2022

# Bloqueo de comunicaciones ilegales en centros penitenciarios

## Retos y soluciones

BLUE NOTE
MANAGEMENT CONSULTING

BlueNote Management Consulting es una firma de consultoría especializada en el sector de tecnologías de la información y las comunicaciones, desarrollando proyectos de estrategia, evaluación de mercados, estructuración de proyectos de inversión, políticas públicas y regulación; colaborando con el sector público y privado, organismos oficiales y entidades regionales.

BlueNote posee dos sedes, una en Buenos Aires, Argentina, y otra en Bogotá, Colombia.

Blue Note cuenta con un equipo de consultores con amplia experiencia y formación en el sector de telecomunicaciones y media, obtenida tanto en labores de consultoría especializada como durante el desempeño de funciones públicas o ejecutivas.

BlueNote ha realizado más de 50 proyectos en los últimos cinco años, relacionados con la industria de telecomunicaciones, desarrollo de nuevos negocios, evaluación de mercados, análisis de impacto de nuevos marcos regulatorio, estructuración y promoción de proyectos de inversión, desarrollo de nuevas soluciones tecnológicas y servicios, entre otros.

# CONTENIDO

# SIGLAS Y DEFINICIONES

| | |
|---|---|
| **3G** | Tecnologías de telecomunicaciones móviles de tercera generación |
| **3GPP** | Proyecto de Asociación de Tercera Generación |
| **4G** | Tecnologías de telecomunicaciones móviles de cuarta generación |
| **5G** | Tecnologías de telecomunicaciones móviles de quinta generación |
| **IA** | Inteligencia artificial |
| **API** | Interfaces de programación de aplicaciones |
| **BS** | Estación base |
| **EIR** | Registro de Identidad de Equipos |
| **EMF** | Campos electromagnéticos |
| **E-SMLC** | Enhanced Serving Mobile Location Center |
| **HLR** | Home Location Register |
| **IMT** | Telecomunicaciones Móviles Internacionales |
| **LCS** | Servicios de localización |
| **LMF** | Location Management Function |
| **MAS** | Soluciones de Gestión de Acceso |
| **MCC** | Código de país móvil |
| **ML** | Machine Learning o Aprendizaje automático |
| **MNC** | Código de red móvil |
| **MNO** | Operador de red móvil |
| **MS** | Estación móvil |
| **MSIN** | Número de identificación de suscriptor móvil |
| **MTLR** | Solicitud de ubicación de terminal móvil |
| **OMV** | Operador de red virtual móvil |
| **OA&M** | Operación, administración y mantenimiento |
| **ODB** | Prohibición determinada por el operador |
| **RF** | Radiofrecuencia |
| **SAS** | Stand Alone SMLC |
| **SMLC** | Serving Mobile Location Center |
| **UE** | Equipo de usuario |
| **WLS** | *Wireless Location Signatures* |

# Resumen ejecutivo

El bloqueo de llamadas en las cárceles se ha convertido en un tema relevante para la mayoría de los gobiernos en las últimas décadas. A medida que las redes de telecomunicaciones inalámbricas crecieron y los dispositivos se hicieron más pequeños, es más fácil para los reclusos ingresar ilícitamente dispositivos a las prisiones y poder realizar comunicaciones no autorizadas utilizando la cobertura de redes inalámbricas en estos establecimientos. Estas comunicaciones no autorizadas se utilizan para continuar con actividades ilegales que amenazan la seguridad nacional.

En particular, los países latinoamericanos han tenido un enfoque activo contra este problema en la última década, con muchas regulaciones emitidas por estos gobiernos que intentan lidiar con las comunicaciones ilegales en las cárceles.

| | NORMATIVA PARA EL BLOQUEO DE LLAMADAS EN LAS CÁRCELES | ENTIDADES RESPONSABLES | SOLUCIÓN DE BLOQUEO ACTUAL IMPLEMENTADA |
|---|---|---|---|
|  BRASIL | Ley Complementaria 79/1994 modificada por PLP 470/2018<br>Resoluciones 306/2002 y 308/2002 | Fondo Nacional Penitenciario (FUNPEN)<br>Ministerio de Justicia Departamento Nacional Penitenciario (DEPEN)<br>ANATEL | Jammers |
|  COLOMBIA | Decreto 4768/2011<br>Ley 1709/2014<br>ANE – Resolución 797/2019 | Ministerio de Justicia<br>Instituto Nacional Penitenciario (INPEC)<br>Ministerio de las TIC (MinTIC) - Agencia Nacional del Espectro (ANE)<br>MNOs (Soporte) | Jammers y restricción de señal en las prisiones |
|  COSTA RICA | Ley 9597 | MNOs<br>Ministerio de Justicia<br>Superintendencia de Telecomunicaciones (SUTEL) | Solución basada en geolocalización y ML |
|  EL SALVADOR | Decreto 953/2015<br>Reglamento técnico de la ley especial contra el delito de extorsión / 2016 | MNOs<br>Supertendencia de Electricidad y Telecomunicaciones (SIGET)<br>Ministerio de Justicia y Seguridad Pública | Jammers y restricción de señal en las prisiones |
|  HONDURAS | Decreto 43/2015<br>CONATEL – Resolución 001/2016 | MNOs<br>Comisión Nacional de Telecomunicaciones (CONATEL)<br>Secretaría de Estado | Jammers y restricción de señal en las prisiones |
|  GUATEMALA | Decreto 12/2014 declarado inconstitucional en 2016 | MNOs<br>Superintendencia de Telecomunicaciones de Terceros (SIT) | Jammers |
|  MÉXICO | Ley general del sistema nacional de seguridad pública / 2009<br>Ley federal de telecomunicaciones y radiodifusión / 2014<br>Lineamientos de colaboración para operadores de telecomunicaciones y autoridades penitenciarias / 2012<br>IFT – Lineamientos de colaboración para la seguridad y la justicia / 2015<br>Disposición técnica IFT – 010 – 2016 | Sistema Nacional de Seguridad Pública<br>Instituto Federal de Telecomunicaciones (IFT)<br>MNOs | Jammers |
|  PANAMÁ | Ley 55/2003<br>Decreto 393/2005<br>Resolución AN 6295-Telco/2013 | MNOs<br>Ministerio de Gobierno (Dirección de Seguridad Penitenciaria)<br>Autoridad Nacional de Servicios Públicos (ASEP) | Restricción de señal en prisiones seleccionadas |
|  PERÚ | Decreto Supremo 015/2003<br>OSIPTEL Resolución 112/2011<br>Decreto Legislativo 1229/2015<br>Decreto Supremo 007/2016 | Ministerio de Justicia<br>Instituto Nacional Penitenciario (INPE) + Terceros (PRISONTEC)<br>Regulador (OSIPTEL)<br>MNOs | Inhibidores y restrictión de intensidad de señal |

**Entre las soluciones de uso común se encuentran los *Jammers*, IMSI Catchers y Managed Access Solutions (MAS).**

Desafortunadamente, la mayoría de las alternativas técnicas para el bloqueo de llamadas han demostrado ser ineficaces por varias razones. Interferencias o bloqueos no deseados de las comunicaciones lícitas, efectos negativos en la calidad de los servicios comerciales, aumento de los costos para los operadores de red, puntos ciegos y sabotaje son algunos de los fenómenos que los hacen ineficaces.

Entre las soluciones de uso común se encuentran los *Jammers, IMSI Catchers y Managed Access Solutions (MAS)*. Cada una de estas alternativas tiene sus propios pros y contras. En general, estas alternativas comparten una base común de operación, utilizan la generación de señales de radiofrecuencia (RF) para interferir las señales de las redes (inhibidores), para generar un ataque man-in-the-middle (IMSI Catchers) o para crear una red de área local pequeña filtrada (MAS); todos ellos tienen algún tipo de efectividad bloqueando las comunicaciones, pero los puntos ciegos, el sabotaje, la falta de inteligencia y los efectos negativos de los usos de señales de RF en las comunicaciones legales opacan sus atributos positivos.

Aunque los inhibidores son una solución de bloqueo eficaz, tienen varios efectos no deseados, como:

**a.** Los inhibidores pueden afectar las comunicaciones legales tanto dentro como fuera del perímetro de las instalaciones penitenciarias. Incluso los servicios esenciales están bloqueados, como las llamadas de emergencia.
**b.** Habrá una zona en la que los servicios no se niegan por completo, sino que están sujetos a una degradación de la calidad debido a señales de interferencia ligeramente débiles.
**c.** Los obstáculos en las implementaciones reales pueden generar puntos ciegos dentro de las prisiones donde las comunicaciones están completa o parcialmente disponibles. Además, el tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.
**d.** Los inhibidores de baja calidad son propensos a generar emisiones fuera de banda o espurias que podrían afectar a otros servicios de telecomunicaciones que no están destinados a ser bloqueados.
**e.** Requiere equipamiento local
**f.** No es posible monitorear el nivel de efectividad del sistema
**g.** No hay capacidad de auditoría para saber qué dispositivos fueron bloqueados
**h.** No hay capacidad para auditar u obtener datos para inteligencia en seguridad

Del mismo modo, los IMSI Catchers tienen algunos efectos y debilidades no deseados.

**a.** Es probable que afecte a las comunicaciones legales. Una vez más, la operación se basa en la emisión de una señal radioeléctrica, que como se ha visto antes se propaga y está sujeta a todos los efectos naturales relacionados con las ondas. Debido a eso, es posible tener puntos ciegos dentro de las instalaciones para que los dispositivos reconozcan el BS real y se conecten directamente a él, evitando el receptor.
**b.** Otra consecuencia relacionada con la naturaleza de las señales radioeléctricas es que habrá zonas fuera de la prisión con una mejor intensidad de señal del IMSI Catcher que de los BS de la red. Por lo tanto, los dispositivos ubicados fuera de la prisión y dentro de la huella efectiva del receptor también serán bloqueados.
**c.** Como el funcionamiento del IMSI Catcher requiere el intercambio de información con los terminales de los usuarios, hay algunos comportamientos inusuales que se pueden utilizar para identificar que hay

**En los últimos años, ha surgido una nueva tecnología que promete corregir todos los efectos no deseados**

un sistema de este tipo. Algunos ejemplos son: uso de frecuencias fuera de banda, identificador de estación base inusual, capacidades no existentes y parámetros de red como GPRS o EDGE deshabilitados, ausencia de cifrado, falta de información, entre otros. Esta debilidad es explotada por contramedidas, tanto como hardware especializado que prioriza el cifrado y puede alertar al usuario de la presencia de un IMSI Catcher

**d.** La "captura" se vuelve más difícil a medida que las tecnologías IMT evolucionan e implementan sistemas de cifrado más complejos.

**e.** Estos sistemas requieren instalación local, por lo que la escalabilidad es difícil y los costos de OA&M son altos. También son propensos a daños o inhabilitaciones por parte de los reclusos o el personal corrupto o la administración. El tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.

**f.** Los captadores IMSI permiten la interceptación, que puede generar información valiosa, pero normalmente estas actividades requieren autorización legal. Esta capacidad concierne a aquellos que no están encarcelados y puede verse afectada por los captadores de IMSI.

**g.** La mayoría de los receptores IMSI trabajan solo con 2G, lo que limita severamente su efectividad.

Finalmente, los sistemas MAS también tienen elementos no deseados como:

**a.** Los sistemas MAS podrían interrumpir los servicios a personas fuera de las prisiones que no están incluidas en la lista blanca.

**b.** Los sistemas MAS son capaces de interceptación o vigilancia, lo que genera preocupaciones legales, especialmente cuando son operados por terceros.

**c.** Como el sistema funciona como parte de la red, requiere coordinación de frecuencia con el MNO para evitar interferencias, lo que afecta el diseño normal de la red. Requiere subarrendamiento del espectro, que no está permitido en todos los países.

**d.** Los MAS forman parte de la red; el sistema debe actualizarse a medida que las redes evolucionan y se enfrentan a contramedidas.

**e.** La instalación en las instalaciones es propensa a daños o inhabilitación por parte de los reclusos o el personal o la administración corruptos. El tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.

**f.** Los sistemas MAS generalmente solo son aplicables para escenarios específicos, principalmente en áreas remotas con baja densidad de población o cobertura celular existente.

**g.** El diseño e implementación del sistema MAS tiene una alta complejidad que implica más costos de inversión y operación en comparación con otras soluciones.

En los últimos años, ha surgido una nueva tecnología que promete corregir los efectos no deseados de sus alternativas anteriores, eliminando el uso de señales de RF y utilizando geolocalización y el aprendizaje automático para resolver el problema del bloqueo de llamadas en las cárceles.

Esta alternativa no emite señales, por lo que los aspectos relacionados con interferencia y propagación está fuera del análisis, también utiliza protocolos e interfaces de tecnologías móviles totalmente estandarizados y es una solución completamente basada en software que no requiere la instalación de equipos locales. Todo ello, combinado con complejos modelos matemáticos, datos de equipos de usuario (UE) en tiempo real e inteligencia artificial, permite al sistema localizar con precisión los dispositivos móviles y, si se encuentran dentro de la prisión, bloqueará el servicio para ese usuario sin afectar a nadie más.

Algunas de las mejores características de la solución son:

**Desde el punto de vista de los costos, esta tecnología alcanza montos comparables con los inhibidores, pero con mayor efectividad y capacidades.**

**a.** Alta precisión de ubicación para bloquear teléfonos dentro de la prisión. El caso particular de la tecnología patentada WLS permite al sistema identificar y localizar los dispositivos con alta precisión. Con la ubicación de los dispositivos, el comando de bloqueo es selectivo y no afecta a otros usuarios.
**b.** Monitoreo y control centralizado para múltiples prisiones. La implementación no requiere instalación local, lo que reduce el CAPEX y el OPEX, simplifica los mantenimientos y permite una fácil escalabilidad. También reduce la propensión a la corrupción.
**c.** Inteligencia en tiempo real para proporcionar información valiosa y procesable, identificando dispositivos específicos utilizados dentro de las prisiones, horas de uso, fechas de actividad de los dispositivos, entre otros.
**d.** Monitoreo avanzado con informes históricos y capacidad de auditoría.
**e.** Características de software configurables y personalizables para cumplir con las necesidades del país y las leyes locales.
**f.** Bloqueo de llamadas en tiempo real con opción de incluir en la lista blanca números

Desde el punto de vista de los costos, esta tecnología alcanza montos comparables con los inhibidores, pero con mayor efectividad y capacidades, ofreciendo inteligencia a los gobiernos y protegiendo todas las comunicaciones legales.

## CUADRO 1

Matriz de evaluación de la tecnología

Fuente: BNMC

| | Jammers | IMSI Catchers | Soluciones de Gestión de Acceso | Soluciones basadas en la Geo-localización y ML |
|---|---|---|---|---|
| **Efectividad** | ★★★☆ Afectado por las características de las ondas de radio | ★★★☆ Afectado por las características de las ondas de radio | ★★★☆ Afectado por las características de las ondas de radio | ★★★★ Bloqueo como un comando de red, deshabilita serv al suscriptor |
| **Escalabilidad** | ☆☆☆☆ Cada prisión es un despliegue completamente nuevo | ☆☆☆☆ Cada prisión es un despliegue completamente nuevo | ★★☆☆ Cada prisión es un despliegue completamente nuevo, pero la coordinación del operador ya está desarrollada | ★★★★ Cada prisión solo requiere una nueva geo cerca y una configuración de software |
| **Protege las comunicaciones comerciales** | ☆☆☆☆ Interfiere la señal, bloquea a los vecinos. Diseño de RF complejo | ★★☆☆ Bloquea a los vecinos en el área de cobertura. Diseño de RF complejo | ★★★☆ Bloquea a los vecinos en el área de cobertura. Puede agregar registros a la lista blanca. Diseño de RF complejo | ★★★★ Bloqueo selectivo. Si se equivoca, puede aprender a minimizar el error |
| **Capacidad de actualización** | ☆☆☆☆ Nueva tecnología, nuevo operador o nueva banda de frecuencias = nuevo despliegue | ☆☆☆☆ Las nuevas tecnologías también desarrollan un cifrado más complejo | ★★☆☆ La nueva tecnología requerirá una nueva red local | ★★★☆ La nueva tecnología solo requerirá una actualización de software |
| **A prueba de manipulaciones** | ☆☆☆☆ | ☆☆☆☆ | ★★★☆ MNO o custodia de terceros | ★★★★ Elementos ubicados en Data center de MNO y autoridad |
| **Seguridad** | ★★☆☆ | ★★☆☆ | ★★★☆ | ★★★★ |
| **Precisión de ubicación** | ☆☆☆☆ | ★★★★ La mejor precisión utilizando equipos locales | ☆☆☆☆ | ★★★☆ Alta precisión utilizando la infraestructura existente |
| **Relación con operador de red** | ☆☆☆☆ Generador de interferencias | ★★☆☆ Afecta a los usuarios y a las preocupaciones legales | ★★★☆ Requiere coordinación, modificación de la planificación de frecuencias | ★★★☆ Requiere integración con la red central. |
| **Funciones de inteligencia** | ☆☆☆☆ | ★★★☆ Puede identificar al suscriptor y el destino, incluso interceptar llamadas únicas en 2G | ★★★★ Puede identificar al suscriptor y el destino, incluso interceptarlo | ★★★★ Identificación del suscriptor, ubicación, patrones, servicios, etc. Complete la información de llamadas y ubicaciones |
| **Costos y complejidad** | ★★★☆ | ★☆☆☆ | ★☆☆☆ | ★★★☆ |
| **En general** | ★☆☆☆ | ★★☆☆ | ★★★☆ | ★★★★ |

Las soluciones basadas en geo-localización sobre redes inalámbricas sobresalen de las alternativas disponibles en el mercado. Ofrece alta precisión, bloqueo selectivo no dañino, mejores costos de implementación y escalabilidad, nuevas alternativas de inteligencia y protección contra la corrupción.

# Introducción

**El contrabando de dispositivos móviles sigue estando presente en las prisiones o centros de detención, lo que permite a los presos establecer comunicaciones ilegales**

La seguridad nacional ha sido una preocupación para los gobiernos al rededor del mundo y una piedra angular para el desarrollo de los estados nacionales modernos. Por lo tanto, el uso estratégico de las redes de comunicaciones, la protección de los servicios públicos de telecomunicaciones y la restricción a las comunicaciones ilegales se convierten en un tema relevante para las agencias de seguridad.

Particularmente, el uso de teléfonos celulares de manera ilegal en las cárceles es un tema de gran interés, considerando que esta actividad permite delitos como:

**a.** Continuar las operaciones de negocios y actividades ilegales;
**b.** Gestionar las operaciones de contrabando (por ejemplo, drogas, dispositivos ilegales) dentro y fuera de las prisiones;
**c.** Coordinar motines dentro de las prisiones y golpes a los oficiales correccionales;
**d.** Manipular a los testigos judiciales, incluso planeando su asesinato; y
**e.** La planificación de escapes o fugas de las prisiones.

La anterior es la razón por la cual varios países han expedido diversas leyes y regulaciones que prohíben el uso de teléfonos en las cárceles y exigen a las agencias gubernamentales que desarrollen e implementen sistemas y procedimientos para cumplir este objetivo, así como para la prevención de llamadas ilegales.

Este no es un problema aislado de un país o región, está presente en todo el mundo, y los gobiernos has llevado a cabo diversos esfuerzos, desplegando por ejemplo varios sistemas y tecnologías para evitar el uso de dispositivos móviles en las cárceles, en la mayoría de los casos sin éxito. El problema sigue creciendo y, a medida que lo hace y la tecnología evoluciona, los gobiernos se ven obligados a revisar sus marcos legales para restringir estas comunicaciones ilegales.

El contrabando de dispositivos móviles sigue estando presente en las prisiones o centros de detención, lo que permite a los presos establecer comunicaciones ilegales y generar problemas de seguridad tanto dentro como fuera de las instalaciones de las prisiones. Las operaciones de contrabando resultan más fáciles debido a que los dispositivos son más difíciles de detectar, ya que son más pequeños, y la corrupción es un fenómeno recurrente en los sistemas penitenciarios.

Bajo la realidad de que la delincuencia sigue y probablemente seguirá encontrando la manera de ingresar dispositivos de comunicaciones a las cárceles, este documento describe y comparar algunas de las soluciones y tecnologías que permiten a los gobiernos restringir las llamadas generadas desde las cárceles y controlar los efectos negativos y las preocupaciones de seguridad derivadas de esas actividades. Se realiza entonces una comparación del marco legal de una muestra de nueve países de América Latina, un análisis sobre varias soluciones utilizadas para abordar el problema, desde los bloqueadores de señal o *jammer*s hasta los sistemas de bloqueo de comunicaciones basado en Inteligencia Artificial (IA) y Machine Learning (ML).

Finalmente se propone un marco para el despliegue de soluciones innovadoras.

Las actividades ilegales siempre son difíciles de abordar, ya que quienes las cometen están continuamente "innovando" sobre cómo llevarlas a cabo. Especialmente en lo relacionado con el problema del uso no autorizado de teléfonos móviles en las cárceles siempre hay nuevas técnicas de los presos para ingresar ilícitamente dispositivos a las cárceles. Así mismo, las soluciones no pueden depender de las personas, considerando las posibilidades de error humano y la propensión a la corrupción en estos entornos, por lo que la tecnología es esencial para ayudar en el esfuerzo. No obstante, otros elementos influyen en la dificultad de controlar esas actividades.

Una solución ampliamente utilizada es la interferencia de señales celulares o *jamming*, de modo que los reclusos que usan teléfonos celulares no pueden hacer llamadas o usar servicios de datos. Este tipo de soluciones genera efectos negativos en el rendimiento de las redes móviles e interfiere con los servicios de comunicaciones legales; de modo que en algunos países se ha optado por categorizar este tipo de equipos de bloqueo como ilegales. En esos casos, la implementación de tecnologías de bloqueo requiere una autorización legal.

Otra dificultad es que las tecnologías móviles están evolucionando rápidamente haciendo uso de más espectro radioeléctrico en nuevas bandas de frecuencias para su despliegue. Eso hace que los equipos de bloqueo o inhibición deban ajustarse a los cambios en las redes de telecomunicaciones, lo que requiere más inversión, energía y espacio. Además, las técnicas que requieren la instalación de equipo local son propensas a daños e inhabilitación por parte de los presos y el propio personal penitenciario. La corrupción se convierte entonces en una debilidad para los sistemas descentralizados y locales.

Todos estos elementos añaden desafíos a las soluciones tradicionales, que se han demostrado ineficaces, ya que los gobiernos todavía están preocupados por eso y actualizando las reglas para luchar contra esas actividades.

# I.
# VISIÓN GENERAL DEL MARCO REGULATORIO EN AMÉRICA LATINA.
## Desafíos y resultados alcanzados

A continuación, encontrará una descripción general de las regulaciones existentes en algunos países de América Latina sobre el bloqueo de llamadas en las prisiones. La mayoría de los países de la región desarrollaron algún tipo de marco legal para restringir las comunicaciones en las cárceles y lo han actualizado a medida que evolucionó la problemática.

### Brasil

El reglamento exige que se instalen inhibidores de señales en todas las prisiones para bloquear los teléfonos móviles y los transmisores de radio, en todas las bandas utilizadas para los servicios de telecomunicaciones y cualquier tecnología, pero no deben interferir con las señales fuera del perímetro de la prisión. También requiere coordinación entre los operadores de red y las autoridades penitenciarias para desplegar los sistemas y mitigar los riesgos de interferencia. Esos sistemas deben cumplir con las regulaciones de exposición a campos electromagnéticos (EMF) y no pueden estar al alcance de los reclusos.

### Colombia

La inhibición de las señales de radio en las cárceles requiere el permiso del Ministerio de las TIC y esfuerzos coordinados entre los operadores de redes móviles (MNO) y las autoridades penitenciarias. Los MNO deben reducir los niveles de señal dentro de las instalaciones penitenciarias y los sistemas de bloqueo deben cumplir con una zona de coordinación de 25 m fuera de la prisión.

La autoridad penitenciaria puede solicitar la autorización para instalar inhibidores cuando existan razones fundadas para inferir que las amenazas, el fraude, la extorsión y otros actos constitutivos de delito se llevan a cabo desde su interior utilizando dispositivos de telecomunicaciones. También existe la posibilidad de que el Ministerio de TIC ordene restricciones a los operadores de redes de comunicaciones o que suspenda la transmisión de sus señales a petición de la autoridad penitenciaria o de una combinación de ambas. Esos sistemas deben cumplir con las regulaciones de exposición a campos electromagnéticos (EMF).

### El Salvador

Los operadores de redes están obligados a implementar los procedimientos comerciales y las soluciones técnicas para evitar la prestación de servicios de telecomunicaciones dentro de las prisiones. Está prohibido que los operadores de redes presten servicios de telecomunicaciones en las ubicaciones físicas de las prisiones, con excepción de los servicios contratados por la administración de la penitenciaría. La Procuraduría General de la República tiene facultades para ordenar la suspensión inmediata de los servicios de telecomunicaciones si están relacionados con delitos de extorsión.

### Honduras

La prestación de servicios de telecomunicaciones en las cárceles está prohibida, por lo que los proveedores de servicios autorizados deben implementar soluciones para bloquear las telecomunicaciones dentro de las instalaciones penitenciarias. Los MNO están a cargo de instalar soluciones técnicas para el bloqueo de señales. Después de la instalación, los operadores de servicios de mantenimiento y tecnología son responsables de la administración, el funcionamiento y el mantenimiento eficaces, y la autoridad penitenciaria es responsable de la protección de los bienes locales.

### Guatemala

El control de las telecomunicaciones móviles en las cárceles fue declarado de interés general y nacional. En 2016 se declaró inconstitucional un marco legal que obligaba a los MNOs a implementar soluciones técnicas para evitar el tráfico de telecomunicaciones móviles generado desde las instalaciones penitenciarias y establecía multas a los MNOs si el sistema no funcionaba correctamente.  Sin embargo, los MNO han seguido operando los equipos de bloqueo en algunos centros penitenciarios.

### México

La Ley Federal de Telecomunicaciones y Radiodifusión requiere la cooperación de los operadores de redes con las agencias de justicia y seguridad en varios temas, que incluyen la geolocalización en tiempo real, el mantenimiento de un registro de comunicaciones muy detallado, el bloqueo de líneas y terminales reportados como robados, el bloqueo de radiocomunicaciones celulares y señales de transmisión de datos dentro de los perímetros de las prisiones en cada banda de frecuencias, entre otros.

Los equipos de bloqueo de señal que se instalen dentro del perímetro de las cárceles deberán cumplir con las disposiciones técnicas emitidas por el Instituto Federal de Telecomunicaciones (IFT) y demás normativas aplicables. Las autoridades penitenciarias, previa autorización, pueden comprar y desplegar sistemas de bloqueo dentro de las instalaciones penitenciarias. Estas autoridades deben trabajar con los operadores de redes para prevenir y resolver cualquier afectación indebida a los usuarios de los servicios de telecomunicaciones.

### Panamá

No existe una regulación general relacionada con el bloqueo de comunicaciones en las cárceles. La Ley Penitenciaria proporciona un marco general que permite actuar en casi cualquier situación. El Director General del Sistema Penitenciario tiene funciones relacionadas con identificar deficiencias en el sistema, informarlas al Ministerio de Gobierno y recomendaciones de mejora. El director también debe preparar y presentar acuerdos para promover la autogestión y la obtención de recursos que deben ser utilizados en el mejoramiento y conservación de las cárceles.

La Autoridad Nacional de Servicios Públicos ordenó la suspensión y restricción de las comunicaciones inalámbricas en algunas prisiones. Pero esa orden no está completamente implementada, ya que afecta a lugares clave en Panama, como la Zona Libre de Colón, el Canal de Panamá y las áreas del aeropuerto.

### Perú

El Código de Ejecución Penal exige a las autoridades penitenciarias que promuevan el acceso a la información de los reclusos medios impresos, la instalación de receptores de radio y televisión en áreas abiertas y cabinas telefónicas públicas con sistemas de identificación de llamadas que permitan a la administración tener reporte de origen y destino de las llamadas. Sin embargo, cualquier otro servicio de telecomunicaciones está prohibido a los presos y se consideran comunicaciones ilegales, también está prohibido llevar cualquier equipo terminal como teléfonos celulares, teléfonos satelitales, transceptores de radio o cualquier otro dispositivo que permita la transmisión de voz o datos.

El marco legal en Perú declara el fortalecimiento de la infraestructura y los servicios penitenciarios de interés público y prioridad nacional, establece los criterios para el corte del servicio y el bloqueo de los equipos terminales móviles en caso de usos ilegales en las prisiones y regula la instalación de dispositivos de bloqueo (*Jammers*). Así mismo, el marco legal habilita al Instituto Nacional Penitenciario a operar los sistemas de bloqueo o inhibición a través de terceros o empresas contratadas.

| | NORMATIVA PARA EL BLOQUEO DE LLAMADAS EN LAS CÁRCELES | ENTIDADES RESPONSABLES | SOLUCIÓN DE BLOQUEO ACTUAL IMPLEMENTADA |
|---|---|---|---|
|  BRASIL | Ley Complementaria 79/1994 modificada por PLP 470/2018<br>Resoluciones 306/2002 y 308/2002 | Fondo Nacional Penitenciario (FUNPEN)<br>Ministerio de Justicia Departamento Nacional Penitenciario (DEPEN)<br>ANATEL | Jammers |
|  COLOMBIA | Decreto 4768/2011<br>Ley 1709/2014<br>ANE – Resolución 797/2019 | Ministerio de Justicia<br>Instituto Nacional Penitenciario (INPEC)<br>Ministerio de las TIC (MinTIC) - Agencia Nacional del Espectro (ANE)<br>MNOs (Soporte) | Jammers y restricción de señal en las prisiones |
|  COSTA RICA | Ley 9597 | MNOs<br>Ministerio de Justicia<br>Superintendencia de Telecomunicaciones (SUTEL) | Solución basada en geolocalización y ML |
|  EL SALVADOR | Decreto 953/2015<br>Reglamento técnico de la ley especial contra el delito de extorsión / 2016 | MNOs<br>Supertendencia de Electricidad y Telecomunicaciones (SIGET)<br>Ministerio de Justicia y Seguridad Pública | Jammers y restricción de señal en las prisiones |
|  HONDURAS | Decreto 43/2015<br>CONATEL – Resolución 001/2016 | MNOs<br>Comisión Nacional de Telecomunicaciones (CONATEL)<br>Secretaría de Estado | Jammers y restricción de señal en las prisiones |
|  GUATEMALA | Decreto 12/2014 declarado inconstitucional en 2016 | MNOs<br>Superintendencia de Telecomunicaciones de Terceros (SIT) | Jammers |
|  MÉXICO | Ley general del sistema nacional de seguridad pública / 2009<br>Ley federal de telecomunicaciones y radiodifusión / 2014<br>Lineamientos de colaboración para operadores de telecomunicaciones y autoridades penitenciarias / 2012<br>IFT – Lineamientos de colaboración para la seguridad y la justicia / 2015<br>Disposición técnica IFT – 010 – 2016 | Sistema Nacional de Seguridad Pública<br>Instituto Federal de Telecomunicaciones (IFT)<br>MNOs | Jammers |
|  PANAMÁ | Ley 55/2003<br>Decreto 393/2005<br>Resolución AN 6295-Telco/2013 | MNOs<br>Ministerio de Gobierno (Dirección de Seguridad Penitenciaria)<br>Autoridad Nacional de Servicios Públicos (ASEP) | Restricción de señal en prisiones seleccionadas |
|  PERÚ | Decreto Supremo 015/2003<br>OSIPTEL Resolución 112/2011<br>Decreto Legislativo 1229/2015<br>Decreto Supremo 007/2016 | Ministerio de Justicia<br>Instituto Nacional Penitenciario (INPE) + Terceros (PRISONTEC)<br>Regulador (OSIPTEL)<br>MNOs | Inhibidores y restrictión de intensidad de señal |

# I.a IMPACTO DE LAS MEDIDAS ADOPTADAS Y RETOS PENDIENTES

Como se mencionó previamente, casi todos los países de la región han desarrollado una regulación para abordar la problemática de las comunicaciones ilegales en las cárceles. Estas regulaciones tienen diferentes niveles de implementación dependiendo del país. Sin embargo, hay algo claro, el problema aún no está resuelto, ya que las regulaciones siguen actualizándose y las "soluciones" implementadas siguen demandando recursos.

Esta situación ha hecho que el bloqueo de llamadas en las cárceles sea un tema prioritario en las agendas gubernamentales, ya que las estadísticas de la actividad delictiva muestran que la mayor proporción de llamadas de extorsión se realizan desde el interior de las cárceles, acentuando los delitos relacionados con las pandillas, el crimen organizado y el tráfico de drogas, junto con los simples motines en las cárceles y la coordinación para este tipo de actividades.

Los inhibidores son el sistema predominante, pero tienen efectos negativos en las comunicaciones legales, como vamos a describir más adelante. Estos efectos negativos están relacionados principalmente con la interferencia que estos sistemas generan alrededor de las áreas de restricción. Las señales de interferencia no solo bloquean las comunicaciones ilegales, sino que también afectan a los vecinos y ciudadanos que pasan, y esas consecuencias no deseadas afectan tanto a los operadores de red como a la comunidad.

Las interferencias generadas por los *jammer*s a los gobiernos a definir restricciones a sus implementaciones, en algunos casos áreas de coordinación donde se aceptan niveles de interferencia aceptables y en otras prohibiciones de casos específicos en los que no se puede utilizar la solución. Hay algunos países donde los inhibidores están prohibidos o solo están permitidos para el bloqueo de llamadas en prisiones.

Los MNO han tenido varios problemas a medida que los sistemas interfieren con sus diseños de propagación de señal deseados o incluso en los casos en que la regulación requiere coordinación entre las autoridades penitenciarias y los MNO. En la mayoría de los casos, además de los costos asociados con el despliegue específico de la solución de bloqueo, las partes interesadas también enfrentan el costo de ajustar el diseño de la red de telecomunicaciones para las estaciones base ubicadas cerca de las instalaciones penitenciarias. Además, en algunos mercados, el mal desempeño en la solución de bloqueo o los problemas relacionados con la restricción de señales pueden generar multas o sanciones sobre los MNO y las disputas legales posteriores.

Otro problema surge a medida que el estándar de las Telecomunicaciones Móvil Internacionales (IMT) siguen evolucionando y las redes móviles se

están desplegando sobre nuevas bandas de frecuencias, lo que requiere más inversiones en equipos de inhibición para incluir los nuevos rangos de frecuencia de las redes.

Está claro que las soluciones implementadas existentes no son efectivas para restringir las comunicaciones no autorizadas desde la prisión. Existe la necesidad de una solución que efectivamente tenga menores costos de implementación, bajos riesgos relacionados con el equipo instalado en las instalaciones y pueda mitigar o eliminar cualquier efecto negativo sobre las comunicaciones legales dentro o alrededor de la prisión.

# II.

# DESCRIPCIÓN DE LAS SOLUCIONES TÉCNICAS: DESDE INHIBIDORES HASTA TECNOLOGÍAS DE APRENDIZAJE AUTOMÁTICO

Aunque las comunicaciones inalámbricas ofrecen una amplia variedad de alternativas en cuanto a tecnologías y sistemas, no cabe duda de que los teléfonos móviles son los más utilizados debido a la cobertura de la red, la disponibilidad de servicios (voz y acceso a Internet) y la adopción masiva de la tecnología. Debido a eso, la mayoría de los esfuerzos para bloquear las comunicaciones en las prisiones se centran en las tecnologías móviles.

Como se ha visto anteriormente, hay diferentes elementos que deben tenerse en cuenta a la hora de planificar el despliegue de soluciones de bloqueo de comunicaciones en las cárceles. Las regulaciones a menudo requieren bloquear las comunicaciones en las prisiones, pero al mismo tiempo requieren proteger los intereses de los ciudadanos alrededor de la prisión que están utilizando comunicaciones legales y también proteger las inversiones que los MNO hacen para proporcionar servicios.

Junto con las restricciones regulatorias, las tecnologías móviles evolucionan a un ritmo particularmente rápido. La primera generación de telefonía móvil se introdujo a principios y mediados de los años 80, luego, la segunda generación comenzó las operaciones comerciales a principios de los años 90 con algunas mejoras incorporadas en la primera mitad de la década que incorporó adicionalmente nuevas bandas de frecuencias a la operación de la red. En 1995 comenzó la investigación para la tercera generación y para el año 2000 las redes 3G comenzaron a desplegarse. Una vez más, en 2005 se introdujeron varias mejoras que exigían nuevo espectro radioeléctrico para ampliar la capacidad de la red y, antes de que finalizara la década, se iniciaron

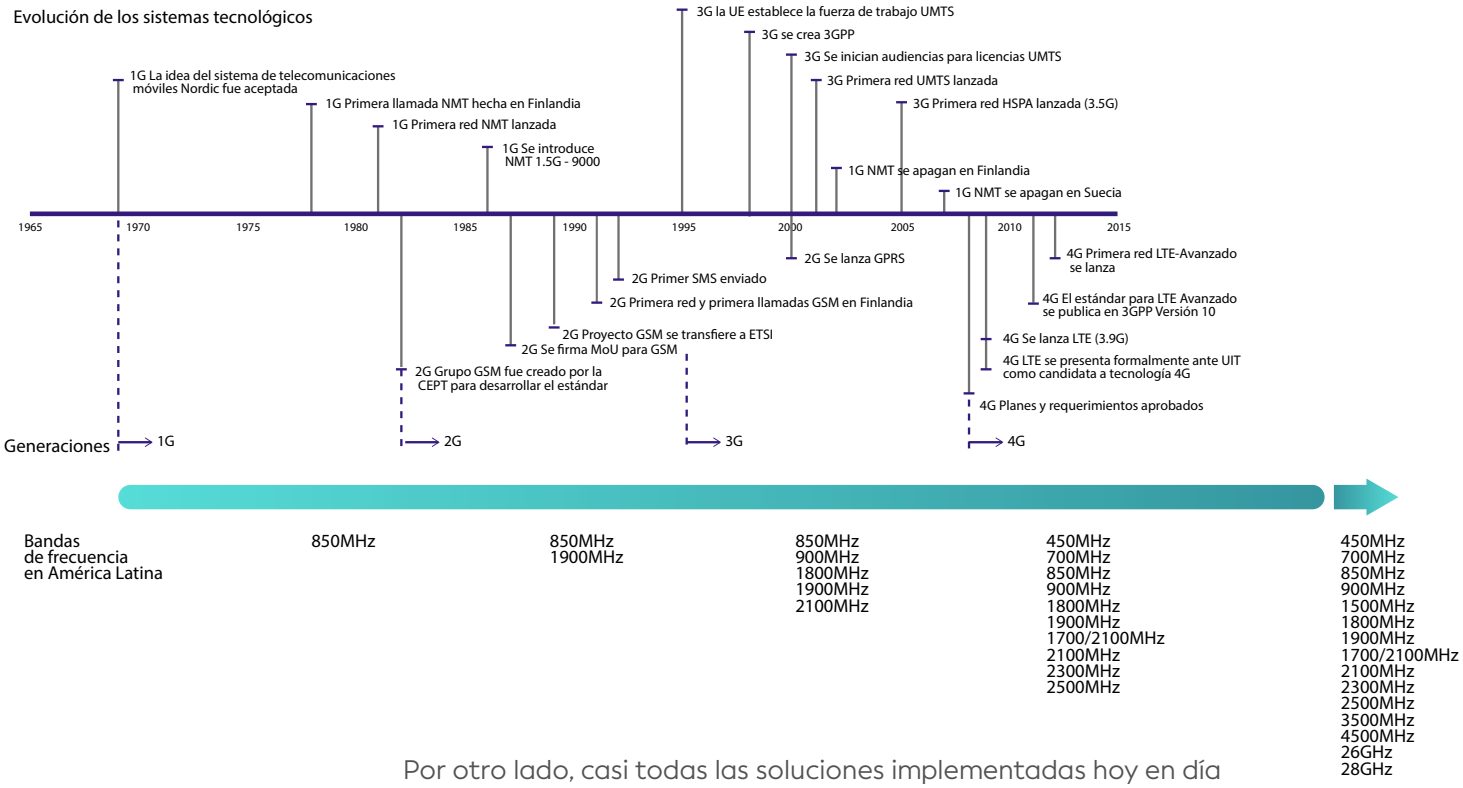
los desarrollos de la cuarta generación tecnológica. A principios de la década de 2010, 4G se lanzó en los mercados utilizando nuevas bandas de frecuencia, nuevamente con algunos complementos a lo largo de la década. Para 2020, 5G comenzó los despliegues comerciales y varios países están preparando subastas de espectro en nuevas bandas de frecuencias por encima de los 3GHz y bandas de ondas milimétricas.

Además, la mayoría de los despliegues de nuevas tecnologías de comunicaciones móviles requirieron nuevas bandas de espectro, lo que dificulta el bloqueo de las comunicaciones móviles en la medida que se necesitan nuevos equipos, además de nuevos diseños para el cumplimiento del marco normativo ya que las condiciones de propagación varían significativamente con la frecuencia, y los gobiernos necesitan asignar más recursos a medida que evoluciona la tecnología. Como referencia, los despliegues de 2G en la mayoría de los países de América Latina utilizaron bandas de 850MHZ y 900MHz, luego las bandas de 1800MHz, 1900MHz y 2100MHz se incorporaron para la implementación de 3G. Para el final de la década de 2010, la mayoría de los países en la región habían asignado las bandas de 700 MHz, AWS y 2,5GHz para los servicios 4G y 5G supone que varias otras bandas están en consideración. Los cambios en las tecnologías y en las bandas de frecuencias requieren de los sistemas de bloqueo la capacidad de adaptarse a un ritmo rápido, de modo que no se puedan ejecutar comunicaciones no autorizadas.

**FIGURA 1**

Cronología de las generaciones de telecomunicaciones móviles

Fuente: (Marcus Holgersson, 2017) adaptado por BNMC




Por otro lado, casi todas las soluciones implementadas hoy en día necesitan de equipamiento o hardware instalado a nivel local en los centros penitenciarios. Esta condición genera varios efectos que no son ideales para el propósito seguido con esos sistemas. Por un lado, se requiere espacio físico y acondicionamiento técnico dentro de las cárceles. Dedicar espacio físico, energía y conectividad no es fácil para las autoridades penitenciarias, especialmente en instalaciones diseñadas hace mucho tiempo, cuando estas necesidades no estaban identificadas.

Desafortunadamente, la implementación local conlleva otros riesgos. El hardware puede ser desactivado o dañado por los prisioneros o el personal y la administración en casos de corrupción. Es lógico inferir que los gastos de operación, administración y mantenimiento (OA&M) aumentan, ya que se requeriría intervención técnica en cada centro penitenciario y el mantenimiento correctivo sería más frecuente. Además, los sistemas descentralizados y locales son más propensos a la corrupción, ya que la administración y el personal de la prisión que tienen acceso al equipo tienen la posibilidad de facilitar la elusión de estos sistemas.

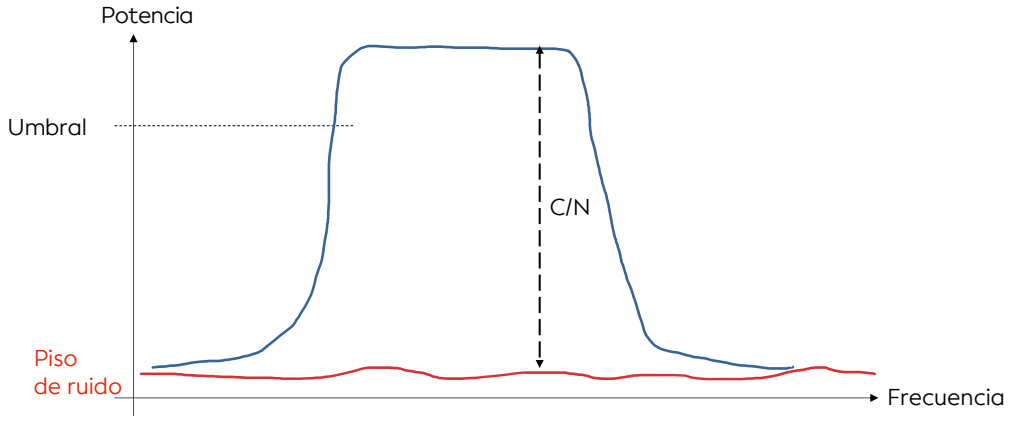
Teniendo en cuenta los desafíos mostrados, a continuación, se describen varias alternativas disponibles en el mercado y cómo se desempeña cada tecnología en relación con el propósito de bloquear las comunicaciones en las prisiones y los efectos no deseados relacionados con ellas.

# II. a INHIBIDORES

La alternativa más antigua, simple y utilizada al bloqueo de comunicaciones se conoce comúnmente como inhibidores o *jammers*. Esta tecnología ha existido desde los usos en la Segunda Guerra Mundial y más tarde desde el inicio de la telefonía móvil y ha sido ampliamente utilizada en la industria. El principio de funcionamiento de este sistema es interferir deliberadamente las señales inalámbricas en los equipos terminales, como los teléfonos móviles. El inhibidor emite una señal de radiofrecuencia (RF) en la banda deseada y con suficiente potencia, de modo que los terminales no pueden demodular la señal deseada (por ejemplo, la señal generada por una estación base celular) y, por lo tanto, no pueden establecer el canal de comunicación.

Es un principio operativo bastante simple y efectivo, pero por muy simple que sea, normalmente viene acompañado de varios efectos colaterales que afectan a otros, diferentes de los reclusos, quienes son los sujetos a los que se pretenden bloquear las comunicaciones no autorizadas. ¿Por qué sucede eso? En general, una señal inalámbrica tiene las características principales que los receptores necesitan para poder "entender" la señal. Estas son la potencia de la señal y la relación Portadora-Ruido (C/N). Para que un receptor demodule una señal, la señal debe tener más potencia que un Umbral definido y un mínimo de C/N, esta es la diferencia entre la potencia y el ruido en el ambiente, como se muestra en la siguiente figura.

**FIGURA 2**
Características básicas de una señal inalámbrica digital
Fuente: BNMC

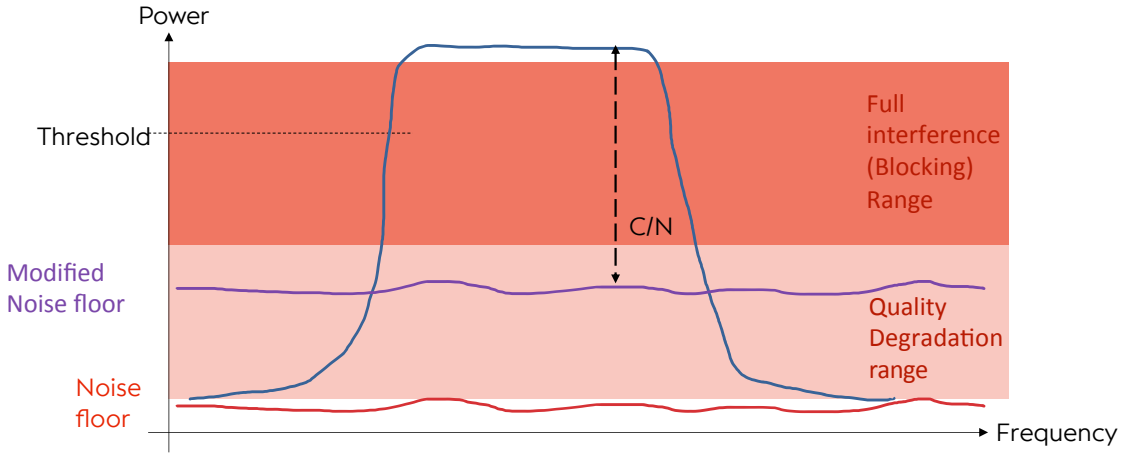


Cuando aparecen señales de interferencia en la zona donde se encuentra el receptor, el dispositivo "ve" o mide un aumento en el piso de ruido. A medida que el piso de ruido crece, la calidad del servicio comienza a degradarse y finalmente cuando el ruido supera cierto nivel, es decir que la relación C/N es demasiado pequeña, la interferencia es suficiente para bloquear el servicio.

**FIGURA 3**

Señal inalámbrica digital con interferencia

Fuente: BNMC

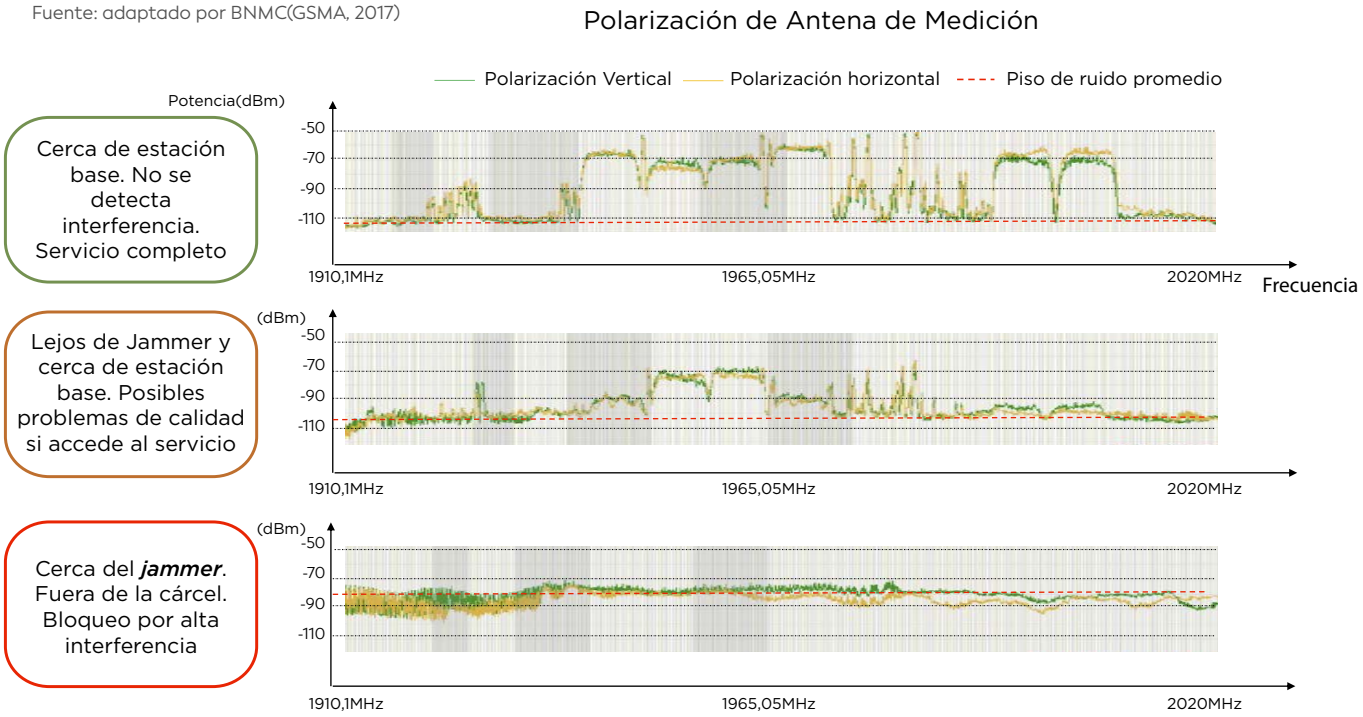



Las señales de RF generadas por los inhibidores están sujetas a todo el fenómeno y comportamiento de las ondas de radio, es decir, propagación, reflexión, refracción, dispersión y difracción, entre otros. La señal generada por el inhibidor pierde potencia a medida que se propaga lejos de la antena de origen y por la atenuación causada por los obstáculos. Por lo tanto, si el terminal móvil comienza a moverse lejos del inhibidor pasará de estar completamente bloqueado / interferido a tener algún tipo de servicio, pero con mala calidad y luego, idealmente fuera de la prisión, el dispositivo tendrá un servicio completo. La siguiente figura es una medición real que muestra el fenómeno descrito anteriormente.

**FIGURA 4**

Ejemplo de la vida real de mediciones de señal móvil con inhibidor de funcionamiento.

Fuente: adaptado por BNMC(GSMA, 2017)

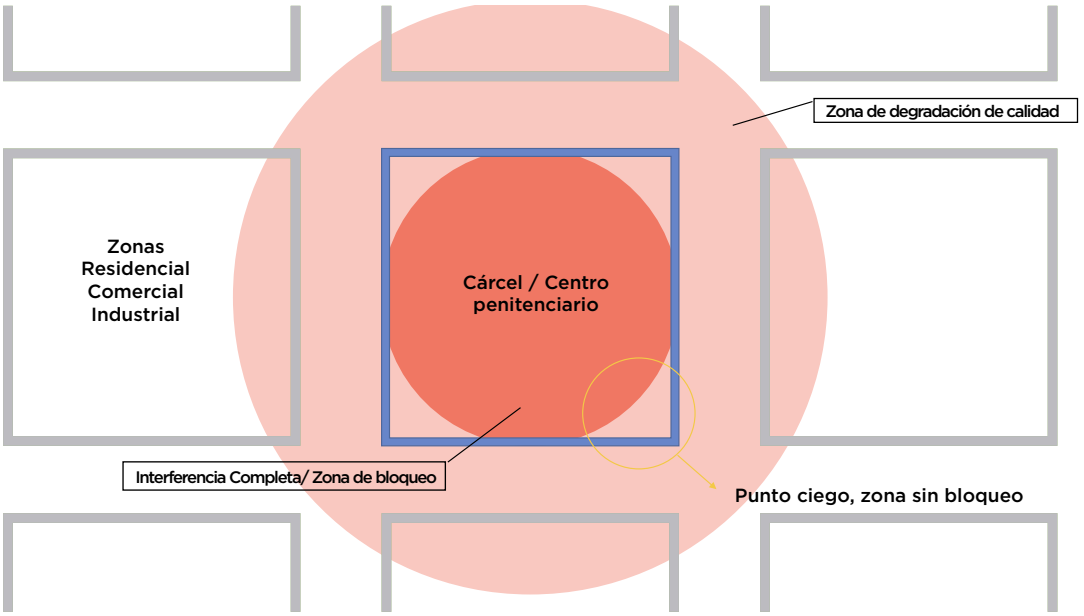


Controlar la propagación de la señal es bastante difícil, ya que su comportamiento físico no responde con nuestras fronteras deseadas, por ejemplo, el perímetro de una prisión. Las siguientes figuras muestran ejemplos simplificados de los efectos generados por los inhibidores en su implementación.

**FIGURA 5**

Interferencia de *Jammer* - Tratando de proteger a los vecinos de la prisión

Fuente: BNMC

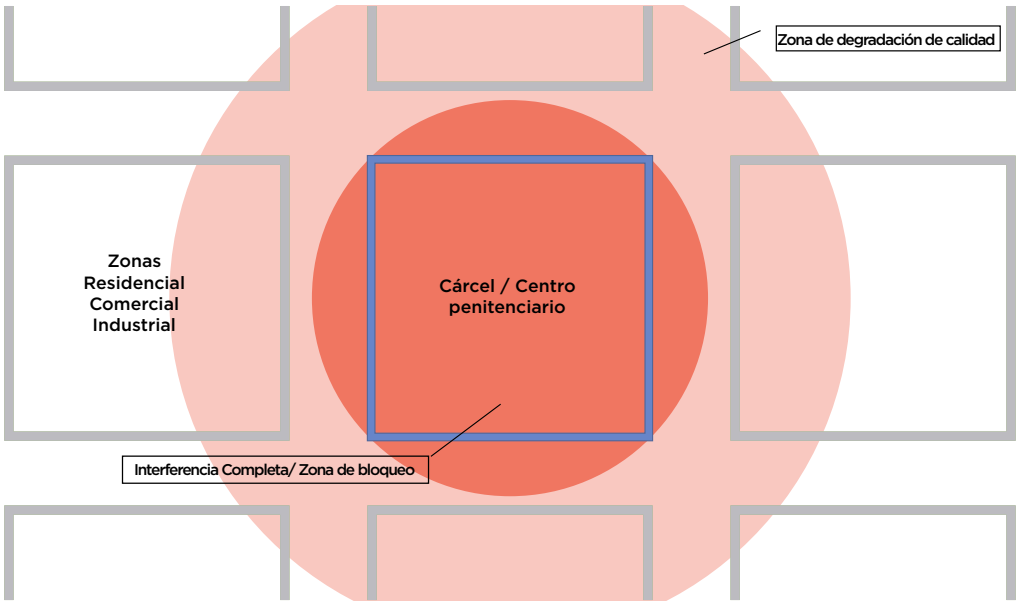



En la figura anterior, la potencia de la señal de interferencia se establece para evitar el bloqueo de señales fuera del perímetro de la prisión. Sin embargo, todavía hay una zona de degradación de calidad, ya que la potencia de la señal del inhibidor sigue siendo suficiente para generar interferencias, incluso si no es un bloque completo. Adicionalmente, debido a las características geométricas de los edificios y a la propia señal, aparecen zonas dentro de la prisión donde aún se permite el servicio o incluso zonas donde no podría haber interferencia alguna, si se consideran atenuaciones generadas por edificios, árboles, o cualquier otro posible obstáculo.

**FIGURA 6**

Interferencia del inhibidor - Tratando de bloquear completamente las instalaciones penitenciarias

Fuente: BNMC



En el anterior, se aumentó la potencia de la señal de interferencia para garantizar que se bloquee todo el perímetro de la prisión. Eso resulta en interferencias fuera del perímetro de la prisión y una mayor huella de la zona de degradación de la calidad. Obviamente, el despliegue real de inhibidores es más complejo, ya que podrían necesitarse varias antenas, lo que significa que se generan varias señales de interferencia, además de configuraciones geométricas irregulares de prisiones y edificios vecinos, y varias redes de telecomunicaciones y bandas de frecuencia en funcionamiento. Los inhibidores también requieren filtros de buena calidad, ya que su implementación debe evitar interferencias en otras bandas de frecuencias, donde funcionan servicios diferentes a los destinados a ser bloqueados.

Los efectos no deseados de los inhibidores han desencadenado su prohibición en algunos países y la imposición de normas estrictas en otros para proteger las comunicaciones legales y, al final, limitar su eficacia. Debido a las características técnicas de los inhibidores, los sistemas están compuestos por varios equipos o hardware dentro de las prisiones: generadores de señal para cada banda de frecuencia que quiere ser bloqueada y las antenas dependiendo del diseño de ingeniería detallado. Cada banda de frecuencia requeriría un diseño independiente y lo más probable es que los sistemas tengan huellas de cobertura diferentes, afectando a algunos servicios más que a otros.

Además, como estos sistemas requieren instalación de hardware dentro de cada locación, tanto los gastos de capital como los operativos aumentan por cada prisión, banda de frecuencias y ancho de banda de espectro que se bloquea. Además es más difícil y costoso operar y mantener implementaciones distribuidas geográficamente. Por último, como se mencionó anteriormente, el equipo en las instalaciones es propenso a ser inhabilitado o dañado tanto por los presos como por el personal o la administración en casos de corrupción.

Aunque los inhibidores son una solución de bloqueo eficaz, tienen varios efectos no deseados, como:

**i.** Los inhibidores pueden afectar las comunicaciones legales tanto dentro como fuera del perímetro de las instalaciones penitenciarias. Incluso los servicios esenciales están bloqueados, como las llamadas de emergencia.
**j.** Habrá una zona en la que los servicios no se niegan por completo, sino que están sujetos a una degradación de la calidad debido a señales de interferencia ligeramente débiles.
**k.** Los obstáculos en las implementaciones reales pueden generar puntos ciegos dentro de las prisiones donde las comunicaciones están completa o parcialmente disponibles. Además, el tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.
**l.** Los inhibidores de baja calidad son propensos a generar emisiones fuera de banda o espurias que podrían afectar a otros servicios de telecomunicaciones que no están destinados a ser bloqueados.
**m.** Requiere equipamiento local
**n.** No es posible monitorear el nivel de efectividad del sistema
**o.** No hay capacidad de auditoría para saber qué dispositivos fueron bloqueados
**p.** No hay capacidad para auditar u obtener datos para inteligencia en seguridad

Hay muchos proveedores que ofrecen inhibidores de RF en el mercado; ya que estos sistemas son la alternativa más utilizada. Algunos ejemplos son Enterprise Control Systems Ltd., HSS Development, WolvesFleet TechnologyCo., SESP Group, RF Technologies, Phantom Technologies, Digital RF, entre otros.

# II. b
# CAPTADORES DE IMSI

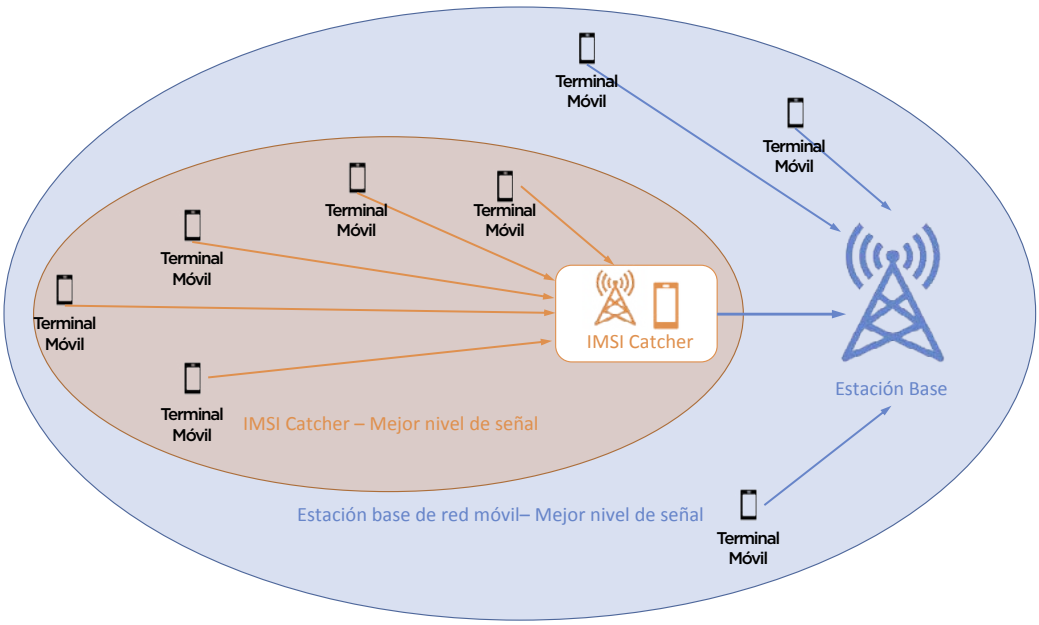
La Identidad Internacional de Suscriptor Móvil (IMSI) es un código numérico único asignado a cada suscriptor móvil en redes móviles en el mundo. El IMSI está compuesto de tres partes:

i. Código de país móvil (MCC): Tres dígitos que identifica el país de origen del abonado móvil.
ii. Código de red móvil (MNC): Dos o tres dígitos que identifica la red móvil local.
iii. Número de identificación de suscriptor móvil (MSIN): de nueve a diez dígitos que identifica cada suscriptor móvil único dentro de una red móvil.

Luego, IMSI Catchers en su comprensión más básica permite registrar el IMSI de los suscriptores definidos. Pero, ¿cómo lo hacen los receptores? Los IMSI Catchers aprovechan una característica técnica propia del terminal móvil, en la cual está constantemente comprobando qué estación base (BS) ofrece la mejor intensidad de señal para establecer la conexión entre este y la mejor estación base disponible. Usando esa característica, los IMSI catchers simulan ser una estación base para los terminales móviles en un área definida y ser una estación móvil (MS) o terminal móvil para la estación base real.

**FIGURA 7**
Interferencia del inhibidor - Tratando de bloquear completamente las instalaciones penitenciarias

Fuente: BNMC



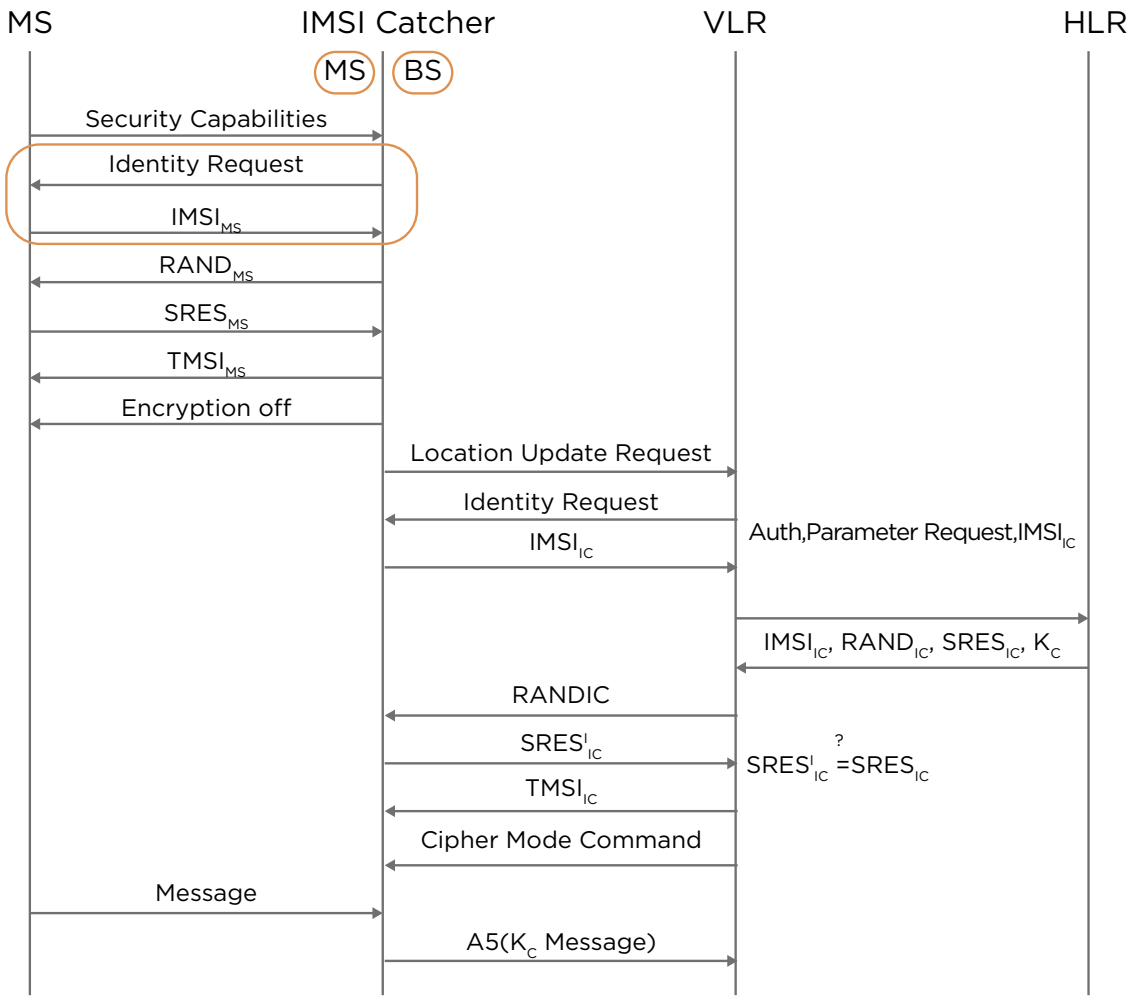

Cuando el termina móvil selecciona la mejor estación base por su intensidad de señal, se lleva a cabo el protocolo utilizado para autenticar al suscriptor. Este protocolo requiere al terminal móvil a proporcionar el IMSI a la red, pero no requiere que la estación base se autentique previamente en el terminal móvil. Esta característica del protocolo es lo que los receptores IMSI explotan para reemplazar a la estación base real y ser un filtro entre el terminal y la

red. A medida que el IMSI Catcher simula ser la estación base real, todos los terminales en su área de cobertura inician sesión en este sistema, pero no en la red de servicios de comunicaciones móviles real.

**FIGURA 8**

Ataque Man-in-the-middle con un IMSI Catcher

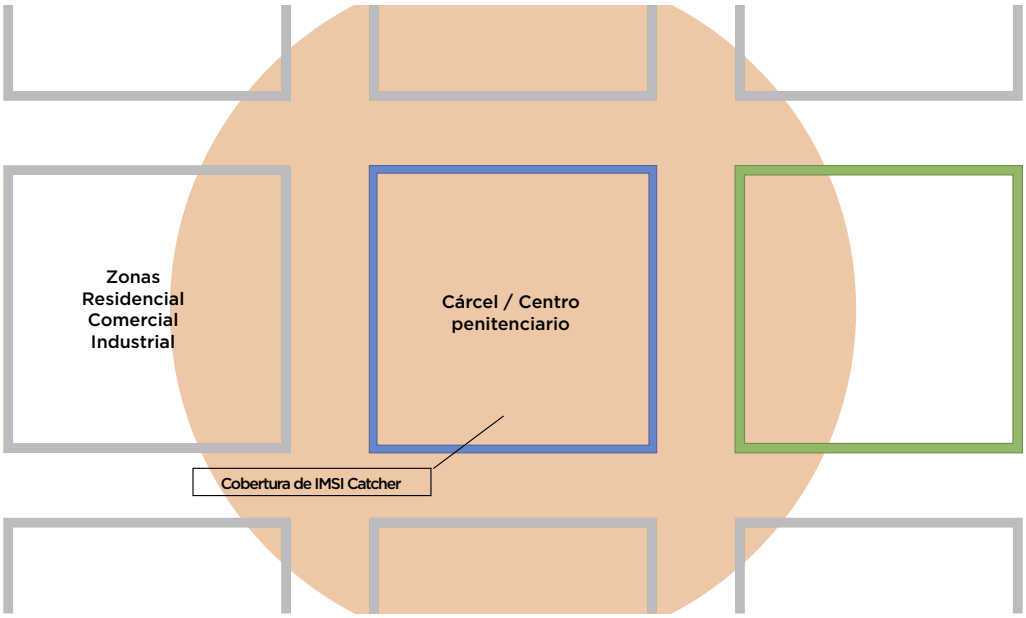
Fuente: adaptado por BNMC(Strobel, 2007)




La figura anterior muestra el protocolo de autenticación y cómo el receptor IMSI se hace pasar por una BS ante la estación móvil y como el terminal móvil (MS) ante la red. Cada terminal móvil en la huella de cobertura del IMSI catcher lo seleccionará como la mejor BS, por lo tanto, se llevará a cabo el proceso de registro en dicho sistema. El IMSI Catcher, entonces, podrá redirigir esas conexiones los terminales móviles a través de sí mismo a nada, lo que lleva al bloqueo deseado en el caso de prisiones. También permite interceptar la comunicación de un IMSI seleccionado o puede usarse para fines de ubicación.

**FIGURA 9**
Huella de cobertura de IMSI Catcher

Fuente: BNMC




Aunque el IMSI Catchers genera una señal en la misma banda de frecuencia del servicio móvil, la forma en que funciona, simulando ser una estación base y un terminal móvil, y con la coordinación adecuada, la posible interferencia sobre la red comercial no es el problema principal. La implementación de IMSI Catchers para bloquear las comunicaciones es bastante simple. Estos dispositivos deben configurarse para ser vistas como las mejores estaciones base por su nivel de intensidad de señal en todo el perímetro de la prisión, debe considerarse un sistema al menos para cada operador y banda de frecuencia, y los dispositivos dentro del área de cobertura se conectarán al receptor y no se les permitirá comunicarse. Sin embargo, hay algunos efectos no deseados de las debilidades de estos sistemas.

**a.** Es probable que afecte a las comunicaciones legales. Una vez más, la operación se basa en la emisión de una señal radioeléctrica, que como se ha visto antes se propaga y está sujeta a todos los efectos naturales relacionados con las ondas. Debido a eso, es posible tener puntos ciegos dentro de las instalaciones para que los dispositivos reconozcan el BS real y se conecten directamente a él, evitando el receptor.
**b.** Otra consecuencia relacionada con la naturaleza de las señales radioeléctricas es que habrá zonas fuera de la prisión con una mejor intensidad de señal del IMSI Catcher que de los BS de la red. Por lo tanto, los dispositivos ubicados fuera de la prisión y dentro de la huella efectiva del receptor también serán bloqueados.
**c.** Como el funcionamiento del IMSI Catcher requiere el intercambio de información con los terminales de los usuarios, hay algunos comportamientos inusuales que se pueden utilizar para identificar que hay un sistema de este tipo. Algunos ejemplos son: uso de frecuencias fuera de banda, identificador de estación base inusual, capacidades no existentes y parámetros de red como GPRS o EDGE deshabilitados, ausencia de cifrado, falta de información, entre otros. Esta debilidad es explotada por contramedidas, tanto como hardware especializado que prioriza el cifrado y puede alertar al usuario de la presencia de un IMSI Catcher
**d.** La "captura" se vuelve más difícil a medida que las tecnologías IMT evolucionan e implementan sistemas de cifrado más complejos.
**e.** Estos sistemas requieren instalación local, por lo que la escalabilidad es

difícil y los costos de OA&M son altos. También son propensos a daños o inhabilitaciones por parte de los reclusos o el personal corrupto o la administración. El tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.

**f.** Los captadores IMSI permiten la interceptación, que puede generar información valiosa, pero normalmente estas actividades requieren autorización legal. Esta capacidad concierne a aquellos que no están encarcelados y puede verse afectada por los captadores de IMSI.

**g.** La mayoría de los receptores IMSI trabajan solo con 2G, lo que limita severamente su efectividad.

Los IMSI Catchers son ofrecidos por varias empresas en el mercado. Tal vez el más famoso es el Harris Corp Stingray, que incluso se convirtió en una especie de nombre estándar para los receptores. Otras empresas como Rohde & Schwarz, Digital Receiver Technology, Inc., Meganet Corporation, Gamma Group, Septier, PKI, entre otras.

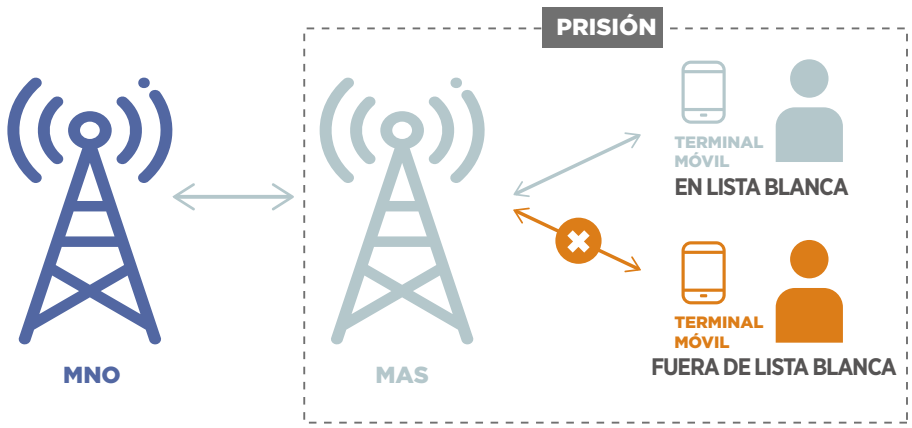
# II. c
# SOLUCIONES DE GESTIÓN DE ACCESO (MAS)

Las Soluciones de Gestión de Acceso (MAS, por sus siglas en inglés) funcionan de manera similar a los IMSI catchers, pero los sistemas MAS no reemplazan a ningún equipo o elemento de red. Un MAS es, básicamente, una pequeña porción de la red móvil dedicada a proporcionar el servicio a una ubicación pequeña y definida, como una prisión. Esta parte de la red puede ser operada por el MNO o un tercero con este enfoque especial, normalmente dependiendo de las regulaciones locales donde el subarrendamiento del espectro está o no permitido.

Una vez establecido el MAS, se debe definir una lista blanca con los suscriptores autorizados a tener acceso a las comunicaciones. El MAS solo permitirá las comunicaciones a los suscriptores de la lista y bloqueará a cualquier otro suscriptor que intente iniciar una comunicación.

**FIGURA 10**
Diagrama básico de MAS

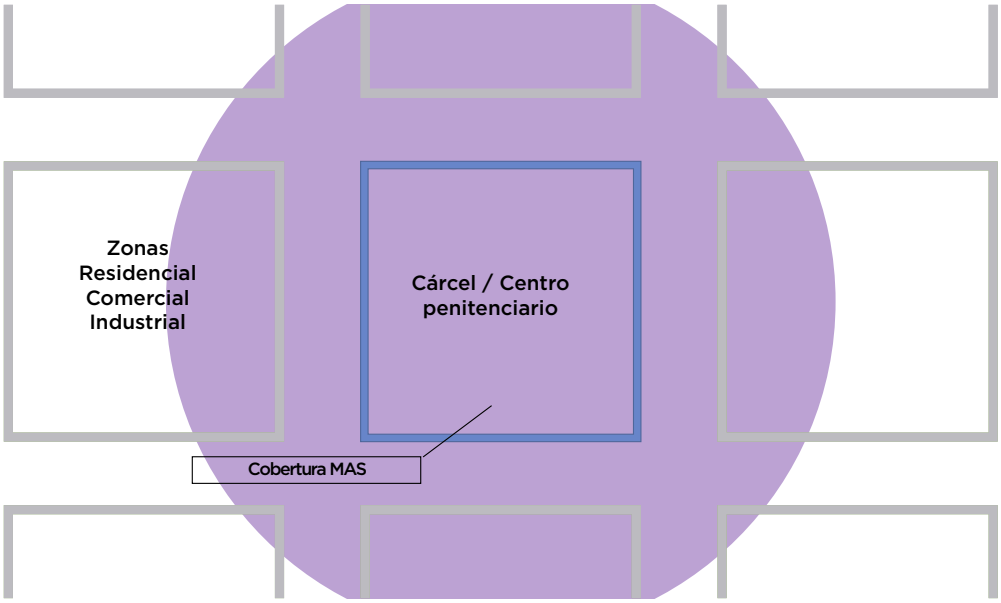
Fuente: BNMC



Este concepto es bastante simple, un MNO o un tercero define una red móvil local que tiene una lista de *"llamadas" permitidas* y todos los que están fuera de la lista no pueden acceder al servicio. Pero nuevamente, este método depende de la emisión de señal, por lo que el sistema se ve afectado por el comportamiento de las ondas radioeléctricas. El sistema puede tener puntos ciegos dentro de las instalaciones penitenciarias que permiten que los terminales móviles se conecten directamente al MNO o la huella puede ir más allá de las fronteras de la prisión, por lo tanto, los residentes de la región deben ser introducidos como suscriptores permitidos, pero siempre existe el riesgo de negar el servicio a las personas que intentan comunicaciones legales.

**FIGURA 11**
Huella de cobertura MAS

Fuente: BNMC




Los sistemas MAS también tienen elementos no deseados de la siguiente manera:

**a.** Los sistemas MAS podrían interrumpir los servicios a personas fuera de las prisiones que no están incluidas en la lista blanca.
**b.** Los sistemas MAS son capaces de interceptación o vigilancia, lo que genera preocupaciones legales, especialmente cuando son operados por terceros.
**c.** Como el sistema funciona como parte de la red, requiere coordinación de frecuencia con el MNO para evitar interferencias, lo que afecta el diseño normal de la red. Requiere subarrendamiento del espectro, que no está permitido en todos los países.
**d.** Los MAS forman parte de la red; el sistema debe actualizarse a medida que las redes evolucionan y se enfrentan a contramedidas.
**e.** La instalación en las instalaciones es propensa a daños o inhabilitación por parte de los reclusos o el personal o la administración corruptos. El tamaño y la geometría de la prisión pueden aumentar los costos de implementación a medida que el diseño se vuelve más complejo.
**f.** Los sistemas MAS generalmente solo son aplicables para escenarios específicos, principalmente en áreas remotas con población general o cobertura celular existente.
**g.** El diseño e implementación del sistema MAS tiene una alta complejidad que implica más costos de inversión y operación en comparación con otras soluciones.

# II. d
# APRENDIZAJE AUTOMÁTICO (ML) Y SOLUCIONES BASADAS EN GEOLOCALIZACIÓN

Todas las opciones tecnológicas analizadas anteriormente tienen efectos no deseados que limitan su efectividad e interrumpen las comunicaciones legales que no son objeto del bloqueo. Además, estas opciones requieren el despliegue de equipamiento en cada una de las instalaciones de los centros penitenciarios lo que hace que sea más difícil de escalar, operar y mantener y vulnerable al sabotaje o el daño por parte de los reclusos o el personal de la prisión en casos de corrupción. Algunos de ellos son generadores de interferencias y los otros requieren una estrecha coordinación con los MNO para el diseño y la gestión. Por último, la mayoría de las soluciones son sensibles a la tecnología y, a medida que las IMT evolucionan, exigen más inversiones para nuevas implementaciones.

Como alternativa a esas opciones, las soluciones basadas en la geolocalización de dispositivos en las redes inalámbricas y algoritmos de aprendizaje automático ofrecen un enfoque diferente para resolver el problema. Este tipo de sistemas funciona apoyado en los servicios de localización (LCS, por sus siglas en inglés) estandarizados para redes móviles, minimizando las inversiones en equipamiento, eliminando interferencias y elementos de radio frecuencias y, lo más importante, protegiendo las comunicaciones legales, minimizando la posibilidad de negar comunicaciones a ciudadanos no destinados a ser bloqueados.

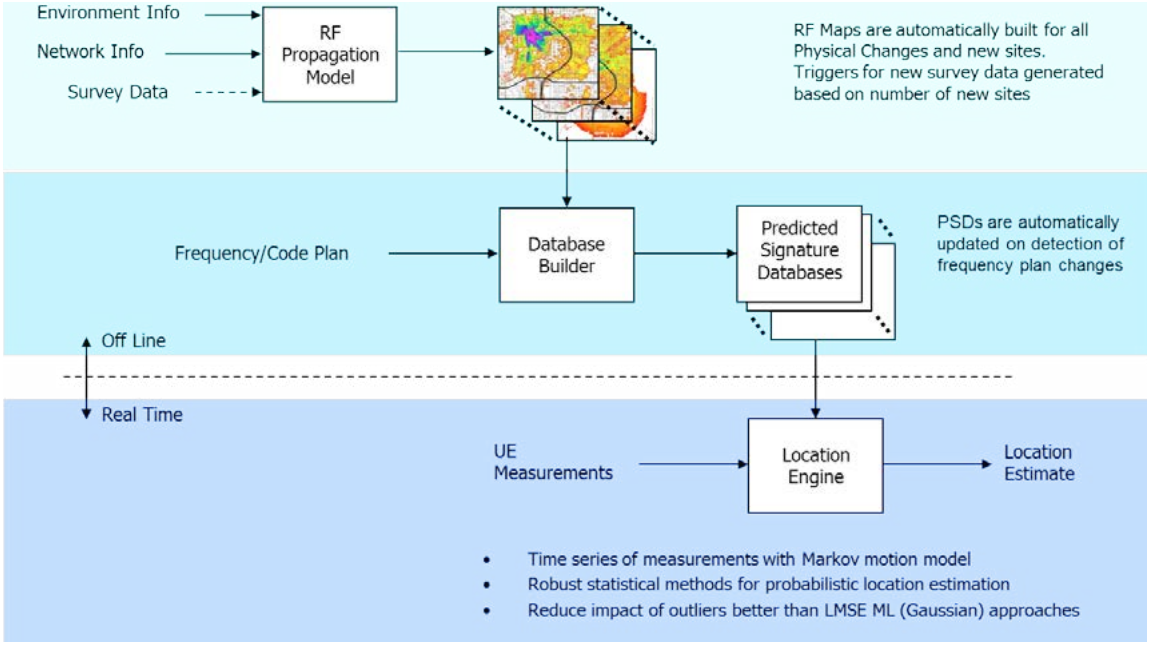
El concepto detrás de estas soluciones es bloquear las comunicaciones a los dispositivos ubicados dentro de los perímetros de la prisión sin emitir señales de RF que puedan afectar a las comunicaciones de las personas que no están destinadas a ser bloqueadas y a la operación normal de las redes de telecomunicaciones. Puede combinar servicios de geolocalización, listas blancas y registros de actividad en la red para bloquear a los suscriptores que no están en una lista blanca, los que están en una lista negra y los que reportan actividad dentro de los perímetros de la prisión. Los sistemas de localización específicamente son ofrecidos por varios fabricantes, utilizando diferentes tecnologías de localización o una combinación de estas. En el mercado están Ericsson, Nokia, Huawei, Comtech, Verint, Mobiliaris, Polaris Wireless, entre otros.

Polaris *Wireless* desarrolló una solución basada en software compuesta por una plataforma de localización y un sistema para el bloqueo del servicio de comunicaciones no autorizadas en las prisiones sin requerir la emisión de ningún tipo de señal inhibidora. La solución de bloqueo de llamadas en prisiones se basa en la tecnología patentada de Polaris *Wireless* denominada *Wireless* Location Signatures (WLS). Esta tecnología se utiliza en otras

soluciones de Polaris *Wireless* centradas en la localización de alta precisión, por ejemplo, para ser utilizadas en sistemas de llamadas de emergencia o aplicaciones de seguridad nacional. La información del entorno geográfico y la red de comunicaciones móviles se combinan utilizando algoritmos patentados para producir mapas de propagación de señales de radiofrecuencias y una base de datos de predicción de "firmas", es decir, una seña o identificación única de cobertura que tendría cada unidad geográfica de análisis dentro del área objetivo. La geolocalización del dispositivo móvil se genera mediante el uso de los reportes de medición en tiempo real que el terminal del usuario reporta a la red junto con la base de datos de firmas a través de modelos matemáticos complejos para desarrollar la estimación de alta precisión de la geo-localización del usuario.

**FIGURA 12**
Componentes de la tecnología WLS

Fuente: (Polaris Wireless, 2022)

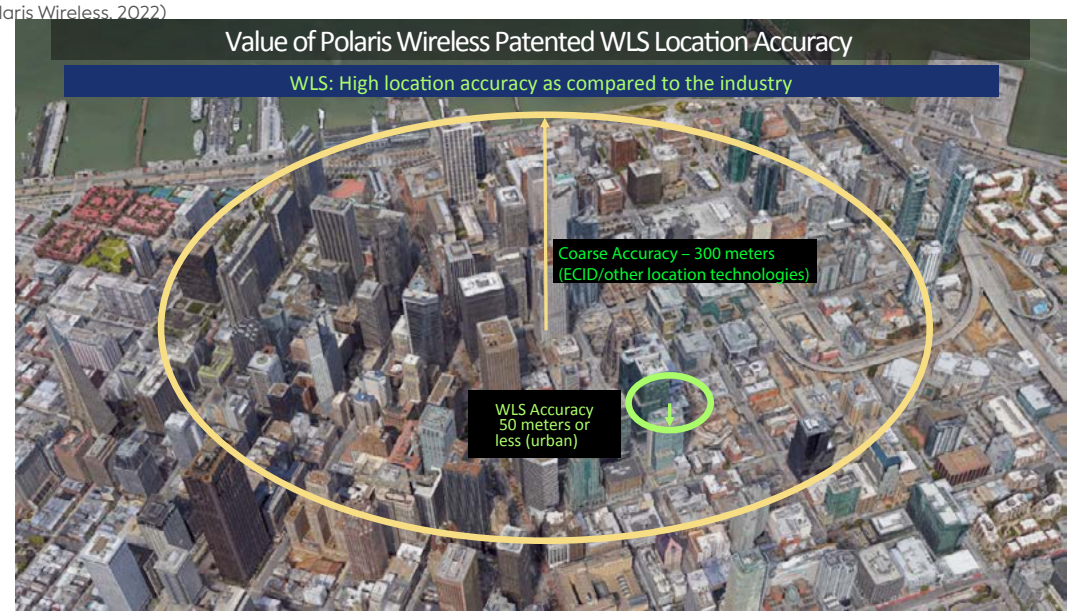



Esta herramienta de localización está 100% basada en software y ofrece una precisión de 50 metros o mejor en un entorno urbano. Debido a que está basada en software, la solución no necesita ninguna nueva infraestructura de hardware, ni ningún software o hardware especial en el teléfono y es compatible con futuros desarrollos tecnológicos. La tecnología WLS está presente en la plataforma de ubicación OmniLocate y utiliza información estándar que es constantemente medida y reportada por los terminales de usuario (UE) en las redes 2G, 3G, 4G y 5G[1] y sus sensores para calcular la ubicación del dispositivo. La plataforma OmniLocate se conecta con el núcleo de red de los MNO utilizando interfaces 3GPP estándar para todas las tecnologías de radio. La tecnología cumple y excede los requisitos del Mandato de la FCC de los Estados Unidos de 2021 sobre la precisión en los sistemas de localización para la línea de emergencia E911.

1. 5G está en desarrollo.

**FIGURA 13**
Precisión de ubicación de WLS

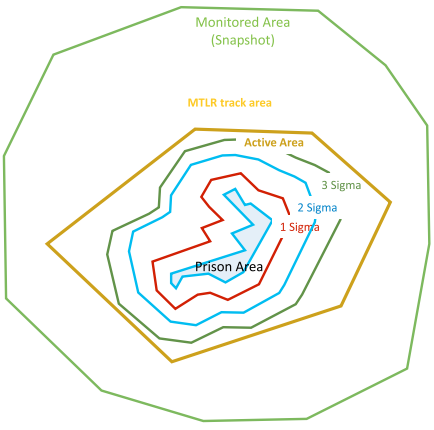
Fuente: (Polaris Wireless, 2022)




En relación con la solución de bloqueo de llamadas en prisiones, el sistema utiliza la plataforma OmniLocate para localizar y rastrear los dispositivos móviles dentro y alrededor de los perímetros de la prisión, luego utiliza Inteligencia Artificial (IA) para realizar análisis heurísticos de ubicaciones, que permite al sistema decidir si bloquea un dispositivo y por cuánto tiempo. Es decir, el sistema utiliza la geolocalización de alta precisión y el análisis de los 'hábitos o patrones' registrados de un dispositivo de usuario para decidir bloquear las comunicaciones de ese terminal en específico, considerando la probabilidad de ser ilícito dentro de la prisión y, como vamos a ver a continuación, utiliza herramientas de gestión de red para minimizar el impacto en los vecinos o población cercana a los centros penitenciarios, a diferencia de los inhibidores que producen bloqueos generales. Además, como utiliza la IA para decidir, el desempeño del sistema mejora con el tiempo ya que puede aprovechar el conocimiento adquirido del comportamiento de los terminales de usuarios. La ubicación y el seguimiento son elementos clave del sistema más que la frecuencia o la red a la que está asociado, como sucede en otras tecnologías. Para aprovechar estas características, la solución de bloqueo de llamadas en prisiones se requiere la definición de geo-cercas que ayudan al sistema a tomar decisiones.

**FIGURA 14**
Geocerca - Geometría de la prisión

Fuente: (Polaris Wireless, 2022)



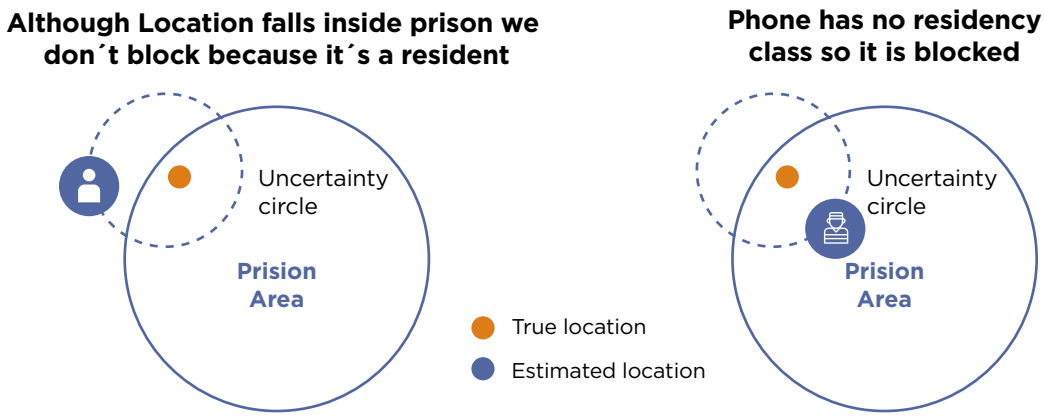

La cerca interior se corresponde con el perímetro de la prisión, que es el área principal de interés, porque cualquier dispositivo "desconocido" dentro de la cerca debe ser bloqueado. El perímetro más lejano es el Área Monitoreada, sobre la cual la aplicación de bloqueo de servicio solicitará al OmniLocate compartir los eventos de la red. Luego, a medida que los dispositivos se acercan a la prisión y entran en el Área Activa, se vuelven de interés y se habilita la Solicitud de Ubicación de Terminal Móvil (MTLR, por sus siglas en inglés) para que el sistema pueda aprender sobre la ubicación y el comportamiento. Finalmente, las áreas sigma están asociadas con el rendimiento del sistema de ubicación y definen la frecuencia con la que el sistema localiza el dispositivo, haciendo que el 1- sigma sea la prioridad más alta y tenga la tasa de actualización más exigente.

Cuando un dispositivo está lo suficientemente cerca del perímetro de la prisión, el sistema tendrá que decidir bloquear la comunicación. Como en todos los sistemas, hay una tasa de error. Sin embargo, la IA permite la mejora debido a que la mayoría de los casos de falsos positivos pertenecerán a residentes conocidos en la zona, por lo que se agregará otra condición a los criterios de bloqueo y se comprobará si es residente o no.

**FIGURA 15**

Aprendizaje y clasificación de la Inteligencia Artificial

Fuente: (Polaris Wireless, 2022)

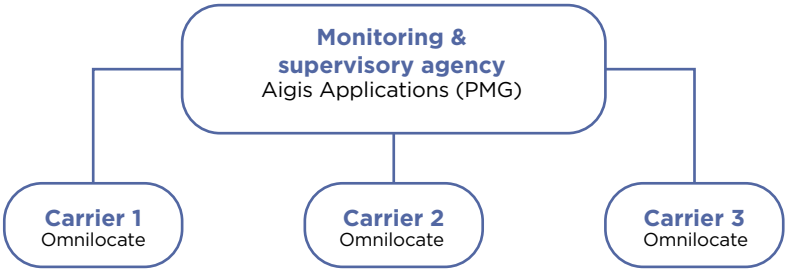



La implementación de Polaris *Wireless* - Prison Call Blocking es muy simple, comparada con las otras alternativas mencionadas en este documento. Dos razones principales son: i) Es una solución basada en software; ii) no hay necesidad de desplegar equipo local. Es un enfoque diferente, que tiene ventajas adicionales: el sistema es fácilmente escalable, solo debe definir tantas geo-cercas como sea necesario; no se necesita equipamiento en las instalaciones de las prisiones por lo que se eliminan los riesgos de sabotaje o daño; y el sistema está centralizado, por lo que los gobiernos pueden tomar el control directo del mismo, minimizando la propensión a la corrupción. Además, esta solución no implica costos operativos para los MNO asociados con las actividades de ingeniería y planeación de radiofrecuencias para ajustar su red a la operación de una señal interferente, además de pruebas de campo y el monitoreo para no proporcionar servicio en las áreas penitenciarias y / o actividades de coordinación con la Institución Penitenciaria. Cualquier cambio en el plan de frecuencia se actualiza fácilmente en la solución sin ninguna actualización adicional de hardware o firmware. Significa esto que los MNO pueden diseñar la red de acceso radioeléctrico para la prestación de servicios en cualquier lugar y el diseño no se ve afectado por la implementación de la solución de bloqueo de servicio en cárceles, como sucede en el caso de cualquier otra alternativa que funcione con base en señales de RF.

**Figura 16**

Solución de bloqueo de llamadas a prisión - Arquitectura básica

Fuente: (Polaris Wireless, 2022)

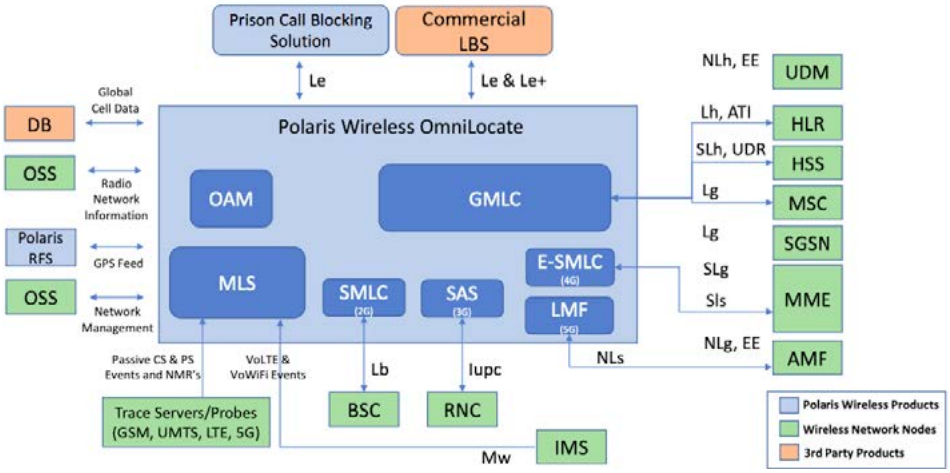


El diagrama anterior muestra que el sistema solo requiere una integración al MNO y/o a los Operadores de Red Móvil Virtual (MVNO) que tengan un núcleo de red móvil independiente del MNO y, a través de software, las geo cercas se definen para las instalaciones penitenciarias deseadas. Entonces, ¿qué requiere la solución de bloqueo de llamadas a la prisión de los MNO? La respuesta se basa en el estándar de redes móviles 3GPP, es decir, la solución utiliza interfaces, protocolos e información totalmente estandarizados, que son accesibles al núcleo de red del MNO. Por lo tanto, las inversiones del lado de la red se reducen al mínimo.

**Figura 17**

Arquitectura de referencia de polaris *Wireless* Solutions (2G, 3G, 4G, 5G-SA, VoLTE y VoWiFi)

Fuente: adaptado por BNMC(Polaris Wireless, 2022)




Polaris *Wireless* OmniLocate utiliza los servicios de ubicación Serving Mobile Location Center (SMLC), Stand Alone SMLC (SAS), Enhanced Serving Mobile Location Center (E-SMLC) y Location Management Function (LMF) definidos por 3GPP para tecnologías de generación móvil 2G a 5G. Estos bloques obtienen información de localización de la red y la plataforma OmniLocate la procesa para obtener la alta precisión prometida por la solución. También utiliza el Home Location Register (HLR) para tener acceso a la información de cada suscriptor en la red móvil respectiva y poder identificar a cada uno de ellos.

Luego, la información se envía a la Solución de Bloqueo de Servicios en Prisiones donde la IA decide qué dispositivos deben bloquearse en función de la localización, el comportamiento, entre otros. Finalmente, los comandos vuelven al Home Location Register (HLR) y al Equipment Identity Register (EIR) de la red para bloquear el servicio en estos dispositivos, de la misma manera que un suscriptor sin crédito para usar el servicio. Esta última característica ayuda a permitir llamadas de emergencia garantizando así la seguridad de todos los ciudadanos.

Para tener una correcta integración con la red móvil, los operadores deben garantizar el acceso a:

- **a.** Interfaces de programación de aplicaciones (API) tanto para HLR como para EIR para el bloqueo del servicio en tiempo real[2].
- **b.** Integración al OSS para la notificación en tiempo real de cualquier cambio en la red de radio; cambios en el plan de RF, modificaciones o adiciones de nuevas estaciones base celulares.
- **c.** Integración al OSS para datos de eventos de seguimiento en tiempo real de la red.
- **d.** Habilitación de licencias de servicios de ubicación (LCS) en la red para activar MTLR.

2. Operator Determined Barring (ODB) permite al operador de red o proveedor de servicios regular, mediante un procedimiento excepcional, el acceso de los abonados a los servicios GSM. (ETSI - Instituto Europeo de Normas de Telecomunicaciones, 1995)

**Figura 18**
Blocking Service Application - Interfaz de usuario

Fuente: (Polaris Wireless, 2022)

El organismo de vigilancia y supervisión tendrá acceso a la Aplicación de bloqueo del servicio, con una interfaz de usuario amigable, que permite:

**i.** Definir el perímetro de la prisión como una geo-cerca para el monitoreo. Tanto como sea necesario.
**ii.** Ventana de alertas para ver teléfonos celulares recién descubiertos dentro del perímetro de la prisión.
**iii.** Observar, en tiempo real, en un mapa todos los teléfonos móviles dentro y alrededor del perímetro de la prisión.
**iv.** Si es necesario, permita que el método bloquee / desbloquee manualmente un teléfono móvil
**v.** Reproduzca la historia de los teléfonos móviles dentro y alrededor del perímetro de la prisión.
**vi.** Buscar datos históricos de teléfonos móviles.
**vii.** Informes de actividad.
**viii.** Se pueden admitir múltiples aplicaciones simultáneas. Esto permite que varios usuarios monitoreen uno o más perímetros de la prisión.

En resumen, Polaris *Wireless* - Prison Call Blocking Solution ofrece un nuevo enfoque, utilizando innovación tecnológica para proporcionar una solución altamente efectiva, elimina los efectos no deseados de las otras alternativas descritas y produce información relevante para inteligencia en seguridad pública. Algunas de las mejores características de la solución son:

**g.** Alta precisión de ubicación para bloquear teléfonos dentro de la prisión. La tecnología patentada WLS permite al sistema identificar y localizar los dispositivos con alta precisión. Con la ubicación de los dispositivos, el comando de bloqueo es selectivo y no afecta a otros usuarios.
**h.** Monitoreo y control centralizado para múltiples prisiones. La implementación no requiere instalación local, lo que reduce el CAPEX y el OPEX, simplifica los mantenimientos y permite una fácil escalabilidad. También reduce la propensión a la corrupción.
**i.** Inteligencia en tiempo real para proporcionar información valiosa y procesable, identificando dispositivos específicos utilizados dentro de las prisiones, horas de uso, fechas de actividad de los dispositivos, entre otros.
**j.** Monitoreo avanzado con informes históricos y capacidad de auditoría.
**k.** Características de software configurables y personalizables para cumplir

con las necesidades del país y las leyes locales.

l. Bloqueo de llamadas en tiempo real con opción de incluir en la lista blanca números de teléfono de confianza.

m. Seguro y a prueba de manipulaciones, ya que está integrado en la red del operador.

Debido a la naturaleza de la solución, puede ofrecer mucha información de inteligencia además de las capacidades de simplemente bloqueo. Este tipo de información puede ser utilizada con fines de seguridad e investigación criminal, que al final es el verdadero interés detrás del control sobre las comunicaciones en las cárceles.

Finalmente, hay otra ventaja importante que debe destacarse, incluso cuando no es el propósito de este documento, y es que como la Solución de Bloqueo de Llamadas a Prisión funciona apoyada en la plataforma OmniLocate, permite otras soluciones con fines comerciales y de seguridad pública.

# II. e
# COMPARACIÓN DE COSTOS

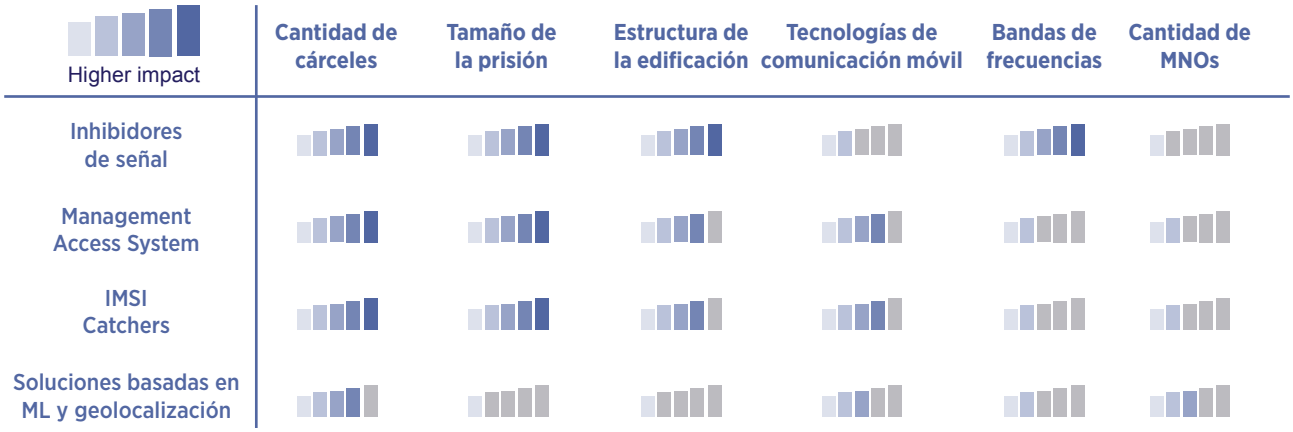
Un aspecto clave de las alternativas técnicas analizadas en este documento es el costo asociado con la implementación de la solución y la operación y mantenimiento anual. En primer lugar, es importante tener en cuenta que existen diferencias en la estructura de costos de estas alternativas. Si bien las soluciones soportadas en hardware específico a desplegar en cada prisión son más exigentes en CAPEX, las soluciones basadas en software permiten un modelo de Software-as-a-Service (SaaS) con una inversión inicial reducida en servidores genéricos y servicios de integración; lo cual significa que los costos están asociados principalmente con el OPEX.

Aunque el costo en todos los casos depende del número de prisiones a cubrir, el costo de las soluciones basadas en la transmisión de señales de radiofrecuencia dependen significativamente de las condiciones específicas de los edificios en cada área objetivo, es decir, el tamaño de las prisiones, el tipo de material y el ancho de las paredes, la distribución arquitectónica, la altura del edificio, etc. El costo de los inhibidores también depende de las bandas de frecuencias utilizadas para los servicios de telecomunicaciones, es decir, más bandas de frecuencia habilitadas en un país requieren más filtros, amplificadores y antenas para evitar llamadas ilegales a través del canal de espectro que no se están inhibiendo. Las soluciones del tipo MAS e IMSI Catchers buscan proporcionar la mejor intensidad de señal y, aunque no es necesario cubrir todas las bandas de frecuencias disponibles, el costo también involucra las tecnologías para comunicaciones móviles (es decir, 2G, 3G, 4G, 5G, etc.) que deben ser compatibles. Finalmente, el principal factor que determina el costo asociado con la solución basada en Machine *Learning* y geolocalización es el número de prisiones y, en un nivel menor, la cantidad de Operadores de Redes Móviles y tecnologías móviles debido a la plataforma OmniLocate instalada dentro de las instalaciones de cada MNOs. El costo no se ve afectado por el tamaño de las prisiones o las características estructurales de la edificación, ni por la existencia o el cambio en las bandas de frecuencias, lo que es una ventaja sobre las otras soluciones descritas en las secciones anteriores.

**Figura 19**

Comparación de factores que impactan el costo de la solución de bloqueo de comunicaciones

Fuente: BNMC

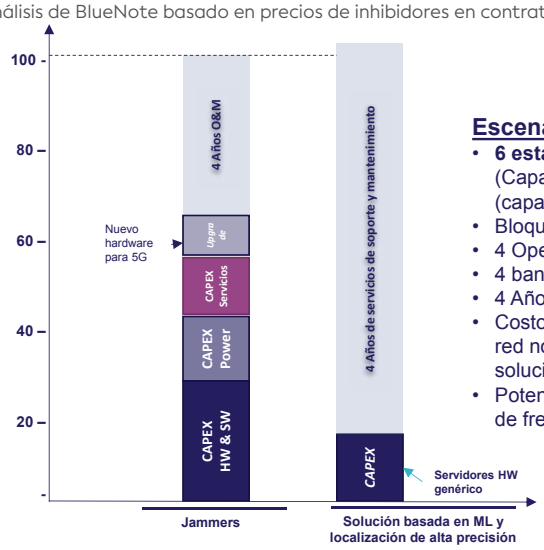



Debido a las diferencias en la estructura de costos entre las alternativas técnicas analizadas, no es posible hacer una comparación directa entre ellas. Sin embargo, bajo un escenario de implementación específico, podemos concluir que las soluciones basadas en geolocalización, soportadas en la tecnología de Polaris, tienen un Total Cost Ownership (TCO) comparable con soluciones de inhibición o *jammers*, pero con un rendimiento mucho mejor y más características.

**Figura 20**

Comparación del TCO relativo entre los inhibidores y la solución basada localización y ML

Fuente: Análisis de BlueNote basado en precios de inhibidores en contratos públicos (Colombia) y estructura de costos de Polaris Wireless




**Escenario de despliegue**:

- **6 establecimientos carcelarios**: 3 de tamaño medio (Capacidad aprox. de 2.000 reclusos) y 3 de gran tamaño (capacidad aprox. de 4.000 reclusos).
- Bloqueo de Comunicaciones para redes **2G, 3G y 4G**
- 4 Operadores de red móvil
- 4 bandas de frecuencias
- 4 Años de operación y mantenimiento o soporte
- Costos operativos de los MNOs para ingeniería de RF en su red no incluidos en el caso de jammers (no aplica para solución basada en localización)
- Potencial despliegue de tecnología 5G en una nueva banda de frecuencias

**Notas:** *Los precios de Polaris no se ven afectados por las nuevas tecnologías o una nueva banda de frecuencias. Las actualizaciones de software están incluidas en el precio anual de los Servicios

En el caso de la solución de interferencia, el costo anual de operación y mantenimiento incluye repuestos, mantenimiento preventivo y correctivo, incluido el trabajo de campo dentro de las prisiones, monitoreo y solución de problemas del sistema y mediciones de radiofrecuencia alrededor de las prisiones, pero no incluye la ingeniería de RF de los MNO para ajustar el diseño de la red para la restricción de la señal o la mitigación de la interferencia dañina de los inhibidores. También consideramos que una nueva banda de frecuencias para desplegar tecnologías 5G podría ser habilitada al mercado en el período de 4 años.

Por otro lado, el costo de operación y mantenimiento de la solución basada en ML y localización corresponde a los servicios de mantenimiento y soporte de licencias de software proporcionados por el proveedor, incluida la actualización del software para admitir una nueva tecnología o banda de frecuencia, así como la calibración periódica del modelo de propagación. Es importante tener en cuenta que esta solución no requiere una alta inversión en hardware específico lo que mitiga el riesgo financiero en caso de que la solución no satisfaga los requisitos.

# II. f
# CONCLUSIONES

El documento evalúa varias alternativas al problema del bloqueo de comunicaciones dentro de las instalaciones penitenciarias, *Jammers*, IMSI Catchers, Soluciones de Acceso Administrado y soluciones basadas en Inteligencia Artificial. Cada una de estas alternativas tiene un nivel de efectividad diferente y algunos efectos no deseados de su implementación. Ahora en adelante, se presenta una tabla de comparación, de modo que la evaluación ayuda al lector a identificar la mejor solución disponible para adaptarse a sus necesidades o intereses.

**Cuadro**
Matriz de evaluación de la tecnología
Fuente: BNMC

| | Jammers | Captadores IMSI | Soluciones de acceso administrado | Soluciones basadas en la ubicación |
|---|---|---|---|---|
| Efectividad | ★★★☆ Afectado por las características de las redes de radio | ★★★☆ Afectado por las características de las redes de radio | ★★★☆ Afectado por las características de las redes de radio | ★★★★ Bloqueo como un componente de red, dependiendo servicio suscriptor |
| Escalabilidad | ☆☆☆☆ Cada prisión es un despliegue completamente nuevo | ☆☆☆☆ Cada prisión es un despliegue completamente nuevo | ★★☆☆ Cada prisión es un despliegue completamente nuevo, pero la coordinación del operador ya está demostrada | ★★★★ Cada prisión solo requiere una nueva gran carga y una configuración de software |
| Protege las comunicaciones comerciales | ☆☆☆☆ Interfiere la señal, bloquea a los vecinos. Diseño de RF complejo | ★★☆☆ Bloquea a los vecinos en el área de cobertura. Diseño de RF complejo | ★★★☆ Bloquea a los vecinos en el área de cobertura. Puede agregar números a la lista blanca. Diseño de RF complejo | ★★★★ Bloqueo selectivo. El software puede agregar números a la lista blanca |
| Especial de actualización | ☆☆☆☆ Nueva tecnología, nuevo operador o nueva banda de frecuencias = nuevo despliegue | ☆☆☆☆ Las nuevas tecnologías también dificultan un diseño más complejo | ★★☆☆ La nueva tecnología requerirá una nueva red local | ★★★☆ La nueva tecnología solo requerirá una actualización de software |
| A prueba de manipulaciones | ☆☆☆☆ | ☆☆☆☆ | ★★★☆ MNO o cambio de tarjetas | ★★★★ Elementos ubicados en Data center de MNO y seguridad |
| Seguridad | ★★☆☆ | ★★☆☆ | ★★★☆ | ★★★★ |
| Precisión de ubicación | ☆☆☆☆ | ★★★★ La mejor precisión obtenida con pocos locales | ☆☆☆☆ | ★★★☆ Alta precisión utilizando la infraestructura existente |

Las soluciones basadas en la ubicación de redes inalámbricas sobresalen de las alternativas disponibles en el mercado. Ofrece alta precisión, bloqueo selectivo no dañino, mejores costos de implementación y escalabilidad, nuevas alternativas de inteligencia y protección contra la corrupción.

# III.
# MARCO PARA LA IMPLEMENTACIÓN DE SOLUCIONES INNOVADORAS

Obviamente, las entidades involucradas en la elaboración e implementación de políticas relacionadas con el bloqueo de comunicaciones en prisión varían en cada país. Sin embargo, es posible identificar a los actores relevantes de una manera genérica, los cuales deben ser considerados al tratar de evolucionar hacia una mejor solución para el problema.

**Ministerios de Justicia y autoridades penitenciarias.**
Normalmente, la administración penitenciaria sigue las políticas definidas por las oficinas de administración de justicia. Bajo la guía de estas oficinas, hay instituciones específicas a cargo de administrar las prisiones, y las operaciones pueden ser administradas por estos o por terceros privados cuando las regulaciones lo permitan. Estas instituciones están llamadas a convertirse en el *Organismo de Supervisión y Monitoreo.*

**Autoridades de telecomunicaciones.**
Los responsables políticos y reguladores de las telecomunicaciones deben participar, ya que estas nuevas tecnologías se basan en las capacidades de las redes móviles, que requieren una relación directa entre los operadores de redes móviles y la Agencia de Supervisión y Monitoreo. Por ello, los acuerdos o incluso los reglamentos deben fomentarse y definirse con la coordinación de las autoridades de telecomunicaciones.

**Operadores de redes móviles.**
Los MNO están involucrados en el despliegue de soluciones de bloqueo indistintamente de si se utilizan *Jammers*, IMSI Catchers, MAS o sistemas basados en localización, la coordinación con los MNO es un factor clave. En algunos casos, tratando de minimizar los efectos de interferencia en los usuarios y las redes, en otros cooperando para diseñar redes locales como en MAS o para tener acceso a redes centrales cuando se utilizan características intrínsecas de las redes, como en las tecnologías basadas en geolocalización.

Las partes interesadas mencionadas anteriormente son las mínimas, pero pueden entrar en escena otras nuevas, ya que las nuevas tecnologías ofrecen nuevas características que los gobiernos pueden aprovechar.

# III. a PROPUESTA DE HOJA DE RUTA PARA LA POLÍTICA Y LA INDUSTRIA

La problemática está claramente identificada. En primer lugar, las comunicaciones no autorizadas originadas en las cárceles están relacionadas con la continuación de las actividades delictivas y los evidentes efectos negativos de ello en las sociedades. Esa es la razón principal para bloquear esas comunicaciones, pero desafortunadamente, las *soluciones* actuales no son efectivas y la evidencia es que los gobiernos siguen trabajando en regulaciones para encontrar una solución real al problema. Además, la mayoría de las soluciones actuales vienen acompañadas de efectos negativos sobre otros ciudadanos y redes públicas de telecomunicaciones.

Los efectos no deseados de algunas soluciones obligaron a los gobiernos a desarrollar complejos reglamentos técnicos para su despliegue o incluso prohibiciones sobre algunas de ellas. Acompañado de costosos esquemas de vigilancia e incluso multas a los MNO cuando los objetivos no se logran adecuadamente. Por lo tanto, el conocimiento de las soluciones técnicas que ofrecen una mayor efectividad y minimizar o eliminar los efectos no deseados debe ser una prioridad para los funcionarios gubernamentales a cargo.

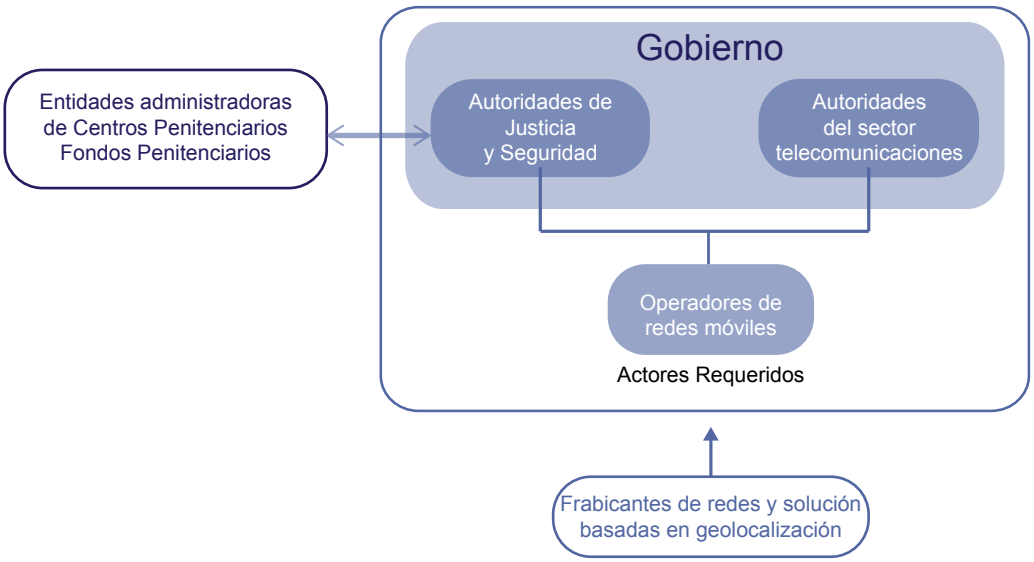
El primer paso podría ser dado por las autoridades de telecomunicaciones o de justicia. Los interesados en proteger los derechos de los usuarios de las comunicaciones, el uso adecuado del espectro radioeléctrico y la protección de las redes de comunicaciones y los demás interesados en encontrar una solución eficaz y rentable a las actividades delictivas relacionadas con las comunicaciones destinadas a bloquear. En cualquier caso, la coordinación entre las autoridades es una necesidad y entre ellas y los MNO.

Las tecnologías basadas en la localización de redes inalámbricas también ofrecen ventajas a los MNOs, al igual que las soluciones completamente

estandarizadas que utilizan características ya presentes en las redes, ofreciendo un mejor control y reduciendo los costos de O&M relacionados con otras alternativas, incluso las multas impuestas por algunas administraciones.

Cuando la propensión a la corrupción es un problema básicamente relacionado con las implementaciones locales distribuidas, los sistemas centralizados basados en localización ofrecen una solución para evitar la desactivación y el daño que reduce la efectividad de las soluciones actuales.

**Figura 21**
Esquema de coordinación propuesto
Fuente: BNMC




Los gobiernos deben decidir que los efectos no deseados de las tecnologías más antiguas ya no son aceptables y están abiertos al mercado para encontrar soluciones que sean efectivas y rentables sin efectos negativos sobre las comunicaciones y redes legales, como las tecnologías basadas en geolocalización de las redes inalámbricas.

Por lo tanto, las regulaciones relacionadas con el bloqueo de comunicaciones, tanto desde el punto de vista político como técnico, deben actualizarse en consecuencia con el estado de los desarrollos tecnológicos. La implementación de nuevas tecnologías puede incluso simplificar las relaciones entre las organizaciones, reduciendo las interacciones y los costos administrativos. Centralizar el funcionamiento de un sistema reduce los problemas de corrupción y abre posibilidades para explotar las nuevas características que vienen junto con las nuevas tecnologías.

Las autoridades de telecomunicaciones tienen un papel clave, ya que las nuevas alternativas requieren que actúen como facilitadores de la adopción. Encontrar el equilibrio entre los intereses públicos y las preocupaciones de la industria de las telecomunicaciones. Esta función habilitante puede ejecutarse a través de acuerdos o reglamentos razonables acompañados de procedimientos de aplicación.

Los MNO pueden reconocer ventajas en la implementación de sistemas basados en la ubicación como: i) Reducir los costos relacionados con la interferencia, ii) la atención del usuario, iii) una mejor gestión del espectro, iv) un mejor y claro control sobre la información compartida desde las redes y v) menos riesgos de multas.

Algunas acciones propuestas como hoja de ruta para las partes interesadas requeridas son las siguientes:

1. Actualizar en cada entidad la información sobre la evaluación comparativa técnica de alternativas o soluciones disponibles para el bloqueo de las comunicaciones penitenciarias. – Todas las partes interesadas.

2. Revisar o actualizar las políticas de justicia relacionadas con el bloqueo de las comunicaciones penitenciarias. – Autoridades judiciales.
   a. Responsabilidades de implementación y cronograma
   b. Agencia de monitoreo y supervisión (Centralización del control y operación de sistemas)

3. Fuentes y modelos de financiación. Fondos penitenciarios. Gastos de infraestructura o gastos de servicios.

4. Revisar o actualizar los acuerdos/reglamentos de telecomunicaciones en consecuencia con el nuevo estado del arte de la tecnología, dado que actualmente la mayoría de los reglamentos están basados en implementación de soluciones del tipo *jammer*s. – Autoridades de telecomunicaciones.

5. Coordinación con todos los MNOs – Autoridades de Telecomunicaciones. Implementación y operación – Agencia centralizada + Proveedores.

# REFERENCIAS


5G Américas. (2019). Temas en regulación de telecomunicaciones: Brasil.

ANATEL. (2002). Resolución 306.

ANATEL. (2002). Resolución 308.

GSMA. (2017). Inhibidores de señal. Uso de *jammer*s en prisiones.

Congreso de la República de Colombia. (2014). Ley 1709.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2011). Decreto 4768.

Agencia Nacional del Espectro. (2019). Resolución 797.

Asamblea legislativa - República de El Salvador. (2015). Decreto 953.

Superintendencia General de Electricidad y Telecomunicaciones - República de El Salvador. (2019).

Reglamento técnico de la Ley Especial contra el delito de extorsión.

Congreso Nacional - República de Honduras. (2015). Decreto 43.

Comisión Nacional de Telecomunicaciones - República de Honduras. (2016). Resolución NR001.

Congreso de la República de Guatemala. (2014). Decreto 12.

Congreso General de los Estados Unidos Mexicanos. (2014). Ley Federal de Telecomunicaciones y Radiodifusión.

Conferencia Nacional del Sistema Penitenciario. (2012). 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.

Instituto Federal de Telecomunicaciones. (2015). Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración.

Instituto Federal de Telecomunicaciones. (2016). Disposición Técnica IFT-010-2016.

Ministerio de Justicia, República Peruana. (2003). Decreto Supremo N° 015-2003-JUS.

Ministerio de Justicia, República Peruana. (2011). Decreto Supremo N° 006-2011-JUS.

OSIPTEL - Organismo Supervisor de Inversión Privada en Telecomunicaciones. (2011). Resolución N° 112-2011-CD.

Marcus Holgersson, O. G. (2017). La evolución de la estrategia de propiedad intelectual en los ecosistemas de innovación: Descubrir regímenes de apropiación complementarios y sustitutivos. Planificación a largo plazo, 303-319.

Strobel, D. (2007). Receptor IMSI.

Ooi, J. (2015). IMSI Catchers y Seguridad Móvil.

ETSI - Instituto Europeo de Normas de Telecomunicaciones. (2012). Sistema digital de telecomunicaciones celulares (Fase 2+); Sistema Universal de Telecomunicaciones Móviles (UMTS); Numeración, direccionamiento e identificación (3GPP TS 23.003 versión 10.5.0 Release 10).

EFF - Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (Probablemente).

Polaris Inalámbrico. (2022). Solución de bloqueo de llamadas a la prisión.

ETSI - Instituto Europeo de Normas de Telecomunicaciones. (1995). Sistema digital de telecomunicaciones celulares (Fase 2+); Prohibición determinada por el operador; (GSM 02.41).

Polaris Inalámbrico. (2020). Soluciones de gestión de teléfonos celulares en prisiones.

Polaris Inalámbrico. (2020). Ubicación inalámbrica para la seguridad nacional.

UIT-D - Unión Internacional de Telecomunicaciones - Desarrollo. (s.f.). Espectro para las IMT. Obtenido de https://www.itu.int/

ITU-D/tech/MobileCommunications/Spectrum-IMT.pdf

Naranja. (2011). Características de las IMT y especificidad del espectro.

GSMA. (s.f.). Guía del espectro 5G: todo lo que necesita saber. Obtenido de https://www.gsma.com/spectrum/5g-spectrum-guide/#:~:text=Today%2C%20a%20majority%20of%20commercial,service%20and%20meet%20growing%20demand.

Departamento de Comercio de los Estados Unidos. (2010). CONTRABANDO DE TELÉFONOS CELULARES EN PRISIONES Posibles soluciones de tecnología inalámbrica.

BLUE NOTE
MANAGEMENT CONSULTING

Patrocinado por:

Polaris Wireless