Inhibidores de señal

Uso de Jammers en prisiones

La GSMA representa los intereses de los operadores móviles de todo el mundo, reuniendo a casi 800 operadores con unas 300 compañías del amplio ecosistema móvil. Estas empresas incluyen fabricantes de teléfonos y dispositivos móviles, empresas de software, proveedores de equipamiento y empresas de internet, así como también organizaciones de sectores adyacentes de la industria. La GSMA también organiza eventos líderes de la industria como el Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas y la serie de conferencias Mobile 360.

Para más información, visite el sitio web corporativo de la GSMA en **www.gsma.com**
Siga a la GSMA en **Twitter: @GSMA y @GSMALatam**

GSMA Latin America es el brazo de la GSMA en la región.
Para obtener más información en inglés, español y portugués, visite **www.gsmala.com**

BlueNote Management Consulting es una firma de consultoría especializada en el sector de telecomunicaciones y media, donde ha desarrollado proyectos de estrategia, políticas públicas y regulación, colaborando con el sector privado, organismos oficiales y entidades regionales.

BlueNote posee dos sedes, una en Buenos Aires, Argentina, y otra en Bogotá, Colombia. Su equipo de consultores posee amplia experiencia y formación en el sector de telecomunicaciones y media, obtenida tanto en labores de consultoría como durante el desempeño de funciones públicas o ejecutivas. El foco de actuación es América, donde su equipo de consultores ha trabajado por más de 15 años en el sector, sirviendo en aspectos técnicos, regulatorios y económicos.
www.bluenotemc.com

Tabla de Contenidos

1 Resumen ejecutivo

Un bloqueador o inhibidor de señal es un dispositivo de radiofrecuencia que intencionalmente transmite señales con el objeto de impactar, bloquear, interferir o saturar los servicios de comunicaciones de usuarios móviles tales como: llamadas de celular, mensajes de texto, señales de posicionamiento GPS, servicios de datos, redes de Wi-Fi, entre otras.

En este sentido, un bloqueador o inhibidor de señales se rige por los fenómenos básicos de la propagación de señales radioeléctricas, así como los sistemas de comunicaciones comerciales. Es decir, la cobertura depende de factores como la potencia máxima del transmisor y la potencia mínima que pueda percibir el receptor, la frecuencia de operación (las frecuencias bajas alcanzan mayores distancias y tiene mejor penetración en edificaciones), la calidad del filtro del transmisor, las características de las antenas y los obstáculos que se encuentren en el medio como edificaciones, árboles, cuerpos de agua, etc. que generan que las señales se reflejen, se refracten, tomen varios caminos, entre otros fenómenos.

El objetivo de la señal generada por los bloqueadores de señal es interrumpir la comunicación entre la estación base de una red de comunicaciones y el dispositivo móvil del usuario, provocando que la relación entre la señal útil o real y la señal interferente medida en el dispositivo o en la estación base sea lo suficientemente baja para que ningún mecanismo digital de recuperación de señal logre diferenciarlas impidiendo así que se establezca o mantenga una comunicación estable. Es importante destacar que los bloqueadores de señal no hacen ningún análisis de las comunicaciones que se desean cursar ni del tipo de usuario que desea establecer la conexión, por esta razón no puede discriminar entre los terminales bajo su zona de cobertura ni evitar el bloqueo a llamadas de líneas de emergencias.

En otras palabras, el bloqueo de las comunicaciones, ya sean autorizadas o que se deseen restringir, estará dado por el nivel de potencia de las señales generadas por la estación base o el dispositivo móvil y el nivel de potencia de la señal interferente. En este sentido, y considerando todos los fenómenos asociados con la propagación de ondas radioeléctricas que afectan la definición de una zona de cobertura y las funcionalidades propias de las redes de telefonía móvil celular, es posible que se presenten puntos dentro de la zona en donde se desean bloquear las comunicaciones en los cuales sea posible establecer una llamada o acceder a servicios de datos; y al mismo tiempo, puntos fuera del área delimitada donde se presenten bloqueos de los servicios de comunicaciones.

Por último, es importante destacar que para impedir las comunicaciones clandestinas no es suficiente con interferir las bandas de la telefonía celular móvil, dado que es posible que éstas se realicen utilizando otros servicios o tecnologías como WiFi, VHF (handies), satelital, etc.

Entre los impactos más comunes del uso de bloqueadores de señal, se destacan los siguientes:

a. **Bloqueo de comunicaciones fuera de los límites de los centros penitenciarios** impidiendo el acceso de los usuarios a servicios de comunicaciones autorizados, incluyendo la restricción de las llamadas a líneas de emergencia.

b. **Degradación de los servicios de comunicaciones** en las zonas aledañas al centro penitenciario representado en constantes caídas de llamadas, mala calidad de las comunicaciones, lentitud en los servicios de datos, entre otros.

c. El uso de dispositivos bloqueadores con filtros y transmisores de baja calidad pueden generar **emisiones perjudiciales fuera de la banda de operación**, afectando otros servicios radioeléctricos que operen en dichas bandas.

d. De manera similar al caso anterior, cuando los bloqueadores operan en múltiples bandas de frecuencias pueden generar **señales interferentes perjudiciales en otras bandas diferentes** afectando todo tipo de servicios. Pudiendo llegar incluso a dificultar la labor policial al interferir también los sistemas radioeléctricos de comunicación utilizados por las fuerzas de seguridad. Esto se debe a un fenómeno denominado Productos de Intermodulación[1].

e. **Zonas "ciegas" dentro del centro penitenciario**, donde aún es posible establecer comunicaciones no autorizadas.

El contexto general de los países de América Latina relevados, en relación con las comunicaciones no autorizadas desde los centros penitenciarios y que representan un riesgo para la seguridad pública, así como las iniciativas para contrarrestarlos, tienen varios puntos en común. Especialmente en lo relacionado con los antecedentes, las iniciativas de solución y las instituciones involucradas. En términos generales, el uso no autorizado de dispositivos de radiofrecuencias que interfieran de manera intencional o maliciosa servicios de comunicaciones autorizados está prohibido en los países relevados o es considerado un uso clandestino o ilegal del espectro, incluso en países como EE.UU. se restringe adicionalmente la venta, comercialización e importación de estos dispositivos. No obstante, existen algunas excepciones sustentadas en razones de seguridad pública o interés general, que contempla autorizar el uso de este tipo de equipos en recintos confinados como centros penitenciarios. En todos los casos analizados se exige que no haya una afectación en los servicios de comunicaciones autorizados fuera de los límites de los penales.

La siguiente tabla se resumen aspectos normativos relacionados con características técnicas de los equipos y procedimientos establecidos para la instalación de bloqueadores de señal.

FIGURA 1

Reglamentación sobre características técnicas de los bloqueadores y procedimientos

Norma equipos	Características técnicas mínimas de los equipos	Equipos
Brasil **ANATEL** Res. 306 de 2002 Res. 308 de 2002	• Bloquear todas las bandas de frecuencias usadas en Serv. de telecomunicaciones • No puede bloquear otras bandas de frecuencia o fuera de los límites físicos del penal • Bloquear señales de cualquier tecnología • Control de potencia independiente en cada banda • No estar al alcance de la población carcelaria • Cumplir con los límites de exposición a campos electromagnéticos	• Notificar a ANATEL 10 días antes de encender el equipo • Mantener informado a operadores de telecomunicaciones • Presentar proyecto técnico • Realizar validación de impacto en puntos de verificación
Colombia **MINTIC - MinJusticia** Decre768 de 2011 Resolución 2774 de 2013	• Cumplir con límites de exposición a campos electromagnéticos	• Sólo aplica a penales donde haya evidencias de delitos desde dispositivos de comunicaciones • Se debe enviar solicitud a MINTIC con condiciones técnicas de la solución, huella de cobertura hasta 500mts fuera de los límites del penal • Apagar en caso de impacto en exteriores hasta solucionar • Coordinar con operadores de telecomunicaciones • No aplica indicadores de calidad en penales afectados
México **Ley General del Sistema de Seguridad Pública IFT** Ley Federal de Telecomunicaciones Disposición Técnica IFT-10-2016	• No exceder 20mts fuera de las instalaciones • Enviar señales ante interrupción de funcionalidad • Control desde centros remotos • Potencia ajustable independiente para cada banda • No contar con controles externos para evitar manipulación • Sólo bloquear el enlace descendente • No bloquear la banda de 380 – 399.9MHz • Cumplir con los límites de exposición a campos electromagnéticos	• Instalar equipos que anulen o cancelen las señales de telefonía celular de manera permanente en todos los centros penitenciarios • Ser operado por autoridades distintas a los establecimientos penitenciarios y en centros remotos

Fuente: BNMC

1. Comentarios realizados por la Industria a la NTIA sobre el uso de jammers en prisiones (NTIA, 2010)

1

Con base en las leyes y regulación de los países relevados, se encuentra que, en el marco de las responsabilidades de cada institución y las normas aplicables a los sistemas penitenciarios, la implementación de soluciones de bloqueo de señal es responsabilidad de las direcciones de centros de reclusión o penitenciarios. Las autoridades de telecomunicaciones tienen un rol de asesoría e instrumentación de regulación aplicable al sector, mientras que los operadores de servicios de comunicaciones cumplen un rol de cooperación y asesoría.

Por otro lado, considerando las experiencias analizadas en los países relevados y el portafolio de productos de algunas empresas líderes en la industria de fabricación de soluciones para restricción de llamadas como Harris, ShawnTech, CellAntenna, SESP, entre otros, es posible identificar cinco categorías básicas de soluciones tecnológicas para el control de comunicaciones no autorizadas desde centros penitenciarios: i) basadas en bloqueo mediante generación de señales de radiofrecuencia interferentes con cierto nivel de selectividad, ii) basadas en captura de las comunicaciones para controlar el acceso a las redes comerciales (Sistemas de Gestión de Acceso), iii) basadas en técnicas que emulan una celda celular, pero no permiten acceso a los servicios (celdas celulares dummy), iv) basadas en detección y v) soluciones híbridas que integran dos o más de las técnicas mencionadas.

FIGURA 2

Análisis comparativos de alternativas

Muy Satisfactorio · Bueno · Regular · Insatisfecho · Deficiente

	Bloqueador de señal selectivo	Gestión de Acceso selec	Celdas Dummy selec	Sistemas de Detección	Híbridos: Detección & Jammer	Híbridos: Detección & Gestión de acceso
Eficiencia en bloqueo	• Escalable a todas las tecnologías y bandas • Riesgo de zonas ciegas	• No abarca tecnología WI-FI • Riesgo de zonas ciegas	• Sólo aplica a redes móviles celulares • Riesgo de zonas ciegas	No aplica Su principio no es bloqueo de comunicaciones	• Escalable a todas las tecnologías y bandas • Riesgo de zonas ciegas	• No abarca tecnología WI-FI • Riesgo de zonas ciegas
Impacto en comunicación es autorizadas	• Riesgo de interferencia perjudicial fuera de límites del penal • Bloqueo de llamadas de emergencia • Riesgo de impacto en otras bandas	• No genera señales interferentes • Riesgo de "captura" de usuario fuera del penal • No bloquea llamadas de emergencia	• No genera señales interferentes • Riesgo de bloqueo de usuario fuera del penal • Bloquea llamadas de emergencia	• No genera interferencia • Riesgo de reporte de usuarios fuera del penal	• Riesgo de interferencia fuera del penal • Bajo riesgo de bloquea llamadas de usuarios autorizados	• No genera señales interferentes • Riesgo de "captura" de usuarios fuera del penal • No bloquea llamadas de emergencia
Costos y complejidad	• Depende de tamaño del penal • Riesgo de vandalismo	• Alto costo de la solución. Depende del área, operadores, bandas y funcionalidades	• Alta complejidad de coordinación. Requiere múltiples soluciones para cada operador, banda y tecnologías	• Depende de tipo y complejidad • Riesgo de vandalismo	• Depende de tipo y complejidad • Riesgo de vandalismo	• Alto costo de la solución
Apoyo a seguridad pública	• No proporciona información	• Información de identificación de usuario, tipo de servicio y destinatario	• Información de identificación de usuario y localización	• No proporciona información	• Información de identificación de usuario y localización	• Información de identificación de usuario, servicio destinatario y localización

Fuente: BNMC

Con base en las características de cada una de las alternativas, se presenta en la siguiente tabla un análisis comparativo de las mismas.

Con base en la anterior tabla se concluye que las alternativas técnicas disponibles en el mercado para la restricción de comunicaciones no autorizadas desde los centros penitenciarios no tienen un desempeño totalmente satisfactorio en todos los factores analizados. Por esta razón, se hace necesario analizar cada centro penitenciario de manera particular e identificar la solución que mejor se ajusta a sus requerimientos y prioridades. Así mismo, es recomendable adoptar las buenas prácticas de instalación de sistemas de radiocomunicaciones sugeridas por la industria y mantener un monitoreo permanente de los posibles impactos que se generen.

Finalmente, es importante destacar que la problemática debe ser analizada de manera integral, desde los procesos de control para restringir el acceso de dispositivos de comunicaciones a los centros penitenciarios, el bloqueo o restricción de las comunicaciones no deseadas, la detección e incautación de los terminales de contrabando que hayan ingresado y el análisis de información de inteligencia para hacer seguimiento a los casos, identificar patrones de comportamiento y evitar reincidencias.

2 Introducción

El uso de dispositivos de comunicación móviles ingresados de manera ilícita a los centros penitenciarios para la realización de actos delictivos como amenazas, extorsiones, estafas, entre otros, ha sido uno de los principales motivadores para la implementación de soluciones técnicas que bloquean, restringen o inhiben las señales de comunicación de celular, dentro de las cuáles se encuentran los dispositivos conocidos como *jammer*.

Estos dispositivos inhibidores son transmisores de señales de radiofrecuencia que generan ondas dentro de las bandas de espectro usadas para las radiocomunicaciones celulares, que se comportan como ruido con altos niveles de potencia que bloquean, perturban o interfieren las comunicaciones recibidas por o enviadas a las estaciones base de una red celular.

Comúnmente, este tipo de equipos no hace distinción entre usuarios o tipos de comunicación, por lo que afectan todas las comunicaciones dentro de su rango del alcance. En este sentido, usuarios comerciales ubicados en zonas urbanas cercanas a las cárceles pueden ver significativamente afectada la calidad de sus comunicaciones, experimentando problemas para acceder al servicio y caídas de llamadas.

Considerando la situación expuesta, la GSMA ha encargado a BLUENOTE MANAGEMENT CONSULTING el desarrollo de un reporte que permita entender los principios de funcionamiento de los sistemas de bloqueo o inhibición de señales y los impactos que generan en los servicios móviles autorización e identificar alternativas de solución.

El presente documento corresponde al informe del estudio encargado y que comprende una explicación de los principios básicos de la propagación de ondas radioeléctricas y redes móviles celulares, así como los conceptos fundamentales, características y análisis de impactos de los dispositivos para el bloqueo o inhibición de señales de comunicación.

El capítulo 3 muestra los resultados del relevamiento realizado en siete países de América Latina y el mundo en relación con el marco normativo y regulatorio relacionado con la instalación de inhibidores de señal en las cárceles, así como la identificación de buenas prácticas.

Finalmente, el capítulo 4 hace una descripción de alternativas técnicas disponibles en el mercado para el bloqueo de comunicaciones no autorizadas en centros penitenciarios, presenta un análisis comparativo de dichas soluciones y las conclusiones y recomendaciones finales del informe.

3

Conceptos generales sobre bloqueadores de señal y redes móviles celulares

El presente capítulo proporciona una explicación de los principios básicos de la propagación de señales de radiofrecuencia, del funcionamiento de las redes de telefonía móvil y de los dispositivos para bloquear o inhibir las comunicaciones celulares, con el objetivo de facilitar el análisis del impacto estos últimos en los servicios de comunicaciones.

3.1 Conceptos básicos sobre propagación de señales radioeléctricas

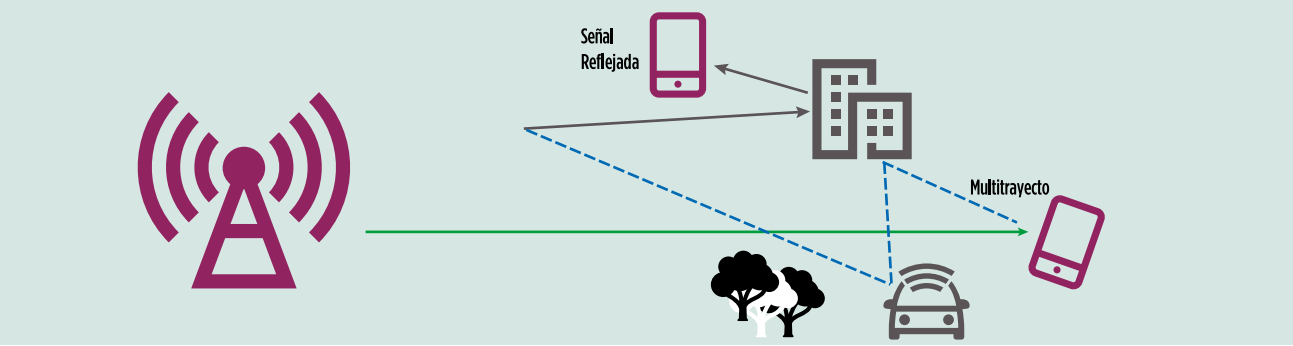
La base de los servicios de comunicación inalámbrica, como la telefonía móvil, la radio, televisión abierta, etc., es la transmisión y recepción de señales en forma de ondas que viajan por el espectro radioeléctrico para llevar información desde una estación transmisora/receptora hasta un dispositivo de usuario. Para que dicha comunicación sea posible en condiciones satisfactorias para los usuarios, cada conexión debe viajar por un carril libre, es decir, una porción del espectro que no esté siendo ocupada. Por esta razón, el espectro está dividido en bandas de frecuencias.

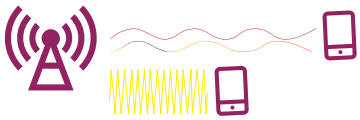
La zona geográfica donde llegan de manera perceptible las ondas electromagnéticas de una o varias estaciones transmisoras o donde un dispositivo de usuario puede enviar señales que sean percibidas por las estaciones receptoras, se denomina zona de cobertura.

La cobertura depende de factores como la potencia máxima del transmisor y la potencia mínima que pueda percibir el receptor, la frecuencia de operación (las frecuencias bajas alcanzan mayores distancias y tiene mejor penetración en edificaciones), la calidad del filtro del transmisor, las características de las antenas (ganancia para incrementar la potencia del transmisor, capacidad de concentrar la señal en una dirección específica), y los obstáculos que se encuentren en el medio como edificaciones, árboles, cuerpos de agua, etc. que generan que las señales se reflejen, se refracten, tomen varios caminos, entre otros fenómenos.

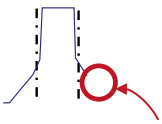
Esta situación genera que la huella de cobertura de una estación base transmisora, comúnmente representada por una circunferencia o un hexágono, realmente tenga una forma imposible de predecir con exactitud, con obstrucciones de la señal o reflexiones que pueden ocasionar que las ondas alcancen mayores distancias, por ejemplo, en vías bordeadas por edificaciones.

Finalmente, cambios en el entorno, como nuevas edificaciones, cambios en los materiales de construcción, nuevas estaciones de transmisión/recepción, fallas temporales de la red, características propias de la tecnología o factores externos, pueden modificar la huella de cobertura de una red de telecomunicaciones inalámbrica.





Las ondas se atenúan con la distancia y son afectadas por condiciones del terreno como edificaciones y vegetación. Las bandas bajas de frecuencia alcanzan mayores distancias.



Los filtros de los transmisores, usados para solo emitir señales en un rango de espectro no son perfectos, por lo que se generan emisiones fuera de banda que pueden afectar otros servicios.

Las antenas directivas no pueden concentrar el 100% de las señales en una dirección, dado que los materiales no son ideales. Existen emisiones hacia la parte posterior, y los costados de la antena.

3.2 Principios básicos sobre redes móviles celulares

Las redes celulares son uno de los sistemas que hace uso de ondas radioeléctricas para permitir enlaces de comunicación de usuarios ubicados en cualquier punto del área de cobertura de la red, incluso cuando los mismos se encuentran en movimiento. El principio de las redes celulares es dividir la zona de cobertura en pequeñas celdas o células permitiendo hacer un re-uso del espectro en diferentes puntos geográficos.

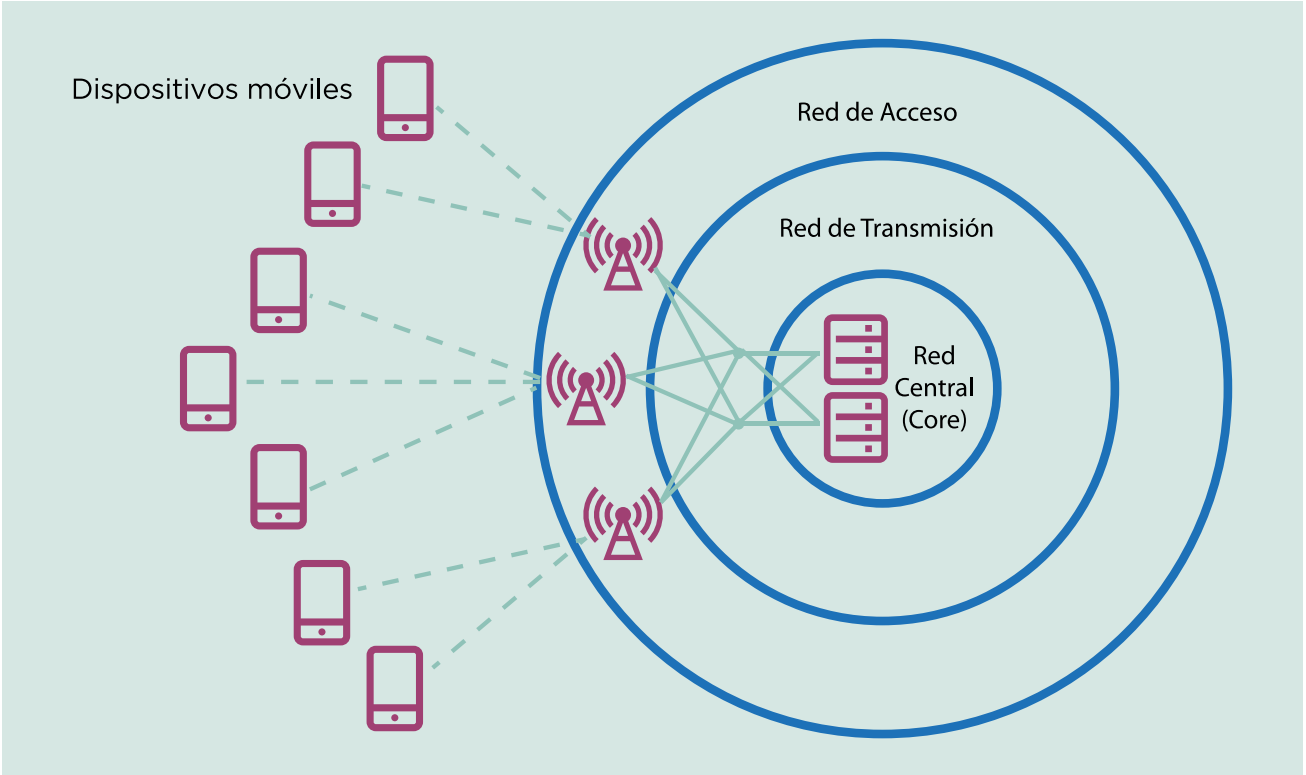
Para asegurar que cada comunicación que se establezca en una red celular tenga un carril libre, como se mencionó previamente, las tecnologías usadas para este tipo de redes adoptan técnicas para hacer uso de diferentes espacios de tiempo o de frecuencia, o diferentes códigos que identifiquen claramente cada enlace, o combinaciones de las técnicas mencionadas. La evolución de las tecnologías móviles, desde las redes GSM hasta los sistemas de cuarta generación - 4G (LTE), han permitido hacer un uso más eficiente del espectro disponible, permitiendo a los usuarios acceder a nuevos y mejores servicios de comunicaciones.

Es importante mencionar que el objetivo primordial de cualquier red de comunicaciones es asegurar el acceso de los usuarios a las comunicaciones. Por esta razón, las redes de telefonía móvil incorporan en sus diseños los efectos de la propagación de señales mencionadas previamente, adoptando técnicas que permitan compensar los fenómenos de las ondas y buscar la calidad en las comunicaciones de los usuarios.

En términos generales, las redes móviles celulares están compuestas por un conjunto de sistemas interconectados que permiten ofrecer servicios de voz y datos en cualquier lugar de la cobertura de la red a través de un dispositivo móvil de usuario. Las redes móviles celulares tienen los siguientes componentes básicos:

FIGURA 3

Componentes básicos de las redes móviles celulares



Dispositivo Móvil (Terminal)

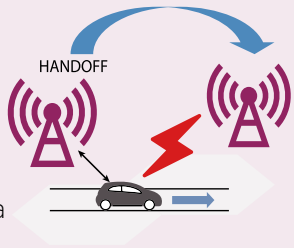
El equipo terminal es la interfaz entre los usuarios finales de la red móvil y el operador de red celular (Red de radio acceso). El equipo terminal debe estar en capacidad de soportar la tecnología y banda de operación de la red a la cual desea conectarse, también contiene la información de identificación que permite hacer el correcto registro en la red de Core. Algunos modelos de terminales contienen la información para el registro de la red directamente en el equipo, sin embargo, la mayoría de los equipos del mercado almacena esta información, en conjunto con el perfil eléctrico homologado por el operador de red celular, en una tarjeta removible conocida como SIM Card (tarjeta SIM). Los dispositivos móviles están identificados de forma única a nivel mundial, por medio del IMEI (por sus siglas en inglés, International Mobile Station Equipment Identity), este código identificador es transmitido por el aparato al momento de conectarse a la red

Red de acceso

Corresponde al conjunto de estaciones de transmisión y recepción que conectan a los dispositivos móviles de usuario con el Core de la Red, a través de la red de transmisión, para hacer posible la comunicación.

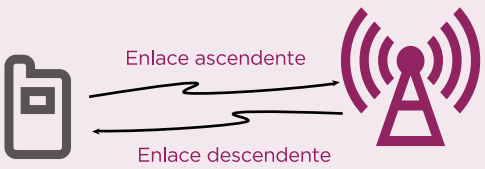
La red de acceso hace uso del espectro radioeléctrico asignado al operador de la red para proveer el servicio. El uso del espectro requiere de una cuidadosa planeación de frecuencias de manera que se permita hacer el máximo aprovechamiento del espectro disponible evitando interferencias.

La red de radio acceso transmite hacia el dispositivo móvil los mensajes que le permiten identificar la red de comunicaciones y recibe de éste la información para poder solicitar su registro en la red o para gestionar un enlace de comunicación. Así mismo se encarga, junto con otros elementos de la red, de mantener el enlace para que el usuario permanezca comunicado, incluso cuando el mismo se encuentra en movimiento, gracias a un proceso conocido como handoff que le permite cambiar de una estación base a otra sin cortar el enlace de comunicación.



La comunicación desde la red de acceso hacia el dispositivo móvil se conoce como enlace descendente (DL-Downlink) y en sentido opuesto se denomina, enlace ascendente (UL – Uplink).

La mayoría de las bandas de frecuencias usadas actualmente en América Latina distribuyen una porción de espectro exclusiva para el enlace descendente y otra para el enlace ascendente, es decir una duplexación en frecuencia (FDD). Las dos porciones deben tener una separación obligatoria entre ellas ejemplo: 45 MHz en la banda de 850MHz). Las bandas de frecuencias que hacen uso del mismo rango de espectro para los dos enlaces deben realizar una separación en tiempo (TDD).



Red de Transmisión

Infraestructura de comunicación responsable de transportar los datos y comunicaciones de voz de los usuarios finales desde los nodos de red (celdas) hasta la infraestructura central de la red (Core) y viceversa. Esta red puede ser implementada por medio de sistemas inalámbricos (microondas, satelitales, etc.) y/o alámbricos (fibra, UTP, coaxial, etc.). También hacen parte de la red de transmisión todos los enlaces requeridos para interconectar las redes centrales de Core de telefonía móvil entre los diferentes operadores móviles, así como la conexión con la salida a Internet.

Red Central (Core)

Consiste en diferentes elementos de red (según la tecnología) que en su conjunto tienen la labor de generar el correcto aprovisionamiento del servicio del usuario, así como los puentes que sean necesarios para lograr la conmutación de llamadas telefónicas y navegación de datos. Dentro de sus funciones principales se encuentran:

- Almacenar los datos de los usuarios así como los servicios que tienen activados.
- Gestionar y administrar la red de acceso.
- Soportar la movilidad de los dispositivos de usuario en la red, lo que permite pasar por diferentes estaciones de la red de radio sin perder la conexión.

- Comprobar el identificador del dispositivo o IMEI (international mobile equipment identification), lo que permite determinar el modelo de terminal que se está conectando a la red y bloquear los dispositivos robados EIR (Equipment Identity Register).
- Establecer las conexiones entre las diferentes redes de operadores móviles y fijos así como la interconexión con Internet.
- Procesar la información de los usuarios para poder establecer las llamadas de voz y/o las comunicaciones de datos.

Adicionalmente, existen otras plataformas conectadas al Core de la Red que permiten realizar la gestión de los usuarios, la tarificación, el monitoreo y gestión de la red, proporcionar servicios especiales, etc.

3.2.1 ¿Qué pasa en una red celular para que sea posible una llamada de voz o acceder a Internet?

Para que sea posible el funcionamiento de los servicios en una red celular, todos los componentes de la misma deben estar operando conforme a lo diseñado y cada uno de los sistemas cumpliendo con su parte del proceso. Así mismo, los sistemas deben estar dimensionados de manera apropiada para poder soportar la cantidad de tráfico que demanden los usuarios y el espectro usado para las comunicaciones debe estar libre de interferencias externas. Esto significa que cada componente del sistema aporta a la experiencia del usuario.

La siguiente figura resume lo expuesto.

FIGURA 4

Condiciones mínimas para que las comunicaciones sean posibles en una red móvil

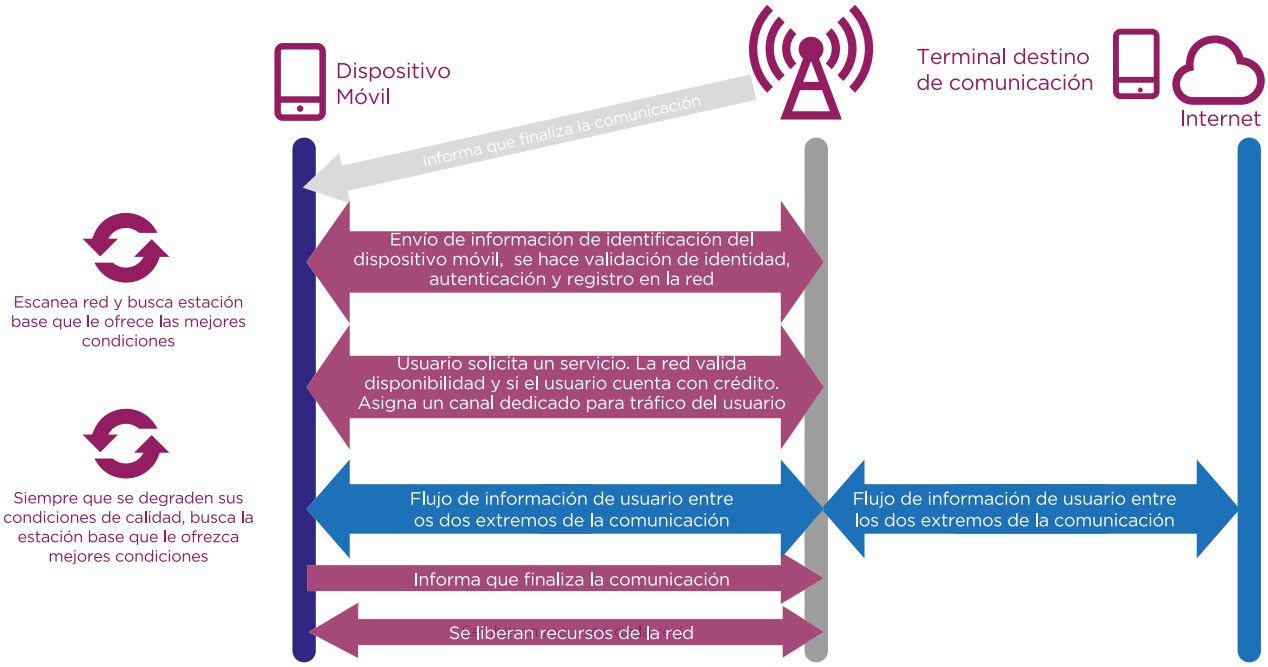
Fuente: BNMC

Ahora bien, tomando como base las condiciones de operación apropiadas para que se establezcan los enlaces de comunicación, se resume en la siguiente figura los pasos básicos para que se establezca una comunicación a través de una red móvil.

Todos los mensajes relacionados con el registro del usuario y solicitudes de servicios (mensajes de señalización) se realizan sobre canales lógicos de control, mientras que los paquetes de datos que contienen información generada por los usuarios o las llamadas de voz se realizan sobre canales lógicos de tráfico.

FIGURA 5

Procesos básicos para que se establezca una comunicación en redes celulares



Fuente: BNMC

3.2.2 Factores que limitan el establecimiento de una llamada o el acceso a un universo de datos en una red móvil celular

Conforme se mencionó previamente, el principal objetivo de los sistemas de comunicaciones y de los operadores de dichos sistemas es proporcionar el acceso de sus usuarios a los servicios de comunicaciones, buscando mantener adecuados niveles de calidad.

Para alcanzar dicho objetivo, los operadores llevan a cabo un dedicado trabajo de ingeniería en el momento de la planeación, diseño e implementación de sus redes, y mantienen un monitoreo permanente de las mismas. Así mismo, la tecnología incorpora funcionalidades para compensar problemas típicos en este tipo de redes, especialmente en la interfaz de radio por los fenómenos propios de la propagación de señales. Por ejemplo, existen técnicas de salto de frecuencia para minimizar la interferencia promedio del sistema, mecanismos de corrección de errores, retransmisión de mensajes de señalización, envío de información redundante para compensar pérdidas de paquetes, monitoreo en el dispositivo móvil de varias estaciones base con el objetivo de hacer uso de aquella que ofrezca las mejores condiciones, entre otros.

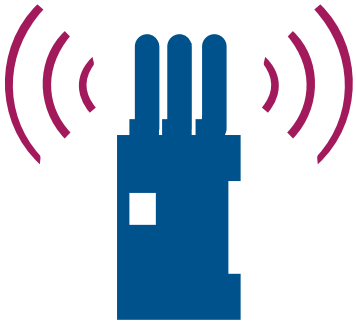
Entre los factores que limitan el establecimiento de una llamada o acceso a un servicio de datos, es posible identificar dos tipos:

- Factores de índole no técnico, relacionados a aspectos como tipo de contrato suscrito con el operador de red, facturación, crédito del usuario, mal manejo del dispositivo móvil, dispositivo móvil reportado en lista negra para bloqueo de acceso (por ejemplo, por hacer uso de terminal hurtado) entre otros.

- Factores de índole técnico inherentes a los componentes de la red considerando los dos extremos del enlace. En este grupo se identifican factores como fallas técnicas en algunos de los componentes, congestión en los recursos de la red (por ejemplo por eventos atípicos), niveles de interferencia por encima de los rangos permitidos para establecer un servicio (es decir, que la relación entre la información real o útil del usuario y la interferencia está por debajo de los necesario para poder decodificar los mensajes en la estación base o en el dispositivo móvil) ocasionados por filtros defectuosos de otros operadores que generan altos niveles de emisiones fuera de banda o interferencia externa en la misma banda de operación de la red móvil celular, entre otros.

3.3 Bloqueador o inhibidor de señal celular (jammer)

Los bloqueadores, inhibidores de señal o Jammers (por su término en inglés), son dispositivos que producen perturbaciones en una banda de frecuencia, con la intención de bloquear o interferir los equipos electrónicos que quieran hacer uso efectivo del espectro radioeléctrico. Su uso más común se genera sobre las señales de radio frecuencia de las tecnologías celulares, pero pueden afectar cualquier tipo de tecnología que opere en sus bandas de funcionamiento.



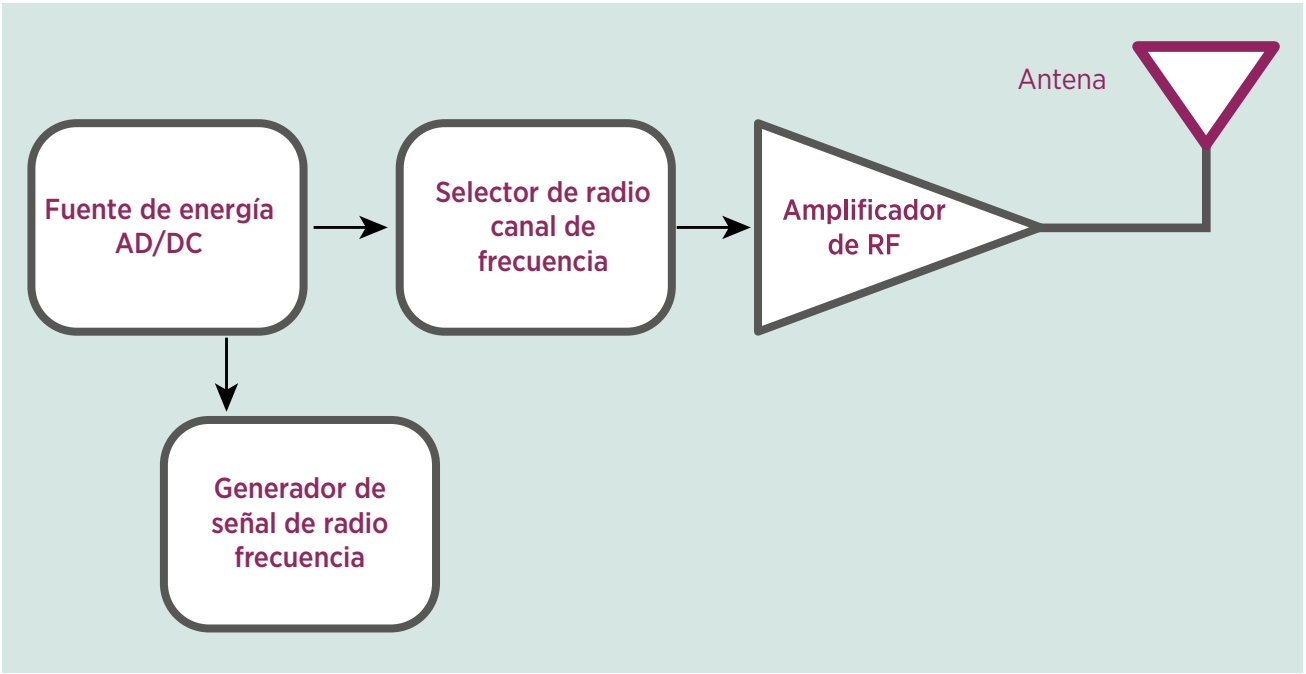
En esta sección se presentan algunos conceptos básicos sobre el funcionamiento de los bloqueadores de señal.

3.3.1 ¿Qué es y cómo funciona?

Un bloqueador o inhibidor de señal es un dispositivo de radiofrecuencia que intencionalmente transmiten señales en bandas específicas del espectro con el objeto de impactar, bloquear, interferir o saturar los servicios de comunicaciones de usuarios móviles tales como: llamadas de celular, mensajes de texto, señales de posicionamiento GPS, servicios de datos, redes de Wi-Fi, entre otras. Para esto introducen en la frecuencia indicada señales de ruido o información inútil falsa que sature la banda, impidiendo que la información verdadera llegue a su destino.

FIGURA 6

Diagrama básico de un bloqueador de señal

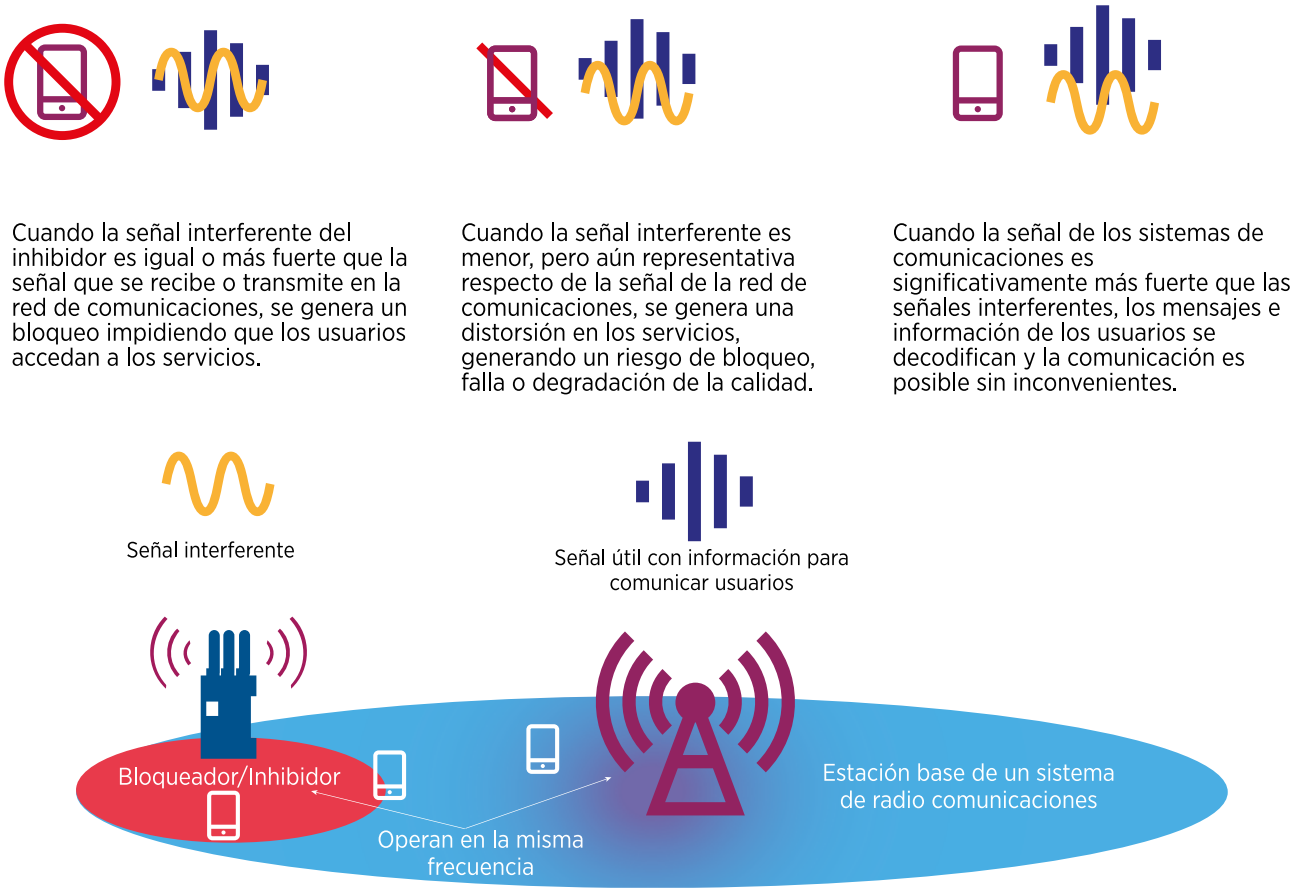


Fuente: BNMC

Los bloqueadores o inhibidores de señal siguen unos principios básicos, con una arquitectura que cuenta con un oscilador que genera la señal, un generador de ruido, una etapa de ganancia para dar suficiente potencia a la señal y finalmente una o varias antenas que transmiten lo generado. El objetivo de la señal generada es interrumpir la comunicación entre la estación base y el dispositivo móvil, generando que la relación entre la señal útil o real y la señal de ruido o interferente medida en el dispositivo o en la estación base sea lo suficientemente baja para que ningún mecanismo digital de recuperación de señal logre establecer o mantener una comunicación estable.

FIGURA 7

Principios de funcionamiento de inhibidores de señal



Fuente: BNMC

En términos generales, los móviles ubicados dentro de la cobertura de una estación base pueden recibir las señales enviadas por esta. Así mismo, la estación base puede recibir todas las señales generadas por dispositivos de transmisión de radiofrecuencias dentro de su zona de cobertura y en la su frecuencia de operación.

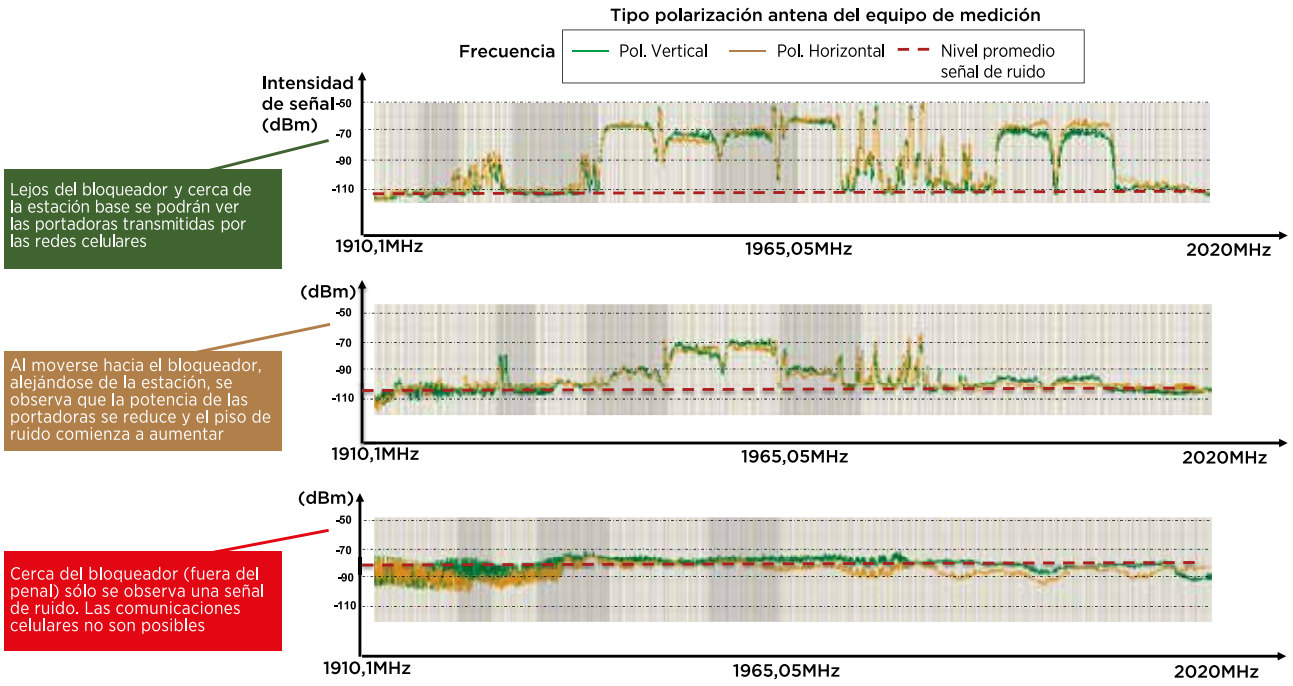
De esta manera, cuando los bloqueadores de señal generan una señal interferente en el enlace descendente que compite con los niveles de potencia de las señales enviadas por las estaciones base en la zona donde se localiza el usuario que se desea bloquear, se genera una degradación de la relación señal a interferencia tan alta que no es posible decodificar los mensajes útiles de la comunicación. Así mismo, cuando los bloqueadores de señal generan una señal interferente en el enlace ascendente que compite con los niveles de potencia generados por el dispositivo móvil, todas las señales que perciba la estación base con potencias cercanas o menores a la señal interferente no podrán ser decodificadas.

En mediciones de campo, haciendo uso de herramientas como analizadores de espectro, se puede observar el comportamiento de los bloqueadores de señal sobre los servicios de comunicaciones. La herramienta de medición puede capturar todas las señales transmitidas en una banda específica de frecuencias. Cuando la herramienta está fuera de la zona de impacto del bloqueador de señal, se pueden observar las ondas electromagnéticas que transportan la información de los servicios de comunicaciones. Estas ondas se suman a la señal de ruido comúnmente encontrada en el ambiente, generada por factores naturales y que es fácilmente soportada por las redes de comunicaciones. En la medida que la herramienta de medición se transporta a zonas más alejadas de las estaciones base de la red y en dirección a un bloqueador de señal, se puede observar que dicha señal de ruido se hace más fuerte, generando que las ondas que transportan la información de los servicios se deformen al punto que sean totalmente indescifrables para los sistemas (dispositivo móvil o estación base).

La siguiente figura resume lo mencionado.

FIGURA 8

Reglamentación sobre características técnicas de los bloqueadores y procedimientos

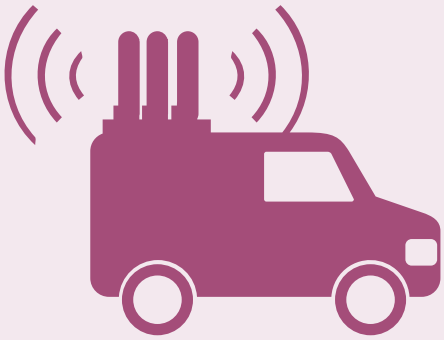


Es importante destacar que los bloqueadores de señal no hacen ningún análisis de las comunicaciones que se desean cursar ni del tipo de usuario que desea establecer la conexión, por esta razón no puede discriminar entre los terminales bajo su zona de cobertura ni evitar el bloqueo a llamadas de líneas de emergencias.

En otras palabras, el bloqueo de las comunicaciones, ya sean autorizadas o que se deseen restringir, estará dado por el nivel de potencia de las señales generadas por la estación base o el dispositivo móvil y el nivel de potencia de la señal interferente. En este sentido y considerando todos los fenómenos asociados con la propagación de ondas radioeléctricas que afectan la definición de una zona de cobertura y las funcionalidades propias de las redes de telefonía móvil celular, es posible que se presenten puntos dentro de la zona donde se desean bloquear las comunicaciones en los que sea posible establecer una llamada o acceder a servicios de datos y puntos fuera del área delimitada donde se presenten bloqueos de los servicios de comunicaciones. En algunas pruebas realizadas por el Instituto Penitenciario de Colombia se encontró que la efectividad en el bloqueo de comunicaciones dentro de los penales puede variar entre el 50% y el 99%, así mismo, mediciones realizadas por operadores móviles fuera de los límites de estos centros, muestran que el bloqueo de acceso a los servicios de comunicaciones autorizados puede superar el 15%.

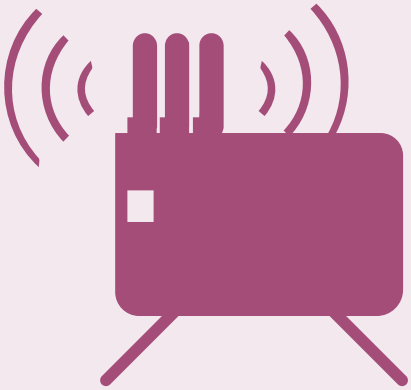
Existen diferentes tipos de inhibidores de señal que se pueden clasificar según su potencia de transmisión, lo cual determina el alcance del dispositivo o según su forma de instalación (portable, vehicular, fija, etc.). En cada clasificación es posible encontrar dispositivos o soluciones de inhibición de señal que soporten una o varias bandas de frecuencias (típicamente bandas UHF, bandas celulares y bandas WiFi), o que hagan uso de antenas directivas o antenas omnidireccionales.

Sistemas interferentes vehiculares



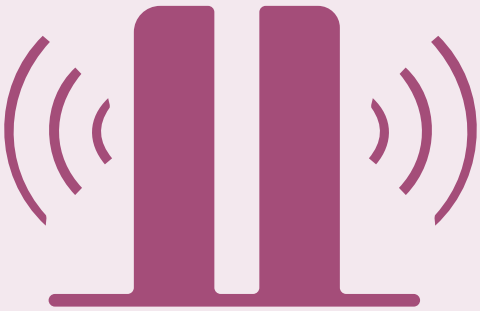
Su uso más frecuente se genera en la protección de convoyes militares y en vehículos de personas con alto riesgo de atentados con uso de explosivos con detonador a base de señales de radio (control remoto) y activadas con el paso de los vehículos. Los equipos inhibidores de señal instalados al interior de los vehículos tienen un rango de acción que va desde 20MHz hasta los 3000MHz adicionalmente son dotados con antenas omnidireccionales de alta ganancia, estos generadores de señales poseen una potencia de transmisión de hasta 1600 vatios y el conductor del vehículo puede contar con total autonomía de selección de rango de canal de frecuencia a interferir. Dichos vehículos también se encuentran acondicionados con generador de corriente AC de hasta 10.000 vatios con sistema de enfriamiento lo que garantiza la alta disponibilidad del sistema en recorridos de distancias largas. Las diferentes empresas que producen este tipo de Jammers ofrecen blindaje de hasta nivel 6 para los vehículos lo que garantiza protección de las personas a bordo y para los equipos inhibidores de señal. Algunos de los fabricantes de este tipo de Jammers personalizan el equipo terminal de manera que el operador o conductor del vehículo puede dejar canales de radio sin bloqueo, lo que facilita la comunicación de los ocupantes de los vehículos en el momento en que sea requerido.

Sistemas Interferentes portátiles/tácticos



Este tipo de Jammer es usado frecuentemente por agentes de control de frontera, negociadores de rehenes, personal de puestos de control, equipos de control de motines, brigadas de control de narcóticos, escuadrones anti explosivos, escuadrones SWAT, unidades de infantería entre muchas otras. Es frecuente encontrar este tipo de soluciones en maletas tipo equipaje de viaje con ruedas o en maletas de tipo campaña. Los Jammers ubicados al interior de las maletas con ruedas pueden llegar a tener entre otras las siguientes características técnicas: potencia de salida de RF de hasta 300 vatios, transmisión en simultánea de 3 a 6 bandas de frecuencia, otros modelos ofrecen interferir de todas las bandas de operación celular con posibilidad de bloqueo de hasta cuatro bandas en simultáneo con una potencia de transmisión de hasta 60 vatios, cuenta con la posibilidad de venir con una antena direccional de alta ganancia de hasta 8dBi o si el cliente lo prefiere puntos de conexión para antenas externas de tipo omnidireccional que van en un rango de los 8 dBi a 16 dBi. Este tipo de unidades opera con baterías internas y conexión a corriente AC o una fuente de corriente DC si el cliente lo solicita. a los casos en que es requerido un bloqueador que brinde mayor movilidad, se encuentran diseños que caben al interior de una maleta, y son más frecuentemente usados por personal que cubre grandes territorios desplazándose a pie o por escuadrones neutralizadores de bombas contra la amenaza de artefactos explosivos improvisados controlados remotamente (AEICR). Este tipo de elementos tiene como principales características técnicas, puede interferir frecuencias VHF/UHF, satelitales y celulares más usadas, está normalmente dotada con baterías recargables de alta duración lo que permite que el equipo inhibidor se encuentre operativo hasta por 8 horas continuas de radiación.

Sistemas interferentes estacionarios o fijos



Las soluciones interferentes estacionarias, están diseñadas para proporcionar una máxima protección contra la detonación de bombas y las comunicaciones indeseables en grandes edificios, establecimientos e instalaciones como, por ejemplo, establecimientos gubernamentales, instalaciones militares, edificios parlamentarios, embajadas, centros de detención, refugios militares, puntos de control militares, aeropuertos, entre otros. Este tipo de bloqueadores son capaces de interferir las señales de comunicación de Radiofrecuencia en grandes áreas definidas. Dentro de sus principales características técnicas tenemos, posibilidad de diferentes niveles de cobertura, adecuados para cualquier instalación de ubicación fija, este tipo de inhibidor es capaz de paralizar completa y simultáneamente todas las frecuencias de comunicación en los rangos de frecuencias de los 20MHz a 3000MHz, sin ningún tipo de espaciamiento, cuentan con hasta 1300 vatios de potencia total de salida de transmisión de Radiofrecuencia, poseen la posibilidad de activar y desactivar en forma independiente la interferencia de cada banda de frecuencia.

3

La necesidad de las instalaciones penitenciarias a nivel global ha generado una demanda de este tipo de bloqueadores por lo que es frecuente encontrar en el mercado inhibidores que se ajustan más a este tipo de estructuras, dentro de las características técnicas más comunes en equipos usados para cárceles tenemos: i) operación por control remoto del sistema lo que permite al operador del sistema tener la opción de activar y desactivar cada banda de frecuencia por separado o también simultáneamente, ii) cuenta con salidas de potencia máxima de 100 vatios por banda de frecuencia, iii) cada unidad puede estar provista de una función de ajuste de potencia, esto permite ajustar el nivel de potencia de transmisión de salida del sistema (su radio de cobertura) según los requisitos de un lugar específico. Cada banda de frecuencia tiene sus propias antenas direccionales de alta ganancia (o de tipo omnidireccional) con una ganancia máxima que puede llegar hasta los 14dBi. Las antenas se pueden conectar a las unidades inhibidoras mediante cables de baja pérdida. Su fuente de alimentación debe ser AC y se pueden llegar a dotar con bancos de baterías para eventos de fallos de corriente eléctrica en los sitios donde se encuentren instalados.

Dentro del ecosistema de dispositivos se cuenta con proveedores en diferentes países alrededor del mundo, siendo Israel y Estados Unidos los países que más jugadores en el mercado. Algunos de los jugadores líderes a nivel mundial son BAE Systems (U.K), Northrop Grumman (U.S.), Raytheon (U.S.), HSS Development (U.S.), Harris Corporation (U.S.), Lockheed Martin (U.S.), Israel Aerospace Industries (Israel), PROjammers (HK), Sesp Group (Israel), MCTECH TECHNOLOGY (U.S.), y Wolves fleet Technology Co. Limited (China), PrisonJammer (U.S.), SESP (U.S), entre otros.

3.3.2 Características de bloqueadores de señal y otras soluciones

Como se mencionó previamente, existen diferentes tipos de bloqueadores de señal, no obstante, estos dispositivos son fabricados con importantes variaciones en sus características técnicas para ajustarse a diferentes usos o aplicaciones. A continuación, se enumeran algunas de las características más relevantes.

- Potencia de transmisión fija o ajustable para cada banda de operación
- Bandas de frecuencia de operación (rangos de DL o UL)
- Emisiones fuera de banda
- Tipo de antena (omnidireccional o directiva)
- Sistema de control y monitoreo remoto
- Consumo de potencia y eficiencia eléctrica
- Autonomía
- Panel de control externo
- Alarmas
- Resistencia a factores ambientales
- Rango de temperatura de operación
- Niveles de campo electromagnético generados

Otros avances han permitido que los nuevos inhibidores detecten la actividad de un teléfono celular móvil y luego reaccionar atascando las frecuencias de ese teléfono. Los Jammers de RF seleccionables por potencia, permiten al usuario aumentar o disminuir la salida de potencia de interferencia de señal para un control estabilizado sobre el radio de interferencia. Por otro lado, se han implementado soluciones alternativas para realizar un bloqueo selectivo de comunicaciones. Estas soluciones se soportan en tecnologías basadas en radio bases para detectar y bloquear dispositivos de comunicaciones inalámbricas dentro de sus límites. Este tipo de soluciones serán detalladas en el capítulo 4 del presente informe.

3.4 Impacto de los bloqueadores de señal

Como se mencionó previamente, el objetivo de los bloqueadores o inhibidores es interferir o generar disrupción en las señales de los sistemas de radiocomunicaciones evitando que se establezcan llamadas, se envíen mensajes o se acceda a Internet o servicios de datos. Este bloqueo es motivado comúnmente por razones de seguridad o interés público. No obstante, dados los principios de propagación de las ondas electromagnéticas mencionados en la sección 3.1., estos equipos que transmiten señales de radiofrecuencia pueden generar impactos no deseados afectando las comunicaciones de usuarios comerciales y de servicios de seguridad pública, como llamadas a las líneas de emergencia.

Los impactos de mayor relevancia generados por el uso de dispositivos bloqueadores o inhibidores de señal en centros penitenciarios son:

a. **Bloqueo de comunicaciones fuera de los límites de los centros penitenciarios** impidiendo el acceso de los usuarios a servicios de comunicaciones autorizados, incluyendo la restricción de las llamadas a líneas de emergencia.

b. **Degradación de los servicios de comunicaciones** en las zonas aledañas al centro penitenciario representado en constantes caídas de llamadas, mala calidad de las comunicaciones, lentitud en los servicios de datos, entre otros.

c. El uso de dispositivos bloqueadores con filtros y transmisores de baja calidad pueden generar **emisiones perjudiciales fuera de la banda de operación**, afectando otros servicios radioeléctricos que operen en dichas bandas.

d. De manera similar al caso anterior, cuando los bloqueadores operan en múltiples bandas de frecuencias pueden generar **señales interferentes perjudiciales en otras bandas diferentes** afectando todo tipo de servicios. Pudiendo llegar incluso a dificultar la labor policial al interferir también los sistemas radioeléctricos de comunicación utilizados por las fuerzas de seguridad. Este se debe a un fenómeno denominado Productos de Intermodulación[2].

e. **Zonas "ciegas" dentro del centro penitenciario**, donde aún es posible establecer comunicaciones no autorizadas.

Por último, es importante destacar que para impedir las comunicaciones clandestinas no es suficiente con interferir las bandas de la telefonía celular móvil, dado que es posible que éstas se realicen utilizando otros servicios o tecnologías como WiFi, VHF (handies), satelital, etc.

En las siguientes secciones se presenta un breve análisis sobre los impactos mencionados, es particular, aquellos relacionados con el bloqueo y degradación de las comunicaciones celulares fuera de los límites de los centros penitenciarios. Dicho análisis fue realizado a partir de conceptos teóricos y mediciones realizadas en casos prácticos de estudio en centros penitenciarios de Colombia. El detalle de dichos casos se presenta en el Anexo 1.

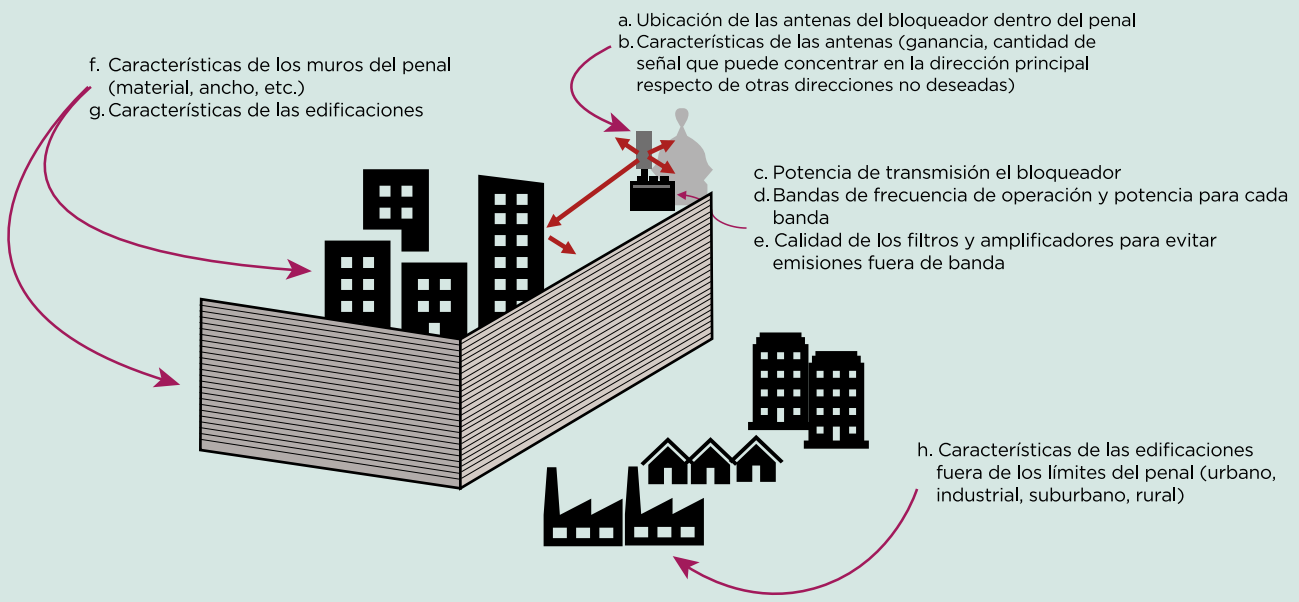
3.4.1 Área potencial afectada por la presencia de un bloquedor de señal

Al igual que cualquier transmisor de señales radioeléctricas, el área de cobertura de un bloqueador de señal dependerá de factores asociados tanto con el diseño de ingeniería, como con las características técnicas de los equipos instalados y de las condiciones físicas del centro penitenciario y de las zonas aledañas.

Los más relevantes son mencionados en la siguiente figura.

FIGURA 9

Factores que influyen en el área de cobertura de un bloqueador



Fuente: BNMC

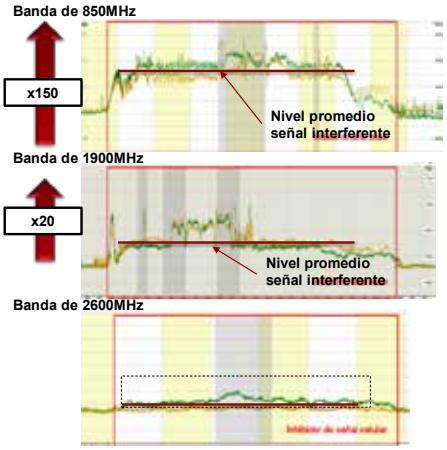
La ubicación de las antenas dependerá del estudio de ingeniería realizado, cuyo objetivo debe ser el cubrimiento de las zonas donde se requiera el bloqueo de las comunicaciones y evitar fugas de señal hacia el exterior de dichos límites, para ello se considera las condiciones físicas de construcción y distribución de cada penal, así como los niveles de señal de los servicios de radiocomunicaciones que se desean bloquear. Antenas ubicadas cerca de los límites del centro penitenciario o en zonas altas generan un mayor riesgo de producir interferencias no deseadas fuera de los límites.

La calidad de los equipos y elementos instalados es otro factor relevante para minimizar riesgos de interferencias no deseadas. El desempeño operativo de todos los elementos del sistema, antenas, conectores, filtro y amplificador del equipo bloqueador, etc. tiene un impacto significativo en el resultado final.

En este mismo sentido, la potencia de transmisión que genere el equipo bloqueador es una característica técnica fundamental para determinar el área de cobertura donde se genera interferencia o restricción de los servicios de comunicaciones. Una mayor potencia de transmisión representa señales interferentes más fuertes para generar el bloqueo de las comunicaciones, pero generar a su vez una mayor afectación fuera de los límites del centro penitenciario. El uso de altas potencias está normalmente asociado con la necesidad de llegar a zonas alejadas de las antenas del bloqueador o de mejorar la penetración de dichas señales en lugares dentro de edificaciones, principalmente, cuando se hace necesario mantener los equipos totalmente aislados de la población carcelaria a fin de evitar manipulación o vandalismos de los mismos.

Finalmente, como se mencionó previamente, las señales transmitidas en bandas bajas de frecuencia (p.e. banda de 700MHz, 850MHz) alcanza mayores distancias que las transmitidas en bandas altas (p.e banda de 1.900MHz, AWS, 2.6GHz). Aunque los bloqueadores instalados en centros penitenciarios

comúnmente permiten ajustar de manera independiente la potencia de transmisión para cada una de las bandas de frecuencia de operación, en pruebas realizadas por operadores móviles fuera de los límites de centros penitenciarios, se observa que la interferencia medida en un punto específico tiende a ser mucho mayor en las bandas bajas de frecuencia. Por ejemplo, en las mediciones que se muestran en la figura, el nivel de la señal interferente transmitida en la banda de 850MHz es aproximadamente 150 veces más fuerte que el nivel de la señal interferente en la banda de 1.900MHz.



En los casos de estudio analizados, se encontró que la señal interferente generada por los bloqueadores de señal tiene un riesgo crítico de bloquear comunicaciones en zonas ubicadas a menos de 400mts de los límites del penal, y generan degradación importante en la relación señal a ruido en zonas entre los 400mts y 1.600mts fuera de los límites del penal, esto es, que el nivel promedio de la señal interferente o de ruido se incrementa entre 10 y 150 veces por encima de los niveles de ruido o interferencia normalmente aceptados por los sistemas de radiocomunicaciones. No obstante, se aclara que también se identificaron algunas zonas más allá de los 1,6km donde los niveles de interferencia resultaban perjudiciales para ofrecer buenas condiciones de calidad en los servicios de comunicaciones móviles.

3.4.2 Impacto en percepción del usuario

Como se ha mencionado, usuarios fuera de los límites penitenciarios pueden verse afectados por las señales interferentes generadas por los bloqueadores de señal. Esta situación se manifiesta en fallas al intentar establecer una comunicación, caída de llamadas o cortes en la sesión de una conexión de datos e incluso que en su teléfono se vea el mensaje “Sin Servicio” debido a que no puede decodificar la información de ninguna red.

Desde el punto de vista del riesgo de que los usuarios no puedan acceder a los servicios de comunicaciones, los impactos medidos mediante información de indicadores de desempeño recopilada por la red y pruebas realizadas en los alrededores de los centros penitenciarios, muestran que la probabilidad de los usuarios en la zona afectada para acceder a los servicios de comunicaciones provistos por redes móviles, se degradan entre un 15% y un 60%, es decir, que debido a la interferencia generada por el bloqueador fuera de los límites del penal, los usuarios tendrán riesgo que se bloqueen entre 2 y 6 intentos de comunicación cada 10 veces que deseen acceder al servicio. Esta variación dependerá de la zona donde se localice el usuario (p.e. la distancia al centro penitenciario) y la demanda de tráfico que puede variar a diferentes horas del día.

En relación con las caídas de llamadas, es posible identificar que en las estaciones base que brindan cobertura a las zonas aledañas a los centros penitenciarios con bloqueadores de señal, el porcentaje de llamadas caídas puede pasar desde un 2% o 3% a valores superiores al 10%, afectando significativamente la percepción de los usuarios.

En términos técnicos, la degradación de los niveles de calidad de los servicios de comunicaciones es generada porque la relación entre la señal útil de la red y la interferencia externa no cumple con las condiciones adecuadas para la prestación de los servicios, incluso llegan a niveles altamente perjudiciales donde no es posible decodificar la información transmitida. En la imagen, correspondiente a mediciones realizadas por un operador móvil alrededor de un centro penitenciario en Colombia, se muestra la existencia de zonas (en rojo) donde la degradación de la relación entre la señal útil y la interferencia impide el establecimiento de los servicios, y otras (en naranja y amarillo) donde dicha relación se ha degradado por encima de los niveles óptimos, afectando la calidad final del servicio, pero aún con probabilidad de poder acceder a los mismos.

4 Experiencia internacional

El ingreso ilegal de dispositivos de comunicación inalámbrica a los centros penitenciarios es una problemática expandida a nivel mundial. Esto es evidenciado por la significativa cantidad de equipos de comunicaciones, como teléfonos celulares y SIM CARDs, incautados en prisiones de diferentes países como Colombia, Brasil, Estados Unidos, México, Reino Unido, Nueva Zelanda, entre otros.

Adicionalmente, el uso de estos equipos de comunicación por parte de criminales para cometer actos delictivos como extorsión, amenazas, secuestros, asesinatos o coordinar escapes, es una situación prioritaria en la agenda de Seguridad Pública de diversos gobiernos. Esta situación ha llevado a que, en los últimos años, algunos de estos gobiernos adelanten trabajos coordinados y cooperativos entre diferentes autoridades administrativas, e incluso involucren al sector privado, para identificar soluciones que permitan contrarrestar la mencionada problemática. Aunque ha habido algunos avances desde el punto de vista de reglamentación, aún existen serias críticas a las medidas adoptadas.

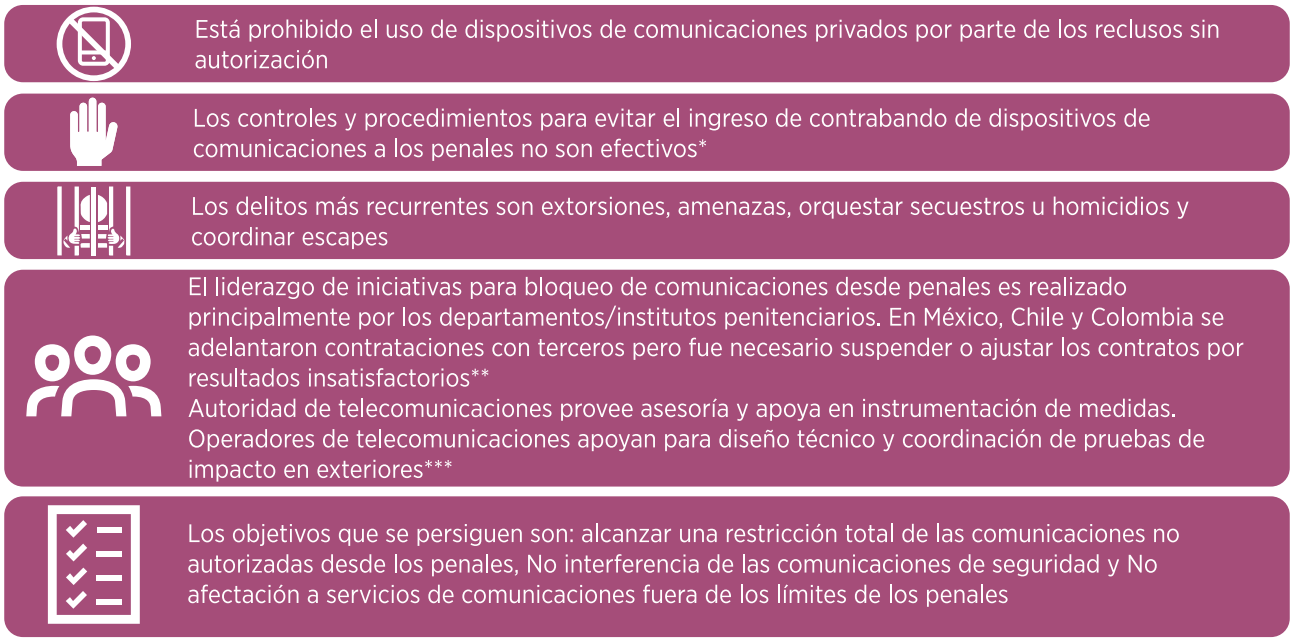
En este capítulo se presenta un resumen de la situación de algunos países de América Latina (México, Brasil, Colombia, Argentina y Chile) y de Estados Unidos y Reino Unido, en relación con el uso de bloqueadores en centros penitenciarios y de las medidas regulatorias adoptadas. Un mayor detalle sobre cada país relevado es presentado en el Anexo I.

4.1 Panorama general de América Latina sobre el uso de bloqueadores de señal

El contexto general de los países de América Latina relevados, en relación con las comunicaciones no autorizadas desde los centros penitenciarios y que representan un riesgo para la seguridad pública, así como las iniciativas para contrarrestarlo, tiene varios en puntos en común. Especialmente en lo relacionado con los antecedentes, las iniciativas de solución y las instituciones involucradas, como se resume en la siguiente figura.

FIGURA 10

Contexto General de la Región (Antecedentes)



* En Colombia hay reportes de más de 65.900 terminales móviles incautados entre 2012 y 2015[3], en Chile la cifra alcanzó los 24.992 en 2015[4].

** En 2012 Chile realizó un concurso público en el que contrató a una empresa para instalación de bloqueadores sin resultados satisfactorios, en 2011 México contrató a la empresa Software DSI S.A. para instalar
155 bloqueadores en 6 penales. El INPEC de Colombia ha realizado varios contratos, uno de ellos con la empresa CURACAO.

*** Otras instituciones de seguridad pública como organismos de inteligencia policial o departamentos de desarrollo tecnológico también participan en calidad de asesores.

Fuente: BNMC

Aunque los sistemas de comunicaciones usados por los reclusos dentro de los penales incluyen terminales para comunicaciones móviles celulares, radios trunking, radios UHF, teléfonos satelitales, Wi-Fi, GPS e incluso el uso de drones[5] para contrabando de armas, drogas o dispositivos de comunicaciones, el foco de los organismos de seguridad de los países relevados se centra en las comunicaciones a través de redes móviles y WiFi, por ser la modalidad más común.

De la figura anterior, es importante resaltar que, de los casos relevados, incluyendo a Estados Unidos y Reino Unido, son los departamentos o institutos penitenciarios de orden nacional o local los encargados de gestionar los proyectos y el presupuesto para la instalación de soluciones para el bloqueo o restricción de comunicaciones desde el interior de los penales o centros de reclusión.

En Colombia, el Instituto Nacional Penitenciario y Carcelario (INPEC) ha gestionado entre 2013 y 2016 la instalación de bloqueadores de señal tipo jammer en 16 penales del país, en los que se identificó el mayor riesgo delictivo, esto se realizó en el marco de un plan de trabajo que incluyó reuniones con el Ministerio TIC y operadores de servicios móviles. En pruebas realizadas por el INPEC la efectividad de dichas soluciones varía entre el 50% y el 99% en el bloqueo de llamadas y se ven afectadas críticamente por hechos de vandalismo por parte de la población carcelaria.

3. (INPEC, 2016).
4. (Economía y Negocios, 2016).
5. El uso de drones para contrabando de drogas, armas y celulares se ha detectado en las prisiones de Reino Unido, por lo que ha sido necesario contemplar el uso de disruptores de señal para este tipo de aparatos.

Adicionalmente, el INPEC en coordinación con la Dirección Antisecuestro y Antiextorsión de la Policía Nacional realizó pruebas con equipos tácticos que permiten la identificación de los números de SIM (IMSI) y códigos de los dispositivos móviles (IMEI), de manera que los mismos puedan ser bloqueados por parte de los operadores móviles[6].

El Departamento Penitenciario Nacional de Brasil (DEPEN) ha realizado la instalación de sistemas de bloqueo de señal tipo jammer en 23 penales en São Paulo, lo cual representa el 14% del total de centros penitenciarios paulistas[7]. No obstante, en los penales que cuentan con sistema de bloqueo aún se realizan incautaciones de terminales móviles, lo que permite concluir que la eficiencia de la solución no es del 100%. Hace algunos años se planteó la posibilidad de trasladar a los operadores de servicios de telecomunicaciones la obligación de instalar y operar estos sistemas de bloqueo de señales. No obstante, considerando que la Seguridad Pública es un deber del Estado y los procedimientos y responsabilidades definidas en las Leyes de Ejecuciones Penales de Brasil, el Supremo Tribunal Federal en decisión del 03 de Agosto de 2016 encontró inconstitucional la mencionada propuesta.

En México, los organismos bajo la Subsecretaría del Sistema Penitenciario Nacional han venido trabajando en actualizaciones normativas y revisión de soluciones técnicas para la instalación de bloqueos en todos los centros penitenciarios del país. No obstante, en 2011 el gobierno de México celebró un contrato para la instalación de bloqueadores de señal tipo jammer en 6 penales, con resultados pocos satisfactorios debido a la baja efectividad y al impacto en el servicio celular de la población alrededor de los penales. Adicionalmente, los organismos de seguridad reportaron manipulación y alteración de los equipos por parte de la población carcelaria.

Gendarmería de Chile tuvo una experiencia similar a México con un contrato realizado en 2012 para la instalación de bloqueadores de señal tipo jammer. Debido a los resultados poco satisfactorios por la baja efectividad en bloqueo y el impacto en los servicios de comunicaciones de la población civil fuera de los límites de los penales, Gendarmería de Chile ha venido adelantando solicitudes de información RFI a la industria con el objetivo de conocer posibles soluciones para el bloqueo de señales de comunicaciones inalámbricas dentro de penales, a fin de adelantar un nuevo concurso público en el corto plazo.

En Argentina, la instalación de un bloqueador de señal tipo jammer en la cárcel Piñero de la Provincia de Santa Fé generó significativos impactos en los servicios de comunicaciones móviles de la población aledaña, por lo que el Ente Nacional de Comunicaciones (ENACOM) ordenó el apagado del mismo.

A diferencia de los casos anteriores, en Estados Unidos, debido al estricto marco regulatorio para el uso de bloqueadores de señal tipo jammers, algunas correccionales (cerca de 52 correccionales en 17 estados) han implementado tecnologías basadas en radio bases para detectar y bloquear dispositivos de comunicaciones inalámbricas dentro de sus límites. Este tipo de sistemas se denominan Contraband Interdiction System (CISs) y requiere autorización por parte de la FCC. Estas soluciones consisten en sistemas de gestión de acceso (MAS, por sus siglas en inglés) y de detección de dispositivos mediante la identificación del usuario (IMSI/IMEI) facilitando la inclusión de los mismos en bases de datos de bloqueo. Reino Unido ha adoptado medidas similares al caso de EEUU.

En todos los casos relevados donde se llevó a cabo la instalación de bloqueadores de señal tipo jammer, se observaron los siguientes efectos indeseados:

- No fue posible obtener o garantizar una eficiencia del 100% en el bloqueo de las comunicaciones no autorizadas desde los penales o centros de reclusión.
- Hubo degradación en los servicios de comunicaciones de la población localizada fuera de los límites de los penales, afectando el acceso de los usuarios a las redes de comunicaciones autorizadas para operar.
- Los equipos fueron afectados por hechos de manipulación y vandalismo por parte de la población carcelaria.

6. (INPEC, 2016)
7. Se estima una inversión de $ 31 millones de Reales. (GLOBO - EPOCA NEGOCIOS, 2017)

4.2 Análisis comparativo de marcos regulatorios vigentes sobre el uso de bloqueadores de señal

El marco normativo aplicable al uso de dispositivos bloqueadores o inhibidores de señal puede ser analizado desde dos enfoques: i) reglamentación aplicable como dispositivo que emite señales de radiofrecuencia y que hace uso de espectro radioeléctrico, y ii) como dispositivo de seguridad para prevención del crimen y el delito.

A continuación, se presenta un resumen de los principales aspectos incluidos en la normativa vigente de los países relevados para cada uno de los enfoques mencionados.

4.2.1 Reglamentación aplicable como dispositivo que emite señales de radiofrecuencia y hace uso de espectro radioeléctrico

En términos generales, el uso no autorizado de dispositivos de radiofrecuencias que interfieran de manera intencional o maliciosa servicios de comunicaciones autorizados está prohibido en los países relevados o es considerado un uso clandestino o ilegal del espectro. No obstante, existen algunas excepciones sustentadas en razones de seguridad pública o interés general, que contempla autorizar el uso de este tipo de equipos en recintos confinados como centros penitenciaros. En todos los casos analizados se exige que no haya una afectación en los servicios de comunicaciones autorizados fuera de los límites de los penales.

La siguiente figura resume los aspectos más relevantes.

FIGURA 11

Normativa aplicable a bloqueadores como dispositivo que hace uso del espectro

Norma equipos	Uso de bloqueadores / inhibiores de señal	Excepciones
Argentina **ENACOM** Ley Argentina Digital	• Interferir servicios de comunicaciones autorizados es uso ilegal del espectro	• No aplica
Brasil **ANATEL** Resolución 308 de 2002	• Interferir o restringir señales autorizadas es uso clandestino del espectro	• Autoriza uso de bloqueadores de señales de radiocomunicaciones en penales. NO PUEDE AFECTAR SERVICIO FUERA DE LOS LÍMITES
Colombia **MINTIC - ANE** Resolución 2774 de 2011	• Uso de bloqueadores es un uso clandestino del espectro	• Entidades públicas o sector financiero por razones de seguridad o interés general, previa autorización del MINTIC. Apagar en caso de afectación en exteriores. • Organismos de seguridad del Estado pueden usar sin autorización
México **IFT** Ley Federal de Telecomunicaciones	• Sólo es legal cancelar o anular señales de radiocomunicaciones en centros penitenciarios	• Uso obligatorio en todos los centros de readaptación social, establecimientos penitenciarios. • No pueden afectar más allá de 20mts de los límites del centro
Estados Unidos **FCC** Ley de Comunicaciones	• Prohibido el uso, venta, importación y/o comercialización de Jammers	• Fabricación exclusiva para exportar • Usado por el gobierno de EEUU con autorización de FCC
Reino Unido **Ofcom**	• Prohibida la instalación de dispositivos inalámbricos en la parte continental de Reino Unido, Irlanda del Norte, aguas territoriales, Isla de Man y las Islas de Canal	• Recintos confinados dentro de prisiones. No puede afectar exteriores

4.2.2 Reglamentación aplicable como dispositivo para prevención del crimen y el delito

Como se mencionó en la anterior sección, las regulaciones en materia de espectro contemplan algunas excepciones para el uso de dispositivos bloqueadores o inhibidores de señal. En algunos de estos casos, se expidieron reglamentos adicionales que definen, entre otros aspectos, características técnicas de los equipos autorizados, roles de las partes involucradas y procedimientos para autorizaciones o monitoreo, en caso de requerirse.

La siguiente tabla resume aspectos normativos relacionados con características técnicas de los equipos y procedimientos establecidos.

FIGURA 12

Reglamentación sobre características técnicas de los bloqueadores y procedimientos

Norma equipos	Características técnicas mínimas de los equipos	Equipos
Brasil **ANATEL** Res. 306 de 2002 Res. 308 de 2002	• Bloquear todas las bandas de frecuencias usadas en Serv. de telecomunicaciones • No puede bloquear otras bandas de frecuencia o fuera de los límites físicos del penal • Bloquear señales de cualquier tecnología • Control de potencia independiente en cada banda • No estar al alcance de la población carcelaria • Cumplir con los límites de exposición a campos electromagnéticos	• Notificar a ANATEL 10 días antes de encender el equipo • Mantener informado a operadores de telecomunicaciones • Presentar proyecto técnico • Realizar validación de impacto en puntos de verificación
Colombia **MINTIC - MinJusticia** Decre768 de 2011 Resolución 2774 de 2013	• Cumplir con límites de exposición a campos electromagnéticos	• Sólo aplica a penales donde haya evidencias de delitos desde dispositivos de comunicaciones • Se debe enviar solicitud a MINTIC con condiciones técnicas de la solución, huella de cobertura hasta 500mts fuera de los límites del penal • Apagar en caso de impacto en exteriores hasta solucionar • Coordinar con operadores de telecomunicaciones • No aplica indicadores de calidad en penales afectados
México **Ley General del Sistema de Seguridad Pública IFT** Ley Federal de Telecomunicaciones Disposición Técnica IFT-10-2016	• No exceder 20mts fuera de las instalaciones • Enviar señales ante interrupción de funcionalidad • Control desde centros remotos • Potencia ajustable independiente para cada banda • No contar con controles externos para evitar manipulación • Sólo bloquear el enlace descendente • No bloquear la banda de 380 – 399.9MHz • Cumplir con los límites de exposición a campos electromagnéticos	• Instalar equipos que anulen o cancelen las señales de telefonía celular de manera permanente en todos los centros penitenciarios • Ser operado por autoridades distintas a los establecimientos penitenciarios y en centros remotos

Fuente: BNMC

La siguiente tabla presenta las responsabilidades de cada una de las partes involucradas en la implementación y/u operación de dispositivos bloqueadores o inhibidores de señal celular

FIGURA 13

Responsabilidades de partes involucradas en implementación u operación de jammers

Operadores de Telecomunicaciones	Autoridad de Telecomunicaciones	Departamento/instituto/centro/penitenciario
Brasil • Confidencialidad de información • Informar sobre cambios en la red que afecten cobertura en zona de interés • Colaborar con validación de impacto en puntos de verificación	• Bloquear todas las bandas de frecuencias usadas en Serv. de telecomunicaciones • No puede bloquear otras bandas de frecuencia o fuera de los límites físicos del penal • Bloquear señales de cualquier tecnología • Control de potencia independiente en cada banda • No estar al alcance de la población carcelaria • Cumplir con los límites de exposición a campos electromagnéticos	• Notificar a ANATEL 10 días antes de encender el equipo • Mantener informado a operadores de telecomunicaciones • Presentar proyecto técnico • Realizar validación de impacto en puntos de verificación • Gestionar presupuesto y contrataciones. Instalar y operar el sistem
Colombia • Colaborar con autoridades • Restringir señales de transmisión, recepción o control dentro de penales en caso de ser requerido por MINTIC	• Vigilar afectaciones en zonas aledañas a los penales • Analizar solicitudes y autorizar uso de bloqueadores • Brindar asesoría a autoridades penitenciarias	• Sólo aplica a penales donde haya evidencias de delitos desde dispositivos de comunicaciones • Se debe enviar solicitud a MINTIC con condiciones técnicas de la solución, huella de cobertura hasta 500mts fuera de los límites del penal • Apagar en caso de impacto en exteriores hasta solucionar • Coordinar con operadores de telecomunicaciones • No aplica indicadores de calidad en penales afectados • Gestionar presupuesto. Instalar y operar el sistema
México • Colaborar con autoridades a nivel técnico para cancelar o anular señales de telefonía celular en penales • Colaborar con el monitoreo de la operatividad de los equipos de bloqueo	• Apoyar y asesorar a autoridades penitenciarias y seguridad • Coordinar con operadores de telecomunicaciones • Monitorear calidad de servicio en zonas aledañas	• Coordinación entre entidades • Gestionar presupuesto y contrataciones • Instalar, operar y supervisar funcionamiento

Fuente: BNMC

4.3 Buenas prácticas identificadas

Con base en las experiencias de los países relevados, se identifican algunas buenas prácticas que favorecen el cumplimiento de los objetivos perseguidos por los gobiernos mencionados en la Figura 1, detalladas a continuación.

Revisar los protocolos y procedimientos para el control de ingreso de dispositivos de comunicaciones a los penales y fortalecer herramientas de detección

Es importante tener presente que el punto de partida de las comunicaciones con fines delictivos generadas desde los centros penitenciarios es el ingreso ilegal de celulares y otros dispositivos de comunicaciones, ya sea por fallas en los controles de ingreso de personal externo, con ayuda de personal de la guardia carcelaria u otras modalidades de contrabando.

Considerando este factor, una de las iniciativas incluidas en el plan de trabajo del INPEC en Colombia, fue la revisión de sus protocolos y controles para el ingreso de elementos a los centros penitenciarios[8], a fin de fortalecer esta etapa.

Así mismo, el INPEC, con apoyo de la Policía Nacional, ha venido realizando pruebas con equipos tácticos para detección de dispositivos de radiocomunicaciones dentro de los penales, de manera que puedan ser incautados o se obtenga la información de identificación del usuario para su posterior bloqueo. Estos equipos ya son usados en Estados Unidos y Reino Unido.

Identificar aquellos centros penitenciarios que necesariamente requieran una solución de bloqueo de comunicaciones móviles

La implementación masiva de dispositivos de bloqueo de señal en todos los centros penitenciaros de un país incrementa sustancialmente el riesgo de los ciudadanos y de las entidades públicas a no acceder a los servicios de comunicaciones, especialmente en situaciones de emergencias. Adicionalmente representa un alto gasto para las entidades públicas tanto en la instalación como en la operación efectiva de la solución.

En este sentido, se destaca la posición de Colombia para identificar exclusivamente los centros penitenciarios donde exista evidencia de actos delictivos desde su interior mediante el uso de dispositivos de comunicaciones, e incluso reubicar reclusos a fin de centralizarlos en penales donde se autorice la implementación de la medida. Así mismo, en Brasil y Estados Unidos, se requiere una solicitud y autorización previa al uso de bloqueadores de señal para cada uno de los centros penitenciarios donde se requiera la instalación de la solución.

Finalmente, considerando la alternativa de reubicar reclusos relacionados con actos delictivos de extorsión, secuestro, etc. desde las cárceles, sería apropiado dar prioridad a centros penitenciarios ubicados en zonas rurales o alejadas de centros urbanos con población que pueda ser afectada con la solución.

Analizar y definir la solución técnica para cada penitenciario según las características y necesidades de cada caso

Los centros penitenciarios de un mismo país pueden tener características físicas diferentes, como localización (urbana, rural), tipo de construcción (características de los muros y edificios), distribución interna, niveles de cobertura de los operadores de telecomunicaciones, etc., así como necesidades diferentes según la problemática de cada caso (tipo de dispositivos de comunicación usado, nivel de riesgo, etc.). Por esta razón, es recomendable analizar la solución apropiada para cada caso (ya sea una tecnología o una combinación de estrategia), de manera que se obtenga la mejor relación costo-impacto/beneficio, conforme lo sugiere los reportes de la FCC de Estados Unidos.

8. (INPEC, 2012)

En este sentido, no resulta conveniente masificar un mismo tipo de solución en todos los centros penitenciarios cuando se obtienen resultados positivos en un caso de prueba.

Coordinar con autoridades del sector TIC y operadores de telecomunicaciones: Flujo de información y colaboración. Realizar pruebas controladas

Una iniciativa común en países como Colombia, México, Brasil, Estados Unidos y Reino Unido, es el trabajo colaborativo de las autoridades penitenciarias con las autoridades del sector TIC y los operadores de servicios de telecomunicaciones. Esta dinámica permite identificar alternativas de solución con la infraestructura existente, mitigar o, por lo menos, monitorear el impacto en las zonas fuera de los límites de los penales, e instrumentar reglamentaciones y procedimientos en caso de requerirse.

Reconocer riesgo de bloquear acceso a comunicaciones de usuarios fuera de límites del penal y definir procedimientos claros de acción

En términos generales, los reglamentos son claros al prohibir que se afecte el acceso a los servicios de comunicaciones fuera de los límites de los centros penitenciarios. Particularmente, el de Colombia exige que, en caso de impacto, el bloqueador deba ser apagado inmediatamente y hasta que se solucione el problema y se hagan las pruebas y mediciones correspondientes.
Adicionalmente, debería eximirse a los operadores móviles de cualquier penalidad por degradaciones en el servicio cuando fueran causadas por la interferencia de inhibidores de señal.

Revisar continuamente el estado del arte en tecnologías para bloqueo y/o restricción de comunicaciones no autorizadas desde los centros penitenciarios

Otra buena práctica común es solicitar información actualizada a fabricantes y a la industria sobre soluciones que permitan restringir o bloquear las comunicaciones no autorizadas desde los penales. Por ejemplo, Chile ha realizado RFI en los últimos años antes de iniciar un nuevo proceso de licitación.

Otras prácticas desde el punto de vista técnico que vale la pena resaltar son:

- Exigir que los equipos para el bloqueo de señales cumplan con los límites de exposición a campos electromagnéticos.
- Restringir el bloqueo de señales a la frecuencia del enlace descendente, conforme lo establece el reglamento de México. Esta condición minimiza el riesgo de interferencia sobre las redes móviles, pero puede disminuir el nivel de eficiencia del sistema.

5 Alternativas técnicas de solución

El uso ilegal de equipos de comunicación desde centros penitenciarios para la realización de actos delictivos es una realidad que afecta la seguridad ciudadana y que demanda la toma de medidas por parte de las autoridades del gobierno. No obstante, el uso de soluciones tecnológicas basadas en la generación de señales de radio que interfieran las comunicaciones de las redes comerciales, sin hacer ningún tipo de reconocimiento sobre la identidad o localización del usuario que la origina o el destino de la llamada, han mostrado en la práctica significativos impactos en la población localizada en las zonas aledañas a los establecimientos de reclusión, desde limitar o restringir su acceso a los servicios de comunicaciones públicos autorizados, hasta impedir la comunicación de los mismos con líneas de emergencia o perturbar comunicaciones orientadas a la protección pública.

Bajo este escenario, resulta relevante analizar las soluciones técnicas disponibles en el mercado para evitar comunicaciones no autorizadas en centros penitenciarios, con el objetivo de evaluar potenciales alternativas para el escenario de América Latina.

5.1 Descripción de alternativas técnicas disponibles en el mercado

Considerando las experiencias analizadas en los países relevados y el portafolio de productos de algunas empresas líderes en la industria de fabricación de soluciones para restricción de llamadas como Harris, ShawnTech, CellAntenna, SESP, entre otros, es posible identificar cinco categorías básicas de soluciones tecnológicas para el control de comunicaciones no autorizadas desde centros penitenciarios: i) basadas en bloqueo con cierto nivel de selectividad mediante generación de señales de radiofrecuencia interferentes, ii) basadas en captura de las comunicaciones para controlar el acceso a las redes comerciales (Sistemas de Gestión de Acceso), iii) basadas en técnicas que emulan una celda celular, pero no permiten acceso a los servicios (celdas celulares dummy), iv) basadas en detección y v) soluciones híbridas que integran dos o más de las técnicas mencionadas.

A continuación, se detallan las características más relevantes de cada una de las categorías mencionadas

5.1.1 Dispositivos de bloqueo o inhibición de señal mediante generación de señales de radiofrecuencia

En esta categoría se enmarcan las soluciones basadas en los principios básicos de los bloqueadores o inhibidores de señal mencionados previamente, pero incorporando técnicas de análisis para permitir un cierto nivel de selectividad en el bloqueo y buscando reducir la interferencia efectiva generada en el sistema, especialmente, fuera de los límites del penal.

Por ejemplo, algunos dispositivos escanean el nivel de actividad de las señales de radiofrecuencia dentro de los centros penitenciarios y realizan el bloqueo (generan una señal interferente) sólo en el rango de frecuencias[9] y/o en la zona geográfica donde se genera dicha actividad[10].

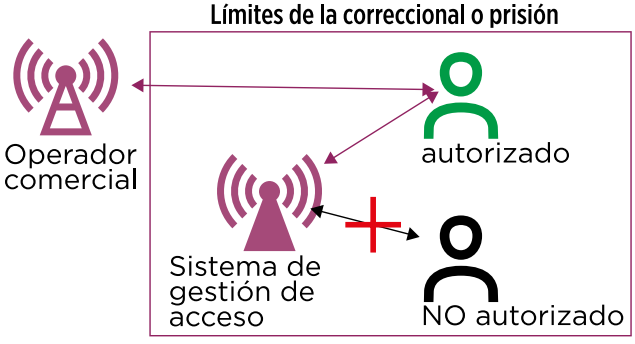
Adicionalmente, incorporan características como el uso de antenas directivas distribuidas, control centralizado y remoto, para reducir el riesgo de vandalismo, control de potencia ajustable para cada banda de frecuencias, bloqueo de todos los sistemas de comunicaciones que operen dentro de las bandas soportadas por el sistema, fácil escalabilidad para incorporar nuevas bandas de frecuencia a ser bloqueadas, etc.

Al igual que los bloqueadores de señal clásicos, la implementación de este tipo de solución requiere de un delicado estudio de ingeniería para que el área de cobertura este restringida, en la medida de lo posible, a los límites del centro penitenciario. Adicionalmente, resulta necesario un monitoreo permanente de la calidad de los servicios de comunicaciones fuera de los mismos, dado que, aunque las técnicas de bloqueo selectivo pueden ayudar a reducir la interferencia promedio generada en el sistema, el riesgo de afectar la prestación de servicios de comunicaciones autorizados fuera del penal sigue existiendo.

Finalmente, se resalta que, debido a que estas soluciones no hacen un análisis de la identidad del usuario que origina la comunicación, del destino de la llamada o de la información transmitida, existe un riesgo crítico de bloquear comunicaciones a líneas de emergencia y no aporta información relevante que pueda ayudar los trabajos de inteligencia de los organismos de seguridad pública.

5.1.2 Bloqueo de comunicaciones no autorizadas mediante de gestión de acceso

Este tipo de soluciones, conocidas como Sistema de Gestión de Acceso (MAS, por sus siglas en inglés), están basadas en una red privada de micro celdas que operan en las bandas de frecuencia autorizadas a los servicios de radiocomunicaciones y que se comporta como una extensión de las redes comerciales, con cobertura dentro del centro penitenciario, y que cuenta con una base de datos para determinar cuáles usuarios están autorizados a acceder a las redes comerciales de telecomunicaciones (Lista Blanca).



9. Jammers fabricados por la compañía PKI-Electronic cuenta con modelos como PKI-6170 o PKI-6200 que detecta actividad de señales para bloquear específicamente en el rango donde es detectado. (PKI-ELECTRONICS, 2017).
10. La compañía Bahia21 Corp. propuso el desarrollo de una técnica de análisis espacial que permitiría bloquear el servicio exclusivamente a terminales de comunicaciones localizados dentro del área no autorizada. El sistema sería reactivo, generando señales interferentes exclusivamente en la zona donde se detecta la actividad. Esta solución es comparable con las técnicas híbridas que involucran sistemas de detección y bloqueo de señales.

Estas soluciones analizan todas las comunicaciones (voz, SMS, datos) que se deseen realizar, permitiendo obtener la identificación del dispositivo inalámbrico que está intentado la comunicación, la compara con la base de datos de usuarios autorizados para permitir o negar el acceso a las redes de comunicaciones inalámbricas comerciales. De esta manera, se evitan bloqueos de las llamadas a las líneas de emergencia o de las comunicaciones autorizadas dentro del penal.

Una de las mayores ventajas de este tipo de soluciones es la captura de información que favorece los trabajos de inteligencia de los organismos de seguridad. Además de obtener información de la identidad del dispositivo dentro del penal que intenta comunicarse, es posible conocer detalles del destino de dicha comunicación.

Soluciones comerciales disponibles abarcan equipos que permiten soportar múltiples operadores, múltiples bandas de operación, y múltiples tecnologías inalámbricas (LTE, UMTS/HSPA, GSM, CDMA, iDEN)[11]. Así mismo, permite realizar una operación remota y centralizada de las soluciones, incorporar alarmas operativas y de actividad, generación automática de reportes y monitoreo de indicadores de desempeño.

Estas soluciones han sido ampliamente implementadas en correccionales de Estados Unidos y Reino Unido. La FCC, por ejemplo, autoriza directamente al establecimiento penitenciario o a un tercero para operar este tipo de sistemas bajo la figura de Operador de Sistema Privado de Radiocomunicaciones Móviles (PMRS, por sus siglas en inglés), para lo cual es necesario que se haga un acuerdo de cesión de espectro con los operadores móviles comerciales, de manera que lo habilite a hacer uso de dicho espectro licenciado dentro de los límites del centro penitenciario[12].

Dado que este tipo de soluciones permiten acceder a información relevante para las tareas de inteligencia de organismos de seguridad, la operación de los mismos implica un trabajo cercado con las entidades de seguridad y control penitenciario; por esta razón resulta una buena práctica que dicha tarea sea realizada directamente por la entidad responsable o por un tercero con la capacidad y experiencia en la gestión del sistema y soluciones de seguridad pública.
Por otro lado, es importante resaltar que la implementación de los MAS requiere de un importante trabajo cooperativo con los operadores comerciales para conocer la huella de cobertura de sus redes, las tecnologías y bandas de frecuencias disponibles en cada uno de los centros penitenciarios donde se desee instalar la solución y para la interconexión que permita el acceso de los usuarios autorizados o de las llamadas de emergencias a las redes públicas o comerciales de comunicaciones móviles.

Similar al caso de los bloqueadores, estas soluciones requieren un detallado estudio de ingeniería para restringir la cobertura, lo máximo posible, a los límites del centro de penitenciario. La generación de transmisiones que alcancen zonas fuera de dichos límites es un riesgo existente, aunque no ocasionaría una interferencia directa en los sistemas de comunicaciones ya que las señales transmitidas tienen el mismo comportamiento que el de las redes comerciales pero en caso de que un usuario sea "capturado" por el sistema y no se encuentre incluido en la lista de autorizados, sus comunicaciones serán bloqueadas, a excepción de llamadas que realice a líneas de emergencia. Para reducir este riesgo, el organismo regulador y el operador del sistema privado de gestión de acceso pueden establecer un procedimiento para registrar en la lista blanca a aquellas personas que frecuenten zonas cercanas a los límites penitenciarios y que no representen un riesgo en seguridad.

El costo de instalación de los Sistemas de Gestión de Espectro está asociado con el área a cubrir, la cantidad de redes inalámbricas comerciales y bandas de frecuencias que deben ser soportadas y las funcionalidades especiales que sean requeridas. Con base en los comentarios enviados por la industria a las consultas realizadas por la NTIA de Estados Unidos en el 2010[13], el alto costo de estas soluciones, comparadas con los bloqueadores de señal tradicionales, en uno de los aspectos que mayores retos representan para los establecimientos de reclusión[14].

Finalmente, es importante mencionar que la mayor limitante de estas soluciones está relacionada con el bloqueo de servicios de comunicaciones que operen sobre bandas no licenciadas, como las redes de WiFi.

5.1.3 Celdas celulares dummy

Las celdas celulares dummy no corresponden propiamente a una solución sino a una alternativa técnica que busca aprovechar algunos aspectos técnicos de la configuración de las estaciones móviles celulares, de manera que se "engaña" al dispositivo móvil del usuario.

11. Características de la solución CellDefender de Harris y de Fixed Management Access System de ShawnTech.
12. (FCC, 2017)
13. (NTIA, 2010)
14. Al respecto de los costos de instalación y operación de estas soluciones, una de las alternativas que se han postulado para solventarlos, en la contratación de un tercero que además de operar el Sistema de Gestión de Acceso, provea los servicios de comunicaciones a los funcionarios de los centros penitenciarios.

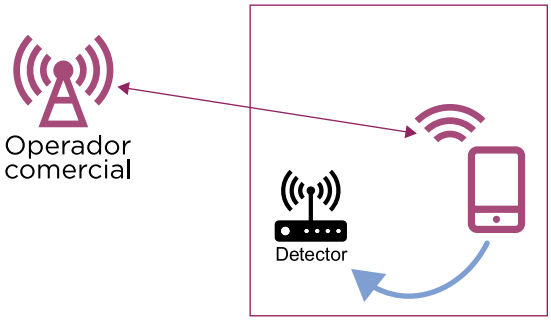
En términos prácticos, el terminal del usuario busca acceder a los servicios de comunicaciones a través de una radio base cuya configuración no le permite la transmisión de su información, por ejemplo, le pueden aparecer mensajes como "Red Ocupada" siempre o, sencillamente, no accede a ningún servicio. Para lograr esto, es necesario implementar una micro celda, por cada operador comercial, cada tecnología y cada banda de frecuencias, en el centro penitenciario con un sistema distribuido de antenas que permita asegurar óptica cobertura de la misma, reducir al máximo los niveles de señal de las estaciones base externas y configurarla apropiadamente para que no sea posible cursar ningún servicio a través de la misma.

Al igual que la solución previamente mencionada, esta alternativa también genera el riesgo de afectar zonas fuera de los límites del centro penitenciario, bloqueando el acceso a servicios de comunicaciones a usuarios autorizados. Así mismo, dadas las funciones del dispositivo móvil de escanear constantemente todas las estaciones base que puedan ofrecerle cobertura, es probable la existencia de zonas ciegas donde se pueda acceder a los servicios comerciales de comunicaciones a través de las estaciones base externas. Adicionalmente, no abarca el bloqueo de tecnologías como WiFi, trunking, satelital, entre otros, ni proporciona información que facilite los trabajos de inteligencia de los organismos de seguridad.

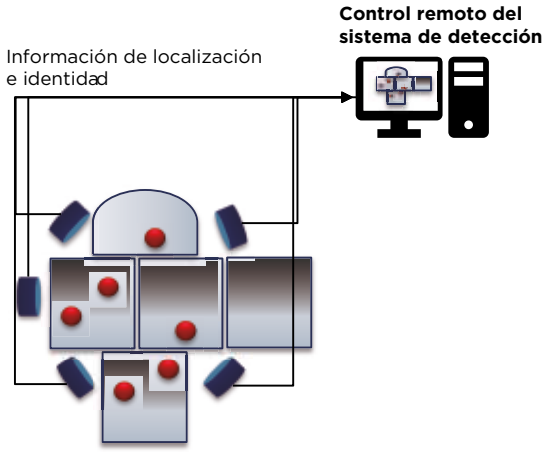
Finalmente, una de las mayores desventajas de esta alternativa, que la hace poco práctica de implementar, es la complejidad administrativa y operativa para coordinar el bloqueo de todos los operadores comerciales, en todas las bandas de frecuencia y en todas las tecnologías móviles disponible.

5.1.4 Técnicas basadas en Detección

Los sistemas de detección están basados en sensores que permiten localizar, rastrear e identificar dispositivos de comunicaciones inalámbricas dentro de los centros penitenciarios. Algunos detectores detectan la generación de señales de radiofrecuencia y determinan una localización aproximada para facilitar el proceso de incautación de los dispositivos, otros más avanzados, conocidos como IMSI Catcher permiten capturar información de identidad del dispositivo (i.e. identificación del dispositivo o IMEI, e identificación de la SIM CARD o IMSI), facilitando su inclusión en listas de bloqueo de operadores comerciales (similar a las listas negras usadas para reportar terminales robados) y estimar la localización del mismo para su incautación.



Los sistemas detectores pueden ser portátiles o fijos con control centralizado[15]. La precisión de localización de las soluciones fijas dependerá de la cantidad de sensores implementados, y puede alcanzar rangos inferiores a los 10mts. Estas soluciones son fácilmente escalables para permitir la detección de dispositivos operando en cualquier tecnología y banda de frecuencia de operación. Algunas soluciones permiten hacer un reporte automático de la información de identificación del dispositivo facilitando una inclusión más ágil en las listas negras de bloqueo de los operadores comerciales; adicionalmente, permiten configurar una lista de dispositivos autorizados los



cuales, a pesar de ser detectados, no son reportados por el sistema.

Dado que estos dispositivos no generan, necesariamente, transmisiones de señales de alta potencia, el riesgo de interferencia en los servicios de comunicaciones fuera de los límites del penal es significativamente más bajo que con las otras soluciones mencionadas previamente. No obstante, vale la pena destacar, que, dado que los sistemas de detección pueden capturar la información de todos los dispositivos dentro de su rango, en importante una adecuada ubicación de los sensores, de manera que no reporte la información de dispositivos localizados fuera de los límites del centro penitenciario.

15. Fabricantes como BLER, Phantom, Prison Jammers, entre otros, cuentan con soluciones de detección tipo IMSI Catcher con diferentes alcances y niveles de precisión.
16. (NTIA, 2010). Estos costos son referidos exclusivamente a los equipos, por los que los costos asociados con la ejecución de las labores de detección u operación del sistema no se encuentran incluidos.

El costo de este tipo de soluciones varía según el tipo y la complejidad de la misma. Considerando las respuestas de la industria a la consulta realizada por la NTIA en 2010, se estima que las soluciones portátiles pueden tener precios alrededor de los US$20,000, mientras que las soluciones fijas, cuyo precio depende fundamentalmente de la cantidad de sensores y funcionalidades, puedes oscilar entre los US$300,000 y US$600.000[16].

Uno de los principales reparos acerca de estos sistemas es el no bloqueo inmediato de las señales, lo que ocasiona que el delincuente lleve a cabo la comunicación no autorizada generando un potencial riesgo de seguridad. Por otro lado, existe riesgo que los sensores queden expuestos a la población carcelaria y sufran actos de vandalismo.
Uno de los principales reparos acerca de estos sistemas es el no bloqueo inmediato de las señales, lo que ocasiona que el delincuente lleve a cabo la comunicación no autorizada generando un potencial riesgo de seguridad. Por otro lado, existe riesgo que los sensores queden expuestos a la población carcelaria y sufran actos de vandalismo.

5.1.5 Soluciones híbridas

Las soluciones híbridas consisten en dispositivos que integran dos o más técnicas de las descritas previamente. Los equipos comerciales disponibles integran soluciones de detección y bloqueo selectivo a partir de la identificación y localización del usuario[17] o soluciones de detección y gestión de acceso[18] que proporciona captura de información de localización de usuarios, localización altamente precisa del dispositivo y control acceso mediante listas negras (usuarios no autorizados) y blancas (usuarios autorizados).

5.2 Descripción de alternativas técnicas disponibles en el mercado

Con el objetivo de analizar la conveniencia de las alternativas técnicas descritas previamente, se propone evaluar cada opción a partir de los factores listados a continuación.

5.2.1 Eficiencia en bloqueo de comunicaciones celulares no deseadas

Este factor hace referencia a la capacidad del sistema para bloquear la totalidad de las comunicaciones no autorizadas que se generen dentro del centro penitenciario, considerando las diferentes tecnologías inalámbricas disponibles (2G, 3G, 4G, WiFi, Satelital, Trunking, WiMax, UHF, VHF) y las zonas dentro del establecimiento donde resulta necesario hacer la restricción.

5.2.2 Impacto en servicios de comunicaciones fuera de los límites de los centros penitenciarios o en bandas adyacentes

Este factor corresponde al riesgo de interferir servicios de comunicaciones fuera de los límites del penal o en otras bandas de frecuencias. Así mismo, considera el riesgo de afectar el acceso a los servicios de comunicaciones por parte de usuarios autorizados.

5.2.3 Costo de implementación y operación

El costo de implementación y operación involucra tanto los potenciales costos asociados con los equipos y elementos que conforman la selección, como la complejidad de las actividades para la operación del sistema y su vulnerabilidad a sufrir actos de manipulación y vandalismos que impacten en costos de reparación y mecanismos de protección.

5.2.4 Apoyo a la seguridad pública

El factor asociado con la seguridad corresponde a la capacidad del sistema para proporcionar información que facilite el trabajo de las autoridades de inteligencia y seguridad pública del país.

La siguiente tabla presenta el análisis cualitativo y comparativo de las alternativas descritas en la sección 4.1 con base en los factores mencionados.

16. (NTIA, 2010). Estos costos son referidos exclusivamente a los equipos, por los que los costos asociados con la ejecución de las labores de detección u operación del sistema no se encuentran incluidos.
17. Algunas soluciones son ofrecidas por empresas como PKI (PKI-6210), Phantom Technologies (IMSI Catcher & selective jammer) y BLER.
18. Solución de CellAntenna CA-STINGER 5G.

FIGURA 14

Análisis comparativos de alternativas

Muy Satisfactorio · Bueno · Regular · Insatisfecho · Deficiente

	Bloqueador de señal selectivo	Gestión de Acceso selec	Celdas Dummy selec	Sistemas de Detección	Híbridos: Detección & Jammer	Híbridos: Detección & Gestión de acceso
Eficiencia en bloqueo	• Escalable a todas las tecnologías y bandas • Riesgo de zonas ciegas	• No abarca tecnología WI-FI • Riesgo de zonas ciegas	• Sólo aplica a redes móviles celulares • Riesgo de zonas ciegas	No aplica Su principio no es bloqueo de comunicaciones	• Escalable a todas las tecnologías y bandas • Riesgo de zonas ciegas	• No abarca tecnología WI-FI • Riesgo de zonas ciegas
Impacto en comunicación es autorizadas	• Riesgo de interferencia perjudicial fuera de límites del penal • Bloqueo de llamadas de emergencia • Riesgo de impacto en otras bandas	• No genera señales interferentes • Riesgo de "captura" de usuario fuera del penal • No bloquea llamadas de emergencia	• No genera señales interferentes • Riesgo de bloqueo de usuario fuera del penal • Bloquea llamadas de emergencia	• No genera interferencia • Riesgo de reporte de usuarios fuera del penal	• Riesgo de interferencia fuera del penal • Bajo riesgo de bloquea llamadas de usuarios autorizados	• No genera señales interferentes • Riesgo de "captura" de usuarios fuera del penal • No bloquea llamadas de emergencia
Costos y complejidad	• Depende de tamaño del penal • Riesgo de vandalismo	• Alto costo de la solución. Depende del área, operadores, bandas y funcionalidades	• Alta complejidad de coordinación. Requiere múltiples soluciones para cada operador, banda y tecnologías	• Depende de tipo y complejidad • Riesgo de vandalismo	• Depende de tipo y complejidad • Riesgo de vandalismo	• Alto costo de la solución
Apoyo a seguridad pública	• No proporciona información	• Información de identificación de usuario, tipo de servicio y destinatario	• Información de identificación de usuario y localización	• No proporciona información	• Información de identificación de usuario y localización	• Información de identificación de usuario, servicio destinatario y localización

Fuente: BNMC

Con base en la anterior tabla y las buenas prácticas identificadas en las experiencias relevadas, se presenta en la siguiente sección las principales conclusiones y recomendaciones del estudio.

5.3 Conclusiones y recomendaciones

Con la ejecución de actos delictivos como amenazas, extorsiones, secuestros, asesinatos, escapes, etc. por parte de criminales dentro de centros penitenciaros a través de dispositivos de comunicaciones inalámbricos es una realidad que afecta la seguridad de la población y que requiere de trabajos coordinados y cooperativos entre entidades de protección pública, directores de establecimiento de reclusión, autoridades de gobierno para el sector de telecomunicaciones y el sector privado.

Así mismo, se debe tener presente que el acceso de los ciudadanos a los servicios de comunicaciones es un objetivo primordial del Estado y es el fundamento del principio de operación de los sistemas de radiocomunicaciones.

Tomando como base lo expuesto, se presentan a continuación las conclusiones más relevantes del estudio y las recomendaciones del consultor.

- La situación general que afrontan los países de la región en relación con esta problemática presenta altas similitudes. Se han implementando soluciones de bloqueo en algunas cárceles de varios países de América Latina con resultados poco satisfactorios. En prácticamente todos los casos se han presentado interferencias perjudiciales fuera de los límites de los centros penitenciarios, los equipos se han visto afectados por vandalismo y la eficiencia de los mismos no ha sido la esperada; incluso ha sido necesario suspender o reformular contratos con proveedores de soluciones tipo jammer. Por otro lado, la regulación califica como ilegal el uso no autorizado de bloqueadores de señal que interfieran con los servicios de comunicaciones autorizados.

- Con base en las leyes y regulación de los países relevados, se encuentra que, en el marco de las responsabilidades de cada institución y las normas aplicables a los sistemas penitenciarios, la implementación de soluciones de bloqueo de señal es responsabilidad de las direcciones centros de reclusión o penitenciarios. Las autoridades de telecomunicaciones tienen un rol de asesoría e instrumentación de regulación aplicable al sector, mientras que los operadores de servicios de comunicaciones cumplen un rol de cooperación y asesoría.

- La problemática debe ser analizada de manera integral, desde los procesos de control para restringir el acceso de dispositivos de comunicaciones a los centros penitenciarios, el bloqueo o restricción de las comunicaciones no deseadas, la detección e incautación de los terminales de contrabando que hayan ingresado y el análisis de información de inteligencia para hacer seguimiento a los casos, identificar patrones de comportamiento y evitar reincidencias.

- Las alternativas técnicas disponibles en el mercado para la restricción de comunicaciones no autorizadas desde los centros penitenciarios no tienen un desempeño totalmente satisfactorio en todos los factores analizados. Por esta razón, se hace necesario analizar cada centro penitenciario de manera particular e identificar la solución que mejor se ajusta a sus requerimientos y prioridades. Así mismo, es recomendable adoptar las buenas prácticas de instalación de sistemas de radiocomunicaciones sugeridas por la industria y mantener un monitoreo permanente de los impactos que se generen.

En este sentido, es recomendable que las soluciones de inhibición de señal tipo jammer se restrinjan lo máximo posible a zonas rurales o alejadas de población que pueda ser afectada por interferencia en los servicios. En zonas urbanas es preferible optar por soluciones que incorporen mayor inteligencia en el análisis de las señales, como los sistemas de gestión de acceso o detección, minimizando el impacto en las áreas aledañas.

6 Fuentes bibliográficas

ANATEL (2002). Resolución 306. Brasil.

ANATEL (2002). Resolución 308. Brasil.

DIARIO OFICIAL DE LA FEDERACIÓN (30/09/2012). LINEAMIENTOS DE COLABORACION ENTRE AUTORIDADES PENITENCIARIAS Y LOS CONCESIONARIOS DE SERVICIOS DE TELECOMUNICACIONES Y BASES TECNICAS PARA LA INSTALACION Y OPERACION DE SISTEMAS DE INHIBICION. Obtenido de http://www.dof.gob.mx/nota_detalle.php?codigo=5266201&fecha=03/09/2012

DIARIO OFICIAL DE LA FEDERACIÓN (01 /08/ 2016). DISPOSICIÓN TÉCNICA IFT-010-2016. Obtenido de http://dof.gob.mx/nota_detalle.php?codigo=5446400&fecha=01/08/2016

DIARIO OFICINAL DE LA FEDERACIÓN (14 /07 2014). LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN Obtenido de http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

ECONOMÍA Y NEGOCIOS (27/08/2016). Gendarmería realiza consulta por tecnología disponible para inhibir celulares en cárceles. Obtenido de http://www.economiaynegocios.cl/noticias/noticias.asp?id=284125

ESTADO MAYOR. (22 /09/ 2013). Desbloquean reos señal de celulares. Obtenido de http://www.estadomayor.mx/33404

FCC. (May 2017). Promoting Technological Solutions To Combat Contraband Wireless Device Use in Correctional Facilities. Obtenido de https://www.federalregister.gov/documents/2017/05/18/2017-09885/promoting-technological-solutions-to-combat-contraband-wireless-device-use-in-correctional

FCC (2017). Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities . Estados Unidos.

FEDERACIÓN, D. O. (30 /04/ 2014). PROGRAMA NACIONAL DE SEGURIDAD PÚBLICA 2014-2018. Obtenido de http://www.dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014

GLOBO - EPOCA NEGOCIOS. (23 /01/ 2017). Só 23 prisões têm bloqueador de celular em São Paulo. Obtenido de http://epocanegocios.globo.com/Brasil/noticia/2017/01/so-23-prisoes-tem-bloqueador-de-celular-em-sao-paulo.html

INPEC. (19 /07/ 2012). Directiva Transitoria 022 de 2012 para Prevenir y Controlar la Extorsión Generada desde los Establecimientos de Reclusión. Obtenido de http://www.inpec.gov.co/portal/page/portal/INPEC_CONTENIDO/NORMATIVIDAD_INTRANET/DIRECTIVAS_PORLET/DIRECTIVA22.pdf

INPEC. (11 /02/ 2016). SISTEMA DE BLOQUEADORES E INHIBIDORES DE SEÑAL. Obtenido de http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/Estad%EDsticas/Estadisticas/Presentaciones%20-%20foros%20encuentros%20INPEC/PRESENTACI%D3N%20BLOQUEADORES%20E%20INHIBIDORES%20DE%20SE%D1AL%20(1).pdf

LA JORNADA. (25 /03/ 2015). Secuestros desde los penales. Obtenido de http://www.jornada.unam.mx/2015/03/25/politica/008n1pol

NTIA. (2010). CONTRABAND CELL PHONES IN PRISONS. USA.

PKI-ELECTRONICS. (2017). Intelligent Cellular Jammer with Detector. Obtenido de http://www.pki-electronic.com/products/jamming-systems/intelligent-cellular-jammer-with-detector/

SENADO DE LA REPÚBLICA. (14 /03/ 2017). PROPOSICIÓN CON PUNTO DE ACUERDO. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2017/03/asun_3507338_20170323_1490203162.pdf

A

Anexo 1
Casos de estudio

En las siguientes imágenes se presenta una infografía que resume los aspectos más relevantes de los resultados observados luego de la instalación de bloqueadores de señal en dos cárceles de Colombia. Una de ellas ubicada en una zona Suburbana conocida como Picaleña cerca de la ciudad e Ibagué, y la otra en Bogota.

El análisis es realizado a partir de mediciones y reporte estadístico realizado por operadores móviles en Colombia

Caso de Estudio I
Cárcel Picaleña (Ibagué - Colombia) 1/2

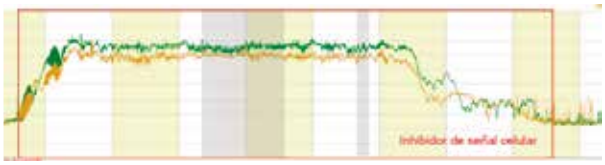
Locación Semi Urbana
Área aprox. 24 hectáreas

Instalación de bloqueador como parte del "Plan Cerrojo" del INPEC en 2013

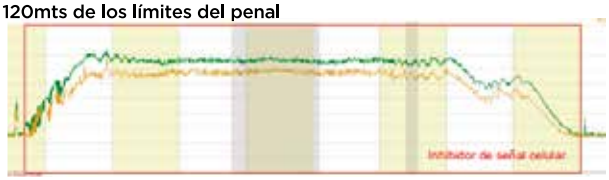
Pruebas realizada por INPEC ⟶ 100% llamadas bloqueadas dentro de penal

Pruebas realizada por operador (20 llamadas) ⟶Todas las llamadas bloqueados – No se identifican señales de operadores 3G/4G

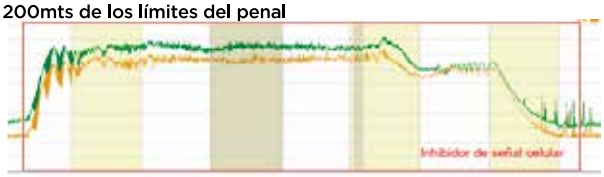
A 50mts de los límites del penal



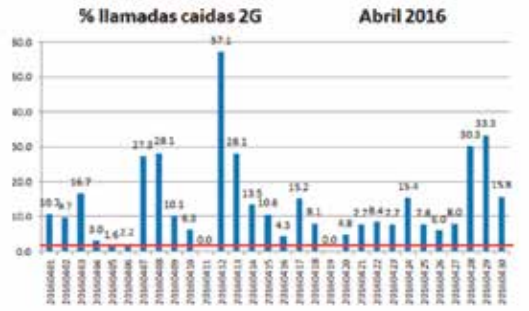
A 120mts de los límites del penal



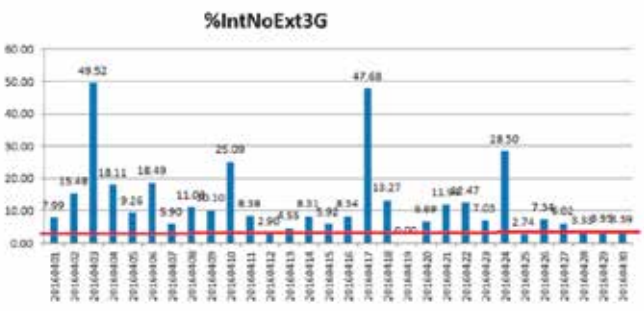
A 200mts de los límites del penal



Los altos niveles de interferencia afectan drásticamente la calidad de servicio de los usuarios



El porcentaje de llamadas caídas pasa de un 2% promedio a más del 20% (alcanza valores del 50% en alto tráfico)



El porcentaje de llamadas bloqueadas pasa de un 3% promedio a más del 11% (alcanza valores del 47% en alto tráfico)

A

8. (INPEC, 2012)

Caso de Estudio II

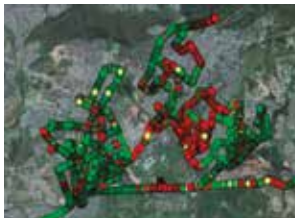
Cárcel Picaleña (Ibagué - Colombia) 2/2

Locación Urbana
Área aprox. 40 hectáreas

Instalación de bloqueador como parte del "Plan Cerrojo" del INPEC en 2013

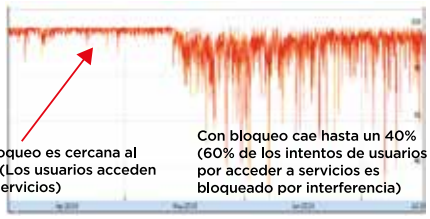
Pruebas realizada por INPEC ⟶ 50% llamadas bloqueadas dentro de penal

Pruebas realizada por operador (20 llamadas) ⟶Todas las llamadas bloqueados – No se identifican señales de operadores 3G/4G

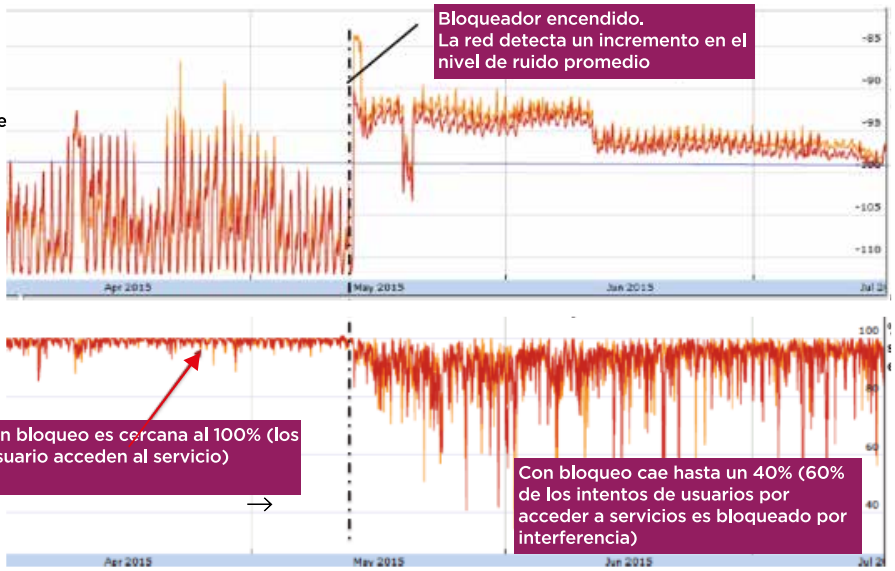


La relación señal a interferencia muestra niveles deficientes alrededor del penal

Porcentaje de acceso a servicios de comunicaciones



El bloqueo en las frecuencias del enlace ascendente genera un mayor impacto en el desempeño global de la estación base afectada



Intensidad de la señal de ruido medido por una estación base que da cobertura a zona afectada (dBm)

% de éxito en acceso a servicios de comunicaciones

Anexo 2
Marco regulatorio sobre uso de bloqueadores de señal

I. México

La práctica de delitos como extorsión, amenaza o fraudes a través de llamadas telefónicas desde el interior de los Centros de Reinserción Social de México es un asunto prioritario para las instituciones de seguridad pública en el país. Algunas cifras reportadas por procuradurías y fiscalías estatales arrojaron que la cantidad de extorsiones y secuestros supera los 400 casos por mes[19] y los considerandos de algunas de las normas expedidas por el Gobierno reconocen que *"desde el interior de los centros penitenciarios y en coordinación con bandas delictivas en libertad se llevan a cabo delitos de extorsión con amenazas de secuestro o de muerte, y fraudes telefónicos contra la sociedad (...)"* así como acciones de intimidación contra familiares de internos, testigos o personal penitenciario, e incluso registros fotográficos para ejecutar evasiones o motines[20].

En este sentido, la Ley General del Sistema de Seguridad Pública de los Estados Mexicanos, en su edición del 2009, estableció en el Artículo 149 que *"el Consejo Nacional establecerá los casos, condiciones y requisitos necesarios para el bloqueo de las señales de telefonía celular en las instalaciones de carácter estratégico para los fines de seguridad pública"*, bajo la responsabilidad de las Instituciones de Seguridad Pública que conforman el Consejo.

Esta reglamentación permitió que, en el 2011, el Gobierno de la Ciudad de México contratara a la empresa Software DSI S.A. de C.V, para la instalación y operación de 155 dispositivos bloqueadores de señal en 6 penales de México con un costo aproximado de US$1.9 millones[21]. No obstante, esta estrategia no generó los efectos deseados dado que la efectividad de estos sistemas en el bloqueo de llamadas fue bajo y se sospecha la posibilidad que reclusos y custodios de los penales hayan manipulado los dispositivos[22]. El contrato fue suspendido en el año 2013.

Así mismo, en 2012 se expidió una reglamentación con los *"lineamientos de colaboración entre autoridades penitenciarias y los concesionarios de servicios de telecomunicaciones, y bases técnicas para la instalación y operación de sistemas de inhibición"* que establece obligaciones para todas las instituciones que administren centro de readaptación social, establecimientos penitenciarios o centros de internamiento para menores y para los concesionarios de servicios de telecomunicaciones con el objetivo de cancelar o anular *"de manera permanente las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen dentro de los perímetros de los centros de readaptación social, establecimientos penitenciarios (...), sin que excedan en ningún caso veinte metros fuera de las instalaciones (...)"* [23].

Adicionalmente, la norma establece que todos los centros mencionados deban contar con equipos para el bloqueo de manera permanente de las señales de telefonía celular y establecer los mecanismos para prevenir y resolver afectaciones indebidas en los usuarios del servicio celular. Así mismo, define los roles de cada una de las instituciones involucradas, las características técnicas a cumplir por parte de estos dispositivos y el monitoreo de los mismos.

La siguiente figura resume las obligaciones de cada una de las partes.

A

19. Durante enero y febrero de 2015 se reportaron 826 denuncias por casos de extorsiones y secuestros. (LA JORNADA, 2015)
20. Considerando de la Reglamentación sobre LINEAMIENTOS DE COLABORACIÓN ENTRE AUTORIDADES PENITENCIARIAS Y LOS CONCESIONARIOS DE SERVICIOS DE TELECOMUNICACIONES Y BASES TÉCNICAS PARA LA INSTALACIÓN Y OPERACIÓN DE SISTEMAS DE INHIBICIÓN. De la Conferencia Nacional del Sistema Penitenciario de México. (DIARIO OFICIAL DE LA FEDERACIÓN, 2012)
21. Nota de prensa (ESTADO MAYOR, 2013). Los 155 dispositivos fueron comprados por un monto de $24.79 millones de pesos mexicanos (Aproximadamente US$1.9 millones de dólares considerando una tasa de cambio de $13 pesos mexicanos por cada dólar americano).
22. Consideraciones expuestas en la PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE SE EXHORTA RESPETUOSAMENTE A LA CONFERENCIA NACIONAL DEL SISTEMA PENITENCIARIO Y AL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA, QUE EN OBSERVANCIA DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA, SE CUMPLA CABALMENTE LO ENUNCIADO EN EL ARTÍCULO 31 DE LA MENCIONADA LEY del Senado de la República de Marzo de 2017. (SENADO DE LA REPÚBLICA, 2017).
23. Artículo 2 (DIARIO OFICIAL DE LA FEDERACIÓN, 2012)

FIGURA 15

Obligaciones de las partes involucradas - México

Secretaría de seguridad pública (Subsecretaría del sistema Penitenciario Federal) Supervisar cumplimiento de acuerdo

- **Conferencia Nacional del Sistema Penitenciario**
  Coordinación entre poderes ejecutivos y D.F., promover acuerdos, buscar presupuesto
- **Organismo Administrativo Desconcentrado Prevención y Readaptación Social (Nivel Federal)**
  Proveer y asegurar instalación y operación de bloqueadores
  Direcciones Generales en estados & Distrito Federal
  Proveer y garantizar instalación y operación de bloqueadores.
  Supervisar funcionamiento
  Direcciones Centros Penitenciarios
  Acondicionar área para instalación. Vigilancia y reportes
- **Centros de operación, monitoreo y supervisión remota**
  Supervisar instalación. Operar, monitorear y mantener funcionalidad de bloqueadores

Secretaría de Comunicaciones y Transporte
Brindar asesoría

- **Instituto Federal de Telecomunicaciones (Antes COFETEL)**
  Apoyar a autoridades penitenciarias, coordinación con concesionarios, monitoreo de calidad de servicio
- **Dirección General de Desarrollo Tecnológico**
  Proveer y asegurar instalación y operación de bloqueadores
  Direcciones Generales en estados & Distrito Federal
  Proveer y garantizar instalación y operación de bloqueadores.
  Supervisar funcionamiento
  Direcciones Centros Penitenciarios
  Acondicionar área para instalación. Vigilancia y reportes
- **Centros de operación, monitoreo y supervisión remota**
  Supervisar instalación. Operar, monitorear y mantener funcionalidad de bloqueadores

Fuente: (DIARIO OFICIAL DE LA FEDERACIÓN, 2012)

Con el objetivo de reforzar este objetivo de gobierno, el Programa Nacional de Seguridad Pública 2014-2018 incluye dentro de sus estrategias la adopción de acciones para *"romper el vínculo de los internos con organizaciones delictivas al interior y exterior de los centros penitenciarios"*[24], involucrando como primera línea de acción la implementación de medidas efectivas para el bloqueo de señales celulares. Adicionalmente, se realiza en Junio de 2017 una reforma a la Ley General del Sistema de Seguridad Pública, adicionando las siguientes obligaciones al respecto del uso de bloqueadores de señal:

Artículo 7: (...) *las Instituciones de Seguridad Pública de la Federación, el Distrito Federal, los Estados y los Municipios, en el ámbito de su competencia y en los términos de esta Ley, deberán coordinarse para:*

(...)

XII. Garantizar que ***todos los centros*** *de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación,* ***cuenten con equipos que permitan bloquear o anular de manera permanente las señales de telefonía celular,*** *de radiocomunicación, o de transmisión de datos o imagen dentro del perímetro de los mismos;*

Artículo 31: (...) *funciones de la Conferencia Nacional del Sistema Penitenciario:*

(...)

VIII. Formular los lineamientos para que la federación y las entidades federativas cumplan, en el ámbito de sus competencias, con la obligación de ***adquirir, instalar y mantener en operación equipos que permitan bloquear o anular de manera permanente las señales de telefonía celular****, de radiocomunicación, o de transmisión de voz, datos o imagen en el perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación.*

Dichos equipos ***serán operados por autoridades distintas a las de los establecimientos penitenciarios en centros remotos****, contarán con sistemas automáticos que envíen señales de alarma ante cualquier interrupción en su funcionalidad y serán monitoreados por el Sistema Nacional de Seguridad Pública, con la colaboración de los concesionarios de redes públicas de telecomunicaciones.*

El bloqueo de señales a que se refiere este artículo se hará sobre ***todas las bandas de frecuencia*** *que se utilicen para la recepción en los equipos terminales de comunicación móvil y* ***en ningún caso excederá de veinte metros fuera de las instalaciones*** *de los centros o establecimientos a fin de garantizar la continuidad y seguridad de los servicios a los usuarios externos.*

Por otro lado, la Ley Federal de Telecomunicaciones de México, establece en su artículo 190 que los concesionarios de telecomunicaciones tienen como obligación *"colaborar con las autoridades competentes para que en el ámbito técnico operativo se cancelen o anulen de manera permanente las señales de telefonía*

24. Estrategia 6.3. del Programa Nacional de Seguridad Pública 2014-2018 de los Estados Unidos Mexicanos (FEDERACIÓN, 2014)

A

celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios(...)

En la colaboración que realicen los concesionarios se deberán considerar los elementos técnicos de reemplazo, mantenimiento y servicio. (...) están obligados a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular (...)"[25].

Conforme lo expuesto por la Ley y considerando que en noviembre de 2015 el Instituto Federal de Telecomunicaciones expidió los Lineamientos de Colaboración en Materia de Seguridad y Justicia, se publica en agosto de 2016 la Disposición Técnica IFT-10-2016 sobre las especificaciones y requerimientos de los equipos de bloqueo de señales de telefonía celular en establecimientos penitenciarios, entre otros.
La mencionada disposición establece, entre otros aspectos, lo siguiente:

- El uso de equipos de bloqueo de señales se limita exclusivamente dentro del perímetro de los centros de readaptación social. Cualquier uso diferente, no está permitido.
- El equipo debe contar con potencia ajustable de manera independiente para cada banda de frecuencias.
- No se permite el uso de amplificadores de potencia externos a los equipos de bloqueo.
- El equipo no puede contar con controles externos para evitar manipulaciones fraudulentas.
- El equipo solo puede bloquear las frecuencias correspondientes al enlace descendente (desde la red al terminal móvil).
- No se permite bloquear la banda de 380 a 399.99 MHz, usada para aplicaciones de seguridad pública.
- Cumplir con los límites de exposición a campos electromagnéticos.
- Los equipos deberán ser homologados en laboratorios especializados.

II. Colombia

El secuestro y la extorsión son dos de los delitos de mayor preocupación para las instituciones de seguridad pública en Colombia. Por esta razón, en 2011 se expidió el Decreto 4768 de 2011 *"por medio del cual se adoptan medidas para restringir la utilización de dispositivos de telecomunicaciones en los establecimientos penitenciarios y carcelarios (...)"*, el cual reconoce que los internos de los centros penitenciarios no pueden portar dispositivos de comunicación privados[26] y que se identificó, en su momento, un significativo incremento de amenazas, estafas, extorsiones y otros delitos desde el interior de penales mediante el uso de dispositivos de comunicaciones.

El mencionado Decreto establece un marco regulatorio en los siguientes tres aspectos:

1. Habilita al Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio TIC) a autorizar al Instituto Nacional Penitenciario y Carcelario (INPEC) para "inhibir o bloquear las señales de transmisión, recepción y control de los proveedores de redes y servicios de telecomunicaciones móviles (...)" en aquellos centros penitenciarios donde se tengan motivos claros que permitan concluir que desde el interior se están cometiendo delitos a través de dispositivos de comunicaciones.

   El INPEC es responsable de elevar la solicitud al Ministerio TIC indicando las condiciones técnicas aplicables a la medida y de operar los equipos de bloqueo de señal evitando su impacto las áreas exteriores. Esto último será vigilado por la Agencia Nacional del Espectro.

2. El Ministerio TIC, por solicitud técnicamente justificada por parte del INPEC, podrá ordenar a los Proveedores de redes y servicios de telecomunicaciones la eliminación o restricción de sus señales de transmisión, recepción y control en los centros penitenciarios identificados.
   Los operadores de telecomunicaciones son los responsables de operar la infraestructura involucrada con la restricción de sus señales evitando afectar las áreas exteriores del centro penitenciario. Esto último será vigilado por el Ministerio TIC.

A

25. (DIARIO OFICIAL DE LA FEDERACIÓN, 2014)
26. Artículo 111 de la Ley 65 de 1993
27. Directiva Transitoria 022 de 2012 para Prevenir y Controlar la Extorsión Generada desde los Establecimientos de Reclusión. (INPEC, 2012)
28. Incluye los centros de reclusión identificados en el Plan Cerrojo (11 centros), Orion (1 centro) e Institucional (5 centros).

3. No se aplica el cumplimiento de indicadores de calidad de servicio en los centros penitenciarios afectados por las medidas mencionadas.

   Bajo este marco, el INPEC establece un plan de acción enfocado en los siguientes ejes27:

- Gestionar la asignación de bloqueadores o inhibidores de señal de telefonía móvil. Para ello se identificaron un total de 16 centros de reclusión[28]. Se realizaron mesas de trabajo con los operadores y entidades de gobierno involucradas a fin de realizar ajustes de cobertura que minimizaran los impactos fuera de los penales.

- Revisar los procedimientos para el control de ingreso y decomiso de Terminales Móviles al interior de los penales. En los últimos años el INPEC ha trabajado en conjunto con la Dirección Antisecuestro y Antiextorsión de la Policía Nacional para hacer uso de equipos tácticos que permita la identificación de los números de SIM (IMSI) y códigos de los dispositivos móviles (IMEI), de manera que los mismos puedan ser bloqueados por parte de los operadores móviles.
- Hacer seguimiento a reclusos vinculados con delitos de extorsión, contemplando incluso el traslado de reclusos a centros penitenciarios sujetos a la medida de bloqueo de señales.

- Cooperar con entidades nacionales y territoriales en la prevención del delito
  El INPEC presentó en 2016 algunos resultados de la implementación del plan de trabajo propuesto.

La siguiente figura presenta los puntos más relevantes.

FIGURA 16

Plan de Acción INPEC - Colombia

Fuente: BNMC

De la gráfica anterior, es importante destacar que con base en las pruebas realizadas dentro de cada uno de los 15 centros penitenciarios en los que se habían instalado bloqueadores al cierre de 2015, se encontró que en 4 de los mismos la efectividad del bloqueo de llamadas fue menor al 85%, en 5 estuvo entre el 85% y 95% y en 7 fue superior al 95%. Así mismo, en más del 70% de los casos se presentaron problemas con manipulación clandestina de los equipos o vandalismo, y que el impacto en la calidad de los servicios de comunicaciones en las zonas exteriores a los penales ha sido significativo.

Por otro lado, con base en el Decreto 4768 de 2011, el Ministerio TIC expidió en agosto de 2013 la Resolución 2774 *"por la cual se reglamenta el uso de inhibidores, bloqueadores y amplificadores de señales radioeléctricas"*, estableciendo los siguientes aspectos sobre el uso de bloqueadores.

a. El uso de bloqueadores sin la debida autorización y en los casos mencionados en la Resolución 2774 de 2013 constituye un uso clandestino del espectro, aplicándole las sanciones y procedimientos establecidos en la Ley TIC de Colombia.
b. Sólo se pueden solicitar autorizaciones las entidades públicas o del sector financiero por razones de seguridad o de interés general para la instalación y operación de bloqueadores en ubicaciones fijas confinadas. Para ello se debe presentar una solicitud con las condiciones técnicas de los equipos, diseño y mapa de cobertura dentro del recinto y 500mts alrededor. Los equipos deben cumplir con los límites de exposición a campos electromagnéticos.

c. En caso de afectación en exteriores, el equipo bloqueador de señal deberá ser apagado hasta que se corrija el problema.

d. Los organismos de seguridad del Estado Colombiano pueden hacer uso de bloqueadores fijos o móviles en ubicaciones fijas confinadas o abiertas exclusivamente en los casos relacionados con la seguridad pública sin querir permiso del Ministerio TIC.

III. Brasil

En 2002, la Agencia Nacional de Telecomunicaciones de Brasil (ANATEL) expide dos resoluciones para reglamentar el uso de dispositivos bloqueadores de señal en el país. La primera corresponde a la Resolución 306 de 2002 que aprueba la *"Norma para la certificación y homologación de bloqueadores de señales de radiocomunicaciones"*, definiendo, entre otras, las siguientes características a ser cumplidas por parte de este tipo de dispositivos.

- Deben bloquear las bandas de frecuencias correspondientes a los servicios de telecomunicaciones.
- No puede bloquear señales de telecomunicaciones fuera de los límites establecidos.
- Debe permitir el bloqueo de señales de cualquier tecnología usada para la provisión de servicios de telecomunicaciones.
- Contar con control de potencia para cada una de las bandas de frecuencias.
- Cumplir con los límites de exposición a campos electromagnéticos.

Por otra parte, la Resolución 308 de 2002 regula el uso de bloqueadores de señales de radiocomunicaciones, autorizando su uso en centros penitenciarios previa solicitud a la ANATEL, estableciendo un proyecto técnico claro que identifique, entre otros aspectos, las bandas de frecuencia que requiere ser bloqueadas y manteniendo una coordinación y contacto permanente con los operadores de servicios de telecomunicaciones y la ANATEL.

La mencionada reglamentación define algunas obligaciones para cada una de las partes involucradas. A continuación, se mencionan los aspectos más relevantes.

- Los operadores de servicios de telecomunicaciones tienen la obligación de mantener en estricta confidencialidad toda la información que se les proporcione relacionada con los equipos de bloqueo de señal. Así mismo, deberán notificar a las partes interesadas sobre cambios que realicen en sus redes y que afecten la huella de cobertura en la zona donde se deseas bloquear la señal, al igual que informar sobre perturbaciones en el servicio en las zonas fuera de los límites establecidos.
- La ANATEL deberá atender los requerimientos de confidencialidad de la información, fiscalizar el cumplimiento de la reglamentación y apoyar al Departamento Penitenciario Nacional (DEPEN) con información requerida para el diseño del proyecto técnico de la solución de bloqueo.
- Los usuarios autorizados para la instalación y operación de equipos bloqueadores de señales deberán contar con un proyecto técnico detallado, mantener contacto y coordinación con los operadores de telecomunicaciones y ANATEL, usar equipos certificados conforme la regulación vigente e instalarlos de manera que queden protegidos de la población carcelaria, no afectar el servicio de telecomunicaciones en la zonas fuera de los límites del penal (para lo cual deberá coordinar con los operadores la validación de impactos en puntos de verificación), entre otras.

Conforme algunas notas de prensa, se estima que en São Paulo hay cerca de 23 penales que cuentas con dispositivos de bloqueo de señales, lo cual representa el 14% del total de centros penitenciarios paulistas[29]. No obstante, en los penales que cuentan con sistema de bloqueo aún se realizan incautaciones de terminales móviles, lo que permite concluir que la eficiencia de la solución no es del 100%.

Por otro lado, la afectación de los servicios de comunicaciones fuera de los límites de los penales es un hecho conocido por las autoridades y la opinión pública. Por esta razón, se planteó la posibilidad de trasladar a los operadores de servicios de telecomunicaciones la obligación de instalar y operar estos sistemas de bloqueo de señales. No obstante, considerando que la Seguridad Pública es un deber del Estado y los procedimiento y responsabilidades definidas en las Leyes de Ejecuciones Penales de Brasil, el Supremo Tribunal Federal en decisión del 03 de Agosto de 2016 encontró inconstitucional la mencionada propuesta.

29. Se estima una inversión de $ 31 millones de Reales. (GLOBO - EPOCA NEGOCIOS, 2017)
30. http://www.economiaynegocios.cl/noticias/noticias.asp?id=284125

IV. Chile

Al igual que otros países de América Latina, en Chile el uso de terminales para comunicaciones móviles dentro de las cárceles para cometer actos delictivos es un asunto crítico y prioritario en las agendas de los organismos de seguridad. Se estima que entre 2011 y 2016 se incautaron cerca de 156,000 terminales dentro de los centros penitenciarios chilenos[30].

La regulación y control para la instalación y operación de dispositivos bloqueadores de señal en centros penitenciarios es realizada por la Gendarmería de Chile, con asesoría de la Subsecretaría de Telecomunicaciones (SUBTEL) en asuntos relacionados con las capacidades instrumentales y reglamentarias.

En 2012 se llevó a cabo un concurso público para contratar la instalación de sistemas de bloqueo de señal celular en 6 centros penitenciarios del país. Dicho proceso requería que la empresa ganadora implementara una solución que i) ofreciera una restricción total de las comunicaciones ilícitas que se generaran dentro de los penales, asegurando la ii) NO interferencia sobre las comunicaciones internas de la Gendarmería y la iii) NO afectación de los servicios de comunicaciones fuera de los límites de cada penal.

Dicho concurso fue ganado por Telefónica Móviles, no obstante, los resultados de la solución no fueron satisfactorios dado que no fue posible cumplir con los tres objetivos mencionados previamente. Por esta razón fue necesario suspender el contrato.

En los últimos años, Gendarmería de Chile ha venido adelantado solicitudes de información RFI a la industria con el objetivo de conocer posibles soluciones para el bloqueo de señales de comunicaciones inalámbricas dentro de penales, a fin de adelantar un nuevo concurso público en el corto plazo.

IV. Estados Unidos

La Comisión Federal de Comunicaciones de Estados Unidos (FCC) ha reglamentado y comunicado de manera explícita que está prohibida la venta, fabricación, comercialización, importación, operación o uso de dispositivos que bloqueen, inhiban o interfieran intencionalmente con los sistemas de radiocomunicación autorizados como telefonía móvil celular, radares de policía, GPS y sistemas WiFi[31].

La principal razón de la medida adoptada por la FCC es que el uso de este tipo de dispositivos, además de afectar los servicios de radiocomunicación autorizados, generan un riesgo crítico para las comunicaciones de seguridad pública, como las llamadas de los ciudadanos a las líneas de emergencia. Adicionalmente, se reconoce que asegurar el acceso de los ciudadanos a los servicios de comunicaciones es una misión primordial del Estado.

En la sección 2.807 de las reglas de la Comisión, se incluyen algunas excepciones a esta prohibición, cobijando la fabricación de estos dispositivos exclusivamente para exportación o para el uso del Gobierno de los Estados Unidos o alguna de sus dependencias, siempre que cuente con autorización por parte de la Comisión.

Por otro lado, el gobierno de los EEUU también reconoce que es necesario combatir el contrabando de dispositivos de comunicaciones inalámbricas dentro de las correccionales y prisiones en el país. Según la Oficina Federal de Prisiones (BOP, por sus siglas en inglés), entre 2012 y 2014 se incautaron 8,700 celulares en las prisiones federales y en 2013 el Departamento de Correccionales y Rehabilitación de California confiscó 12,151 teléfonos[32]. Así mismo, se reportaron numerosos casos de hecho ejecución de hecho delictivos mediante el uso de estos dispositivos.

Para dar solución a esta situación, algunas correccionales han implementado tecnologías basadas en radio bases para detectar y bloquear dispositivos de comunicaciones inalámbricas dentro de sus límites. Este tipo de sistemas se denominan Contraband Interdiction System (CISs) y requiere autorización por parte de la FCC. Así mismo, este tema ha generado mesas de trabajo con el objetivo de buscar alternativas a la problemática.

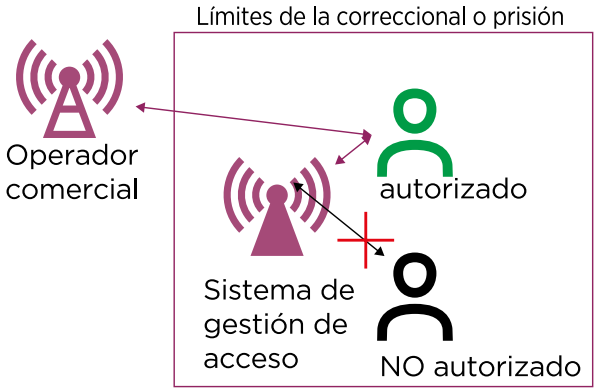
En términos generales, las tecnologías usadas en las correccionales de Estados Unidos se pueden dividir en dos categorías: i) gestión de acceso y ii) detección. La siguiente figura describe las características principales de cada tipo.

31. FCC – Jammers Enforcement (https://www.fcc.gov/general/jammer-enforcement). La Sección 301 de la Ley de Comunicaciones establece que ninguna persona puede operar ningún aparato de transmisión de señales vía radio sin autorización. La sección 303 establece que ninguna persona puede interferir intencional o maliciosamente alguna estación de radiocomunicaciones autorizada.
32. Report and Order and Further Notice of Proposed Rulemaking – GN Docket 13-111 (2017). (FCC, 2017).

FIGURA 16

Tecnologías usadas para combatir uso de dispositivos inalámbricos en prisiones - EEUU

Sistema de Gestión de acceso



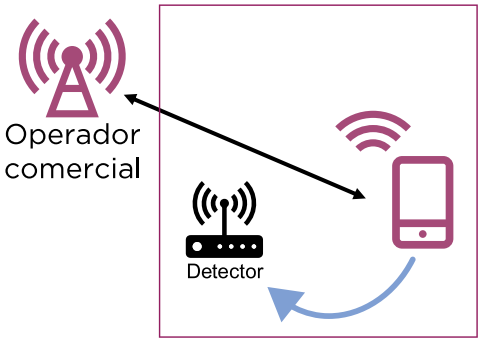
Red privada basada en micro celdas (opera en bandas de operadores comerciales). Requiere autorización FCC.

Analiza las transmisiones desde y hacia los terminales móviles.
Restringe a usuarios no autorizados o permite a usuarios autorizados conectarse con redes comerciales.

Cruza la información de identificación del usuario con una línea de registro

No interfiere con llamadas 911

Detección



Localización, rastreo e identificación de señales de radio originadas desde dispositivos.

- Pasivos: Detecta señales de radio
- Activos: Obtienen información de identificación del usuario (IMSI/IMEI) para incluir en lista de bloqueo

No requiere autorización FCC

Fuente: Basado en (FCC, 2017)

Para la instalación de este tipo de soluciones de gestión de acceso, la FCC debe analizar y autorizar la cesión o préstamo de espectro por parte de operadores de telecomunicaciones a los operadores de este tipo de sistemas dentro de las prisiones o correccionales. Se estima que este tipo de soluciones de han probado y/o implementado en cerca de 52 correccionales de 17 estados.

En Marzo de 2017, la FCC se pronunció con una serie de iniciativas para promover soluciones tecnológicas para combatir el uso de dispositivos inalámbricos de contrabando que ingresan a las correccionales y prisiones. Las iniciativas toman como base los siguientes aspectos:

- Agilizar los procesos de autorización por parte de la FCC para la instalación y operación de soluciones CISs en correccionales. Entre ellas, facilitar, para este tipo de casos, los procesos de sesión de espectro entre operadores de servicios de telecomunicaciones y operadores de los sistemas de gestión de acceso MAS.

- Cooperación de los operadores de servicios de comunicaciones inalámbricas

- Una persona dentro de la FCC dedicada a atender asuntos relacionados con estos procesos. Una figura similar a un Defensor de estas soluciones.

A

VI. Reino Unido

Desde el punto de vista del sector de telecomunicaciones, es importante resaltar que conforme la Ley de Comunicaciones Inalámbricas del 2006, está prohibida la instalación de dispositivos inalámbricos en la parte continental de Reino Unido, Irlanda del Norte, aguas territoriales, Isla de Man y las Islas de Canal sin la licencia otorgada por la Oficina de Comunicaciones del Reino Unido (Ofcom) y cumpliendo los requerimientos de la misma. En este sentido, el uso de equipos que interfieran o bloqueen las señales de comunicaciones, con riesgo de generar afectaciones en comunicaciones de emergencias, va en contra de la ley[33].

Por otro lado, los organismos de seguridad reportan que el uso de teléfonos no autorizados dentro de las prisiones por parte de bandas criminales organizadas se está empleando para importar armas y drogas, coordinar escapes y ejecutar asesinatos. Así mismo, el Servicio Nacional de Manejo de Delincuentes (NOMS, por sus siglas en inglés) estima que entre 2013 y 2014 se incautaron 7,400 SIM CARDS en prisiones de Inglaterra y Gales[34]. Estos resultados se presentan a pesar de que en 2012 se iniciaron pruebas de dispositivos bloqueadores de señal celular en 10 penales del Reino Unido.

A raíz de la problemática identificada, se empezaron a implementar técnicas para detección de dispositivos inalámbricos, por lo que en 2015 se ordenó a los operadores de telecomunicaciones a desconectar los terminales y SIM Cards reportados por la Corte del Condado como no autorizados para operar dentro del penal. Para ello, no sería necesario que la misma tenga posesión de los dispositivos, si no que contemplan su detección mediante mecanismos electrónicos.

33. https://www.ofcom.org.uk/spectrum/radio-spectrum-and-the-law/jammers
34. Serious Crime Act 2015

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601

GSMA LATAM
Av. Del Libertador 6810,
piso 15
Buenos Aires, C1429BMO,
Argentina
Tel: +54 (11) 5367 5400