



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**Z.331**

**LENGUAJE HOMBRE-MÁQUINA**

---

**INTRODUCCIÓN A LA ESPECIFICACIÓN  
DEL INTERFAZ HOMBRE-MÁQUINA**

**Recomendación UIT-T Z.331**

(Extracto del *Libro Azul*)

---

## NOTAS

- 1 La Recomendación UIT-T Z.331 se publicó en el fascículo X.7 del Libro Azul. Este fichero es un extracto del Libro Azul. Aunque la presentación y disposición del texto son ligeramente diferentes de la versión del Libro Azul, el contenido del fichero es idéntico a la citada versión y los derechos de autor siguen siendo los mismos (Véase a continuación).
- 2 Por razones de concisión, el término «Administración» se utiliza en la presente Recomendación para designar a una administración de telecomunicaciones y a una empresa de explotación reconocida.

© UIT 1988, 1993

Reservados todos los derechos. No podrá reproducirse o utilizarse la presente Recomendación ni parte de la misma de cualquier forma ni por cualquier procedimiento, electrónico o mecánico, comprendidas la fotocopia y la grabación en micropelícula, sin autorización escrita de la UIT.

## **INTRODUCCIÓN A LA ESPECIFICACIÓN DEL INTERFAZ HOMBRE-MÁQUINA**

### **1 Alcance de la sección**

El interfaz hombre-máquina comprende el conjunto de entradas, salidas y acciones especiales, junto con los mecanismos de interacción hombre-máquina, incluidos los procedimientos de diálogo. Estos elementos se combinan para manejar las variadas funciones de las telecomunicaciones que abarca la gestión de los sistemas de telecomunicaciones con control por programa almacenado (CPA). La consideración de estas funciones ha constituido una condición esencial para el desarrollo de las Recomendaciones del LHM del CCITT.

Como se indica en la Recomendación Z.301, el LHM del CCITT puede utilizarse para facilitar la operación, el mantenimiento, la instalación y las pruebas de aceptación de los sistemas CPA. Con la tendencia de las Administraciones a centralizar los trabajos de operación y mantenimiento, muchas de las funciones de los sistemas CPA pueden controlarse en terminales asociados con los sistemas de operación y mantenimiento, así como en los terminales asociados con sistemas CPA. Estos terminales pueden ser locales o distantes con relación al sistema.

Para ayudar a las Administraciones que se han propuesto lograr una uniformidad entre los diferentes sistemas, las Recomendaciones del LHM no sólo incluyen la sintaxis del lenguaje y de los procedimientos de diálogo, sino también la semántica relativa al interfaz hombre-máquina. La sección 4 proporciona los medios para obtener tal semántica.

### **2 Organización de la sección 4**

La sección 4 consta de las siguientes Recomendaciones:

- Z.331 Introducción a la especificación del interfaz hombre-máquina
- Z.332 Metodología para la especificación del interfaz hombre-máquina – Procedimiento general de trabajo
- Z.333 Metodología para la especificación del interfaz hombre-máquina – Instrumentos y métodos
- Z.334 Administración de abonados
- Z.335 Administración del encaminamiento
- Z.336 Administración de las mediciones de tráfico
- Z.337 Administración de la gestión de red

La *Recomendación Z.331* enumera las funciones de operación, mantenimiento, instalación y pruebas de aceptación que han de controlarse mediante el LHM.

La *Recomendación Z.332* presenta la primera parte, relativa al procedimiento general de trabajo, de una metodología mediante la cual puede generarse el interfaz hombre-máquina para una determinada zona o subzona funcional.

La *Recomendación Z.333* presenta la segunda parte, relativa a los instrumentos y métodos, de una metodología mediante la cual puede generarse el interfaz hombre-máquina para una determinada área o subárea funcional.

Las *Recomendaciones Z.334 a Z.337* se basan en la aplicación de las fases 1, 2 y 3 de la metodología definida en las Recomendaciones Z.332 y Z.333 para la administración de abonados, administración del encaminamiento, administración de mediciones de tráfico y administración de la gestión de red.

La parte principal de cada Recomendación contiene el modelo del área o subárea funcional. El anexo A de cada Recomendación contiene la lista de funciones que deben controlarse por medio del LHM y la lista de trabajos considerados en el desarrollo del modelo. El anexo B de cada Recomendación contiene una lista de funciones LHM y los diagramas de estructura de la información asociada, para que se utilicen como líneas directrices.

### 3 Funciones a controlar por medio del LHM

Las funciones a controlar por medio del LHM se subdividen en cuatro áreas principales: operación, mantenimiento, instalación y prueba de aceptación. La lista de dichas funciones figura más adelante. Sobre la base de las relaciones existentes entre ellas, las funciones de cada área principal se agrupan en áreas funcionales y a veces en subáreas funcionales. Al ser potencialmente diferentes las necesidades de organización y los principios de diseño del sistema, no todas las funciones se aplican a todos los sistemas.

Esta lista de funciones no está completa y se prevé que continúe evolucionando.

En particular, la existencia de Recomendaciones sobre áreas o subáreas específicas conducirá a mejorar la lista preliminar identificada en esta Recomendación para dichas áreas o subáreas funcionales. Hasta ahora esta mejora se ha conseguido para la administración de abonados, administración del encaminamiento, administración de la gestión de red (parcialmente), que se especifican en las Recomendaciones Z.334 a Z.337.

#### 3.1 *Funciones de operación*

##### 3.1.1 *Administración de abonados* (véase la Recomendación Z.334)<sup>1)</sup>

- administración de datos relativos a las líneas de abonado;
- seguimiento de llamadas maliciosas;
- extracción de información de tasación de abonados;
- observación de la tasación de abonados.

##### 3.1.2 *Administración del encaminamiento y del análisis de cifras*

###### 3.1.2.1 *Administración del encaminamiento* (véase la Recomendación Z.335)

- gestión de la base de datos de encaminamiento;
- búsqueda en la base de datos de encaminamiento.

###### 3.1.2.2 *Administración del análisis de cifras*

- gestión de los datos de análisis de cifras;
- búsqueda en la base de datos de análisis de cifras.

##### 3.1.3 *Administración del tráfico*

###### 3.1.3.1 *Administración de las mediciones de tráfico* (véanse las Recomendaciones E.502 y Z.336)

- realización de mediciones de tráfico;
- calendario de la ejecución de mediciones de tráfico y la salida de resultados;
- gestión de datos de mediciones;
- obtención de datos de mediciones.

###### 3.1.3.2 *Administración del análisis del tráfico* (véase la Recomendación E.502)

- introducción de datos medidos;
- introducción de la identificación e información de capacidad del objeto de medición;
- gestión de registros de datos de tráfico;
- gestión de la salida de informes;
- gestión de datos de descripción del análisis;
- supervisión del control del retardo de las diferentes operaciones de análisis.

---

<sup>1)</sup> La administración de abonados se ocupa de abonados con una sola línea y de abonados multilíneas.

#### 3.1.4 *Administración de tarifas y tasas*

- modificación de la tarifa aplicada a un determinado destino de tráfico;
- modificación de los parámetros que determinan la tarifa;
- cambio de la hora de paso de tarifa diurna a nocturna;
- lectura de estadísticas de contabilidad (contabilidad entre compañías de explotación);
- modificación de los parámetros utilizados en los métodos de contabilidad para tráfico entre diferentes compañías de explotación;
- extracción de información de tasación.

#### 3.1.5 *Operaciones de control del sistema*

- establecimiento y lectura de calendarios de operaciones;
- administración del encaminamiento de salida;
- administración de ficheros;
- administración de capacidades de terminal LHM;
- gestión de la configuración del sistema (soporte físico/soporte lógico).

#### 3.1.6 *Administración del control de acceso usuario-sistema* (véase el apéndice I a la Recomendación Z.331)

- autoridad de administración;
- extracción de información relativa a la autoridad.

#### 3.1.7 *Administración de la gestión de red* (véase la Recomendación Z.337)

- realización de mediciones del estado y comportamiento de la red;
- realización de acciones de gestión de red;
- distribución de información de gestión de red.

### 3.2 *Funciones de mantenimiento*

#### 3.2.1 *Mantenimiento de líneas de abonado*

- prueba de una línea de abonado y del equipo asociado;
- prueba de un grupo de líneas de abonado y del equipo asociado;
- medición de una línea de abonado y del equipo asociado;
- medición de un grupo de líneas de abonado y del equipo asociado;
- bloqueo o desbloqueo de una línea de abonado con fines de mantenimiento;
- observación o supervisión de líneas y equipos de abonado.

#### 3.2.2 *Mantenimiento de los circuitos entre centrales y del equipo asociado* (véase la Recomendación M.250)

- prueba/medición de un circuito o haz de circuitos y del equipo asociado;
- observación y supervisión de circuitos y del equipo asociado;
- control del estado de un circuito o haz de circuitos y del equipo asociado;
- análisis de datos de mantenimiento;
- administración y control de informes de mantenimiento.

#### 3.2.3 *Mantenimiento de la red de conmutación*

- realización de llamadas de prueba;
- iniciar la localización de una llamada;
- retención de conexiones defectuosas;
- prueba y medición de equipos periféricos (juegos de relés, receptores y emisores de señalización, etc.);

- prueba y medición de órganos de conmutación;
- reducción del servicio a abonados con bajo orden de prioridad;
- establecimiento de una conexión por un trayecto específico a través de la red;
- supervisión y medición de la calidad de servicio de la red de conmutación;
- localización de averías (o fallos) en la red de trayectos de conversación;
- creación de un acceso para observación de tráfico con fines de mantenimiento;
- avisos de alarma;
- registro del estado de los órganos de conmutación.

#### 3.2.4 *Mantenimiento del sistema de control*

- avisos sobre el estado del sistema;
- avisos de alarma y localización de averías (o fallos);
- localización de averías;
- prueba sobre una base funcional después de una reparación;
- inicio de operaciones de pruebas periódicas;
- modificación de la configuración del sistema con fines de mantenimiento;
- verificación de la coherencia de los datos;
- re arranque;
- establecimiento de controles para localizar defectos de programas;
- modificación del contenido de la memoria;
- vaciado de la memoria con fines de mantenimiento;
- control de los parámetros de sobrecarga;
- modificación de los criterios para el reconocimiento de la degradación del servicio;
- reducción del servicio a abonados con bajo orden de prioridad.

### 3.3 *Funciones de instalación<sup>2)</sup>*

#### 3.3.1 *Instalación de sistemas CPA*

##### 3.3.1.1 *Instalación de soporte físico de sistemas CPA*

Instalar:

- bloques de red;
- circuitos (entre centrales);
- equipo de señalización;
- equipo de prueba;
- bloques de circuitos de abonado;
- equipo de interfaz;
- equipo de control;
- equipo de memoria;
- dispositivos de entrada/salida.

---

<sup>2)</sup> La instalación incluye también las ampliaciones o reducciones del sistema después de su puesta en servicio.

### 3.3.1.2 *Instalación de soporte lógico de sistemas CPA*

Instalación de:

- paquetes operacionales;
- programas de prueba;
- programas estadísticos;
- parches de programas;
- programas de sistemas de señalización;
- programas de servicios, facilidades;
- datos de sistema.

### 3.4 *Funciones de prueba de aceptación*

Las funciones de prueba de aceptación incluyen cualesquiera otras funciones adicionales a las indicadas anteriormente que ayudan a las Administraciones a comprobar si un sistema cumple las especificaciones de las Administraciones.

## APÉNDICE I

(a la Recomendación Z.331)

### **Administración de control de acceso usuario-sistema**

#### I.1 *Consideraciones generales*

El presente apéndice se ha elaborado con arreglo a la metodología definida en las Recomendaciones Z.332 y Z.333.

La parte principal de este apéndice trata del modelo de administración del control de acceso usuario-sistema. También se incluye un glosario de términos.

En el anexo A figuran la lista de funciones que han de controlarse y la lista de trabajos.

Para cada función que debe controlarse mediante el LHM, pueden derivarse una o más funciones, cada una de las cuales puede describirse utilizando el metalenguaje definido en la Recomendación Z.333, a fin de ofrecer con detalle la estructura de información pertinente.

El anexo B contiene una lista de funciones LHM y diagramas de estructura de información vinculados a cada una de ellas, y que pueden utilizarse como líneas directrices.

#### I.2 *Introducción*

El control de acceso usuario-sistema (denominado en adelante control de acceso) se proporciona dentro de un sistema para restringir las entradas que se permite introducir a fin de prevenir una modificación no autorizada del sistema, y/o la observación no autorizada de información.

El control de acceso es la función de sistema que efectúa el control del acceso a los sistemas y sus funciones por los usuarios.

La administración del control de acceso se define como la administración de los derechos de acceso de los usuarios.

Esta Recomendación se refiere principalmente a los usuarios humanos.

Este apéndice no trata de la administración de control de acceso máquina-máquina.

Se reconoce por tanto que este apéndice necesitará ulterior estudio dentro de un amplio escenario que incluye los diversos aspectos del control de acceso (hombre-máquina, máquina-máquina, etc.).

#### I.3 *Modelo de control de acceso*

##### I.3.1 *Introducción*

Los criterios de acceso son, por definición, los atributos que caracterizan el acceso al sistema.

Los permisos se definen como los derechos concedidos al usuario.

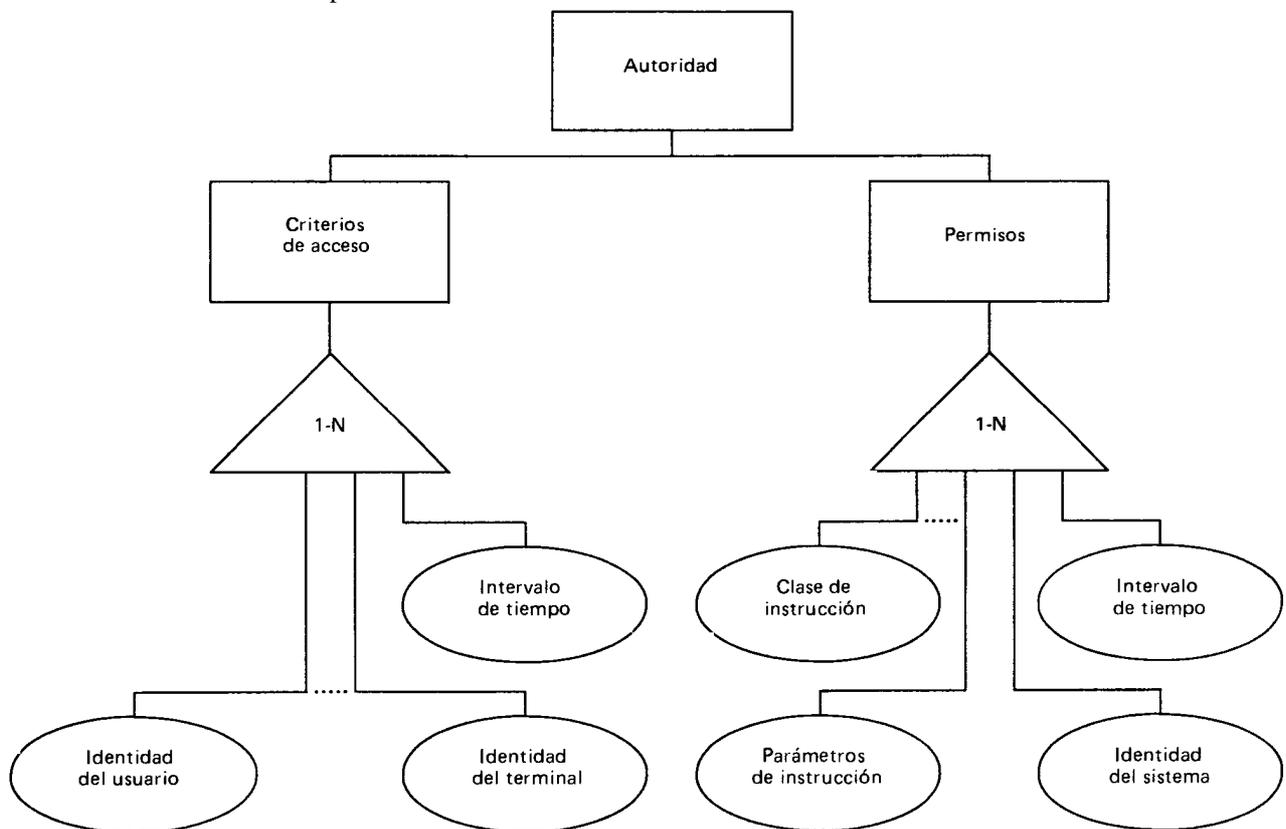
La autoridad se define como la relación existente entre los criterios de acceso y los permisos.

Las entradas presentadas son aceptadas por el sistema, siempre que éste haya verificado la autoridad para introducirlas.

### I.3.2 Modelo

Los principales atributos (véase la figura I-1/Z.331) que se han adoptado para identificar los criterios de acceso y los permisos son los siguientes (pueden adaptarse otros atributos de las dos categorías según las necesidades de la Administración):

- a) para los criterios de acceso
  - identidad del usuario;
  - identidad del terminal;
  - intervalo de tiempo;
- b) para los permisos
  - clase de instrucción;
  - parámetros de instrucción;
  - identidad del sistema;
  - intervalo de tiempo.



T1002700-88

FIGURA I-1/Z.331

#### Administración del control de acceso usuario-sistema

Algunos de los atributos enumerados pueden no realizarse según los requisitos de la Administración.

Para facilitar la administración del control de acceso, pueden formarse grupos a partir de atributos de control de acceso de un mismo tipo (por ejemplo, un grupo de identidades de usuario puede formar un grupo de mantenimiento).

En la figura I-2/Z.331 se representa un ejemplo de realización.

Autoridad					
Criterios de acceso			Permisos		
Identidad del usuario	Identidad del terminal	Intervalo de tiempo	Identidad del sistema	Clase de instrucción	Parámetros de instrucción
Usuario 1	Terminal 1	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Usuario 1	Terminal 2	8–17 h de lunes a viernes	Sistema 1	Administración de abonado	Número directo: 81 000–82 000
Usuario 2	Terminal 3	20–8 h	Sistema 1	Mantenimiento del enlace	Identidad del enlace 1A23 1800
Usuario 3	Cualquiera	8–17 h	Sistema 2	Mantenimiento de abonado	Número directo: 73 000–87 000
Cualquiera	Terminal 4	8–17 h	Cualquiera	Administración de abonado	–
–	–	–	–	–	–

FIGURA I-2/Z.331

### Ejemplo de una aplicación

#### I.3.3 Atributos del control de acceso

A continuación se describe el significado de los principales atributos que se pueden utilizar en la administración del control de acceso.

a) Identidad del usuario

La identidad del terminal resulta del proceso de identificación (véase la Recomendación Z.317) e identifica unívocamente al usuario frente al sistema.

En el procedimiento de identificación se utiliza generalmente la identidad del usuario individual.

b) Identidad del terminal

La identidad del terminal es la identidad del dispositivo E/S tal como la conoce el sistema, a través de su soporte físico o conexión lógica.

c) Intervalo de tiempo

El control de acceso puede depender de la hora en que se introduce y/o ejecuta la entrada.

d) Clase de instrucción

Una clase de instrucción puede estar constituida por un solo código de instrucción (véase la Recomendación Z.315) o por un conjunto identificable de códigos de instrucción.

e) Identidad del sistema

La identidad del sistema es la identidad del sistema o de una aplicación en la que se permite que la instrucción sea ejecutada. En un sistema de soporte centralizado, los sistemas individuales conectados pueden tener su propio control de acceso. Otra posibilidad consiste en utilizar el control centralizado basándose en la identidad del sistema solicitado.

f) **Parámetros de instrucción**

El control de acceso puede depender de un parámetro (véase la Recomendación Z.315) o de una combinación de parámetros. El control puede basarse en el nombre de parámetros o en el nombre de parámetro y sus valores.

Si se utiliza un parámetro, puede ser conveniente limitar dicho uso a los principales objetos del sistema de importancia para las necesidades específicas de operación y mantenimiento de la Administración.

I.4 *Glosario de términos*

**criterios de acceso**

Conjunto de atributos que caracteriza el acceso al sistema. Ejemplos de atributos son la identidad del usuario y la identidad del terminal.

**permisos**

Derechos concedidos al usuario.

**autoridad**

Relación entre criterios de acceso y permiso.

**identidad del terminal**

Identifica un terminal físico, un canal o un puerto de un sistema de control por programa almacenado (CAP).

I.5 *Lista de funciones y trabajos*

I.5.1 *Lista de funciones de clase B independientes del sistema*

I.5.1.1 Administración de autoridad.

I.5.1.2 Extracción de información de autoridad.

I.5.2 *Lista de trabajos*

I.5.2.1 *Crear/cambiar autoridad*

- el objetivo del trabajo es crear/cambiar una autoridad específica mediante la gestión de los atributos pertinentes;
- el sistema registrará los datos y verificará su exactitud;
- el operador introducirá todos los datos necesarios;
- la complejidad del trabajo puede ser alta según la cantidad de datos a introducir;
- la frecuencia del trabajo es baja.

I.5.2.2 *Borrar una autoridad específica*

- el objetivo del trabajo es borrar todos los datos relativos a la autoridad específica;
- el sistema borrará los datos relativos a la autoridad;
- el operador introducirá la identidad de la información de la autoridad a borrar;
- la complejidad del trabajo es baja;
- la frecuencia del trabajo es baja.

I.5.2.3 *Interrogar la información de autoridad*

- el objetivo del trabajo es extraer información de autoridad;
- el sistema presentará la información solicitada en el dispositivo seleccionado;

- el operador introducirá la identidad de los atributos de control de acceso;
- la complejidad del trabajo es baja;
- la frecuencia del trabajo es baja.

#### I.5.2.4 *Activar/desactivar una autoridad*

- el objetivo del trabajo es activar/desactivar una autoridad específica previamente creada/cambiada; este trabajo puede formar parte del trabajo de creación/cambio;
- el sistema activará/desactivará la autoridad;
- el operador introducirá la fecha y la hora de activación/desactivación y la identidad de la autoridad;
- la complejidad del trabajo puede ser media;
- la frecuencia del trabajo es baja.

### I.6 *Líneas directrices para la lista de funciones LHM y los diagramas de estructura de información asociados*

#### I.6.1 *Introducción*

Esta sección contiene líneas directrices para la elaboración de la lista de funciones LHM y los diagramas de estructura asociados relacionados con el modelo de administración del control de acceso definido en el § 3 de esta Recomendación,

#### I.6.2 *Lista de funciones LHM*

La presente lista contiene posibles funciones LHM para la administración del control de acceso.

La lista no es obligatoria ni completa; puede variar según las necesidades de la Administración, niveles de la red de telecomunicación, necesidades de reglamentación, etc.

##### I.6.2.1 *Crear*

- crear autoridad.

##### I.6.2.2 *Cambiar*

- cambiar autoridad.

##### I.6.2.3 *Borrar*

- borrar autoridad.

##### I.6.2.4 *Interrogar*

- interrogar autoridad.

##### I.6.2.5 *Activar/desactivar*

- activar/desactivar autoridad.

#### I.6.3 *Diagramas de estructura de información*

(pendiente de preparación).