 Comunicaciones entre sistemas (para OSI) .....	23
Anexo B – Enmiendas y corrigenda .....	24

## Introducción

Esta Recomendación | Norma Internacional, junto con otras Recomendaciones | Normas Internacionales, ha sido elaborada para facilitar la interconexión de sistemas de procesamiento de información con el fin de proporcionar servicios de directorio. El conjunto de todos estos sistemas, junto con la información de directorio que contienen, puede considerarse como un todo integrado, denominado el *directorio*. La información contenida en el directorio, denominada colectivamente base de información de directorio (DIB), se utiliza típicamente para facilitar la comunicación entre, con o sobre objetos tales como entidades de aplicación, personas, terminales y listas de distribución.

El directorio desempeña un papel importante en la interconexión de sistemas abiertos (OSI), cuyo objetivo es permitir, con un mínimo de acuerdos técnicos fuera de las propias normas de interconexión, la interconexión de sistemas de procesamiento de información:

- de diferentes fabricantes;
- sometidos a gestiones diferentes;
- de diferentes grados de complejidad; y
- de diferentes fechas de construcción.

Esta Recomendación | Norma Internacional presenta y modela los conceptos de directorio y de la DIB y expone los servicios y capacidades que las mismas proporcionan. Otras Recomendaciones | Normas Internacionales utilizan estos modelos para definir el servicio abstracto prestado por el directorio y para especificar los protocolos mediante los cuales se puede obtener o propagar este servicio.

Esta Recomendación | Norma Internacional establece los marcos fundamentales con los que otros grupos de normalización y foros de la industria podrán definir perfiles de la industria. Muchas de las prestaciones que se definen como facultativas en dichos marcos podrán ser autorizadas para que se apliquen en determinados entornos a través de perfiles. Esta quinta edición revisa y mejora técnicamente la cuarta edición de esta Recomendación | Norma Internacional, pero no la sustituye. Aún es posible realizar implementaciones conformes con la cuarta edición. Sin embargo, en determinado momento dejará de sustentarse la cuarta edición (no se resolverán los defectos notificados). Se recomienda pues que las implementaciones sean conformes a esta quinta edición lo antes posible.

Esta quinta edición especifica las versiones 1 y 2 de los protocolos de directorio.

En las ediciones primera y segunda se especifica solamente la versión 1. La mayor parte de los servicios y protocolos especificados en esta edición están diseñados para funcionar según la versión 1. No obstante, algunos servicios y protocolos mejorados, por ejemplo, los errores signados, no funcionarán a menos que todas las entidades de directorio que participan en la operación hayan negociado la versión 2. Cualquiera que sea la versión negociada, las diferencias entre los servicios y entre los protocolos definidas en las cinco ediciones, salvo las asignadas específicamente a la versión 2, se resuelven aplicando las reglas de extensibilidad definidas en esta edición de la Rec. UIT-T X.519 | ISO/CEI 9594-5.

El anexo A, que es parte integrante de la presente Recomendación | Norma Internacional, describe los tipos de utilización a los que puede aplicarse el directorio.

El anexo B, que no es parte integrante de esta Recomendación | Norma Internacional, detalla las enmiendas e informes de defectos incorporados en la presente edición de esta Recomendación | Norma Internacional.





**NORMA INTERNACIONAL  
RECOMENDACIÓN UIT-T**

**Tecnología de la información – Interconexión de sistemas abiertos –  
El directorio: Visión de conjunto de conceptos, modelos y servicios**

**1 Alcance**

El directorio proporciona las capacidades de directorio que necesitan las aplicaciones OSI, los procesos de gestión OSI, otras entidades de capa OSI y los servicios de telecomunicaciones. Entre las capacidades que proporciona están la de "denominación fácil para el usuario", lo que permite aludir a los objetos por nombres adecuados para uso de usuarios humanos (si bien no todos los objetos necesitan contar con nombres fáciles para el usuario) y la de "correspondencia de nombre con dirección" lo que permite una vinculación dinámica entre los objetos y su ubicación. Esta última capacidad permite, por ejemplo, la "autoconfiguración" de las redes OSI, en el sentido de que la adición, supresión y cambios de ubicación de objeto no afecta a la operación de la red OSI.

El directorio no pretende ser un sistema de base de datos para fines generales, si bien puede construirse a partir de dichos sistemas. Por ejemplo, se supone, como es típico en los directorios de comunicaciones, que existe una frecuencia bastante superior de "interrogaciones" (o "indagaciones") que de actualizaciones. La tasa de actualizaciones se supone estará determinada por la dinámica de las personas y organizaciones más bien que, por ejemplo, la dinámica de las redes. Tampoco son necesarias actualizaciones globales instantáneas: las condiciones transitorias, en que se dispone tanto de la versión antigua como nueva de una misma información, son perfectamente aceptables.

Es una característica de directorio que, salvo si existen diferentes derechos de acceso o actualizaciones no propagadas, los resultados de las interrogaciones de directorio no dependerán de la identidad o ubicación del interrogador. Esto hace que el directorio no sea adecuado para ciertas aplicaciones de telecomunicaciones, por ejemplo, algunos tipos de encaminamiento. En los casos en que los resultados dependen de la identidad del interrogador, puede negarse el acceso a la información de directorio y a las actualizaciones del mismo.

**2 Referencias normativas**

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se aconseja que los participantes en acuerdos basados en la presente Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

**2.1 Recomendaciones | Normas Internacionales idénticas**

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación UIT-T X.501 (2005) | ISO/CEI 9594-2:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos.*
- Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*
- Recomendación UIT-T X.511 (2005) | ISO/CEI 9594-3:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto.*
- Recomendación UIT-T X.518 (2005) | ISO/CEI 9594-4:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Procedimientos para operación distribuida.*
- Recomendación UIT-T X.519 (2005) | ISO/CEI 9594-5:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo.*

- Recomendación UIT-T X.520 (2005) | ISO/CEI 9594-6:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados.*
- Recomendación UIT-T X.521 (2005) | ISO/CEI 9594-7:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Clases de objetos seleccionadas.*
- Recomendación UIT-T X.525 (2005) | ISO/CEI 9594-9:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación.*
- Recomendación UIT-T X.530 (2005) | ISO/CEI 9594-10:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Utilización de la gestión de sistemas para la administración de directorio.*

### **3 Definiciones**

A los efectos de la presente Recomendación | Norma Internacional, son aplicables las definiciones siguientes.

#### **3.1 Definiciones relativas al modelo de comunicación**

Los siguientes términos se definen en la Rec. UIT-T X.519 | ISO/CEI 9594-5:

- a) entidades de aplicación;
- b) capa de aplicación;
- c) proceso de aplicación.

#### **3.2 Definiciones relativas al modelo de directorio**

Los siguientes términos se definen en la Rec. UIT-T X.501 | ISO/CEI 9594-2:

- a) control de acceso;
- b) dominio de gestión de directorio de Administración;
- c) alias;
- d) ancestro
- e) atributo;
- f) tipo de atributo;
- g) valor de atributo;
- h) autenticación;
- i) inserción compuesta;
- j) contexto;
- k) árbol de información de directorio (DIT);
- l) dominio de gestión de directorio (DMD);
- m) agente de sistema de directorio (DSA);
- n) agente de usuario de directorio (DUA);
- o) nombre distinguido;
- p) inserción;
- q) familia (de inserciones)
- r) grupo jerárquico
- s) cliente LDAP;
- t) peticionario LDAP;
- u) respondedor LDAP;
- v) servidor LDAP;
- w) nombre;
- x) objeto (de interés);
- y) dominio de gestión de directorio privado;
- z) inserciones conexas;

- aa) nombre distinguido relativo;
- bb) raíz;
- cc) esquema;
- dd) política de seguridad;
- ee) objeto subordinado;
- ff) inserción superior o asiento superior;
- gg) objeto superior;
- hh) árbol.

### 3.3 Definiciones relativas a la operación distribuida

Los siguientes términos se definen en la Rec. UIT-T X.518 | ISO/CEI 9594-4:

- a) uniconcatenación;
- b) multiconcatenación;
- c) referimiento.

### 3.4 Definiciones relativas a la replicación

Los términos siguientes se definen en la Rec. UIT-T X.525 | ISO/CEI 9594-9:

- a) velado;
- b) copia caché;
- c) copia de inserción;
- d) DSA maestro;
- e) replicación;
- f) consumidor de duplicado;
- g) suministrador de duplicado;
- h) información duplicada;
- i) acuerdo de duplicación.

### 3.5 Definiciones básicas relativas al directorio

Los siguientes términos se definen en esta Recomendación | Norma Internacional.

**3.5.1 directorio:** Conjunto de sistemas abiertos que cooperan para proporcionar servicios de directorio.

**3.5.2 base de información de directorio (DIB, *directory information base*):** Conjunto de informaciones regido por el directorio.

**3.5.3 usuario (de directorio):** Usuario final de directorio, es decir, entidad o persona que obtiene acceso al directorio.

## 4 Abreviaturas

A los efectos de la presente Recomendación | Norma Internacional se aplican las siguientes siglas:

ACI	Información de control de acceso ( <i>access control information</i> )
ADDMD	Dominio de gestión de directorio de Administración ( <i>Administration directory management domain</i> )
DAP	Protocolo de acceso a directorio ( <i>directory access protocol</i> )
DIB	Base de información de directorio ( <i>directory information base</i> )
DISP	Protocolo de sombreado de información de directorio ( <i>directory information shadowing protocol</i> )
DIT	Árbol de información de directorio ( <i>directory information tree</i> )
DMD	Dominio de gestión de directorio ( <i>directory management domain</i> )

## ISO/CEI 9594-1:2005 (S)

DOP	Protocolo de gestión de vinculaciones operacionales de directorio ( <i>directory operational binding management protocol</i> )
DSA	Agente de sistema de directorio ( <i>directory system agent</i> )
DSP	Protocolo de sistema de directorio ( <i>directory system protocol</i> )
DUA	Agente de usuario de directorio ( <i>directory user agent</i> )
LDAP	Protocolo ligero de acceso al directorio ( <i>lightweight directory access protocol</i> )
OSI	Interconexión de sistemas abiertos ( <i>open systems interconnection</i> )
PRDMD	Dominio de gestión de directorio privado ( <i>private directory management domain</i> )
RDN	Nombre distinguido relativo ( <i>relative distinguished name</i> )

## 5 Convenios

Con pequeñas excepciones, esta Especificación de directorio se ha preparado con arreglo a las *Reglas para la representación de texto común del UIT-T | ISO/CEI*, noviembre de 2001.

Cuando se escribe "Especificación de directorio" (como en "esta Especificación de directorio") se trata de la Rec. UIT-T X.500 | ISO/CEI 9594-1. Cuando se escriba "Especificaciones de directorio" se entenderá que se trata de las Recomendaciones de la serie X.500 y todas las partes de ISO/CEI 9594.

En esta Especificación de directorio se utiliza el término *sistemas de la primera edición* para hacer referencia a los sistemas conformes a la primera edición de las Especificaciones de directorio, es decir, la edición 1988 de las Recomendaciones CCITT de la serie X.500 y la edición de ISO/CEI 9594:1990. En esta Especificación de directorio se utiliza el término *sistemas de la segunda edición* para hacer referencia a sistemas conformes a la segunda edición de las Especificaciones de directorio, es decir, la edición 1993 de las Recomendaciones UIT-T de la serie X.500 y la edición de ISO/CEI 9594:1995. En esta Especificación de directorio se utiliza el término *sistemas de la tercera edición* para hacer referencia a sistemas conformes a la tercera edición de las Especificaciones de directorio, es decir, la edición 1997 de las Recomendaciones UIT-T de la serie X.500 y la edición de ISO/CEI 9594:1998. En esta Especificación de directorio se utiliza el término *sistemas de la cuarta edición* para hacer referencia a sistemas conformes a la cuarta edición de las Especificaciones de directorio, es decir, las ediciones 2001 de las Recs. UIT-T X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.525 y X.530, la edición 2000 de la Rec. UIT-T X.509 y las partes 1-10 de la edición ISO/CEI 9594:2001.

En esta Especificación de directorio se utiliza el término *sistemas de la quinta edición* para hacer referencia a sistemas conformes a la quinta edición de las Especificaciones de directorio, es decir, las ediciones 2005 de las Recs. UIT-T X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525 y X.530 y las partes 1-10 de la edición ISO/CEI 9594:2005.

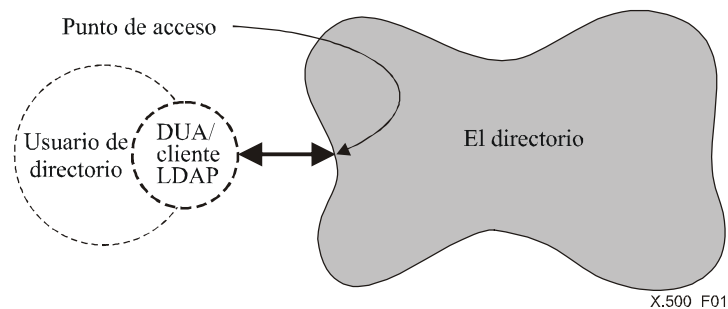
Esta Especificación de directorio presenta la notación de sintaxis abstracta uno (ASN.1) en letra Helvética en negritas. Cuando en el texto normal se hace referencia a los tipos y valores ASN.1, éstos se diferencian del texto normal por estar presentados en la tipografía mencionada. Los nombres de los procedimientos, utilizados generalmente al especificar la semántica de los procesos, se diferencian del texto normal mediante la tipografía Times en negritas. Los permisos de control de acceso se presentan en letra Times en cursiva.

## 6 Descripción general del directorio

El *directorio* es un conjunto de sistemas abiertos que cooperan para mantener una base de datos lógica de información sobre un conjunto de objetos del mundo real. Los *usuarios* de directorio, que son personas y programas de computador, pueden leer o modificar la información, o partes de ella, a condición de que estén autorizados a hacerlo. Al obtener acceso al directorio, cada usuario está representado por un agente de usuario de directorio (DUA, *directory user agent*) o un cliente LDAP que se consideran como procesos de aplicación. Estos conceptos se ilustran en la figura 1.

NOTA – Las Especificaciones de directorio se refieren al directorio en singular, y reflejan la intención de crear, por medio de un espacio de nombre único y unificado, un directorio lógico compuesto de muchos sistemas que sirven a muchas aplicaciones. El hecho de que estos sistemas decidan o no interfundarse dependerá de las necesidades de las aplicaciones soportadas por dichos sistemas. Es posible que aplicaciones referentes a mundos de objetos no intersectantes no tengan esa necesidad. El espacio de nombre único facilitará ese interfundamiento, en caso de que las necesidades cambiasen. Por varios motivos, tales como seguridad, conectividad, o decisiones de tipo comercial, es probable que algunas porciones de directorio puedan no ser alcanzables por otras porciones de directorio que utilizan operaciones de la tercera edición. Esto resulta en enfoques distintos del directorio, que pueden contener inserciones conexas sobre un objeto dado del mundo real. Estas inserciones conexas pueden tener o no el mismo nombre distinguido. Si se utilizan los sistemas de la cuarta edición o subsiguientes, es posible efectuar operaciones a través de múltiples enfoques distintos para proporcionar una respuesta integrada al usuario. Concretamente:

- Los administradores de DMD (véase 9.2) pueden tener necesidad de publicar su propio enfoque (o enfoques) de algunos objetos específicos del mundo real; un objeto del mundo real puede ser modelizado por múltiples inserciones independientes en el directorio, lo cual puede suceder necesiten o no interfuncionar. Puede además no soportarse el interfuncionamiento utilizando DSP.
- No obstante la última frase de la nota, es también posible que determinados DMD decidan publicar información respecto a objetos del mundo real dentro de sus propios espacios asignados de nombres de directorio (es decir en uno de múltiples DIT); en este caso, sería posible tener un objeto específico del mundo real modelizado por inserciones en el mismo o en distintos espacios de nombre DIT, con el mismo o distintos nombres distinguidos en cada uno de ellos. Obsérvese que ciertas facilidades de directorio (por ejemplo la adquisición de certificados, y funciones conexas basadas en firmas digitales) no pueden ser implementadas cuando se permite que objetos distintos compartan nombres distinguidos.
- El objetivo de las inserciones conexas es proporcionar un medio por el cual los usuarios pueden acceder a tales inserciones, agrupando la información resultante, si es posible. Esto se aplicaría a la situación descrita en los dos incisos precedentes.



**Figura 1 – Acceso al directorio**

La información contenida en el directorio se conoce colectivamente como *base de información de directorio* (DIB, *directory information base*). En la cláusula 7 se analiza su estructura.

El directorio proporciona a sus usuarios un conjunto bien definido de capacidades de acceso, conocido como el servicio abstracto de directorio. Este servicio, que se describe brevemente en la cláusula 8, proporciona una capacidad simple de recuperación y modificación. Ésta puede combinarse con funciones DUA locales para proporcionar las capacidades requeridas por los usuarios finales.

El directorio se distribuye según líneas tanto funcionales como de organización. En la cláusula 9 se presenta un análisis de los modelos correspondientes de directorio. Estos han sido elaborados con el objeto de establecer un marco de cooperación de los diversos componentes, a fin de ofrecer un todo integrado.

El directorio existe en un entorno en el que diversas autoridades administrativas controlan el acceso a su parte de información. En la cláusula 10 se describe el control de acceso.

En un directorio distribuido podría ser conveniente replicar información a fin de mejorar las prestaciones y la disponibilidad. El mecanismo de replicación de directorio se analiza en la cláusula 11.

El suministro y consumo de los servicios de directorio requiere que los usuarios (en realidad los DUA y/o los clientes LDAP) y los diversos componentes funcionales de directorio cooperen entre sí. En muchos casos esto requerirá una cooperación entre procesos de aplicación de diferentes sistemas abiertos, lo que a su vez exige protocolos de aplicación normalizados, que se describen brevemente en la cláusula 11, para regular esta cooperación.

El directorio está concebido de manera que soporte múltiples aplicaciones, entre una amplia gama de posibilidades. La naturaleza de las aplicaciones soportadas determina qué objetos aparecen en el directorio, cuáles usuarios tienen acceso a la información, y qué tipos de acceso se realizan. Las aplicaciones pueden ser específicas, como por ejemplo el suministro de listas de distribución para el correo electrónico, o genéricas, como la aplicación "directorío de comunicaciones interpersonales". El directorio ofrece la posibilidad de explotar los aspectos comunes a las diversas aplicaciones:

- un mismo objeto puede concernir a más de una aplicación y tal vez incluso una misma información sobre un mismo objeto;
- para permitir esto se definen varias clases de objeto y tipos de atributo que son útiles para toda una gama de aplicaciones. Estas definiciones se encuentran en la Rec. UIT-T X.520 | ISO/CEI 9594-6 y la Rec. UIT-T X.521 | ISO/CEI 9594-7;
- algunos patrones de utilización de directorio serán comunes a toda una gama de aplicaciones; este aspecto se analiza en el anexo A.

## 7 La base de información de directorio (DIB)

NOTA 1 – La DIB y su estructura se definen en la Rec. UIT-T X.501 | ISO/CEI 9594-2.

La DIB está formada por información sobre objetos. Está compuesta de *inserciones (de directorio)*, cada uno de los cuales consiste en una colección de informaciones sobre un objeto. Una inserción puede ser un conjunto de inserciones de miembros, cada una de las cuales contiene información sobre un aspecto particular de un objeto. Esta inserción agrupada se denomina una inserción compuesta. Cada inserción está formada por *atributos*, cada uno con un tipo y uno o más valores. Los tipos de atributo presentes en una determinada inserción dependen de la *clase* de objeto descrita por dicha inserción. Cada *valor* de un atributo puede ser rotulado con uno o más *contextos* que especifican la información sobre un valor que puede utilizarse para determinar la aplicabilidad del valor.

Las inserciones de la DIB están organizadas en forma de árbol, el árbol de información de directorio (DIT, *directory information tree*), donde los vértices representan las inserciones. Las inserciones superiores del árbol (más cercanas a la raíz) representarán a menudo objetos tales como países u organizaciones, mientras que las inserciones inferiores representarán personas o procesos de aplicación.

NOTA 2 – Los servicios definidos en las Especificaciones de directorio operan únicamente en una estructura arboriforme. Esta Especificación de directorio no excluye la existencia futura de otras estructuras (según las necesidades).

Cada inserción tiene un nombre distinguido, que identifica dicha inserción en forma única e inequívoca. Estas propiedades del nombre distinguido se derivan de la estructura arboriforme de la información. El nombre distinguido de una inserción está compuesto del nombre distinguido de su inserción superior, junto con los valores de atributo especialmente nominados (los valores distinguidos) de la inserción.

Algunas de las inserciones en las hojas del árbol son inserciones de alias, mientras que otros asientos son inserciones de objeto e inserciones compuestas. Las inserciones de alias apuntan a inserciones de objeto, y proporcionan la base de nombres alternativos para los objetos correspondientes.

Una inserción compuesta es una inserción que representa un solo objeto y es un conjunto de inserciones de miembros, cada una de las cuales representa una parte de la información sobre el objeto.

El directorio aplica un conjunto de reglas para garantizar que la DIB permanezca bien formada ante las modificaciones que surjan con el tiempo. Estas reglas, conocidas por el nombre de *esquema de directorio*, evitan que las inserciones tengan tipos de atributo incorrectos para su clase de objeto, que los valores de atributo tengan una forma errónea para el tipo de atributo, e incluso que las inserciones tengan inserciones subordinadas de una clase errónea.

La figura 2 ilustra los conceptos antes mencionados del DIT y sus componentes.

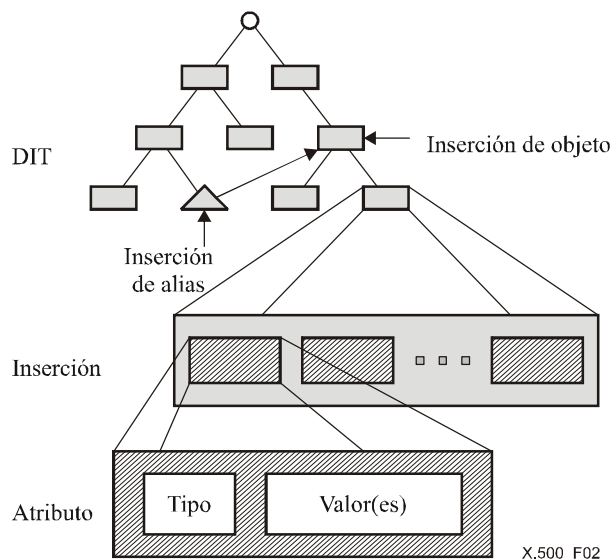


Figura 2 – Estructura del DIT y de las inserciones

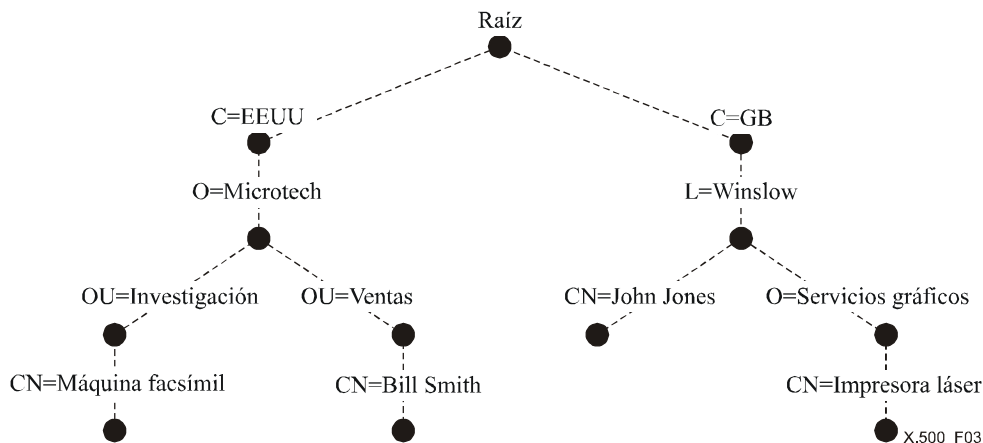
La figura 3 presenta un ejemplo teórico de DIT. El árbol proporciona ejemplos de algunas de las clases de atributo utilizadas para identificar diferentes objetos. Por ejemplo, el nombre:

{C=GB, L=Winslow, O=Servicios gráficos, CN=Impresora láser}

identifica la entidad de aplicación "Impresora láser" que tiene, en su nombre distinguido, el atributo geográfico de localidad.

El abonado residencial John Jones, cuyo nombre es {C=GB, L=Winslow, CN=John Jones} tiene el mismo atributo geográfico en su nombre distinguido.

El crecimiento y forma del DIT, la definición del esquema de directorio y la selección de nombres distinguidos para las inserciones conforme se añaden, es la responsabilidad de diversas autoridades cuyas relaciones jerárquicas se reflejan en la forma del árbol. Por ejemplo, las autoridades garantizarán que todas las inserciones bajo su jurisdicción tengan nombres distinguidos inequívocos, manejando cuidadosamente los valores y tipos de atributo que aparecen en dichos nombres. La responsabilidad se transmite hacia abajo a lo largo del árbol, pasando de autoridades superiores a autoridades subordinadas, ejerciéndose el control por medio del esquema.



**Figura 3 – Ejemplo teórico de árbol de información de directorio**

La función de grupo jerárquico permite establecer una relación jerárquica alternativa entre inserciones independientes de la relación jerárquica reflejada por la estructura del DIT. La operación búsqueda de directorio (véase 8.3.4) puede devolver no sólo información sobre inserciones concordadas, sino también otros miembros del grupo jerárquico al cual pudiera pertenecer la inserción concordada. La función de grupo jerárquico tiene también la ventaja que permite cambiar las relaciones jerárquicas sin cambiar la estructura del DIT y por ende de los nombres distinguidos de las inserciones.

## 8 El servicio de directorio

NOTA – La definición del servicio abstracto de directorio figura en la Rec. UIT-T X.511 | ISO/CEI 9594-3.

### 8.1 Introducción

En esta cláusula se presenta una descripción general del servicio proporcionado a los usuarios, representados por sus DUA y/o los clientes LDAP. Todos los servicios son proporcionados por el directorio en respuesta a solicitudes de los DUA y/o los clientes LDAP. Unas peticiones permiten interrogar al directorio, como se describe en 8.3 y otras modificarlo, como se describe en 8.4. Además, las peticiones de servicio pueden calificarse como se describe en 8.2. El directorio siempre informa del resultado de cada petición que se le hace. La forma del resultado normal es peculiar de la petición y resulta evidente a partir de la descripción de la petición. La mayoría de los resultados anormales son comunes a varias peticiones. Las posibilidades se describen en 8.5.

El directorio garantiza que los cambios de la DIB, ya sea como consecuencia de la petición de un servicio de directorio o por otro medio (local), siempre resultan en una DIB que siga obedeciendo las reglas del esquema de directorio.

Un usuario y el directorio están vinculados por un periodo de tiempo en un punto de acceso al directorio. En el momento de la vinculación, el usuario y el directorio pueden verificar sus identidades respectivas (es facultativo).

### 8.2 Calificación del servicio

#### 8.2.1 Controles de servicio

Se pueden aplicar una serie de medios de control (denominados brevemente controles) a las diversas peticiones de servicio, principalmente con el objeto de que el usuario pueda imponer límites al uso de recursos, que el directorio no debe sobrepasar, pero también para controlar el progreso del funcionamiento de directorio. Se prevén controles, entre otras cosas, del periodo de tiempo, la magnitud de los resultados, el alcance de la búsqueda, o modos de interacción y la prioridad de la petición.

## **8.2.2 Parámetros de seguridad**

Cada petición puede ir acompañada de información de soporte de mecanismos de seguridad para proteger la información de directorio. Dicha información puede incluir la petición del usuario de diversos tipos de protección, una firma (signatura) digital de la petición, junto con la información necesaria para que la parte legítimamente interesada pueda verificar la firma.

## **8.2.3 Filtros**

Cierto número de peticiones cuyos resultados implican información procedente de o relativa a cierto número de inserciones pueden llevar uno o más filtros. El filtro expresa una o más condiciones que la inserción o la inserción compuesta debe satisfacer para poder ser devuelta como parte del resultado. Esto permite reducir el conjunto de inserciones devueltas únicamente a las pertinentes.

## **8.3 Interrogación de directorio**

### **8.3.1 Lectura**

Una petición de lectura va dirigida a una determinada inserción o inserción compuesta y origina la devolución de los valores de algunos o de todos los atributos de dicha inserción. En el caso de inserciones compuestas, la información de miembros de familia está contenida en un lote (de sintaxis similar a la de un atributo) que comprende la información de familia seleccionada. Cuando sólo deben ser devueltos algunos de los atributos, el DUA suministra la lista de tipos de atributo que interesan como parte de la petición. Un DUA puede suministrar también uno o más contextos para uno o más tipos de atributo que interesan, con el fin de seleccionar únicamente los valores aplicables en los contextos especificados.

NOTA – Los clientes LDAP no soportan la operación Lectura.

### **8.3.2 Comparación**

Una petición de comparación va dirigida a un determinado atributo de una determinada inserción o inserción compuesta y hace que el directorio verifique si el valor suministrado concuerda con el valor de dicho atributo. Un DUA puede suministrar también uno o más contextos para el valor de atributo que interesa a fin de limitar la operación de comparación.

NOTA – Por ejemplo, esto puede utilizarse para realizar verificaciones de contraseñas; la contraseña, registrada en el directorio, puede ser inaccesible para lectura pero accesible para comparación.

### **8.3.3 Listado**

Una petición de listado hace que el directorio devuelva la lista de subordinados inmediatos de una determinada inserción nombrada en el DIT. Un DUA puede suministrar también uno o más contextos para seleccionar qué contextos se utilizan en los RDN retornados.

NOTA – Los clientes LDAP no soportan la operación Listado.

### **8.3.4 Búsqueda**

Una petición de búsqueda hace que el directorio devuelva información de todas las inserciones o inserciones compuestas dentro de una o más porciones del DIT que satisfacen algunos filtros. La información devuelta de cada inserción consiste en algunos o todos los atributos de dicha inserción y en algunos o todos los valores de esos atributos, como en lectura. La información devuelta de inserciones conexas puede ser combinada de acuerdo con algunos criterios comunes.

Es posible utilizar reglas de búsqueda para restringir los tipos de búsqueda que se pueden efectuar. También es posible, como una facilidad de reglas de búsqueda, aligerar o restringir progresivamente las búsquedas dentro de una operación de directorio, si hubiere que devolver muy pocos o demasiados ítems de información de inserción.

### **8.3.5 Abandono**

Una petición de abandono, aplicada a una petición de interrogación pendiente, informa al directorio que el originador de la petición ya no está interesado en que se atienda la petición. El directorio puede, por ejemplo, dejar de procesar la petición, y descartar cualquier resultado que haya logrado hasta ese momento.

## **8.4 Modificación de directorio**

### **8.4.1 Adición de inserción**

Una petición de adición de inserción hace que se añada al DIT una inserción (una inserción de objeto o una inserción de alias) que constituirá una nueva hoja. Los contextos pueden incluirse con los valores de atributo para la nueva inserción.



### 8.4.2 Supresión de inserción

Una petición de supresión de inserción hace que se suprima del DIT una inserción constitutiva de hoja o, si se requiere, las inserciones que comprenden una inserción compuesta.

### 8.4.3 Modificación de inserción

Una petición de modificación de asiento hace que el directorio ejecute una secuencia de cambios en una determinada inserción o miembro de familia. Se hacen todos los cambios o ninguno de ellos y la DIB queda siempre en un estado conforme al esquema. Los cambios permitidos son la adición, eliminación o reemplazo de atributos o de valores de atributo. Los contextos pueden incluirse con los valores de atributo añadidos a la inserción. Esta operación sólo se puede utilizar en un miembro de familia, pero no puede manipular una inserción compuesta completa.

Una operación de modificación de asiento puede suministrar en el resultado, si se requiere, la información contenida en la inserción o en la inserción compuesta después que se ha efectuado satisfactoriamente una modificación.

### 8.4.4 Modificación de nombre distinguido

Una petición de modificación de nombre distinguido (DN, *distinguished name*) se utiliza para cambiar el nombre distinguido relativo de una inserción (sea ésta una inserción de objeto o una inserción de alias o un miembro de familia) o para desplazar una inserción, si no es un miembro de familia, a una nueva superior en el DIT. Si una inserción tiene subordinados, todos ellos son denominados de nuevo o desplazados de manera consecuente. Los contextos pueden incluirse en el nuevo RDN de la inserción. En el caso de miembros de familia, éstos pueden ser trasladados para tener nuevos superiores, a condición de que permanezcan dentro de la misma inserción compuesta.

## 8.5 Otros resultados

### 8.5.1 Errores

Cualquier servicio puede fallar, debido por ejemplo a problemas relacionados con los parámetros suministrados por el usuario, en cuyo caso se informa de un error. Siempre que sea posible, con la indicación del error se retorna información para facilitar la solución del problema. Sin embargo, en general el directorio únicamente comunica el primer error que encuentra. Además del ejemplo antes mencionado sobre los problemas que puedan plantear los parámetros suministrados por el usuario (especialmente nombres no válidos de inserciones o tipos de atributo no válidos) también pueden surgir errores a causa de violaciones de la política de seguridad, las reglas de esquema y los controles de servicio.

### 8.5.2 Remisiones

Un servicio puede fallar porque el punto de acceso específico al que está vinculado el DUA o el cliente LDAP no es el más adecuado para atender la petición: por ejemplo, la información que es objeto de la petición está lejos (lógicamente) de ese punto de acceso. En este caso, el directorio puede efectuar una remisión que indique otro punto de acceso en el que el DUA o el cliente LDAP pueden presentar su petición.

NOTA – El directorio y el DUA pueden tener una preferencia respecto al uso de remisiones o a la *concatenación* de las peticiones (véase 9.3). El DUA puede expresar su preferencia por medio de controles del servicio. El directorio toma la decisión final en cuanto al método que se va a utilizar.

## 9 El directorio distribuido

NOTA – Los modelos de directorio se definen en la Rec. UIT-T X.501 | ISO/CEI 9594-2 y los procedimientos para la operación de directorio distribuido se especifican en la Rec. UIT-T X.518 | ISO/CEI 9594-4.

### 9.1 Modelo funcional

El modelo funcional de directorio se muestra en la figura 4.

Un *agente de sistema de directorio* (DSA, *directory system agent*) es un proceso de aplicación que forma parte de directorio y cuyo papel es proporcionar a los DUA, clientes LDAP y/u otros DSA el acceso a la DIB. Un DSA puede utilizar información almacenada en su base de datos local o interactuar con otros DSA o servidores LDAP para atender las peticiones. Como otra posibilidad, el DSA puede remitir un peticionario a otro DSA que pueda ayudar a atender la petición. Cuando un DSA tiene la capacidad de emitir una petición LDAP y comprender la respuesta LDAP conexas, se dice que se trata de un peticionario LDAP. Cuando un DSA tiene la capacidad de comprender una petición LDAP y contestarla, se dice que se trata de un respondedor LDAP. Las bases de datos locales dependen enteramente de la implementación.

Un *servidor LDAP* representa un proceso de aplicación que forma parte del directorio, que da respuesta a las peticiones mediante el protocolo LDAP y cuyo cometido es proporcionar acceso a los clientes LDAP y/o peticionarios LDAP a la DIB. Este servidor puede aprovechar la información almacenada en su base de datos local o puede remitir al peticionario a otro respondedor o servidor LDAP que pueda atender la petición. Como en el caso de los DSA, las bases de datos locales dependen completamente de la implementación.

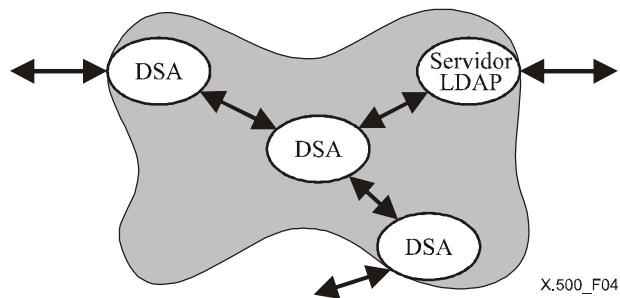


Figura 4 – Modelo funcional de directorio

## 9.2 Modelo de organización

Un conjunto de uno o más DSA y/o servidores LDAP, y ninguno o varios DUA y/o clientes LDAP manejados por una misma organización, pueden formar un dominio de gestión de directorio DMD. Esta organización puede optar por utilizar o no las Especificaciones de directorio para gobernar las comunicaciones entre los componentes funcionales dentro del DMD.

Las Especificaciones de directorio especifican ciertos aspectos del comportamiento de los DSA. Con este propósito, un grupo de DSA dentro de un DMD pueden, a modo de opción de la organización que maneja el DMD, comportarse como un DSA único.

Un DMD puede ser un DMD de Administración (ADDMD, *Administration directory management domain*) o un DMD privado (PRDMD, *private directory management domain*), lo que dependerá de que sea o no operado por una organización de telecomunicaciones del sector público.

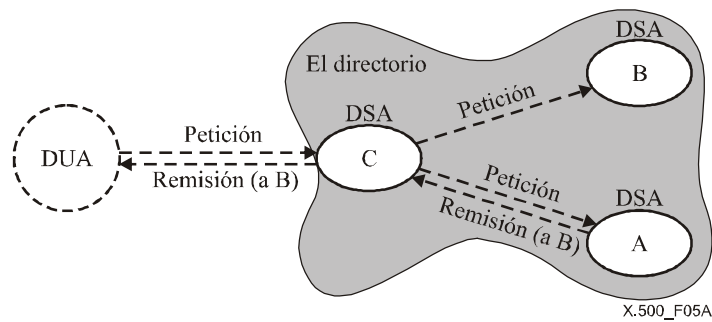
## 9.3 Funcionamiento del modelo

El DUA o cliente LDAP establece una comunicación con el directorio a través de uno o más DSA y/o servidores LDAP. Un DUA o cliente LDAP no necesita estar vinculado a ningún DSA o servidor LDAP específico. Puede interactuar directamente con varios DSA y/o servidores LDAP para hacer peticiones. Por razones administrativas, no siempre es posible interactuar directamente con el DSA o servidor LDAP que tiene que atender la petición, por ejemplo, devolviendo información de directorio. También es posible que el DUA o cliente LDAP pueda obtener acceso al directorio a través de un solo DSA. Para esto, los DSA necesitarán interactuar entre sí.

El DSA está encargado de atender las peticiones de los DUA y clientes LDAP y de obtener la información necesaria cuando no cuenta con ella. Puede asumir la responsabilidad de obtener la información interactuando con otros DSA y/o servidores LDAP en nombre del DUA o cliente LDAP.

Se han determinado varios casos de tratamiento de peticiones, que se ilustran en las figuras 5 a 7 y se describen a continuación.

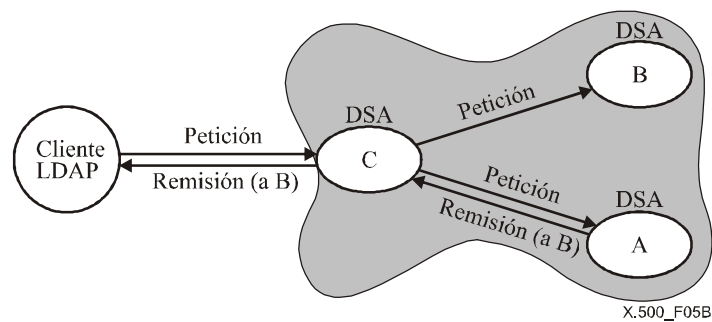
En la figura 5a, el DSA C recibe una remisión del DSA A y es responsable de transportar la petición al DSA B (designado en la remisión del DSA A) o de devolver la remisión al DUA de origen.



**Figura 5a – Remisiones**

NOTA 1 – Si DSA C devuelve la remisión al DUA, la "petición (a B)" no tendrá lugar. De manera similar, si DSA C transporta la petición a DSA B, no devolverá una remisión al DUA.

En la figura 5b, el DSA C recibe una remisión del DSA A y debe dirigirla al DSA B (designado en la remisión de DSA A), o devolverla al cliente LDAP originador.



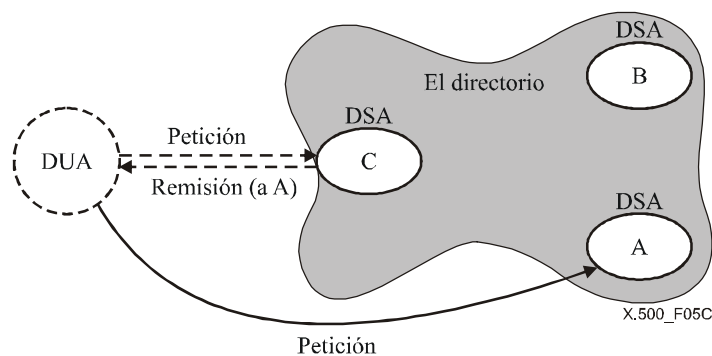
**Figura 5b – Remisiones**

NOTA 2 – En la figura 5b el DSA C debe ser un respondedor LDAP y puede soportar otros protocolos X.500.

NOTA 3 – Si el DSA C devuelve la remisión al cliente LDAP, la "petición (a B)" no tendrá lugar. Asimismo, si el DSA C transporta la petición a DSA B, no devolverá una remisión al cliente LDAP.

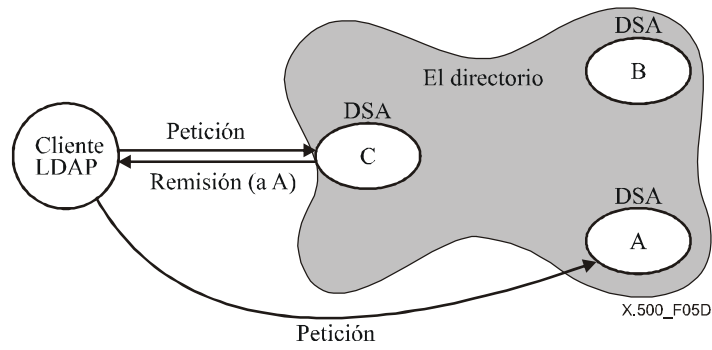
NOTA 4 – Si el DSA C devuelve la remisión al cliente LDAP, la remisión tendrá la forma de una remisión LDAP. Si la remisión devuelta por el DSA A es LDAP, el DSA C podrá devolverla directamente al cliente LDAP; de lo contrario, el DSA C transportará la petición al DSA B o traducirá la remisión a una remisión LDAP. Si el DSA C devuelve la remisión al cliente LDAP, éste se vinculará directamente con el DSA B, el cual será también un respondedor LDAP. Además, será necesario que el DSA B sea un respondedor LDAP si el DSA A devuelve una remisión LDAP y el DSA C transporta la petición directamente al DSA B.

En la figura 5c, el DUA recibe la remisión del DSA C, y se encarga de retransmitir la petición directamente al DSA A (nombrado en la remisión del DSA C).



**Figura 5c – Remisiones**

En la figura 5d, el cliente LDAP recibe la remisión del DSA C y se encarga de retransmitir la petición directamente al DSA A (nombrado en la remisión del DSA C).

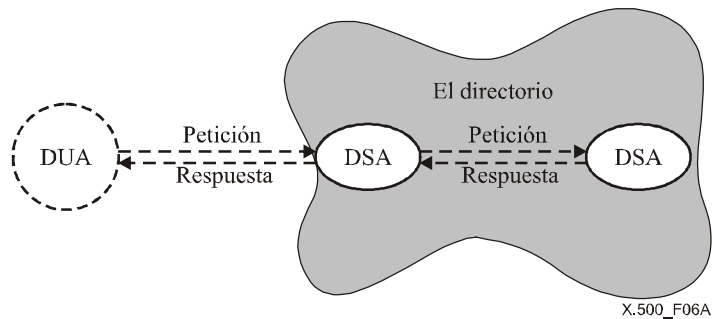


**Figura 5d – Remisiones**

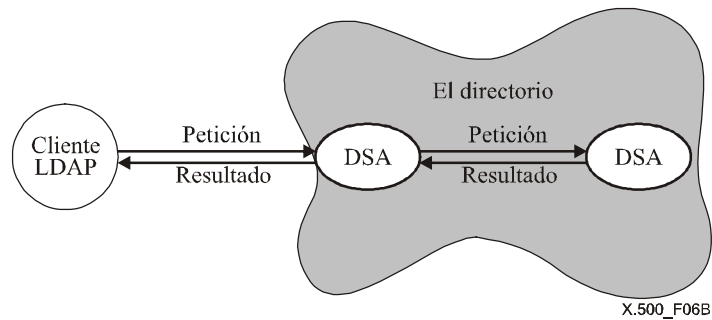
NOTA 5 – En la figura 5d, el DSA A y el DSA C son respondedores LDAP. Otra posibilidad sería que uno de los dos fuera un servidor LDAP.

NOTA 6 – La remisión que se devuelve al cliente LDAP tendrá la forma de una remisión LDAP.

Las figuras 6a a 6c muestran una uniconcatenación de DSA, en virtud de la cual la petición puede pasar por varios DSA antes de que se retorne la respuesta.

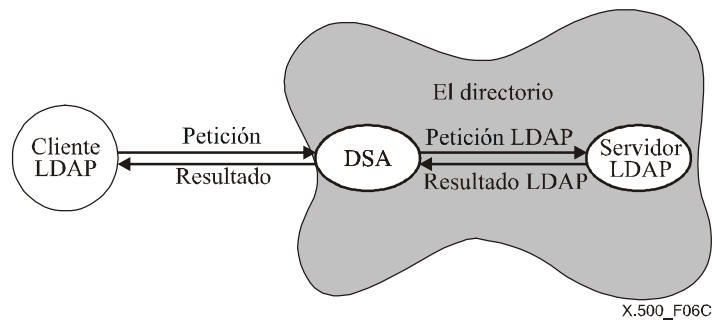


**Figura 6a – Uniconcatenación**



**Figura 6b – Uniconcatenación**

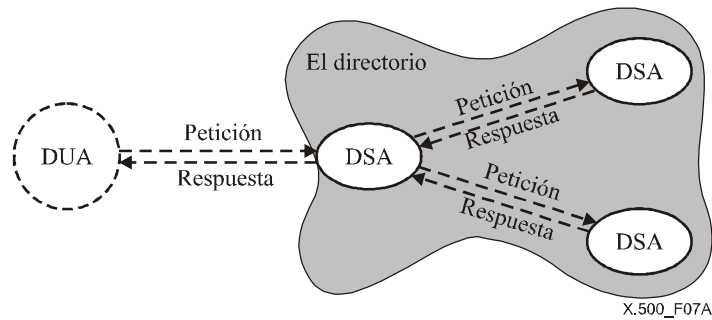
NOTA 7 – En la figura 6b, el DSA de la izquierda debe ser un respondedor LDAP, y puede soportar otros protocolos X.500.



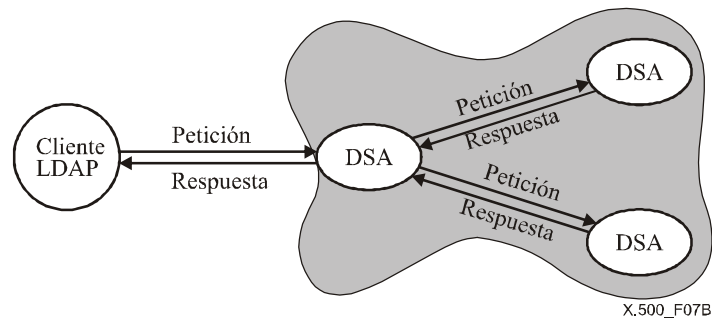
**Figura 6c – Uniconcatenación**

NOTA 8 – En la figura 6c, el DSA debe ser tanto un respondedor LDAP como un peticionario LDAP y puede soportar otros protocolos X.500.

Las figuras 7a a 7c muestran la multiconcatenación, en virtud de la cual el DSA asociado con el DUA o el cliente LDAP efectúa la petición enviándola a dos o más otros DSA y/o servidores LDAP, siendo idéntica la petición a cada DSA o servidor LDAP.

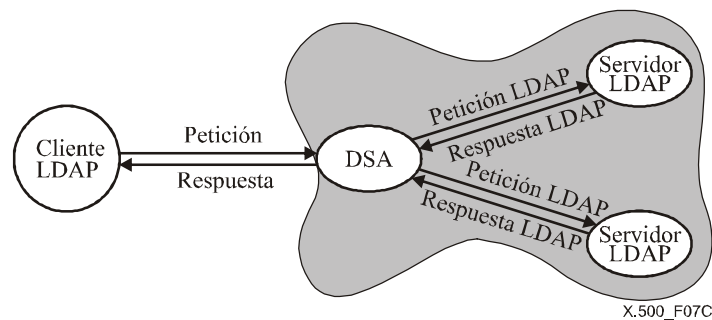


**Figura 7a – Multiconcatenación**



**Figura 7b – Multiconcatenación**

NOTA 9 – En la figura 7b, el DSA de la izquierda debe ser un respondedor LDAP y puede soportar otros protocolos X.500.



**Figura 7c – Multiconcatenación**

NOTA 10 – En la figura 7c, el DSA de la izquierda debe ser tanto un respondedor LDAP como un peticionario LDAP y puede soportar otros protocolos X.500.

Cada uno de estos métodos tiene sus propias ventajas. Por ejemplo, los métodos de las figuras 5b y 5d pueden utilizarse cuando convenga aligerar la carga del DSA local. En otras circunstancias será necesario un método mixto que combine un conjunto más elaborado de interacciones funcionales, a fin de satisfacer las exigencias del peticionario, como se ilustra en las figuras 8a y 8b.

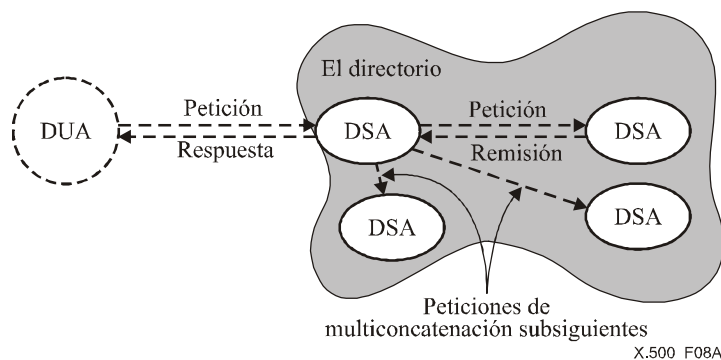


Figura 8a – Método que combina varios modos

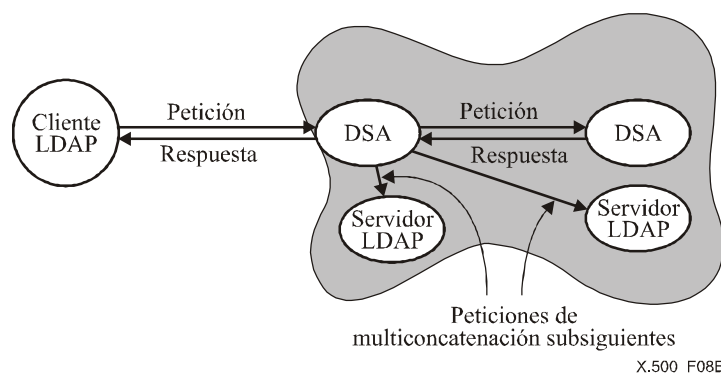


Figura 8b – Método que combina varios modos

## 10 Control de acceso en el directorio

NOTA – El modelo de control de acceso a directorio se define en la Rec. UIT-T X.501 | ISO/CEI 9594-2.

El acceso a información de directorio viene determinado por alguna política de seguridad administrativamente controlada. Dos aspectos de la política de seguridad que afectan al acceso al directorio son los procedimientos de autenticación y el esquema de control de acceso.

Los procedimientos y mecanismos de autenticación para soportar el directorio incluyen métodos para verificar y divulgar, cuando sea necesario, la identidad de los DSA, usuarios de directorio y el origen de la información recibida en un punto de acceso. Los procedimientos de autenticación generales se definen en la Rec. UIT-T X.509 | ISO/CEI 9594-8.

La definición de un esquema de control de acceso para soportar el directorio incluye métodos para especificar información de control de acceso, poner en vigor derechos de acceso definidos por esa información de control de acceso y mantener la información de control de acceso. La puesta en vigor de los derechos de acceso comprende el acceso con control a información de directorio relacionada con la estructura del DIT, a información de usuarios de directorio y a información operacional de directorio, incluida información de control de acceso.

En la Rec. UIT-T X.501 | ISO/CEI 9594-2 se define un esquema de "control de acceso básico" para el directorio (puede haber muchos). Las autoridades administrativas pueden utilizar la totalidad o partes de este esquema al implementar sus políticas de seguridad, o pueden definir libremente sus propios esquemas de acceso a su discreción. El esquema de control de acceso básico proporciona un medio de controlar el acceso a la información de directorio dentro del DIB (que potencialmente incluye información de estructura y de control de acceso). El control del acceso a la información permite la prevención de la detección, revelación o modificación no autorizadas de dicha información.

El control del acceso a la información permite prevenir la detección, revelación o modificación no autorizadas de dicha información. La Rec. UIT-T X.501 | ISO/CEI 9594-2 define tres esquemas de control de acceso específicos para el directorio denominados "control de acceso básico", "control de acceso simplificado" y "control de acceso basado en normas". Las autoridades administrativas pueden utilizar la totalidad o partes de estos esquemas al implementar sus políticas de seguridad, o pueden definir libremente sus propios esquemas de acceso a discreción. El esquema de control de acceso básico proporciona un medio de controlar el acceso a la información de directorio dentro del DIB (que potencialmente incluye información de estructura y de control de acceso). El esquema de control de acceso simplificado proporciona un subconjunto de funcionalidad del esquema de control de acceso básico. El esquema de control de acceso

basado en normas proporciona medios adicionales de controlar el acceso a la información de directorio dentro del DIB (que potencialmente incluye información de estructura y de control de acceso), basados en autorizaciones y etiquetas. El esquema de control de acceso basado en normas puede utilizarse junto con el control de acceso simplificado o el control de acceso básico, o bien puede utilizarse solo.

El modelo de control de acceso básico de directorio define, para cada operación, uno o más puntos en los que pueden tener lugar decisiones de control de acceso. En todas las decisiones de control de acceso hay que considerar:

- el componente al que se accede dentro del directorio, posiblemente una inserción compuesta completa;
- el usuario que solicita la operación;
- un derecho específico necesario para completar una parte de la operación; y
- la política de seguridad que rige el acceso a ese elemento.

El modelo de control de acceso basado en normas de directorio define, para cada operación, uno o más puntos en los que pueden tener lugar decisiones de control de acceso. En todas las decisiones de control de acceso hay que considerar:

- una autorización asociada con la petición de acceso del usuario;
- etiquetas de seguridad asociadas con la información a la que se accede;
- normas de política de seguridad que rigen ese acceso y que definen si debe negarse el acceso dada una relación entre la autorización y la etiqueta de seguridad.

## 11 Administración de servicios

El servicio abstracto de directorio, definido en la Rec. UIT-T X.501 | ISO/CEI 9594-2 proporciona el medio poderoso y eficaz de hojear y leer la información de directorio.

Estas Especificaciones de directorio proporcionan amplias capacidades de administración de servicios que permiten que las autoridades administrativas administren y restrinjan el servicio al usuario. Puede haber varias razones para que una autoridad administrativa restrinja y ajuste el servicio prestado a un usuario:

- Una autoridad administrativa tiene conocimiento de la calidad de la información que mantiene. Para mejorar la tasa de búsquedas exitosas de directorio y para asegurar que sólo se devuelve información de calidad, una autoridad administrativa puede restringir los tipos de atributos que se permiten en un filtro de búsqueda y la información que puede ser devuelta.
- Para proteger la inversión en información verificada y limpia, una autoridad administrativa puede imponer severas restricciones en cuanto a la información que puede ser devuelta, adaptada al tipo de usuario y al tipo de servicio prestado.
- Una autoridad administrativa puede desear impedir el uso inadecuado de la información, por ejemplo, para fines de propaganda comercial masiva: cuando se recopila el nombre de todas las personas que viven en una calle determinada, o de todas las personas con una determinada profesión, etc.
- Para proteger los datos personales aún más de lo que es posible utilizando el control de acceso. Esto incluye la devolución de direcciones postales falsas, no permitir búsquedas basadas en cadenas de caracteres muy cortas, no permitir búsquedas que utilizan ciertas combinaciones de atributos, o que requieren determinadas combinaciones, etc.
- Las restricciones y las adaptaciones que se deben hacer del servicio prestado pueden depender del grupo de usuarios.

## 12 Replicación en el directorio

NOTA – La replicación de directorio está definida en la Rec. UIT-T X.525 | ISO/CEI 9594-9.

### 12.1 Introducción

La replicación es la creación de copias de inserciones de directorio e información operacional de directorio en otros DSA que no son el DSA responsable de la creación y actualización de la información. Este DSA, que contiene la información original, es denominado DSA maestro.

Es posible construir sistemas de directorio que no hacen uso de información replicada.

La replicación de información de directorio sirve para satisfacer dos tipos generales de requerimientos: uno de ellos, relacionado con la calidad general del servicio proporcionado por el directorio, y el otro, relacionado con la gestión de sistemas de directorio.

## ISO/CEI 9594-1:2005 (S)

La creación de copias adicionales de inserciones de directorio podrá ser útil para la mejora del servicio proporcionado por el directorio:

- a) mejora de las prestaciones de los sistemas de directorio gracias al "acercamiento" de la información de directorio a determinados usuarios de directorio;
- b) mejora de la disponibilidad del servicio de directorio gracias a la introducción de componentes de directorio e información de directorio redundantes, de forma que el fallo de un determinado componente no impida todo acceso a la información en alguna porción del DIT.

La creación de copias adicionales de inserciones de directorio podrá ser útil en la gestión de sistemas de directorio:

- a) al facilitar la distribución de cierta información operacional (por ejemplo, conocimientos); y
- b) al proporcionar una oportunidad de recuperación a raíz de fallos de sistema graves, mediante la reconstrucción de la información destinada a estar contenida en un componente de directorio a partir de una copia de dicha información contenida en otro componente de directorio.

### 12.2 Formas de replicación de directorio

Existen tres formas de información de inserciones replicadas en los componentes del directorio: copias caché, información sombreada y múltiples implementaciones maestras.

Las copias caché son copias de información de inserción que un componente de directorio obtiene y utiliza de manera no especificada en estas Especificaciones de directorio.

Copias por sombreado son copias de información de directorio que un componente de directorio obtiene y utiliza de manera especificada en la Rec. UIT-T X.525 | ISO/CEI 9594-9.

Múltiples implementaciones maestras mantienen más de un ejemplar modificable de cada inserción dentro de un conjunto determinado de inserciones en el directorio. Cada copia modificable de una inserción en el directorio está completa (es decir, tiene todos los atributos de usuario y los atributos de funcionamiento que se comparten entre los DSA). Uno de los ejemplares se identifica de tal forma que el directorio lo identifique como el ejemplar maestro principal, para los casos en que es necesario realizar actualizaciones con un solo DSA (por ejemplo, cuando se aumenta el valor de un atributo que se emplea como un contador). La forma en la que un componente de directorio obtiene copias modificables de una inserción, y la forma en que se garantiza la coherencia de dichas copias tras una modificación queda fuera del alcance de esta Recomendación | Norma Internacional.

Los DSA podrán conservar información obtenida de otro DSA sólo si ello está permitido por la política y por el acuerdo en virtud del cual ha sido suministrada originalmente la información. Un DSA que conserve dicha información sólo puede suministrarla a los DUA y/o clientes LDAP de acuerdo con la política de control de acceso correspondiente a la información. Si se sabe que no existen controles de acceso a lectura en la información, puede suministrarse como si se concediera permiso de lectura.

Un DSA que contenga información caché o sombreada remite todas las peticiones que pudieran modificar la información de copia a un DSA maestro que contenga la información. Un DSA que contenga información copiada remite todas las peticiones que indiquen que no será utilizada información de copia, al DSA maestro que contenga la información.

Al responder a una interrogación con información de copia caché o sombreada, el DSA que contiene ese tipo de información indica que ha sido utilizada una copia para satisfacer la petición.

Las autoridades administrativas responsables de dos DSA podrán establecer un acuerdo de sombreado en virtud del cual un DSA (suministrador) proporcionará información sombreada a otro DSA (consumidor) a partir de una porción convenida del DIT. Si lo permite el acuerdo suscrito para proporcionar información sombreada, el consumidor puede concertar acuerdos con otros DSA para convertirse en suministrador de sombreados de esa información.

Además de actualizar las copias de información que tiene el consumidor de sombreados, el suministrador podrá proporcionarle información operacional (por ejemplo, datos de filiación).

En los acuerdos de sombreado, la información a replicar constará típicamente de tres elementos:

- Información de inserciones replicada procedente del interior de un subárbol del DIT.
- Información operacional pertinente, incluida información de control de acceso requerida para dar pleno acceso de lectura de la información replicada.
- Opcionalmente, información de conocimientos subordinada.



La información replicada podrá constituir un subconjunto de la información completa interna al subárbol, en los sentidos siguientes:

- Podría efectuarse una selección de las inserciones especificando únicamente aquellas que cumplen ciertos criterios con respecto a sus clases de objeto.
- Dentro de cada inserción podría efectuarse una selección de los atributos con arreglo a una especificación de atributos.
- Dentro de cada atributo podría efectuarse una selección de los valores de atributo basada en sus contextos.

### 12.3 Replicación y congruencia de información de directorio

Se logra la congruencia en el directorio cuando todas las copias de un atributo específico son idénticas. En ocasiones, la congruencia podría estar sujeta a compromiso, dado que pueden existir dentro de directorio incongruencias transitorias con respecto a la información duplicada, e inconsistencias permanentes con respecto a la información caché.

La información de inserciones caché puede seguir siendo incongruente con la información de inserciones mantenida por el componente de directorio al cual se dirigen las actualizaciones. En cambio, la información sombreada conservada por un consumidor de sombreado se pone en concordancia con la información correspondiente conservada por un suministrador con arreglo a un programa contratado como parte del acuerdo de sombreado.

Es esencial que la información contenida en un ejemplar de una entrada de objeto sea internamente congruente. Todo mecanismo de replicación irá acompañado de mecanismos que mantengan la congruencia interna de la información replicada y la fiabilidad del servicio. El directorio define procedimientos de esquema que aseguren la congruencia interna de una entrada.

También hay que garantizar la exactitud de los datos de filiación que permiten al DIT estar distribuido entre DSA. Todo mecanismo de replicación deberá ir acompañado de mecanismos que mantengan la exactitud de la información de conocimientos y la fiabilidad del servicio. El directorio define procedimientos de manipulación de la información de conocimientos mínima necesitada por un DSA para asegurar la coherencia del DIT.

En un entorno en que es replicada la información de directorio, el directorio no tiene limitaciones de tiempo específicas para lograr la congruencia. Un usuario de información sombreada tendrá un alto grado de confianza en él, puesto que:

- la información duplicada es internamente congruente;
- la filiación en el DIT es exacta;
- la inserción sombreada será al cabo congruente con la inserción en el DSA maestro.

### 12.4 Enfoques de la replicación

En esta subcláusula se describen las distintas maneras en que la existencia de replicación de información de directorio se manifiesta desde los puntos de vista de:

- a) usuarios de directorio;
- b) usuarios administrativos;
- c) los componentes operacionales de directorio (DSA).

#### 12.4.1 Enfoque del usuario de directorio

Dada la naturaleza de la operación de directorio, la información replicada será por lo general congruente con la información contenida por el DSA maestro con respecto a dicha información. Por consiguiente, en el caso general la información pedida, retornada al usuario extremo, será de naturaleza aceptable, y la circunstancia de que proceda de una copia carecerá de importancia.

El usuario de directorio es notificado siempre que se utiliza una copia para responder a una petición. En caso de necesidad absoluta del usuario, o de que éste detecte una incongruencia, el usuario puede optar por pedir acceso a información del DSA maestro.

Por consiguiente, el usuario de directorio tiene la posibilidad de elegir entre un nivel superior de prestaciones y disponibilidad, con el inconveniente de recibir ocasionalmente información anticuada, y un grado máximo de oportunidad de la información, con el inconveniente de una posible disminución de prestaciones y disponibilidad.

#### 12.4.2 Enfoque del usuario administrativo

Un usuario administrativo está encargado de gestionar el servicio proporcionado por un DSA y la información contenida en el mismo. Para efectuar esta función de gestión, el usuario administrativo requiere útiles que le permitan supervisar, controlar y optimizar el servicio del DSA.

La capacidad normalizada (y local) de un DSA de soportar replicación es uno de los principales útiles disponibles al usuario administrativo a la hora de optimizar el servicio proporcionado por un DSA.

#### 12.4.3 Enfoque del DSA

Aunque un DSA puede detectar la diferencia entre información replicada e información contenida por un máster, por lo general utiliza ambas de la misma manera; es decir, satisface las peticiones de interrogación de usuario con aquella de las dos de la que tenga más fácil disponibilidad.

Esta equivalencia entre máster e información replicada tiene dos excepciones. Un DSA solamente utiliza información de inserciones para satisfacer peticiones de modificación de la DIB y peticiones de interrogación que señalen que la información replicada no es aceptable.

Además, dado que podría eventualmente saberse que la información contenida localmente es parcial (véase 12.2), un DSA podrá pasar una encuesta a otro DSA más habilitado para proporcionar la información requerida.

NOTA – Un DSA puede contener información replicada de varias fuentes, información que podría superponerse. Si así ocurriera, el DSA mantendrá separadamente cada enfoque de la información, tal como la proporcione la replicación.

### 12.5 Replicación y control de acceso

El modelo de control de acceso permite especificar información de control de acceso para un área del DIT. Dicha área podrá abarcar fronteras de DSA. De estar involucrados múltiples DSA, cada uno de ellos contendrá la información de control de acceso apropiada.

En cada ocasión en que sean replicadas entradas con destino a otro DSA, la información de control de acceso deberá ser también replicada.

## 13 Protocolos de directorio

NOTA – Los protocolos de directorio definidos para permitir que DUA y DSA de sistemas abiertos diferentes cooperen, están especificados en la Rec. UIT-T X.519 | ISO/CEI 9594-5.

Hay cuatro protocolos de directorio:

- el protocolo de acceso a directorio (DAP, *directory access protocol*), que define el intercambio de peticiones y resultados entre un DUA y un DSA;
- el protocolo de sistema de directorio (DSP, *directory system protocol*), que define el intercambio de peticiones y resultados entre dos DSA;
- el protocolo de duplicación de información de directorio (DISP, *directory information shadowing protocol*), que define el intercambio de información de replicación entre dos DSA que han establecido acuerdos de sombreado;
- el protocolo de gestión de vinculaciones operacionales de directorio (DOP, *directory operational binding management protocol*), que define el intercambio de información administrativa entre dos DSA para administrar vinculaciones operacionales entre ellos.

Cada protocolo está definido como un conjunto de elementos de protocolo. Así, por ejemplo, el DAP contiene elementos de protocolo asociados a interrogación y modificación de directorio.

## 14 Gestión de sistemas de directorio

NOTA – La gestión de sistemas de directorio se define en la Rec. UIT-T X.530 | ISO/CEI 9594-10.

### 14.1 Introducción

La finalidad de la gestión de directorio es asegurar que los usuarios dispongan según lo previsto, de la información de directorio necesaria y precisa con el tiempo de respuesta, la integridad, la seguridad y el nivel de coherencia esperados. Además, la gestión de sistemas debe lograrse imponiendo la mínima carga posible en el tiempo de procesamiento y la memoria en las plataformas y el sistema de comunicaciones.

La gestión de directorio se divide en cuatro segmentos principales:

- a) Gestión del dominio DIT: gestión de información de directorio;
- b) Gestión del funcionamiento de un único DSA;
- c) Gestión de un único DUA; y
- d) Gestión del DMD – gestión integrada de los componentes funcionales de directorio.

La especificación de la gestión de sistemas se ocupa de los tres primeros segmentos. La gestión del dominio de gestión de directorio queda en estudio.

## **14.2 Gestión del dominio DIT**

El protocolo de acceso de directorio (DAP) gestiona los atributos de usuario en el directorio. Los atributos de funcionamiento pueden gestionarse también utilizando DAP. Esto incluye atributos en la estructura de información, atributos del subesquema, atributos de control de acceso, y los atributos en el árbol de información DSA, incluido conocimientos. Los conocimientos pueden gestionarse también utilizando el protocolo de vinculación operacional de protocolo, el protocolo de duplicación de información de directorio y el protocolo del sistema de directorio.

## **14.3 Gestión de componentes de directorio**

La especificación de la gestión de sistema define los objetos gestionados de la gestión de sistemas OSI utilizados para gestionar los componentes de directorio (los DUA y DSA) dentro de un dominio de directorio. La gestión de estos componentes de directorio puede lograrse utilizando los servicios y el protocolo de información de gestión común.

El directorio o los servicios de gestión no satisfacen algunos requisitos de gestión pero ello puede subsanarse mediante servicios definidos localmente.

## Anexo A

### Aplicación de directorio

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

#### A.1 El entorno de directorio

NOTA – En esta subcláusula, el término *red* se utiliza en su acepción general, para designar el conjunto de sistemas y procesos interconectados relacionados con cualquier servicio de telecomunicaciones y no únicamente de uno relacionado con la capa de red OSI.

El entorno de directorio, en el que éste ofrece servicios, es el siguiente:

- a) Muchas redes de telecomunicaciones serán de gran envergadura y sufrirán constantes cambios:
  - 1) objetos de diversos tipos entrarán y saldrán de la red sin ningún aviso, bien por separado o en grupos;
  - 2) la conectividad de los objetos (especialmente los nodos de la red) cambiará debido a la adición o eliminación de trayectos entre ellos;
  - 3) diversas características de los objetos, tales como sus direcciones, disponibilidad y ubicación física, pueden cambiar en cualquier momento.
- b) Si bien la frecuencia general de modificación es elevada, la vida útil de un objeto determinado no es corta. Por lo común, un objeto participará en comunicaciones con mucha mayor frecuencia que la de cambio de su dirección, disponibilidad, ubicación física, etc.
- c) Los objetos que participan en los actuales servicios de telecomunicaciones se identifican por lo general mediante números u otras cadenas de símbolos, seleccionados en función de su facilidad de atribución y procesamiento pero no en función de su facilidad de utilización por los humanos.

#### A.2 Características del servicio de directorio

La necesidad de capacidades de directorio obedece:

- a) al deseo de aislar (tanto como sea posible) al usuario de la red de los cambios frecuentes que ocurren en ella. Esto puede lograrse creando un 'nivel de indirección' entre los usuarios y los objetos tratados por ellos. Esto implica que los usuarios se refieran a los objetos dando un nombre y no por ejemplo, una dirección (postal). El directorio proporciona el servicio para establecer la necesaria correspondencia;
- b) al deseo de presentar una imagen de la red, que sea más "cómoda para el usuario". Por ejemplo, el uso de alias, la prestación del servicio de *páginas amarillas* (véase A.3.5), etc., ayudan a aliviar la labor de encontrar y utilizar la información de la red.

El directorio permite a los usuarios obtener una diversidad de informaciones sobre la red y ofrece los medios necesarios para el mantenimiento, la distribución y la seguridad de dicha información.

#### A.3 Patrones de utilización de directorio

NOTA – Esta subcláusula se refiere únicamente a la extracción de información de directorio; se supone que los servicios de modificación de directorio son utilizados únicamente para el mantenimiento de la DIB en el tiempo, en la forma necesaria para la aplicación.

##### A.3.1 Introducción

El servicio de directorio se define en estas Especificaciones de directorio en base a las peticiones concretas que puede realizar un DUA y a los parámetros de las mismas. Sin embargo, el diseñador de una aplicación, al considerar las exigencias de extracción de información de directorio en dicha aplicación, adoptará probablemente un punto de vista más conforme a su objetivo específico. Por lo tanto, en esta cláusula se describe una serie de patrones de utilización de alto nivel del servicio de directorio que podrían ofrecer interés para muchas aplicaciones.

##### A.3.2 Consulta

En una consulta directa de directorio, el DUA suministra el nombre distinguido de un objeto junto con un tipo de atributo. El directorio devolverá todo valor o valores que correspondían a ese tipo de atributo. Ésta es una generalización de la función clásica de directorio, que se obtiene cuando el tipo de atributo solicitado corresponde a un tipo específico de dirección. Los tipos de atributo para los diversos tipos de direcciones están normalizados, lo que incluye la dirección de PSAP de OSI, la dirección O/R de tratamiento de mensajes y los números de teléfono y de télex.

La consulta es soportada por el servicio de lectura, que además permite las siguientes generalizaciones adicionales:

- la consulta puede basarse en nombres que no sean el nombre distinguido del objeto, por ejemplo, alias;
- los valores de una serie de tipos de atributos pueden solicitarse en una sola petición, siendo el caso extremo aquel en el que deban devolverse los valores de todos los atributos de la inserción en cuestión;
- se pueden solicitar los valores particulares de un atributo sobre la base de un contexto (por ejemplo, en valor francés del nombre de una organización).

### A.3.3 Denominación cómoda para el usuario

Pueden elegirse nombres de objetos que una persona pueda suponer (o recordar) más fácilmente. Los nombres que tienen esta propiedad suelen estar formados de atributos que, de alguna manera, son inherentes al objeto, y no ser inventados con dicho propósito. El nombre de un objeto será común a todas las aplicaciones que se refieran al mismo.

### A.3.4 Examen rápido ("hojeado")

En muchos usos de directorio por el ser humano, tal vez no sea posible para el usuario (o DUA) indicar directamente un nombre, sea este del tipo fácil para el usuario, o de otro tipo, del objeto sobre el cual busca información. Sin embargo, tal vez el usuario 'lo reconocerá cuando lo vea'. La posibilidad de hojear el directorio permitirá al usuario humano recorrer la DIB para buscar las inserciones adecuadas.

El examen rápido se logra por una combinación de los servicios de listado y de búsqueda, posiblemente junto con el de lectura (aunque el servicio de búsqueda incluye la capacidad de lectura).

### A.3.5 Páginas amarillas

Hay una diversidad de formas de proporcionar una capacidad del tipo *Páginas amarillas*. La más sencilla se basa en filtrado, utilizando las aserciones sobre atributos particulares cuyos valores son las categorías (por ejemplo, el tipo de atributo 'categoría comercial' definido en la Rec. UIT-T X.520 | ISO/CEI 9594-6). Este método no requiere el establecimiento de ninguna información especial dentro del DIT, salvo para garantizar que están presentes los atributos necesarios. Sin embargo, en el caso general, cuando hay una población, la búsqueda puede resultar costosa ya que el filtrado requiere la generación del conjunto universal que se ha de filtrar.

Se puede utilizar otro posible método basado en el establecimiento de subárboles especiales cuyas estructuras de denominación están especialmente concebidas para la búsqueda del tipo *Páginas amarillas*. La figura A.1 muestra un ejemplo de un subárbol del tipo *Páginas amarillas* en el cual sólo figuran asientos de alias. En realidad, las inserciones en los subárboles de *Páginas amarillas* pueden ser una combinación de inserciones de objeto y de alias, a condición de que sólo exista una inserción de objeto para cada objeto almacenado en el directorio.

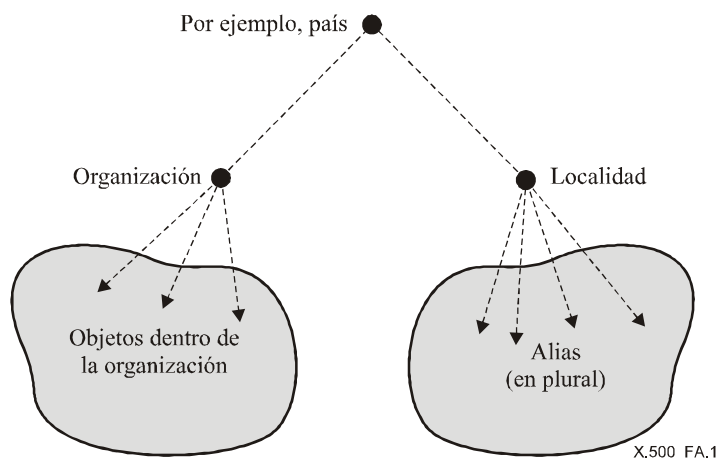


Figura A.1 – Subárbol del tipo páginas amarillas

### A.3.6 Restricciones y facilitación de búsquedas

En muchas indagaciones, un intento inicial de buscar información resulta en la obtención de muy poca o demasiada información. El directorio contiene disposiciones que permiten "facilitar" una búsqueda para permitir mayores posibilidades de éxito (por ejemplo, efectuando automáticamente una segunda búsqueda que intenta la concordancia fonética en vez de una concordancia de cadena estricta), o puede "restringir" una búsqueda, para reducir el número de intentos. El directorio permite también una regla de concordancia local más apropiada que sustituya a la regla de concordancia normalizada que de otro modo pudiera aplicarse.

## ISO/CEI 9594-1:2005 (S)

Por ejemplo, se puede utilizar una regla de concordancia que concuerda una localidad con una localidad almacenada utilizando la concordancia geográfica en vez de una regla de concordancia de cadena. Es posible combinar ambas: si una concordancia geográfica estricta no produce resultados (concordar "Warfield" con "Bracknell" fracasaría), una concordancia geográfica menos estricta podría tener éxito (en este caso concordar "Warfield" con "Bracknell" podría tener éxito si la concordancia abarca Bracknell y los pueblos inmediatamente cercanos, incluido Warfield).

Se puede utilizar también esta flexibilidad para ampliar el poder de búsqueda en las *Páginas amarillas*: una categoría más genérica podría sustituir a una más específica. Por ejemplo, "Restaurantes" como una cadena no concordaría con "Restaurantes chinos", pero podría hacerse concordar sustituyendo o haciendo más flexible la regla de concordancia.

### A.3.7 Grupos

Un grupo es un conjunto cuya composición puede cambiar con el tiempo por la adición o supresión explícitas de miembros. El grupo es un objeto, al igual que sus miembros. Se puede pedir al directorio que:

- indique si un objeto dado es o no miembro de un grupo;
- enumere los miembros de un grupo.

Para soportar grupos se hace que la inserción para el grupo contenga un atributo 'miembro' de múltiples valores (este tipo de atributo se define en la Rec. UIT-T X.520 | ISO/CEI 9594-6). Las dos capacidades mencionadas pueden entonces realizarse por medio de comparación y lectura respectivamente.

Un miembro de un grupo puede en sí mismo ser un grupo, si esto resulta significativo para la aplicación. Sin embargo, el DUA tendría que crear los servicios de verificación y expansión recursivos necesarios a partir de las versiones no recursivas con que cuenta.

### A.3.8 Autenticación

Muchas aplicaciones requieren que los objetos participantes ofrezcan cierta prueba de su identidad antes de que se les permita realizar una acción. El directorio soporta este proceso de autenticación. (Por otra parte, el propio directorio requiere que sus usuarios se autentiquen a sí mismos, para soportar el control de acceso.)

El método de autenticación más directo denominado 'autenticación simple', se basa en el uso por el directorio de un atributo 'contraseña de usuario' en la inserción de cualquier usuario que desee poder autenticarse a sí mismo ante un servicio. A petición del servicio, el directorio confirmará o negará que un valor específico suministrado es realmente la contraseña del usuario. Esto evita que el usuario tenga que poseer una contraseña diferente para cada servicio. En aquellos casos en que se considere inapropiado, el intercambio de contraseñas en un entorno local que utiliza la autenticación simple, el directorio podrá, facultativamente, proporcionar medios para proteger esas contraseñas contra una reproducción o uso indebido por una función unidireccional.

El método más complejo, denominado 'autenticación fuerte', se basa en la criptografía de claves públicas, en la cual el directorio actúa como un depositario de claves públicas de criptación de los usuarios, debidamente protegidas contra las maniobras fraudulentas. El procedimiento que los usuarios pueden seguir para obtener, de directorio, las claves públicas de cada uno de los demás usuarios, y después autenticarse mutuamente, se describen detalladamente en la Rec. UIT-T X.509 | ISO/CEI 9594-8.

### A.3.9 Ubicación basada en los atributos

Muchas aplicaciones exigen la capacidad de poder determinar rápidamente la existencia o no existencia de una inserción con un valor de atributo específico y para las inserciones cuya existencia ha sido determinada, exige la capacidad de encontrarlas y recuperarlas rápidamente. En un directorio que consiste en un solo DSA, esto resulta relativamente fácil. No obstante, en un directorio distribuido, las búsquedas basadas en los atributos pueden presentar problemas ya que puede ser difícil controlar el tiempo máximo de búsqueda.

Hay una solución relativamente sencilla en entornos en los cuales se conoce el conjunto de los DSA y éste puede gestionarse de manera cooperativa. Para poder soportar la búsqueda rápida de atributos específicos, podrá configurarse un solo DSA (o un conjunto de DSA específicos) para mantener una zona replicada y filtrada que contenga esos atributos de interés. De esta manera, el proceso de búsqueda puede restringirse a un solo DSA, con una respuesta rápida (sí o no), y señalando, cuando la inserción existe, el DSA maestro correspondiente a esa inserción. La replicación se examina con detalle en la Rec. UIT-T X.525 | ISO/CEI 9594-9.

## A.4 Aplicaciones genéricas

### A.4.1 Introducción

Cabe imaginar varias aplicaciones genéricas que pueden ser soportadas implícitamente por el directorio, es decir, aplicaciones que no son peculiares de ningún servicio en especial de telecomunicaciones. Seguidamente se describen

dos de estas aplicaciones: el directorio de comunicaciones interpersonales y el directorio de comunicaciones intersistemas (para OSI).

NOTA – La autenticación, descrita en A.3.8 como un patrón de acceso, podría igualmente considerarse una aplicación genérica de directorio.

#### A.4.2 Comunicaciones interpersonales

El propósito de esta aplicación es proporcionar a las personas, o a sus agentes, información sobre la forma de comunicarse con otras personas o grupos de personas.

Entran en juego sin duda las siguientes clases de objetos: persona, función en la organización y grupo. Intervienen también muchas otras clases, probablemente en menor proporción, como: país, organización, unidad de la organización.

Los tipos de atributos que entran en juego, aparte de los utilizados en la denominación, son generalmente atributos de direccionamiento. Típicamente, la inserción para una persona determinada contendrá las direcciones correspondientes a cada uno de los métodos de comunicación por medio de los cuales se puede alcanzar a dicha persona, elegidos de una lista abierta que incluye cuando menos los siguientes: telefonía, correo electrónico, télex, RDSI, entrega física (por ejemplo, el sistema postal), facsímil. En algunos casos, como en el del correo electrónico, la inserción contendrá información adicional, como los tipos de información que puede tratar el equipo del usuario. Si se ha de soportar la autenticación, se necesitarán credenciales y/o contraseñas del usuario.

Los esquemas de denominación utilizados para las diversas clases de objeto deben ser cómodos para el usuario, con los alias adecuados para poder proporcionar nombres alternativos, asegurar la continuidad después del cambio de un nombre, etc.

En esta aplicación se verificarán los siguientes patrones de acceso: consulta, denominación cómoda para el usuario, examen rápido, *páginas amarillas* y grupos. En diversos grados, también se utilizará autenticación.

#### A.4.3 Comunicaciones entre sistemas (para OSI)

De acuerdo con el modelo de referencia de OSI, la OSI requiere dos funciones de directorio, a saber, una en la capa de aplicación que establece la correspondencia de los títulos de aplicación con direcciones de presentación, y otra en la capa de red, que hace establecer la correspondencia de las direcciones NSAP con direcciones de punto de asociación de subred (SNPA, *subnetwork point of attachment*).

NOTA – En el resto de esta subcláusula se trata únicamente el caso de la capa de aplicación.

Esta función se realiza consultando el directorio si la información requerida para establecer la correspondencia no está disponible localmente.

Los usuarios son entidades de aplicación y las clases de objeto que interesan son también entidades de aplicación, o subclases de las mismas.

El principal tipo de atributo que interviene, aparte de los utilizados para la denominación, es el de dirección de presentación. Otros tipos de atributos, que no se consideran necesarios para la propia función de directorio, podrían soportar la verificación o determinación del tipo de entidad de aplicación, o las listas de contextos de aplicación, sintaxis abstractas, etc. soportados. Los tipos de atributos relacionados con la autenticación también pueden ser aplicables.

## Anexo B

### Enmiendas y corrigenda

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

La presente edición de esta Especificación de directorio incluye el siguiente proyecto de enmienda que fue votada y aprobada por ISO/CEI:

- enmienda 3 para armonizar en lo posible los sistemas X.500 y LDAP.

La presente edición de esta Especificación de directorio no incluye ningún corrigendum técnico porque no se ha aceptado ningún informe de defectos en la anterior edición de esta Especificación de directorio.





## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación