



# Clonación de teléfonos móviles

Comisión de Turismo y Telecomunicaciones  
del Congreso de la República

Jorge Kunigami Kunigami  
Presidente de OSIPTEL  
Lima, enero de 2001

# Agenda

- Funciones de OSIPTEL
- El servicio de Telefonía Móvil
- Fraude en Telefonía Móvil
- Clonación de Teléfonos Móviles
- Acciones Preventivas y Correctivas
- Conclusiones



# Funciones

- Establecer las políticas de protección al Usuario.
- Regular y supervisar el comportamiento de las empresas de telecomunicaciones en un ambiente de libre y leal competencia.
- Establecer las políticas tarifarias de los servicios públicos de telecomunicaciones.
- Promover la inversión privada en el sector.
- Administrar FITELE: Telefonía rural y acceso universal.



# El servicio de Telefonía Móvil



# Servicios de Telefonía Móvil

*“ . . . es aquel que se presta a través del medio radioeléctrico en las bandas específicamente determinadas por las autoridades de cada país, mediante terminales móviles (...) dentro del área de servicio de la empresa operadora, la misma que se encuentra configurada en células o celdas. ”*

# Uso de las Frecuencias (1)

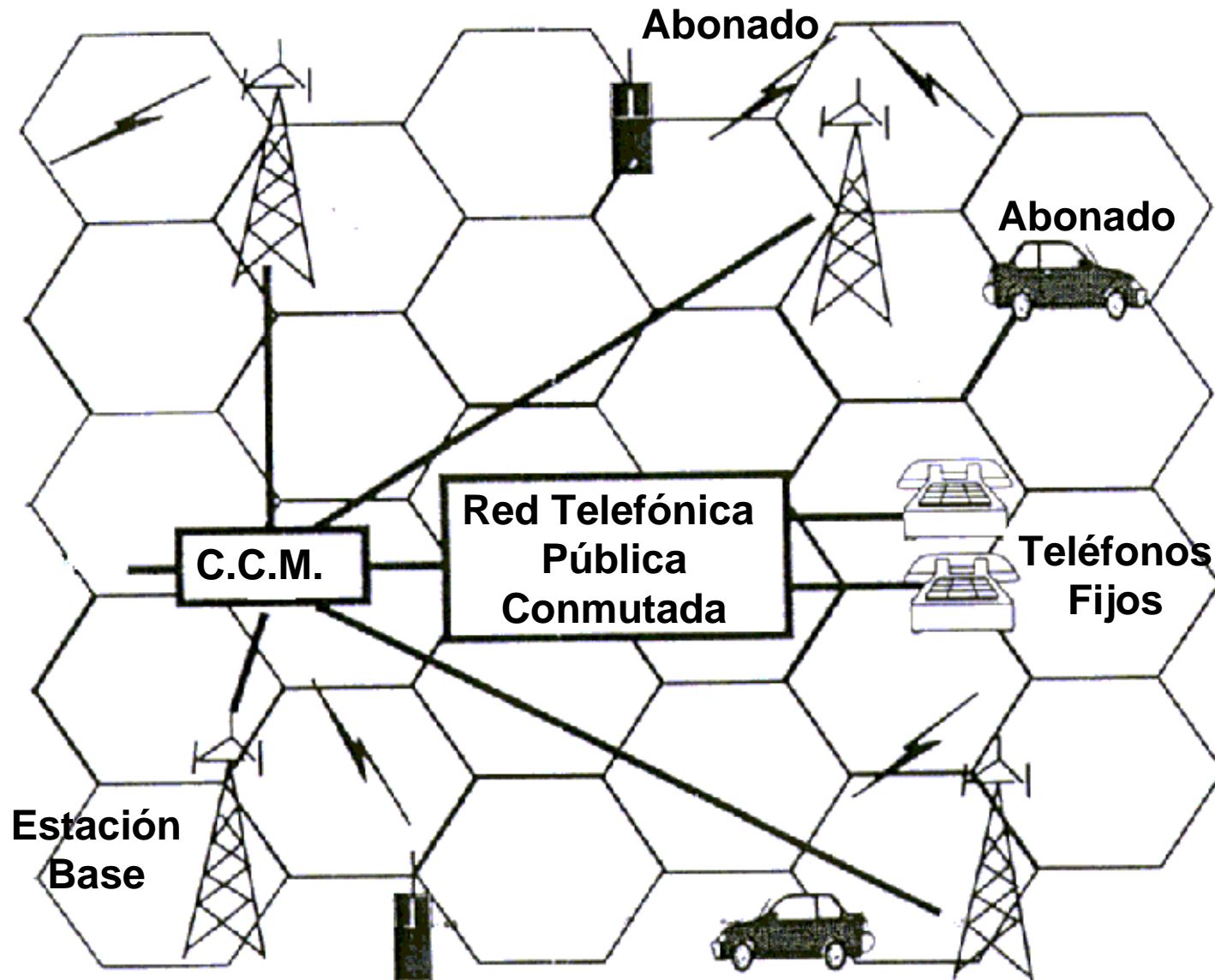
- El principal recurso para el funcionamiento de los sistemas de telefonía móvil es el Espectro Radioeléctrico.
- El Espectro Radioeléctrico es un recurso escaso que pertenece al Estado Peruano.
- El MTC administra y asigna bandas (conjuntos) de frecuencias para el uso de los servicios públicos y privados de telecomunicaciones, según el Plan Nacional de Atribución de Frecuencias (PNAF).
- Las frecuencias del Espectro Radioeléctrico asignadas a una empresa, por las cuales pagan un “canon radioeléctrico”, indican a que frecuencia esa empresa puede emitir las ondas radioelectricas (usadas para enviar información en un medio inalámbrico).



## Uso de las Frecuencias (2)

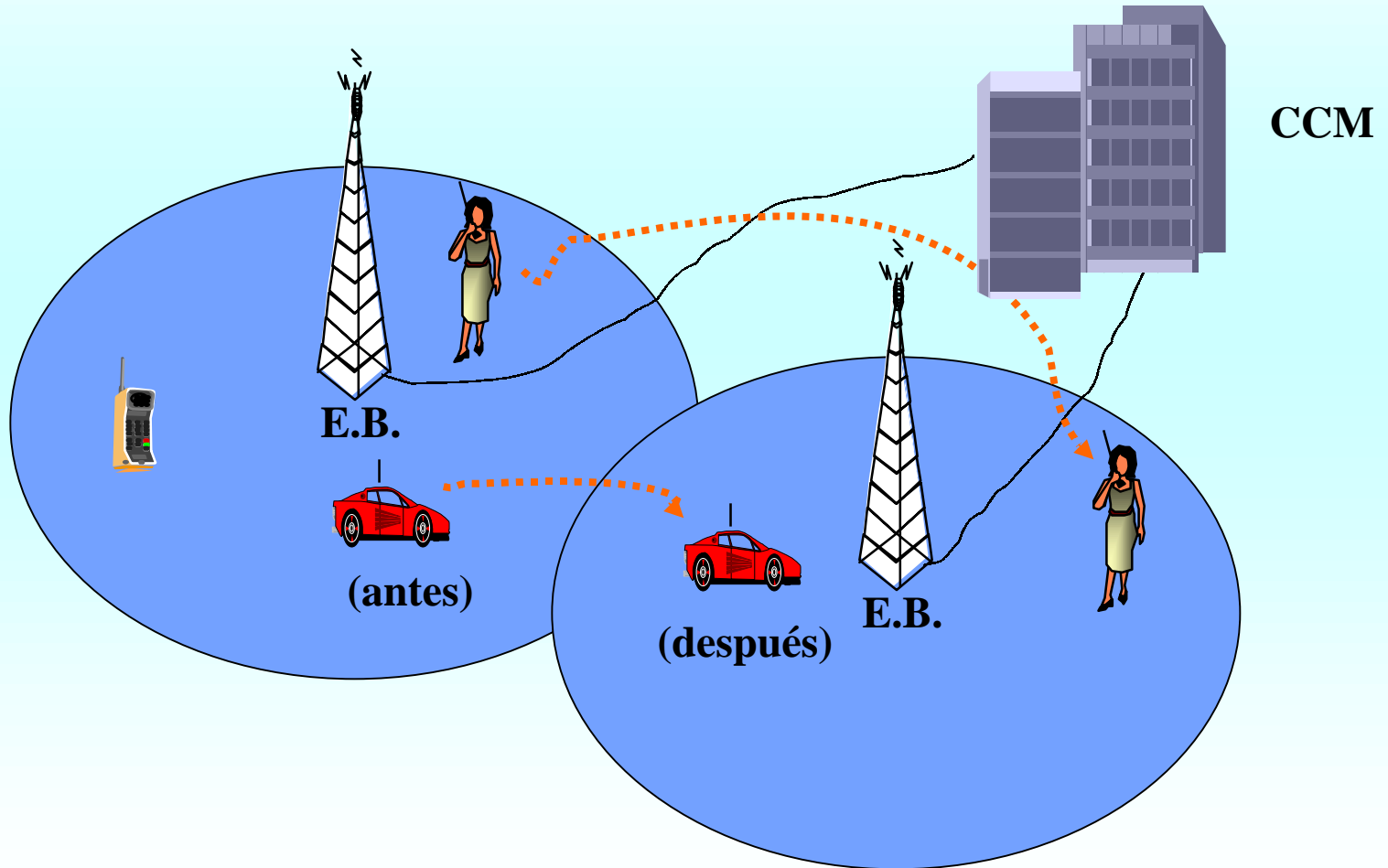
- Las empresas operadoras del servicio móvil requieren tener la Concesión del Servicio Público de Telefonía Móvil para que el MTC les asigne las bandas de frecuencias según el PNAF.
- Dentro de las frecuencias disponibles, y dependiendo de la tecnología que se utilice, se configuran los canales de comunicación que son de dos clases:
  - canales de voz: que llevan las conversaciones telefónicas
  - canales de control: que llevan la información necesaria para procesar las llamadas

# Arquitectura de un Sistema de Telefonía Móvil

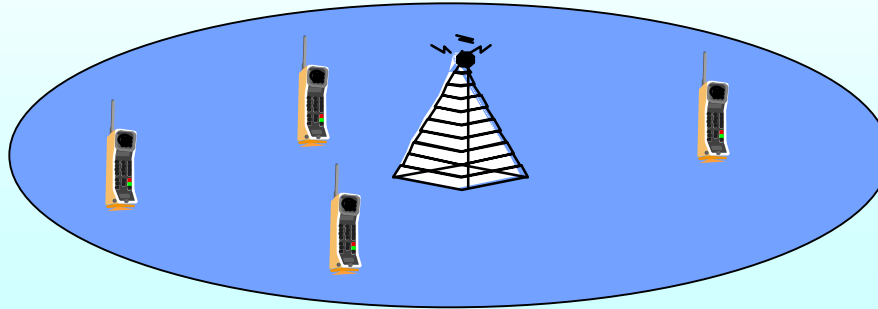




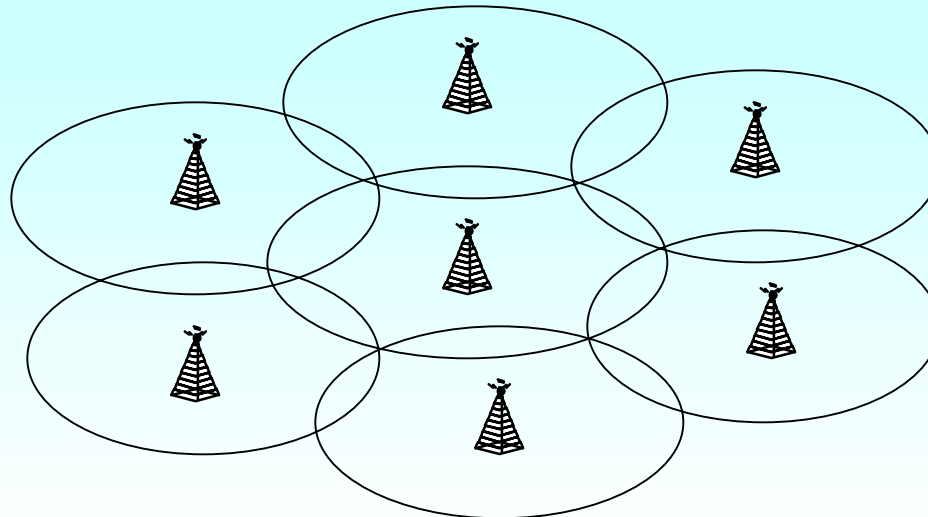
# ¿ Por qué “ Móvil ” ?



## ¿ Por qué “ Celular ” ?



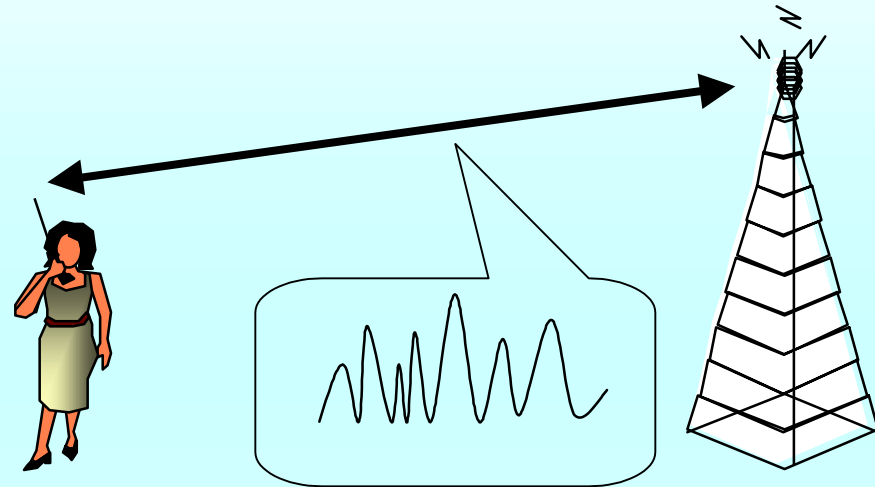
**Cobertura radioeléctrica de una Estación Base o “celda”**



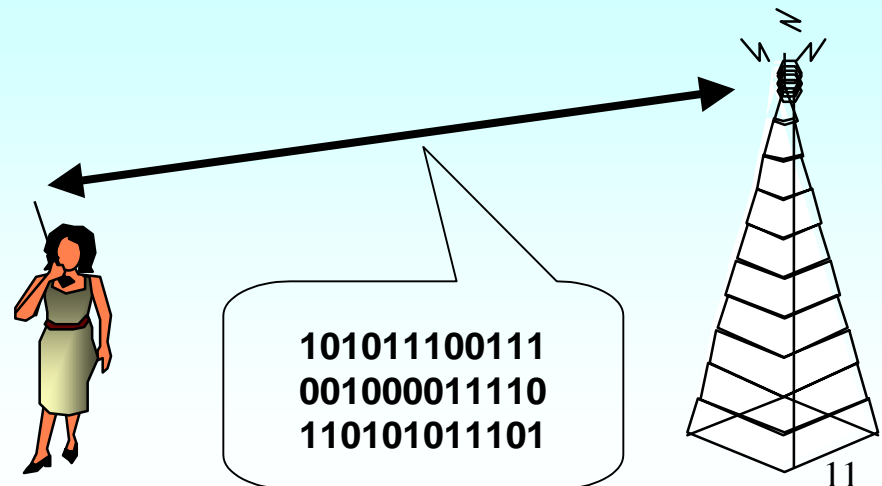
**Patrón de celdas**

# Sistemas Analógico vs. Digital

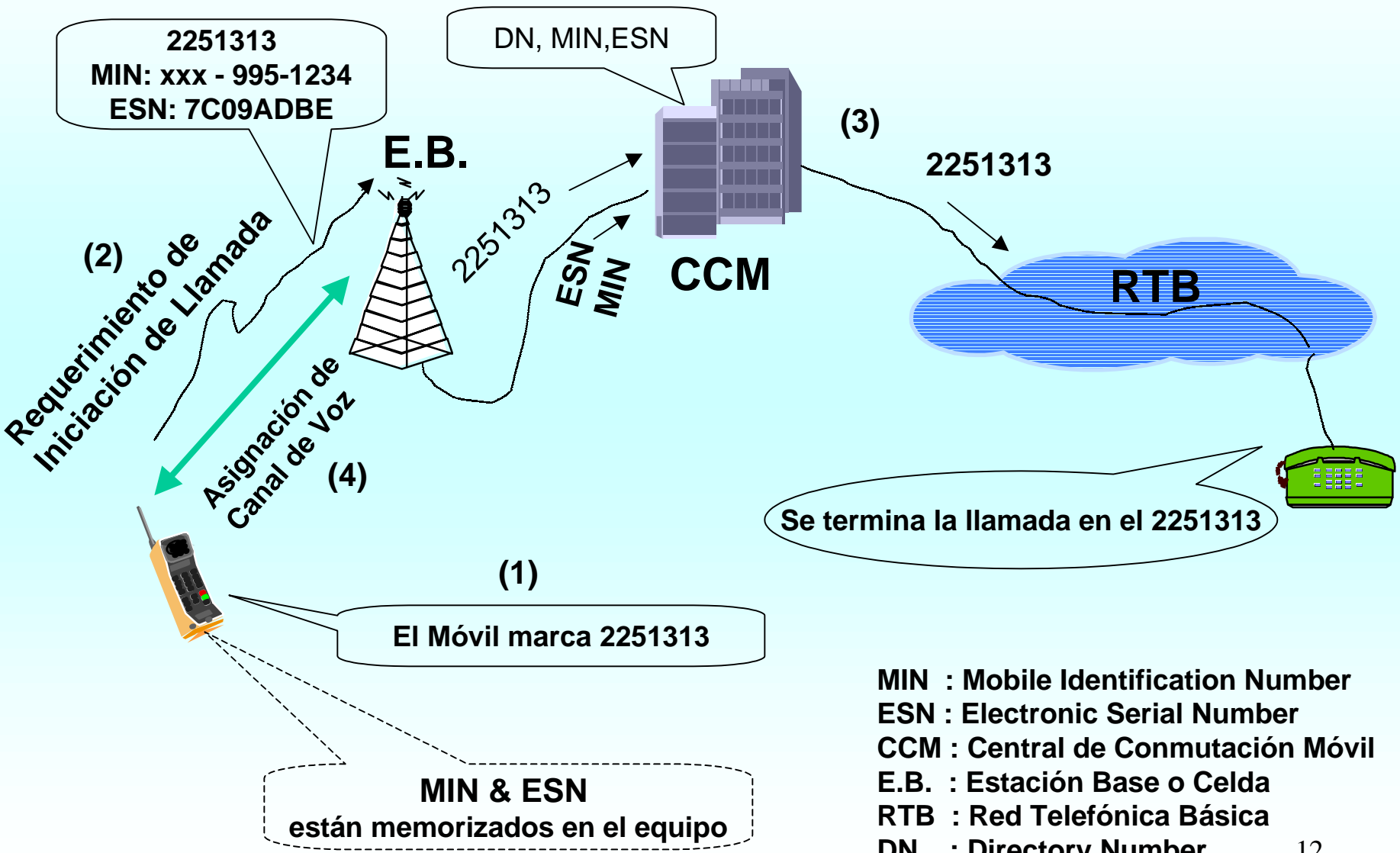
- En un sistema de telefonía móvil celular **analógico**, las conversaciones telefónicas (canal de voz), viajan en las ondas radioeléctricas, similar al servicio de radiodifusión comercial FM.



- En un sistema **digital** las conversaciones van en formato digital (codificación binaria de unos y ceros).

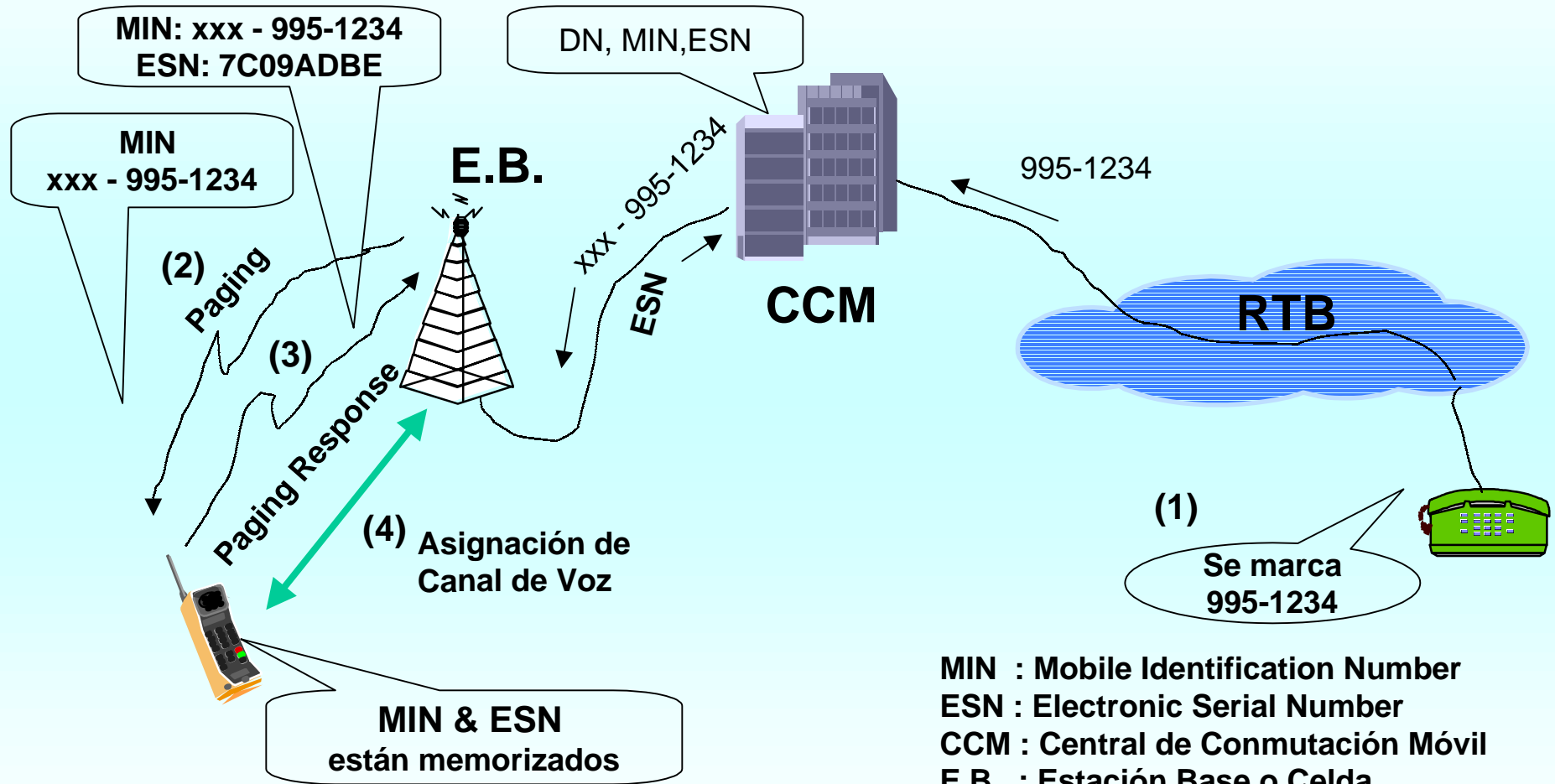


# ¿Cómo se realiza una llamada? (saliente)



- MIN : Mobile Identification Number
- ESN : Electronic Serial Number
- CCM : Central de Conmutación Móvil
- E.B. : Estación Base o Celda
- RTB : Red Telefónica Básica
- DN : Directory Number

# ¿Cómo se realiza una llamada? (entrante)



**MIN** : Mobile Identification Number  
**ESN** : Electronic Serial Number  
**CCM** : Central de Conmutación Móvil  
**E.B.** : Estación Base o Celda  
**RTB** : Red Telefónica Básica  
**DN** : Directory Number

# Datos de Mercado

Empresas	Tecnología	Número de Usuarios *	Telefonos Prepago (%)
<b>Telefónica Móviles</b>	Analógica: AMPS Digital:CDMA	883.046	75%
<b>BellSouth</b>	Analógica: AMPS Digital:TDMA	361.368	70%
<b>Telecom Italia Mobile</b>	Digital GSM	- -	- -
Total:		1.244.414	73.5%

\* Datos al 30/11/2000

Fuente: Empresas



# Validación de una llamada móvil

- Cuando se efectúa una llamada desde un equipo terminal móvil:
  - Se envía a través del aire el **ESN** y el **MIN** (únicos por cada equipo terminal móvil).
  - Dicho envío se realiza en forma de bits a fin de ser recibidos en las respectivas centrales telefónicas.
  - Esta central compara los dos códigos con los registrados en la central móvil del operador.
  - Si esta comparación es positiva se da paso a la llamada. De lo contrario, ésta es denegada.

# Códigos utilizados en una llamada móvil

## **ESN** - Número Electrónico de Serie

- Asignado en forma única por el fabricante a cada equipo terminal móvil y grabado en una memoria imborrable (ROM) dentro del mismo.
- Código de 32 bits (11 dígitos decimales u 8 dígitos hexadecimales).

## **MIN** - Número de Identificación Móvil

- Usado para la identificación del terminal móvil en el sistema celular. El operador programa un único MIN por cada equipo terminal móvil.
- Código de 34 bits asignado por la empresa operadora del servicio (o 10 dígitos decimales).
- A través de este número se ubica al terminal celular tanto para una llamada originada o terminada, así como también para servicios de Roaming (larga distancia).





# Fraude en Telefonía Móvil



# Tipos de Fraude

- Fraude Técnico.- Se basa en aprovechar y/o generar vulnerabilidades en la red que permiten acceder al servicio sin la necesidad de ser abonado.
- Fraude por Suscripción.- Se basa en adquirir comercialmente un servicio con la intención de no pagar por ellos al vencimiento de las facturas, proporcionando identificación falsa o suplantando identidad.



# Fraude Técnico

- Tumbling: Utilizar al azar combinaciones de **ESN/MIN** por cada llamada hasta dar con una combinación válida o aprovechar un fallo en la validación por roaming.
- Hacking: Intrusión y/o reprogramación de plataformas de red para permitir servicios no autorizados.
- Falsa Estación Base: Simular una estación base real para obligar a los teléfonos móviles cercanos a transmitir sus datos de **ESN/MIN**.
- **Clonación**



# Clonación de Teléfonos Móviles



# Clonación de Teléfonos Móviles

- Práctica ilegal que duplica los datos del **ESN** y **MIN** en otro teléfono móvil distinto al original.
- Genera un costo adicional por llamadas realizadas ilícitamente.

## ¿Cómo se obtienen los códigos?

- Scanners o Equipos de monitoreo que captan las frecuencias celulares, buscando los **ESN/MIN** enviados entre una unidad móvil y su estación base transmisora durante el establecimiento de las llamadas. Esta modalidad afecta más a los teléfonos móviles analógicos.
- Revelación de los números **ESN/MIN** - Fuga de información en las mismas empresas operadoras del servicio o por parte del usuario.



# Proceso de Clonación

- PASO 1            Contar con los códigos de identificación del equipo terminal móvil (**ESN/MIN**).
- PASO 2            Programación del teléfono “clon” a través de:
- Cambio de un microchip que contiene el código **ESN**.
  - Cambio manual del código **MIN**.
- PASO 3            Comercialización fraudulenta de llamadas:
- A través de la venta del telefono “clon”
  - A través de la venta de minutos con el uso de teléfonos especiales que contienen una lista de varios grupos de códigos **ESN/MIN**.



# Acciones Preventivas y Correctivas





# Acciones de las empresas (1)

## Preventivas y Correctivas

- Seguimiento en los sistemas de facturación de consumos habituales de los usuarios a fin de detectar consumos atípicos que podrían ser causados por prácticas de clonación.
- Uso de claves o PIN (Personal Identification Number) para el acceso a la Larga Distancia.
- Medidas preventivas para reducir el acceso de información sensible y bajo responsabilidad.



# Acciones de las empresas (2)

## Preventivas y Correctivas

- Implementación de Sistemas de “**Autenticación**”, que es una tecnología de prevención de fraude que permite verificar en cada llamada que el teléfono móvil que realiza la llamada sea el teléfono legítimo y activado por la empresa.
- Campañas progresivas de autenticación o cambio de los teléfonos móviles por otro equipos terminal móvil autenticables, según corresponda.
- Operativos sorpresa con ayuda de la policía en zonas de comercio ambulatorio para evitar la comercialización de los teléfonos móviles “clon” o la venta fraudulenta de tráfico.



## Acciones de OSIPTEL (1)

- Inspección de las acciones preventivas y correctivas por parte de las empresas.
  - Reuniones periódicas con empresas operadoras del servicio.
  - Visitas de inspección para verificar los procesos de Autenticación.
  - Supervisión de reclamos de los usuarios con teléfonos móviles que presentan probabilidades de clonación.
- Revisión de aspectos técnicos para combatir la clonación.
  - Reuniones con proveedores de teléfonos móviles.



## Acciones de OSIPTEL (2)

- Cordinación con autoridades del Ministerio Público
  - Reuniones de trabajo con la Fiscalía Provincial de Prevención del Delito.
- Regulación para la seguridad de los teléfonos móviles.
  - Propuesta de normas para evitar el uso fraudulento de teléfonos móviles “clon”. Actualmente en proceso de consulta.



# Conclusiones

- La clonación es la alteración de la identidad de un teléfono móvil asumiendo la de otro legítimo, con el fin de usar el servicio sin responsabilidad de pago.
- La Autenticación es la mejor herramienta para evitar la práctica ilegal de clonación.
- Adopción de medidas para que las empresas operadoras brinden seguridad a los usuarios en el uso de teléfonos móviles.
- Se requiere que la clonación sea tipificada como delito para reducir su proliferación.