USO DE TIC Y APLICACIONES

CASOS EXITOSOS DEL USO DE TIC EN SEGURIDAD PÚBLICA EN AMÉRICA LATINA

Informe

Sector de Desarrollo de las Telecomunicaciones

Casos exitosos del uso de TIC en seguridad pública en América Latina

Octubre de 2015

El presente informe sobre “Casos exitosos del uso de TIC en seguridad pública en América Latina” se llevó a cabo por decisión de la Oficina Regional de la UIT como parte del Plan Operativo ejecutado por la BDT en 2015.

El Señor Oscar Sady Orellana, experto consultor de la UIT, llevó a cabo el trabajo de campo y preparó el presente informe, el cual fue a su vez revisado por el Sector de Desarrollo de la UIT.

El consultor agradece la colaboración de las entidades de seguridad pública y de las autoridades de Telecomunicación que colaboraron con el estudio.

Índice

Página

Lista de figuras, tablas y recuadros

Figuras

Página

Tablas

Recuadros

Prefacio

Es para mí un gran placer presentar este estudio preparado por la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT. El objetivo de este informe es proporcionar un análisis de las mejores prácticas con respecto al uso de TIC en seguridad pública en América Latina.

Haciendo uso de herramientas de investigación y trabajo de campo, este estudio hace una presentación de casos exitosos a nivel mundial, regional y nacional, en el uso de las TIC en seguridad pública. Los casos presentados han sido detallados y referenciados para facilitar su adopción por otras ciudades y por otros países interesados. En el mismo, se describen las tecnologías utilizadas, las normas existentes y las tendencias a futuro de la intersección entre seguridad pública y las tecnologías de la información y de las comunicaciones.

El haber levantado la información secundaria y a la de campo, nos permite proponer un ecosistema de seguridad ciudadana, compuesto por marcos jurídicos y regulatorios, datos abiertos, interoperabilidad, impacto en la ciudadanía y aplicaciones sociales. El análisis de casos, las conclusiones y recomendaciones se hacen siguiendo dicho ecosistema, lo que ofrece desde ya una prueba de su utilidad a futuro.

La Oficina que presido espera que el presente estudio sea una contribución tanto a las Autoridades de TIC/Telecomunicaciones como a las Autoridades de Seguridad Pública en la adopción de políticas públicas en TIC exitosas para mejorar la seguridad ciudadana.

Estoy seguro de que las conclusiones y recomendaciones de estudios como el presente, contribuirán para apoyar a los miembros de América Latina en el establecimiento o la mejora del uso de las TIC en seguridad pública.

Brahima Sanou
BDT Director

“Casos exitosos del uso de TIC en seguridad pública en América Latina”

Parte I: Condiciones de Seguridad Pública en América Central y República Dominicana

Introducción

La inseguridad ciudadana se ha convertido en un reto inaplazable para el desarrollo humano de América Latina y el Caribe. Los ciudadanos de la región señalan los delitos, las violencias y las conflictividades principalmente urbanas como factores que limitan sus oportunidades reales y su derecho a vivir una vida libre de temor y de amenazas.

Según PNUD (2014), en su informe regional de desarrollo humano, la inseguridad 2013-2014 es un problema compartido en la región, pero existen variaciones importantes entre ellos y al interior de los mismos. América Latina es la única región del mundo donde la violencia letal aumentó entre 2000 y 2010. Mientras que la tasa de homicidio en la mayoría de las regiones del mundo fue negativa (de 0% a -50%), en América Latina presentó un alza del 12%: en una década, han muerto más de un millón de personas en Latinoamérica y el Caribe por causa de la violencia criminal.

Las TICs pueden facilitar para el beneficio de los ciudadanos, ante la demanda de mayor seguridad, una mejor convivencia y menos impunidad:

(i) El desarrollo de sistemas únicos de control de delitos, violencias y conflictividades en tiempo real donde se puedan recibir todas las colaboraciones ciudadanas y denuncias (llamadas, mensajes, correos electrónicos y redes sociales), que faciliten gradualmente consolidar una agenda electrónica de TICs vinculadas a la Seguridad Pública y Ciudadana.

(ii) Concentrar sistemas informáticos que ayuden a evaluar las tendencias y patrones con la participación interinstitucional que incluya los entes reguladores.

(iii) Consolidar la interoperabilidad de equipos de comunicación principalmente de instituciones policiales a través de la sustitución de los equipos analógicos a digitales, y/o la integración de ambos en plataformas de última generación con una tendencia gradual hacia dispositivos que tengan la capacidad de transporte de datos, imágenes, videos y voz en tiempo real, permitiendo una facilidad de uso y mejora de la respuesta ciudadana y la integración de infraestructuras existentes.

(iv) Analizar y estudiar las facilidades de maximización de recursos que ofrecen nuevas tecnologías de redes como Long Term Evolution (LTE) que no sólo optimizan el transporte de datos y la integración de otros servicios de multimedia, sino que facilitan la comunicación con otros países en materia de Seguridad Pública Regional y Global.

(v) Implementar la aplicación de las redes sociales en el trabajo policial facilitando el acceso de las instituciones de seguridad pública a facilidades de Apps (applications) para facilitar sus labores diarias y de gestión general de las actividades de Seguridad y Convivencia.

1. Condiciones de Seguridad pública en América Central y República Dominicana.

1.1 Conceptualización base.

"La Seguridad Ciudadana se ha convertido en una de las principales preocupaciones de la población en América Latina y el Caribe y constituye un obstáculo objetivo para el desarrollo humano sostenible. Las personas y comunidades ven restringidas sus opciones reales de vida y de organización debido a las amenazas contra la seguridad personal y patrimonial, así como contra bienes públicos fundamentales." (Abrir espacios para la Seguridad Ciudadana y el Desarrollo Humano, IDHAC2009-2010)

La noción de (in)seguridad es intuitivamente obvia, pero su manejo correcto en realidad exige un tipo especial de razonamiento, el "probabilístico" o "aleatorio", que requiere la formación especial de estadísticos y otro personal especializado para su estudio y análisis.

Pero además de la (in)seguridad objetiva, existe la (in)seguridad *subjetiva*, o estimación que cada quien hace sobre el grado de riesgo al que está expuesto. Esta estimación puede estar basada en datos estadísticos, puede coincidir con la medición objetiva, y hasta puede ser más confiable debido al conocimiento personalizado del contexto urbano y/o rural.

"El desarrollo humano es un proceso de ampliación de la gama de opciones de que dispone la gente; la seguridad humana significa que la gente puede ejercer esas opciones en forma segura y libre (PNUD, 1994:26)."

Aunque el concepto "seguridad humana" en principio es tan amplio como lo es el propio "desarrollo humano", el Informe citado destacó dos fuentes principales de inseguridad humana: "los riesgos crónicos, tales como el hambre, la enfermedad o la represión", y "las alteraciones súbitas y dolorosas en la vida cotidiana, ya sea en el hogar, en el trabajo o en la comunidad".

Según PNUD (2009), En primer lugar, puede decirse que *la Seguridad Ciudadana está en la base de la seguridad humana*. En efecto: el hecho de estar vivo es la oportunidad más básica que puede disfrutar un ser humano; la integridad personal es condición necesaria de su libertad y dignidad; y el patrimonio que es necesario para adquirir casi cualquier bien o servicio es fácilmente la siguiente oportunidad en importancia. La violencia o el despojo criminal sin duda califican como amenazas "graves y pre-visibles" contra estas tres oportunidades fundamentales, cuya protección viene a ser el objeto de la seguridad ciudadana. En segundo lugar, *la seguridad ciudadana es la forma principal de la seguridad humana*. Pudimos y aún hoy podemos vivir indefensos frente a la naturaleza frente a los terremotos, la enfermedad y la muerte, pero nuestra supervivencia como especie depende de un "*contrato social*" que nos impida destruirnos los unos a los otros. Lo contrario sería aquella "guerra de todos contra todos", el hipotético estado previo a la sociedad donde "el hombre es un lobo para el hombre", donde se roba y se mata para vivir y donde, para seguir con las palabras clásicas de Hobbes, "la vida humana es solitaria, pobre, desagradable, brutal y breve" (Hobbes, 1979:47-48).

La convergencia de los Conceptos entre Seguridad y Desarrollo

Durante muchos años se creyó que el desarrollo consistía en aumentar la riqueza o el ingreso promedio de un país.

La relación entre los dos conceptos es muy estrecha, pero el de "seguridad" subraya la protección y el de "desarrollo" la realización; el uno mira al riesgo, el otro a las oportunidades; la seguridad alude al "núcleo central" de la vida humana, el desarrollo a todas sus posibilidades; este piensa más en las libertades "positivas", aquella en las libertades "negativas"; la seguridad si se quiere es más apremiante, pero el desarrollo no será genuino si no es seguro, tampoco tendera a ser holístico sino es participativo.

Al atentar contra la vida, la integridad o el patrimonio de sus víctimas, la incidencia de delitos impide el ejercicio de una libertad concreta, sacrifican una opción legítima o destruyen una oportunidad de realización humana: la inseguridad ciudadana es una negación flagrante del desarrollo humano. Pero además de este impacto inmediato, los delitos afectan negativamente

otras variables o procesos económicos, sociales y políticos que a su vez facilitan el desarrollo humano.

1.2. Enfoques de Seguridad Humana y Seguridad Ciudadana Versus el enfoque tradicional de Seguridad Pública

La seguridad ciudadana se diferencia de la seguridad pública, porque la primera se considera desde y para la ciudadanía con una mirada de efectividad para el desarrollo y la seguridad humana, posicionando a las personas como el centro de sus acciones, en tanto la seguridad pública se concibe en una visión céntrica de control interno de la seguridad o enfoque de seguridad nacional, lo que poco contribuye a la gobernanza (esquema horizontal) local o nacional de las problemáticas, pero si es incidente la demanda de gobernabilidad (esquema vertical) para cortar la inseguridad existente bajo un esquema de control.

La Seguridad Ciudadana busca llevar a la ciudadanía una garantía de sus derechos y deberes, con una función incluyente de la sociedad y de las instituciones, en la seguridad pública únicamente de instituciones.- Esto es vinculante a una administración pública que no solo se sirva de las TICs para llegar a sus ciudadanos, sino que además sea capaz de idear los medios incluyentes para que los ciudadanos sean escuchados (ejemplo sobre su protección personal, para los abordajes prevención de violencias, delitos, conflictos, recepción y respuesta a denuncias) y puedan tener injerencia en la gestión pública de la Seguridad Humana (disuasión, formas de vigilancia comunitaria con el uso TICs, apoyo en emergencias cotidianas, respuestas vinculadas a la gestión de riesgos, sistemas de protección humana, etc), que permita consolidar bienes públicos regionales, nacionales y locales, para estos grandes males públicos existentes como el de la inseguridad, (principalmente en un triángulo de participación, normativa y de inversiones en TICs).

El enfoque en el Ser Humano y su Desarrollo, en los procesos de reducción, previsión y prevención de los riesgos requieren ser intensificados y articulados, los compromisos fortalecidos y las inversiones aumentadas. Un enfoque de Gestión Territorial, Gobernabilidad y Gobernanza debe considerar y promover el empoderamiento, el desarrollo institucional y la capacidad de planificación de las autoridades locales, promover los capitales locales, la cultura para la gestión del riesgo, produciendo el intercambio de experiencias entre ciudades, países y regiones como una estrategia dinamizadora de esfuerzos, que demanda de las TICs ser ágil, expedita, flexible y entendible.

Figura 1: Análisis y abordaje de la inseguridad pública y ciudadana

Fuente: *Desarrollado a partir del concepto de Seguridad Humana. Elaboración propia*

Tres Conceptos[1] vinculados

Como punto de partida para el análisis de los "riesgos" naturales nos enfocamos en la definición de los tres principales conceptos relacionados con la temática, riesgo, amenaza y vulnerabilidad, partiendo de las definiciones establecidas y la terminología oficial de la UNISDR actualizada en el 2009 http://www.unisdr.org/we/inform/terminology, de Corrales y Miquilena (2008):

Riesgo: La combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

Amenaza: Un fenómeno, sustancia, actividad humana o condición peligrosa que pueden ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales.

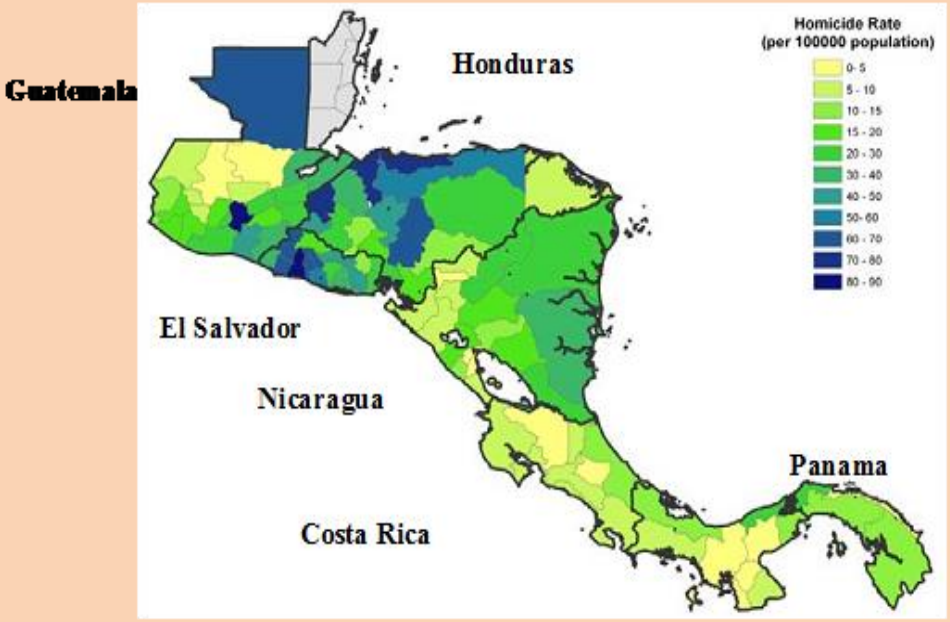
Desastre: Una seria interrupción en el funcionamiento de una comunidad o sociedad que ocasiona una gran cantidad de muertes al igual que pérdidas e impactos materiales, económicos y ambientales que exceden la capacidad de la comunidad o la sociedad afectada para hacer frente a la situación mediante el uso de sus propios recursos.

[1] Estas definiciones se tomaron de las Adaptaciones realizadas por COSUDE en el año 2005 de los Glosario multilingüe de términos convenidos internacionalmente relativos a la gestión de desastres (IDNDR, 19920)

1.3 Análisis de líneas de base sobre Seguridad Ciudadana y Construcción de Paz

Según datos de Banco Mundial, América Central en su entorno estratégico territorial se ve afectada por la incidencia del crimen organizado, de forma diferenciada[2] como se puede apreciar en el siguiente mapa:

Figura 2: Tasa de homicidios en Centro América



Fuente: *Banco Mundial*

Equivocadamente se cree que las intervenciones contra la inseguridad ciudadana, deben traer el estado de beneficio a la sociedad de la "Seguridad Pública y Ciudadana", como fruto de sus intervenciones, sin embargo, se debe en un enfoque multidimensional clarificar que estas intervenciones tiene como fin la consolidación de ambientes de "Paz y Convivencia".- El Índice de Paz Global (GPI) es un intento de medir la posición relativa de las naciones y la tranquilidad de las regiones. Es el producto del Instituto para la Economía y la Paz (IEP) y se desarrolla en consulta con un panel internacional de paz expertos de centros de paz y de los grupos de reflexión con los datos recogidos y recopilados por la Unidad de Inteligencia de The Economist[3]. Fue lanzado en mayo de 2007 y las actualizaciones se han hecho sobre una base anual desde entonces, hay que considerar que esta iniciativa si bien cuenta con reconocimiento internacional, en algunas ocasiones cuenta con criticas por la no inclusión de todas las variables para el análisis para la construcción de Paz que los países desearan y carece de la inclusión de indicadores como el índice de Cibercrimen.

[2] Tasa de Homicidios en Gobiernos locales, Crime and Violence in Central America: A Development Challenge (2011), Banco Mundial

[3] http://www.visionofhumanity.org/#page/indexes/global-peace-index/2014/HND/OVER

Tabla 1: Tabla desagregada del Índice Global de Paz (GPI 2015) México, América Central y Panamá

http://www.visionofhumanity.org/#page/indexes/global-peace-index/2015	Costa Rica	Panamá	Nicargua	República Dominicana	Guatemala	El Salvador	Honduras	México
Índice de Paz Global	1654	1903	1947	2089	2215	2263	2210	2530
Criminalidad percibida en la sociedad	3	3	3	4	5	5	5	4
Oficiales de seguridad y policía	2.3	3.6	1.8	2.6	1.8	2.7	1.8	2.8
Homicidios	3	4	4	5	5	5	5	5
Población encarcelada	3.5	3.8	2	2.7	1.7	4.2	2.3	2.5
Acceso a las armas pequeñas y las armas ligeras	4	3	4	3	4	4	4	4
Conflicto organizado (interno)	1	1	2	2	3	2	2	2
Manifestaciones violentas	2	3	3	3	4	2	3	3
Crímenes violentos	2	3	3	3	5	5	5	5
Inestabilidad política	1	2	3	2	2.3	2	2.5	2
Terror Político	2	2	3	3	2	3	3	4
Importaciones de armas convencionales	1	1	1	1	1	1	1	1
Actividad terrorista	1	1	1	1.5	2	1	2	3
Muertes por conflictos organizados (internos)	1	1	1	1	1	1	1	5
Gasto militar	1.3	1.5	1.2	1.2	1.1	1.2	1.3	1.1
Personal de las fuerzas armadas	1	1	1	1	1.1	1	1	1
Financiación de las misiones de paz de la ONU	1	2.3	1.6	4.2	2.1	2.6	2.1	1.1
Armas nucleares y pesadas	1	1	1.1	1	1	1	1	1.2
Exportaciones de armas convencionales	1	1	1	1	1	1	1	1
Personas Desplazadas	1	1	1	1	1	1	1	1
Relaciones con los países vecinos	2	2	2	2	2	2	2	1
Conflictos luchados	1	1	1	1	1	2.1	1	1
Muertes por conflictos (externos)	1	1	1	1	1	1	1	1

Fuente: *vision of humanity.* (*http://www.visionofhumanity.org/#page/indexes/global-peace-index/2015/NIC/OVER*)

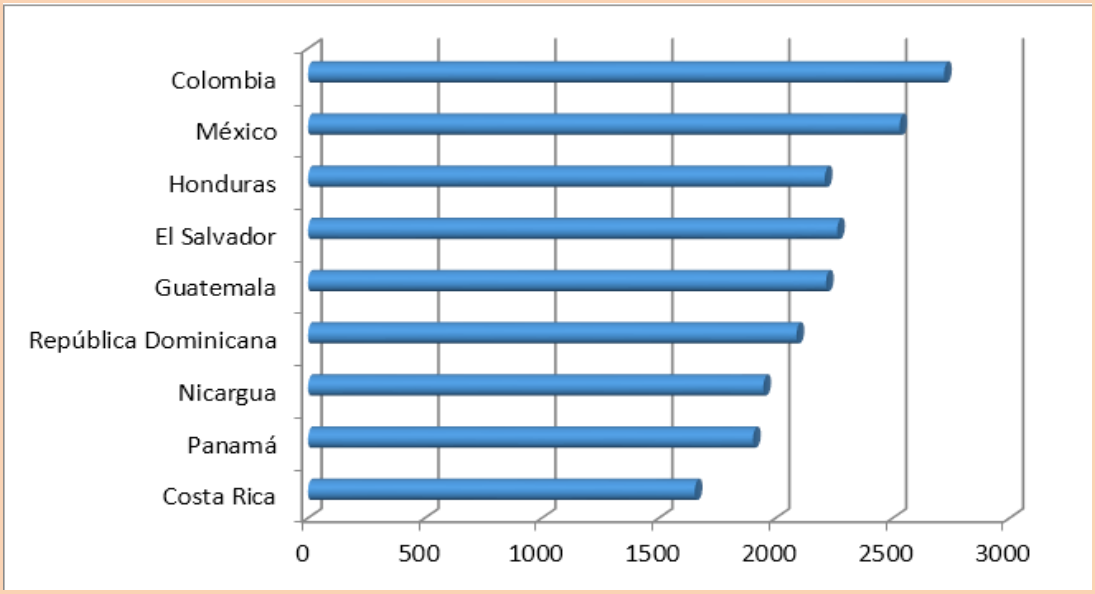
Es así que fenómenos como la criminalidad percibida por la Sociedad son más altos en El Salvador, Guatemala, y Honduras respectivamente en Centro América; el acceso a armas pequeñas y a armas ligeras tienen una alta tendencia de incidencia en la inseguridad en los paises como se aprecia en la tabla desagregada del GPI, factores que inciden en las violencias, delitos y conflictos principalmente urbanos en los diferentes territorios.

El análisis de datos del año, 2015, del Índice Global de Paz (GPI) sitúa a Colombia (lugar 150 de 162 a nivel mundial) y México (144 de 162) como los países con menor índice de Paz del continente[4], comparándolos en el ámbito de América Central y República Dominicana, les sigue el Salvador(123 de 162), Guatemala (118 de 162), Honduras (116 de 162), y República Dominicana (100 de 162), en un segundo nivel Nicaragua (74 de 162), Panamá(64 de 162), situando a Costa Rica (45 de 162) en la mejor ubicación[5] del área de América Central.

[4] http://www.visionofhumanity.org/#page/indexes/global-peace-index/2015/NIC/OVER

[5] No existen datos de Belice, por este motivo este estudio no referencia su ubicación en el contexto subregional.

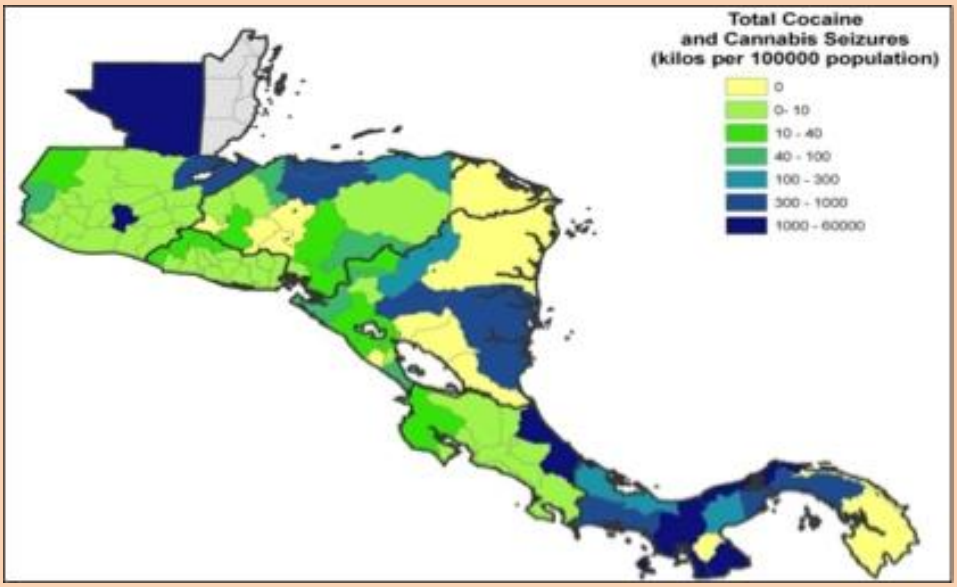
Figura 3: Índice Global de Paz para países seleccionados



Fuente: *Elaboración propia con base en los datos del GPI 2014*

Informes del Banco Mundial, nos indican que otra variable a considerar es el Narcotráfico, la incidencia de tráfico de Cocaína[6], por América Central y el Caribe, permite que el flujo de dinero ilícito genere una marcada lucha territorial por el mercado de las drogas, demandando armas, estructuras e infraestructuras operativas de crimen organizado para el tráfico de drogas, personas y armas en la región.

Figura 4: Decomisos totales de cocaína y canabis en Centro América



Fuente: *Intensity of Drug Trafficking, Crime and Violence in Central America: A Development Challenge (2011) Banco Mundial*

[6] Intensity of Drug Trafficking , Crime and Violence in Central America: A Development Challenge (2011), Banco Mundial

1.4 Cruce de líneas de base de GNDR[7] (Gestión de Riesgos y Seguridad Ciudadana) en el Cono Norte de América Central

VPL es un proyecto de investigación y acción promovido a nivel internacional por la Red Global de Organizaciones de la Sociedad Civil para la Reducción del Riesgo de Desastres-GNRD (siglas en inglés), creada en la primera sesión de la Plataforma Global para la Reducción de Riesgos de Desastres (RRD) en julio del 2007 (Ginebra, Suiza).

Síntesis de Resultados regionales 2014-2015: su análisis y estudio en Honduras, Nicaragua, Guatemala y El Salvador, combina factores de riesgo y vulnerabilidades, se enfoca las amenazas predominantes a nivel de los pases, muestran una tendencia hacia la prevalencia en una visión más holística sobre los factores que se enuncian a continuación:

1. Inundación
2. Inseguridad Ciudadana
3. Deslizamientos
4. Sequia
5. Contaminación, degradación ambiental
6. Pobreza
7. Huracanes
8. Cambio Climático
9. Tornados y vientos huracanados
10. Plagas
11. Nuevas enfermedades virales
12. Migración
13. Violencia Domestica
14. Sobre explotación de recursos naturales
15. Incendios
16. Deforestación
17. Terremotos
18. Marejadas
19. Violencia en género
20. Alcoholismo
21. Frentes Fríos
22. Inseguridad Alimentaria

Su último enfoque fue de cara a obtener una visión de primera línea, para generar recomendaciones y medidas de políticas globales en la recién pasada reunión en Sendai, Japón la GNDR, para las propuestas para un mundo más seguro MAH15, según datos recabados a Noviembre del 2014 los países de Honduras, Nicaragua, Guatemala y El Salvador, brindan una percepción de la ciudadanía quien considera que la principal amenaza que se considera a nivel regional es la inundación (14.99%), seguida de la Inseguridad Ciudadana (11.97%), con consecuencias de afectación de pérdida de viviendas (12.08%) con daños a producciones y cultivos (11.76%) y pérdida de vidas humanas (10.43%), que demanda acciones de ejecución de campañas de concientización (12.44%), el mejoramiento de técnicas agrícolas, formas de producción, semillas y cuidados del agua y suelos (8.24%).- Siendo la principal barrera la falta de interés por parte de algunas autoridades locales (apatía o desatención) con 12.09%.

Este análisis de percepción regional, nos permite observar en el caso de los tres países del triángulo Norte de América Central, como la percepción de la inseguridad es más alta en Guatemala y Honduras, hasta el 2014 con menos incidencia en ese momento en El Salvador.

[7] http://www.globalnetwork-dr.org/tableau

Siendo a nivel de análisis de riesgos, según la percepción más incidente la vinculada a los riesgos cotidianos por fenómenos naturales como ser inundaciones, sequias, pobreza, degradación ambiental y deslizamientos, muy coincidentes con la demanda de mayor Seguridad Humana, asociada a los medios de vida vitales y al enfoque territorial como parte de un ecosistema de vida.

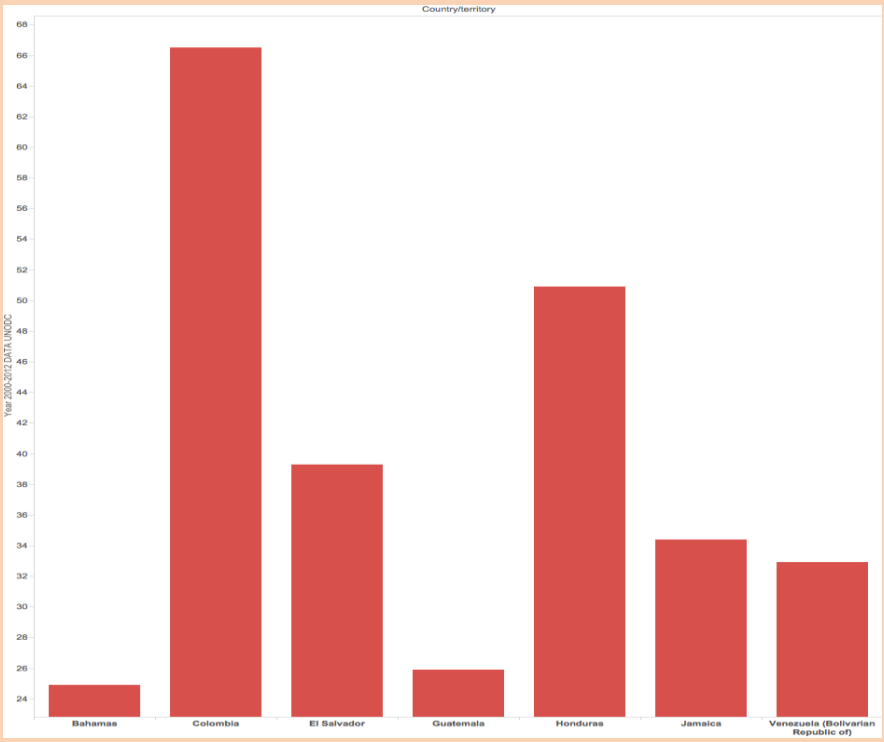
1.5 Análisis de contextos diferenciados (América Central y República Dominicana)

El análisis sobre el tema de la seguridad ciudadana adquiere mucha relevancia en el contexto del desarrollo de las naciones centroamericanas y caribeñas. La constante preocupación por garantizar el pleno desenvolvimiento de los seres humanos, coloca el tema del incremento de la inseguridad en una destacada posición en la agenda política de estos países, principalmente en el triángulo norte de América Central.

Entre los 47 países clasificados por el Programa de las Naciones Unidas para el Desarrollo (PNUD) en la categoría de Desarrollo Humano Medio, la República Dominicana está entre las seis naciones con la percepción más baja en seguridad ciudadana. Sólo el 38% de la población se considera segura y el 15% dice tener confianza en las personas. El "Informe sobre desarrollo humano 2013[8]", dado a conocer detalla que otros cinco países con la más baja percepción de seguridad son Botswana (31%), Namibia (33%), Sudáfrica (38%) y Gabón (39%), todos africanos, y Paraguay (38%), en América del Sur. Sin embargo, República Dominicana comparada con los 47 países con Desarrollo Humano Medio, no es el país con la más alta tasa de homicidio, pero es el sexto con más casos. Solo es superada por Sudáfrica (31,8), Guatemala (38,5), Belice (41,4), El Salvador (69,2) y Honduras (91,6). Los países más afectados por el nivel de violencia durante el periodo de los años 2000-2012 según análisis de datos de [9] UNODC, analizados sobre la incidencia del delito Homicidio (tasa por cada 100,000 habitantes) son en primer lugar Colombia, en segundo lugar Honduras, en tercer lugar El Salvador, seguidos de Jamaica, Venezuela, Guatemala y Bahamas en su orden.

[8] http://www.undp.org/content/undp/es/home/presscenter/events/2013/March/HDR2013.html#
[9] http://www.unodc.org/gsh/en/data

Figura 5: Tendencia de impacto del delito Homicidio



Fuente: *Elaboración propia con base en los datos UNODC 2000-2012*

1.6. Alcances, aplicaciones y niveles de TICs para la Seguridad Ciudadana y la Justicia

Sobre la Seguridad Ciudadana no hay un concepto único, se trata de un concepto complejo por las diferencias que presenta, por lo tanto el mismo debe ser abordado en forma sistémica y considerando facilidades participativas comunitarias en los que las TICs facilitan estrategias de ingreso a la comunidad, mediante la organización, creación de capacidades comunitarias, cohesión comunitaria y el fomento de empoderamiento personal y comunitario para la toma de decisiones locales con un enfoque global.-Sobre esto es importante que las soluciones a considerar deben al menos considerar estos cuatro factores:

a) **Calidad de las Soluciones Tecnológicas**: Procurando que los productos de las soluciones tecnológicas en base al uso de TICs desarrolladas o adquiridas, cumplan con los requerimientos especificados con calidad.

b) **Desarrollo de Soluciones Tecnológicas**: En un marco de referencia para la construcción de una solución tecnológica en base a TICs, incluyendo la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios.

c) **Definición de requerimientos de soluciones**: para el desarrollo de soluciones mediante acciones coordinadas con las unidades responsables solicitantes

d) **Administración de Soluciones**: Definiendo los compromisos y costos de servicios de TIC necesarios para mantener el adecuado funcionamiento de la Seguridad Ciudadana y Pública, así como identificar iniciativas de creación de servicios de TIC susceptibles de aportar beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución

"Los Estados deberán prepararse para la efectiva implantación del Gobierno Electrónico acometiendo las transformaciones organizativas que consideren necesarias, así como la progresiva implantación de sistemas, equipos y programas en las Administraciones Públicas. En tal sentido, es recomendable que los Estados: a. Reconozcan los desarrollos propios de sistemas o sus adaptaciones como capital estatal intangible, generando mecanismos de transferencia y sistemas de apoyo, para lo cual se requiere acordar nuevos marcos regulatorios" (Carta Iberoamericana de Gobierno Electrónico (CIGE 2007), punto 23, Las 23 transformaciones de las Administraciones Públicas).

Aunque el objetivo principal del Gobierno Electrónico (eGovernment) radica en la transparencia de la gestión pública, es indudable que sus alcances pueden ser un aporte en la cooperación entre Estados propiciada por las TICs frente a los delitos, las violencias y las conflictividades. Bajo las consideraciones de la Carta Iberoamericana de Gobierno Electrónico (CIGE 2007) existen dos objetivos inseparables en el proceso de reconocimiento del Derecho de acceso electrónico a las Administraciones Públicas:

Un objetivo final y directo: al reconocer a los ciudadanos un derecho que les facilite su participación en la gestión pública y sus relaciones con las Administraciones Públicas y que contribuya también a hacer estas más transparentes y respetuosas con el principio de igualdad, a la vez que más eficaces y eficientes. **Un objetivo estratégico e indirecto**: debe ser la promoción de la construcción de una sociedad de información y conocimiento, inclusiva, centrada en las personas y orientada al desarrollo, para facilitar la seguridad y convivencia ciudadana

"Los Estados iberoamericanos deberían fomentar en la mayor medida posible acuerdos entre sí para que la **interoperabilidad**[10] de los servicios y sistemas no se reduzca al ámbito de cada Estado, sino que desde el principio comprenda a todos los Estados de modo que el acceso al Gobierno Electrónico se haga de manera más o menos conjunta como Región, potenciando así las sinergias que se seguirán de un acceso lo más amplio posible, simultáneo y sostenido de todos los países iberoamericanos a la sociedad de la información y el conocimiento y con especial precaución acerca de la obsolescencia de las diversas ofertas tecnológicas.

[10] Carta Iberoamericana de Gobierno Electrónico (CIGE 2007), punto 25, La Interoperabilidad de Servicios

En especial se tratará de lograr un estándar común de interoperabilidad entre todos los países iberoamericanos."

Figura 6: Criterios iniciales de Gestión del Cambio para Consolidar la Interoperabilidad

Fuente: *Elaboración propia*

“Casos exitosos del uso de TIC en seguridad pública en América Latina”

Parte II: Presentación de Soluciones y Tecnologías para la Seguridad Pública.

2. Presentación de Soluciones y Tecnologías para la Seguridad Pública.

2.1 Introducción

La efectividad de utilizar a las TICS para prevenir los delitos, las violencias y la conflictividad social, debe suponer la articulación de esfuerzos de la ciudadanía y de las autoridades entorno a objetivos comunes para promover la seguridad. Factores importantes para lograr la efectividad alrededor de las TICs en la lucha contra la inseguridad como ser marcos jurídicos y regulaciones, interoperabilidad, datos abiertos, conectividad, participación ciudadana y destrezas digitales, comunicación digital y redes sociales.

En este documento sobre la gestión de la respuesta a la ciudadanía se referencian consideraciones para generar herramientas y aplicaciones para la denuncia, innovación y desarrollo de instrumentos para la prevención y previsión social, gestión de conocimiento para la sociedad e innovación participativa. - En materia de justicia y derechos humanos las plataformas para la promoción de derechos, para el control y la investigación.

En cuanto a la seguridad pública y la inteligencia, se referencian plataformas para la inteligencia y los sistemas de información especializados.- Sobre sistemas de información ciudadana y redes sociales se amplia sobre contenidos de participación ciudadana y las tecnologías de información y comunicación como ser el caso de la Alerta AMBER, el ecosistema en base al ciclo de la experiencia, observatorios de seguridad ciudadana.- Sitúa al lector en seguridad pública y la justicia, un entorno práctico realizando una mirada sobre las APPs en el sur del continente y brinda un panorama de enlaces y redes sociales que están siendo utilizadas por las Secretarías de seguridad a nivel continental.

2.2 Presentación de Soluciones y Tecnologías para la Seguridad Pública.[11]

La expansión de la utilización de las TICs ha transformado las costumbres delictuales, generando el surgimiento de nuevas formas de delito que utilizan a su favor la capacidad y amplitud de comunicaciones ofrecidas por la red.

Así, los delitos informáticos, cuyo objetivo primordial radica en el uso de la información existente con fines ilícitos, han ido aumentando su capacidad de acción e impacto a través del espionaje cibernético, la falsificación o difusión de información altamente confidencial y la infracción a la propiedad intelectual.

Estos hechos han afectado a personas, sistemas y organismos cuya información se encuentra digitalizada y que a su vez han instalado al hackerismo como una nueva cultura delictual muchas veces sin presencia en las legislaciones de los Estados (Salom C., 2008). Un reporte realizado en el año 2012 por la empresa Norton de Symantec ilustró que aproximadamente 556 millones de adultos en todo el mundo, fueron víctimas de los delitos informáticos ese año, cifra que representa un 46% del total de individuos que se conectan al Ciberespacio (América Economía, 2012).

Otro punto importante a destacar es que el Estado debe considerar la masificación y deslocalización de las tecnologías. El crimen no tiene fronteras, lo que configura un nuevo escenario en cuanto a las políticas de control y prevención del delito (Bello-Montes, 2012), dando origen a un paradigma de seguridad "entre" Estados, generando una modalidad de seguridad "intra-estatal" (Prince & Jolías, 2011), lo que implica un desafío de apertura a la cooperación internacional debido al carácter transnacional de este tipo de figuras criminales.

[11] Tomado de la Seguridad en América Latina, Universidad de Santiago de Chile & Motorola Foundation, 2014

2.3 Soluciones y Tecnologías para la Seguridad Pública en la administración de la Seguridad Ciudadana.

La efectividad de utilizar a las TICs para prevenir los delitos, las violencias y la conflictividad social, debe suponer la articulación de esfuerzos de la ciudadanía y de las autoridades entorno a objetivos comunes para promover la seguridad, y también para prevenir y mitigar los daños causados por desastres naturales, que permita facilitar en un entorno amplio la gobernanza en la lucha contra la inseguridad, consideran el entorno total de los riesgos.

Factores importantes como los siguientes, se deben considerar para lograr la efectividad de las TICs de cara a establecer una gestión pública holística ante la inseguridad ciudadana vigente:

a) **Marcos Jurídicos y Regulaciones**: con la aplicación y armonización de marcos jurídicos y regulaciones vigentes para propiciar un entorno de certeza y confianza en la adopción, uso y fomento de las TICs.
b) **Interoperabilidad:** alrededor de las capacidades estructurales, técnicas, organizacionales, de gobernanza, necesarias para compartir información y gestar conocimiento.
c) **Datos abiertos**: disponibilidad de información gubernamental en formatos útiles y reutilizables por distintas entidades de gobierno, la población, organizaciones de sociedad civil, cooperantes y universidades entre otros, para fomentar el emprendimiento y gobernanza en la seguridad ciudadana desde los niveles locales y con acompañamiento ciudadano.
d) **Conectividad**: fortalecimiento y desarrollo de redes (gubernamentales y ciudadanas) y la ampliación de una mejor infraestructura en los territorios, la ampliación de la capacidad de las redes existentes, y el desarrollo de competencias en el sector de TICs para estimular aplicaciones principalmente en las redes celulares de forma masiva.
e) **Participación Ciudadana y Destrezas Digitales**: en un desarrollo equitativo de habilidades para desarrollar y operar tecnologías y servicios digitales, contemplando la cobertura social y el desarrollo de habilidades en sistemas comunitarios.
f) **Comunicación digital y Redes Sociales**: como una facilidad de empoderamiento y sensibilización social para el apoyo de estrategias digitales, una comunicación digital centrada en la ciudadanía y sus necesidades como demandante de Seguridad y Convivencia, que provea servicios digitales en base a gestión de conocimiento, y no solo información.

En este entorno la Presentación de Soluciones de Tecnologías para la Seguridad Pública, sobre la administración de la Seguridad Ciudadana se centra esencialmente en los niveles centralizado y local: con plataformas básicas para respuesta, con tendencias graduales a un Sistema Integrado de Emergencias y Seguridad, con acceso a sistemas de información, por ejemplo:

- Centros de operaciones de la policía en los niveles locales.
- Sistemas de información de seguridad ciudadana de la policía.
- Sistemas de operaciones de organismos de emergencia.
- Sistemas de información y posicionamiento geográfico.
- Sistemas de Vigilancia Ciudadana CCTV.
- Sistema integrado de identificación balística (IBIS).
- Sistemas de dactiloscopia.

- Sistema de identificación de vehículos.
- Sistema de identificación aeroportuaria.
- Sistema de identificación y reconocimiento facial.
- Sistema de información de la Organización Internacional de Policía Criminal (INTERPOL).
- Sistema de intercambio de información de la Comunidad de Policías de América (AMERIPOL) en desarrollo.
- Vínculos a los Sistemas Información Forenses: de informática, humanos, drogas, armas y explosivos, medio ambiente, lavado de activos, terrorismo, etc
- Observatorios de Seguridad Ciudadana.
- Centros integrados con interoperabilidad con las soluciones anteriores tipo 911.

Estas soluciones que gradualmente se han desarrollado principalmente en los Estados Unidos de Norte América en nuestro continente, hoy por hoy se diseminan a lo largo de todo el continente con sus facilidades, recursos y contextos propios de cada territorio.

2.4 Soluciones y tecnologías para la seguridad pública en la gestión de la respuesta a la ciudadanía

En este entorno la presentación de soluciones de tecnologías para la seguridad pública en la gestión de la respuesta a la ciudadana se centra esencialmente en los siguientes niveles:

a) **Generar herramientas y aplicaciones para la denuncia** en múltiples plataformas: por medios digitales y análogos, a través de dispositivos fijos o móviles.
b) **Innovación y desarrollo de instrumentos para la prevención Social**: basado en la evidencia que permita la caracterización de patrones y tendencias para proveer información por medios digitales o análogos que facilita a los ciudadanos desarrollar acciones preventivas para no ser víctimas de las violencias, los delitos y las conflictividades.
c) **Gestión de conocimiento para sociedad:** aplicaciones principalmente para atender problemas de violencias, delitos y conflictividades en niños, niñas y jóvenes, como población más vulnerabilizada.
d) **Innovación Participativa:** con TICs que incrementen la capacidad de la ciudadanía para participar en los asuntos públicos en materia de seguridad y emergencias cotidianas.

La creación y modificación de aplicaciones también han aumentado las interacciones en red.- Hoy, los principales hábitos de los usuarios que tienen acceso a Internet son acceder a las redes sociales, revisar el correo electrónico, interactuar en foros, usar mensajería instantánea, trabajar en contenidos de su interés (por ejemplo en blogs) y hacer o recibir llamadas telefónicas por Internet.- El aprovechamiento de las Tecnologías de Información y Comunicación (TICs) en el modelo de operación de las instituciones de seguridad pública, en contextos diferenciados de altos índices de delitos y violencias que se viven principalmente en los países del Triángulo Norte como Honduras, Guatemala y El Salvador hacen de las TICs, soluciones prometedoras para aumentar y mejorar la respuesta gubernamental en la reacción, la prevención y la previsión sobre los delitos y otras situaciones de emergencia.

2.5 Soluciones y Tecnologías para la Seguridad Pública en la administración de Justicia y Derechos Humanos

La seguridad es una de las funciones principales del Estado; le otorga la potestad del uso de la fuerza para garantizar el orden y la paz dentro de la sociedad organizada, es un “contrato social” que debe prevalecer ante la necesidad colectiva en las comunidades de seguridad humana. Los Estados, por consiguiente,

asumen esta responsabilidad con base en una normatividad (Estado de Derecho), generalmente bajo regulaciones y normativas nacionales e internacionales, que delimita acciones, establece las conductas de convivencia civil, así como en un aparato que busca garantizar y ejercer estas reglas para castigar a los que deciden transgredirlas. En este sentido el uso de TICs bajo las anteriores consideraciones permite la existencia de:

a) **Plataformas para la promoción de Derechos**: desarrollando servicios y aplicaciones en línea para hacer frente a los riesgos de la población ante fenómenos cotidianos de inseguridad, emergencias y desastres naturales y vinculados a los derechos humanos, a la protección, la educación, la salud y los medios de vida.
b) **Plataformas para el Control:** que permiten como efectividad de la seguridad apoyar el desempeño [12] de la justicia principalmente en centros de detención y centros penitenciarios en procesos como:

Seguridad perimetral:

- Sistemas de observación móviles y aéreos (drones).
- Radios comunicadores en vehículos de patrulla y para guardias penitenciarios.
- Sistema de bloqueo de comunicaciones a través de servicios de Internet WI-Fi, telefonía satelital y otros sistemas

Vigilancia y Monitoreo:

- Cámaras de circuito cerrado de televisión.
- Seguimiento e interferencia telefonía celular.
- Monitoreo mediante brazalete electrónico.

Control de Acceso:

- Centros de operaciones penitenciarios.
- Dispositivos de detección de metales.
- Dispositivos de detección de explosivos.
- Escáneres de vehículos y personal.

Sensores y Dispositivos:

- Botones de alarma.
- Botones de pánico,
- Detectores de ruido en tiempo real,
- Soluciones de identificación interna por radiofrecuencia (RFID)
- Seguimiento de los presos y dispositivos de control de presencia interna en las cárceles.

Sistemas de posicionamiento:

- Monitoreo y traslado de presos a centros judiciales
- Monitoreo y traslado de presos para actividades sociales

Sistemas de pánico celular:

- Para uso institucional de policía penitenciaria

[12] Implementado con éxito en centros penales de México

c) **Plataformas para la investigación:** que facilitan el seguimiento de la "Ruta Judicial", de los casos en proceso de investigación fiscal. "En otras palabras, se ha señalado que la "…e-justicia[13], es decir, el uso de las tecnologías de la información y el conocimiento en la administración de justicia puede suponer importantes beneficios en el funcionamiento de la Administración de Justicia[14]: los profesionales de la justicia pueden ahorrar tiempo y trabajo; el Gobierno[15] y la Administración de Justicia pueden obtener mayor información y transparencia[16] sobre el funcionamiento de la justicia, y ofrecerla de manera más eficaz y eficiente; los justiciables (según la Real Academia, quien puede o debe someterse a la acción de los tribunales de justicia) pueden relacionarse directamente con la justicia, lo que les puede facilitar el acceso a la misma; los usuarios de la justicia pueden suponer una mayor eficiencia en el tratamiento de los casos, un ahorro de tiempo, una disminución de los costes y un mejor acceso a una justicia de mayor calidad", como se puede apreciar su uso actual en la Cumbre Judicial Iberoamericana, lo implementado por la Unión Europea y más especificamente en España donde existe un "Marco jurídico TICs en Administración de Justicia", o por ejemplo el Sistema Juridico de Costa Rica que permite consultas online[17]

Considerando lo anteriormente mencionado sobre las TICs, no solo basta contar con capacidades para monitorear la Seguridad Ciudadana, también se debe considerar los vínculos de las TICs en el sector justicia para:

1. **Mejorar la gestión y desempeño**: con sistemas de información como herramientas de fortalecimiento y mejoramiento de la gestión y trámites judiciales; de mejoramiento de la calidad de la información producida en audiencia; para facilitar el fallo de la causa, o para el seguimiento de la ruta judicial.
2. **Mejorar el acceso a la justicia**: con sistemas de información que, mediante la utilización de herramientas, normalmente basadas en tecnologías Web permitan brindar mayor acceso a la información y facilitar el acceso a diversos servicios judiciales y de seguridad, mejorando la interoperabilidad y la relación de los operadores de seguridad y justicia, así como su interrelación con la ciudadanía y la sociedad.

2.6 Soluciones y Tecnologías para la Seguridad Pública y la Inteligencia

Considerando el ciclo básico para la prevención social de violencias, delitos y conflictividades las actividades que realizan los Estados pueden dividirse en dos grandes áreas: las relacionadas con acción inmediata para la "Plataformas para la Inteligencia"[18] como es el caso de la Plataforma mundial de INTERPOL, y las de prevención con acciones que demandan la administración de la Seguridad, con "Sistemas de Información Especializados"[19] como el caso de open data en Honduras. El trabajo en prevención reduce los costos en las tareas de acción inmediata y mejora la calidad de la atención a la Ciudadanía, sin duda esto en un "Entorno de Cultura Ciudadana para el buen uso de las TICs" que permite bajo acciones de sensibilización y gestión de conocimiento que las comunidades generen espacios de uso de TICs bajo el respeto de normas y de

[13] El Uso de Nuevas Tecnologías en el Sistema Judicial: experiencias y precauciones, Ricardo Lillo Lobos, investigacion base del Centro de Estudios de Justicia de las Américas, y que fuera presentada durante el VIII Seminario de Gestión Judicial realizado en la ciudad de Brasilia, entre los días 29 a 30 de noviembre de 2010.
[14] http://www.cumbrejudicial.org/web/guest/ejusticia/
[15] https://e-justice.europa.eu/home.do?action=home&plang=es
[16] http://www.iijusticia.org/docs/LOBOS.pdf
[17] https://pjenlinea.poder-judicial.go.cr/SistemaGestionEnLineaPJ/Publica/wfpConsultas.aspx
[18] http://www.interpol.int/es/
[19] https://www.sepol.hn/

autorregulación personal[20] como es el caso de la dinámica Bogotá Segura, que también alimentan los sistema de inteligencia de los estados y gobiernos locales. Sobresalen dos tipos de aplicaciones:

1. **Plataformas para la inteligencia:** que facilitan el seguimiento de la "Ruta", de la delincuencia común y organizada, la delincuencia económica y financiera, inteligencia criminal, análisis y estudio de casos de drogas, terrorismo, extorsión.
2. **Sistemas de información Especializados**: que permitan generar facilidades locales nacionales y transnacionales de inteligencia para recabar "indicios" como los manejados por los cuerpos de Fiscalía, para su incidencia en los asuntos Judiciales y que son sistemas de información para la gestión pericial que permiten e inciden en los procesos judiciales, asegurando conocimiento baso en la evidencia.

Hoy en día, como las carreteras, el agua, o el suministro eléctrico, las infraestructuras de la información deben formar parte de la infraestructura nacional, sin la cual la vida pública y privada se detendría.[21]

Debido a que la sociedad actual depende ampliamente de las tecnologías de la información (TI)[22], esto conlleva la irrupción de nuevas amenazas desconocidas en el pasado.- Debido al carácter global de las redes, los incidentes de seguridad de las TICs que les afectan pueden ocasionar interrupciones o fallos permanentes en la infraestructura de información de loa paises, las instituciones y de las personas.

Estas plataformas para la inteligencia y los sistemas de información especializados buscan estratégicamente fortalecer:

a) **La Prevención**: para proteger las infraestructuras de información de forma adecuada.
b) **La Preparación**: para responder de forma efectiva a los incidentes de seguridad.
c) **La Sostenibilidad**: para mejorar las competencias de los países bajo estándares internacionales y normativa regulatoria nacional
d) **La previsión**: para contrarrestar de forma efectiva amenazas, vulnerabilidades y riesgos.

La seguridad se ha convertido en una de las mayores amenazas en el planeta y las instituciones demandan soluciones que combinen capacidades de análisis, seguridad y movilidad en una única plataforma integrada. Considerando que muchos usuarios cuentan con facilidades web, cloud, movilidad y analítica. - Demandando seguridad para eliminar las preocupaciones que en muchas ocasiones actúan como inhibidores para desplegar más confianza en aplicaciones que aporten un verdadero valor en su diario interactuar.

En este sentido ya existen equipos nacionales para coordinar, colaborar, y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas y de comunicaciones principalmente de las entidades gubernamentales como es el caso de Panamá[23] y Guatemala[24], que cuentan con un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

[20] http://bogota.gov.co/temasdeciudad/cultura-y-recreacion
[21] Seguridad y Ciberdefensa, Acosta, Rodríguez, de la Torre y Ballesteros 2009, página 32 de 179 el Caso de Alemania
[22] Idem
[23] http://www.innovacion.gob.pa/csirt
[24] http://www.csirt.gt/

2.7 Sistemas de Información Ciudadana y Redes Sociales

Participación ciudadana y las Tecnologías de Información y Comunicación: El Caso de la Alerta AMBER

Un elemento muy importante, es el impacto que tiene el uso de las Tecnologías de Información y Comunicaciones (TIC) en la relación entre el Estado y la ciudadanía.

La Alerta AMBER es un sistema de notificación de menores de edad desaparecidos, implementado en varios países desde 1996 [25]. AMBER es un retroacrónimo en inglés de ***"America's Missing: Broadcasting Emergency Response"*** pero que originalmente hace referencia a Amber Hagerman, niña que fue secuestrada y días después localizada sin vida.

Los expertos han indicado que las primeras horas son vitales, por ello la alerta se emite lo antes posibles y es transmitida por diversos medios como televisión, radio, sms, correo electrónico, pantallas electrónicas, entre otras; a fin de poder llegar al mayor número de personas posibles

La Alerta AMBER representa un mecanismo de comunicación de gran envergadura entre el Estado y sus ciudadanos[26] principalmente en USA, sistema de notificación que es el resultado de una colaboración entre la The Wireless Association , originalmente conocida como la Asociación de Industrias de teléfono celular CTIA[27] , la Comisión Federal de Comunicaciones (FCC) y la Agencia Federal de Manejo de Emergencias (FEMA). Hace uso de tecnologías tradicionales como una llamada telefónica, o bien, mediante tecnologías actuales, replicada ya como el portal oficial de Alerta AMBER en México[28], solicita en línea la activación de la alerta; asimismo el ciudadano puede hacer la misma solicitud a través de aplicaciones móviles. También, hace uso de tecnologías de comunicación de proveedores de servicio y de medios de comunicación de radio y televisión.

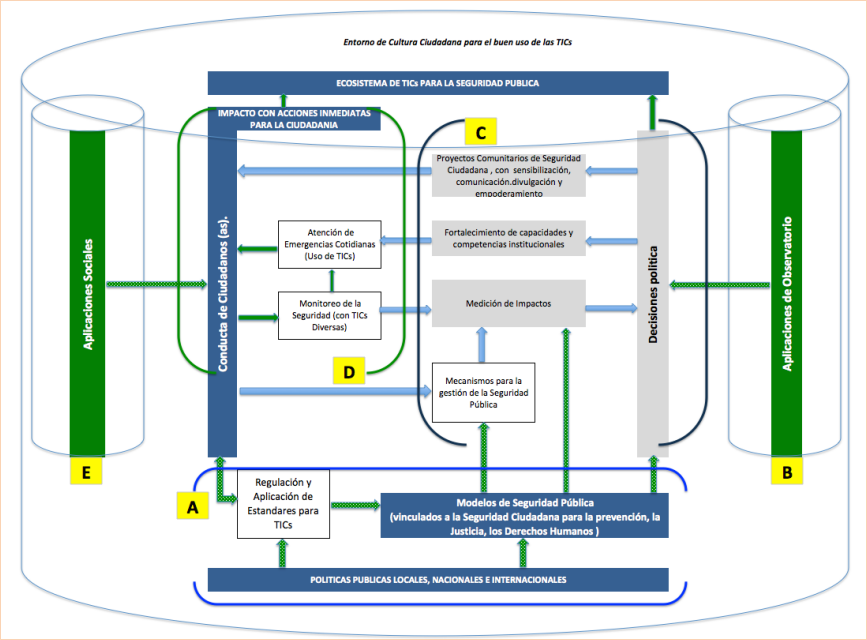
La comunicación inicia entonces con el ciudadano cuando éste reporta la desaparición o posible privación ilegal de la libertad de un menor. La solicitud de Alerta AMBER es analizada por el Comité Estatal, y en su caso por el Comité Nacional, para decidir si la activación de la alerta procede y de ser así detonar los mecanismos de comunicación masiva a través de todos los medios al alcance. De esta manera, se da a conocer la alerta entre la población, con una escala estatal, inter-estatal, nacional o si el caso lo requiere, más allá de las fronteras nacionales.

2.8 El ecosistema en base al ciclo de la experiencia

Un ecosistema, describe un entorno colectivo de gestión de información y conocimiento, interoperabilidad tecnológica, respeto de normativas y la participación de la ciudadanía en la gestión pública de la Seguridad Ciudadana, ya que como se aprecia las aplicaciones sociales y las aplicaciones de observatorio son importantes y básicas para su interoperabilidad, ante esto el ecosistema óptimo evoluciona en un entorno de cultura ciudadana para el buen uso de las TICs, en una demanda de mejorar el "contrato social para la seguridad" inclusivo y regulado, como se puede ver en la figura siguiente :

[25] http://www.aguascalientes.gob.mx/segob/LOCATEL/amber.aspx
[26] http://www.amberalert.gov/
[27] http://www.ctia.org/
[28] http://www.alertaamber.gob.mx/

Figura 7: Ecosistema de la Seguridad Ciudadana



Fuente: *Elaboración propia*

Entendiendo el ecosistema: para facilitar el entendimiento de la presentación de Soluciones y Tecnologías para la Seguridad Pública, se ha elaborado un Marco Estructural que permite comprender con claridad el ecosistema alrededor de las TICs en la Seguridad Pública y Ciudadana sobre los siguientes componentes:

A. Marcos Jurídicos y Regulatorios
B. Datos abiertos
C. Interoperabilidad
D. Impacto en la ciudadanía
E. Aplicaciones sociales

Los componentes y factores a considerar para la funcionalidad de un ecosistema de TICs para la Seguridad Pública y Ciudadana se presentan en la siguiente tabla.

Tabla 2: Componentes y factores para la funcionalidad de un ecosistema de TICs para la Seguridad Pública y Ciudadana.

COMPONENTE	FACTORES
A. Marcos Jurídicos y Regulatorios	En la armonización del marco político y jurídico con la finalidad de propiciar un entorno de certeza y confianza favorables para la adopción y fomento de las TIC con: • Políticas públicas vinculadas al entorno de la TICs • Regulación y aplicación de estándares para TICs. • Modelos de Seguridad Pública vinculados a las TICs para la Seguridad Ciudadana que permitan abordajes en la previsión y prevención de

COMPONENTE	FACTORES
	violencias, delitos y conflictividades, el acceso a la Justicia y el respeto de los Derechos Humanos.
B. Datos abiertos	Análisis y estudio de Problemáticas mediante la facilidad de observatorio y centros de estudio y análisis para la disponibilidad de información gubernamental y de la sociedad en general en formatos útiles y reutilizables por la población en general, para fomentar la "toma de decisiones" a través de la gestión de conocimiento sobre seguridad pública y ciudadana.
C. Interoperabilidad	Se refiere a las capacidades técnicas, organizacionales, de gobernanza y de innovaciones, necesarias en las TICs para compartir información y conocimiento de forma consistente, considerando la necesidad de: • Crear y consolidar mecanismos para la gestión de la seguridad pública como mesas y comités interinstitucionales. • El fortalecimiento de capacidades y competencias institucionales. • La gestión de proyectos Comunitarios de Seguridad Ciudadana fundamentados en el conocimiento y evidencia de las problemáticas en los territorios.
D. Impacto en la ciudadanía	El impacto en la ciudadanía debe estar llevado por dos facilidades básicas: • El monitoreo y evaluación de los resultados en la seguridad, alrededor de la respuesta que se demanda • El grado de efectividad en la atención de las emergencias cotidianas y riesgos por situaciones naturales.
E. Aplicaciones sociales	Analizar y estudiar las facilidades de nuevas tecnologías de redes como • Principalmente LTE que no solo optimizan el transporte de datos y la integración de otros servicios de multimedia, sino que facilitan la comunicación entre ciudades, países y regiones en materia de Seguridad Pública • Implementar aplicaciones de redes sociales en el trabajo policial facilitando el acceso de las instituciones de seguridad pública y de la ciudadanía

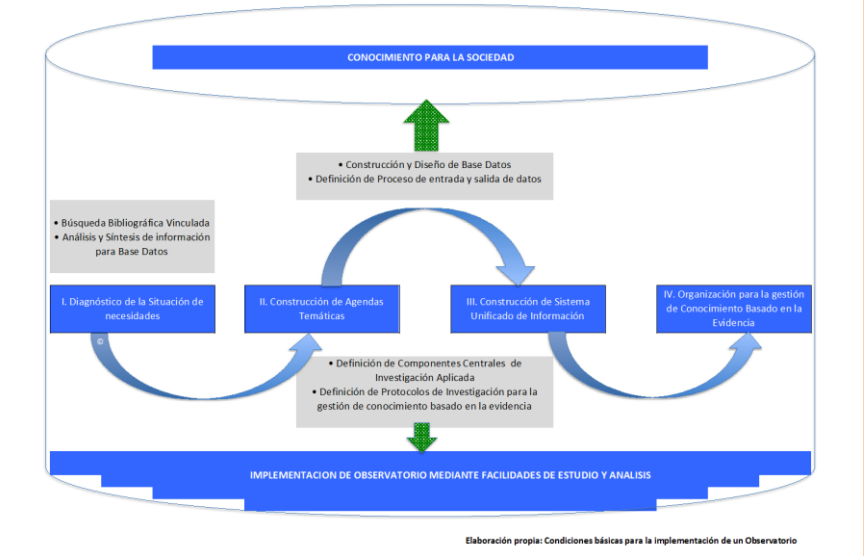
a) Observatorios de Seguridad Ciudadana

Dado que el espíritu mismo de la metodología de observatorio es constituirse en un mecanismo para a la recopilación sistemática y permanente de datos y su conversión en información, para dotarla de importancia y propósito en la contribución de la edificación de bienes públicos[29] (considerando los males públicos existentes como el de la Inseguridad); de manera que pueda aportar elementos de decisión para monitorear y validar el comportamiento y evolución del fenómeno o campo de observación que se desea monitorear o visibilizar; sin embargo este concepto se extiende más allá del análisis institucional de la información, al estudio y análisis conjunto para gestionar conocimiento, aunque puede limitarse a esto.

Sin embargo, tal y como lo ha definido el Observatorio del Desarrollo, de la Universidad de Costa Rica (UCR), "*un observatorio temático tiene implicaciones más profundas y se convierte en "una instancia que abre un espacio de reflexión e interacción entre actores estratégicos, quienes trabajan intercambiando inquietudes y perspectivas con el objetivo de ejecutar iniciativas o sustentar políticas públicas hacia metas comunes en un área temática del desarrollo."*

[29] Isabelle Grunberg, Inge Kaul, Marc A. Stern. "Bienes públicos mundiales, Cooperación internacional en el siglo XXI" Publicado por el Programa de las Naciones Unidas para el Desarrollo (PNUD), 1999

Figura 8: Flujo de datos e información en un Observatorio Temático



Fuente: *Elaboración propia*

Un observatorio tiene como misión el proveer metodologías innovadoras para sistematizar y transformar la información existente en nuevas mediciones que permitan, gestionar conocimiento para la sociedad basado en la evidencia.

Considerando que trabajar con información basada en la evidencia demanda acciones de estudio y análisis, que vinculan el proceso básico de la investigación aplicada: observando, estudiando y analizando; un observatorio debe ser considerado como un mecanismo que facilita el estudio y el análisis, usando TICs con aplicaciones públicas para la Seguridad Ciudadana y Pública.

Las principales actividades[30] de un observatorio de Seguridad y Convivencia Ciudadana se pueden esbozar sobre lo siguiente:

- **La investigación aplicada**: Desarrollando estudios interdisciplinarios de reflexión e investigación en previsión y prevención de violencias, delitos, conflictividades urbanas para la convivencia y seguridad ciudadana.
- **Recomendaciones:** Generando los insumos para formular políticas públicas con base en el conocimiento adquirido de la realidad de las comunidades, los paises y la región.
- **Monitoreo y Evaluación**: Realizando el seguimiento y evaluación a las distintas políticas que se implementen sobre seguridad y convivencia ciudadana.
- **Participación Ciudadana**: Propiciando espacios de discusión a nivel local, regional, nacional e internacional para el intercambio de experiencias y el aprendizaje de procesos llevados en diferentes sitios en conjunto con la ciudadanía.
- **Sensibilización y Comunicación**: Publicando los resultados de los estudios desarrollados en el campo institucional, académico y en la sociedad en su conjunto, mediante publicaciones, eventos y en ambientes virtuales.

[30] Desarrollado en base a buenas prácticas con Observatorios, elaboración propia el consultor

Un Observatorio de Seguridad Ciudadana debe considerar aspectos importantes para su operatividad como los siguientes:

1. Conocer lo que sucede: sobre la incidencia delictiva, de violencias y conflictividades accediendo a bases de datos de fuentes primarias para el conocimiento objetivo de la inseguridad;
2. Conocer lo que siente la ciudadanía: mediante encuestas e instrumentos de percepción de la seguridad y la convivencia, el miedo al delito y la percepción de la victimización, para el conocimiento subjetivo y de contexto de la inseguridad.
3. Conocer lo que se hace: seguimiento a la efectividad de las intervenciones en materia de seguridad de las políticas, modelos, y regulaciones vigentes y aplicadas principalmente por gobiernos (centrales y locales) en base al estudio y análisis realizado.

b) APPs para la Seguridad Pública y la Justicia, un entorno práctico

Una mirada de APPs en el Sur del Continente

Se considera la observancia de APPs relevantes que actualmente inciden en la seguridad ciudadana en paises de Sur America como ser:

Venezuela[31]:

App de Seguridad: Patrullaje de Inteligente[32]

Esta aplicación detecta el cuadrante de seguridad correspondiente a su ubicación, proporcionada por el GPS de su móvil, o mediante su proveedor de red, y le indica la información para que pueda contactar el teléfono de emergencia asociado.

- La ciudadanía[33] puede llamar a autoridades policiales y militares más cercanas a su cuadrante y realizar sus denuncias de manera anónima.
- El GPS del teléfono debe estar activo para garantizar el buen funcionamiento de la aplicación de Patrullaje Inteligente.

¿En qué consisten los cuadrantes policiales?

Consiste en el despliegue operativo de unidades policiales y militares encargadas de ejecutar de manera oportuna funciones de vigilancia y prevención del delito en sectores específicos para garantizar la seguridad ciudadana.

El Patrullaje Inteligente permite el contacto directo de los funcionarios y funcionarias con las comunidades, con el propósito de atender de forma inmediata sus requerimientos y disminuir la incidencia delictiva.

¿Cómo se organizan los equipos?

- Los funcionarios y funcionarias están divididos por cuadrantes.
- Se desplazan mediante patrullas o motocicletas en cada uno de los cuadrantes. Esta organización proporciona alta movilidad y oportuna atención de las denuncias que realizan las comunidades.

[31] http://gobiernoenlinea.gob.ve/home/homeG.dot

[32] https://www.youtube.com/watch?v=B3kRtrLoj9Y

[33] http://www.rnv.gob.ve/index.php/descarga-y-enterate-aqui-como-funciona-la-aplicacion-de-patrullaje-inteligente

- Por cada cuadrante se asigna un número telefónico que está a disposición de todos los miembros de la comunidad, quienes podrán comunicarse con los efectivos policiales y militares para denunciar algún hecho delictivo.
- Se establecen diferentes turnos para la rotación de los funcionarios funcionarias.

¿Cuáles denuncias se pueden realizar?

Cualquier hecho delictivo (Hurto, robo, tráfico de drogas, porte ilícito de armas de fuego y municiones, secuestro, extorsión, cobro de vacunas, contrabando de gasolina y alimentos, otros).

- Violencia de género y maltrato de niños, niñas y adolescentes.
- Déficit de convivencia (música a alto volumen, conflictos comunitarios).
- Otros temas que afecten la seguridad de tu comunidad.

Colombia:

App: Legal App

LegalApp es una herramienta electrónica para todos los ciudadanos que necesiten conocer cómo adelantar un trámite o hacer uso de algún servicio relacionado con la Justicia.

Digitando palabras claves, esta herramienta orienta a las personas sobre qué hacer, la autoridad o institución a la cual puede acudir y la ubicación exacta en su municipio.

123 Emergencias (911)

Es una plataforma "Centralizada", que atiende llamadas de emergencia de su centro de operaciones , también tiene facilidades de atención "descentralizada"[34] para la ciudadanía. Cuenta también con un sistema digital de quejas y denuncias, realiza acciones conjunta de estudio y análisis mediante alianza con el Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana (CEACSC), funciona como **Número Único de Seguridad y Emergencias (NUSE)**[35]

Ecuador[36]**:**

App de atención al 911: Ecu 911

El Servicio Integrado de Seguridad ECU 911 reserva los derechos de la aplicación e impone las sanciones que estime pertinentes en caso de mal uso. Mal uso contempla reportes de emergencias que impliquen el desplazamiento innecesario de recursos.

- Mal uso inicial, bloqueo del aplicativo por 30 días.
- Reincidencia inicial de mal uso, bloqueo del aplicativo por 6 meses.
- Segunda reincidencia de mal uso, bloqueo definitivo del aplicativo.

[34] http://www.123bogota.gov.co/index.php/atencion-a-la-ciudadania/puntos-de-servicio-de-atencion-a-la-ciudadania
[35] https://www.youtube.com/watch?v=4_PhhwXQL0g
[36] http://www.seguridad.gob.ec/

Toda información que se solicita e ingresa a esta aplicación será utilizada exclusivamente con el propósito para el cual fue requerido. La información ingresada debe ser verídica[37], a fin de brindar una asistencia oportuna[38].

Cómo reportar una Emergencia:

Paso 1.- Escoge la Institución para atender tu emergencia.

Paso 2.- Escoge el incidente que describa tu emergencia.

Paso 3.- Confirma el envío de tu emergencia.

Perú

Aplicativo para Justicia y Derechos Humanos

App móvil del sistema jurídico de Perú: SPIJ

Sistema Peruano de Información Jurídica del Ministerio de Justicia.[39]

Aplicación móvil que permite realizar consultas de las normas publicadas en el Perú de manera similar a las versiones del Sistema Peruano de Información Jurídica (SPIJ)

Escritorio y SPIJ Web.

- El aplicativo también permite descargar los resúmenes del día, así como las normas publicadas en el Diario Oficial el Peruano.
- Permite mostrar las sedes, módulos y laboratorios del SPIJ.
- También ofrece un servicio de notificaciones para avisar oportunamente los eventos programados en el Ministerio de Justicia.

Chile[40]:

App de justicia: Busca Justicia

Busca Justicia es una aplicación que facilita la búsqueda de servicios de justicia en todo Chile, permitiendo a los ciudadanos acceder a ella en cualquier momento y desde diversos dispositivos móviles.

Desarrollada por el Ministerio de Justicia, esta aplicación ha sido implementada en el marco del proyecto Justicia Responde, plataforma que busca solucionar los diferentes requerimientos judiciales de la ciudadanía, a través de la entrega de orientación, soluciones a los requerimientos de las personas además de la realización de trámites en línea. En la actualización de base de datos[41], ahora se incluyen:

- Carabineros
- Policía de Investigaciones

[37] https://www.youtube.com/watch?t=17&v=wQkAeqzeUQM , Información sobre ECU911

[38] https://www.youtube.com/watch?v=IdD75JHfUN0

[39] http://spij.minjus.gob.pe

[40] http://www.gob.cl/ministros/interior/

[41] Busca Justicia Chile: https://play.google.com/store/apps/details?id=cl.gob.minjusticia.buscadorjusticia

- Fiscalías
- Centros de Mediación
- Tribunales especializados

“Casos exitosos del uso de TIC en seguridad pública en América Latina”

Parte III: Casos de éxito en el mundo.

3. Casos de éxito en el mundo.

Según datos publicados por la UIT indican que en los últimos 15 años las tecnologías de la información y la comunicación(TIC) han experimentado un crecimiento sin precedentes, ofreciendo ingentes oportunidades de desarrollo socioeconómico.

Los nuevos datos muestran la evolución de las TIC y las diferencias en conectividad desde el año 2000, cuando los líderes mundiales establecieron los Objetivos de Desarrollo del Milenio (ODM) de las Naciones Unidas.[42]

Hoy en día, hay más de 7,000 millones de abonados a la telefonía móvil en el mundo, cifra que el año 2000 era de 748 millones. A escala mundial, 3 200 millones de personas utilizan Internet, de los cuales 2,000 millones viven en países en desarrollo.

"Además de mostrar el rápido progreso tecnológico logrado hasta la fecha, estos nuevos datos ayudan a identificar a los que han quedado a la zaga de la economía digital, que tan rápido evoluciona, así como los ámbitos que requieren mayor inversión en TIC", declaró el Secretario General, Sr. Houlin Zhao, en la conferencia de prensa para la presentación del informe Foro de la CMSI de 2015 en Ginebra.

"Las TIC desempeñarán un papel más significativo en la era posterior a 2015 y en el futuro cumplimiento de los objetivos de desarrollo sostenible a medida que el mundo evoluciona cada vez más rápido hacia una sociedad digital", declaró el Sr. Brahima Sanou, Director de la Oficina de Desarrollo de las Telecomunicaciones de la UIT.

"Nuestra misión es conectar a todos y crear una sociedad de la información realmente integradora, para lo cual necesitamos disponer de datos y estadísticas de elevada calidad que nos permitan cuantificar el progreso."

La penetración de usuarios Internet se multiplicó por siete desde el año 2000

Entre 2000 y 2015 la penetración de Internet se ha multiplicado casi por siete, pasando de 6,5 al 43 por ciento de la población mundial.

La proporción de hogares con acceso a Internet aumentó del 18 por ciento en 2005 al 46 por ciento en 2015.

Los datos de la UIT también indican que en el mundo en desarrollo sigue habiendo 4,000 millones de personas sin acceso a Internet. De los casi 1,000 millones de personas que viven en países menos adelantados (PMA), 851 millones no utilizan Internet.

La cobertura 3G de banda ancha se expande rápidamente

La banda ancha móvil es el segmento de mercado más dinámico, con una penetración móvil de banda ancha que asciende a 47 por ciento en 2015, 12 veces más que en 2007. En 2015, el 69 por ciento de la población mundial tiene cobertura en banda ancha móvil 3G, cifra que en 2011 era del 45 por ciento.

También se ha producido una rápida expansión de la banda ancha móvil 3G en zonas rurales; y la UIT estima que a finales de 2015 el 29 por ciento de los 3 400 millones de personas que habitan en zonas rurales tendrán cobertura en banda ancha móvil 3G. De los 4 000 millones de personas que viven en zonas urbanas, el 89 por ciento tiene acceso a la banda ancha móvil 3G.

[42] https://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx

La banda ancha fija crece a un ritmo más pausado

La banda ancha fija crece a un ritmo más lento, a saber, un siete por ciento anual en los últimos tres años. Si bien los precios de los servicios de banda ancha fija han disminuido considerablemente entre 2008 y 2011 en los países en desarrollo, desde entonces se han quedado estancados e incluso han aumentado ligeramente en los PMA.

Según GSMA que representa los intereses de los operadores móviles en todo el mundo, que une a casi 800 operadores de más de 250 empresas en el más amplio ecosistema móvil, incluyendo fabricantes de teléfonos móviles y dispositivos, compañías de software, proveedores de equipos y compañías de Internet, así como organizaciones de los sectores industriales adyacentes en su publicación "The Mobile Economy", la industria móvil continúa escalando rápidamente, con un total de 3,6 billones de suscriptores móviles únicas a finales de 2014. Un billón adicional de suscriptores se prevé para el año 2020, tomando la tasa de penetración mundial de aproximadamente el 60%. Había 7.1 billones conexiones SIM globales a finales de 2014, alrededor de 243 millones de conexiones de máquina a máquina (M2M).

Según el Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC[43] Al 2010, sobre la verificación de objetivos de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en su examen intermedio el 75% de la población rural del mundo tenía cobertura de señal móvil celular.- Según las proyecciones de GSMA[44] sobre la incidencia de como contribuye la economía móvil al desarrollo social en todo el mundo se proyecta sobre lo siguiente:

Tabla 3: Proyecciones sobre la incidencia de la economía móvil al desarrollo social, según datos de la GSMA

	Ejes	Proyecciones
	La entrega de la inclusión digital a las poblaciones todavía no conectadas.	Penetración de Internet móvil Al 2014: 33% Al 2020: 49%
	La entrega de la inclusión financiera a las poblaciones no bancarizadas.	255 cruces de servicios en vivo En 89 países a diciembre 2014
	La entrega de nuevos servicios innovadores y aplicaciones (APPs).	Número de conexiones M2M por llegar a 1billon en 2020

Hoy en día se considera al siglo XXI como el siglo de las Tecnologías de Información y Comunicación (TIC). El continente americano no se excluye de las tendencias de disponibilidad de Internet y del uso de dispositivos móviles e inteligentes, que han ampliado y aumentado la comunicación e información en nuestras vidas.

El mercado móvil latinoamericano está dominado por Brasil[45], con 114 millones de suscriptores únicos para septiembre de 2014, lo que representa más de un tercio de la base total de la región. Brasil ocupa

[43] https://www.itu.int/pub/D-IND-WTDR-2010/es
[44] Se conservan los iconos originales del estudio The Mobile Economy
[45] The mobile Economy Latin America 2014, de GSMA

actualmente el quinto mayor mercado a nivel mundial en términos de suscriptores, y se prevé que superará a Japón para convertirse en el cuarto mayor a finales de 2015. Los cinco países más grandes de la región cuentan con más de 230 millones de suscriptores entre ellos, equivalente a más del 70% del total de América Latina.

El mismo estudio nos indica, que América Latina es muy diversa en términos de desarrollo económico y social, e igualmente en términos de penetración móvil (tanto en suscriptores como en conexiones únicas). Las tasas de penetración de conexión van de un mínimo del 73% en Haití a un máximo de 157% en Costa Rica. La tasa de penetración de la región en su conjunto se situó en el 112% a partir de septiembre de 2014, muy por encima de la media mundial del 96%.

América Latina está viendo una aceleración en la adopción de la banda ancha móvil y el crecimiento del tráfico de datos. Esto ha sido impulsado por un rápido cambio tecnológico a las conexiones de mayor velocidad que está en marcha en toda la región. A finales de 2012, los servicios de 2G todavía representaron el 78% de las conexiones totales, pero en septiembre 2014, habían caído a 60%. En consecuencia, las conexiones 3G aumentaron de 22% a finales de 2012 a 39% en el tercer trimestre de 2014. Esto es más alto que el promedio mundial de 32% y superior a la media del mercado en desarrollo del 27%.

Por el contrario, 4G esta todavía en su infancia relativa. A septiembre de 2014, sólo un poco más del 1% de las conexiones eran 4G, en línea con la media del mercado en desarrollo, pero en comparación con el 35% en América del Norte, el principal mercado de LTE. Sin embargo, se espera que el número de conexiones 4G siga creciendo a una tasa promedio de 85% anual en los siete años hasta 2020.

América Latina es una región que ha sufrido profundas transformaciones a lo largo de los últimos veinte años. Se puede observar la presencia de aspectos positivos, tales como el desarrollo de una economía regional más próspera e integrada, así como la existencia de democracias más consolidadas. Sin embargo, también es posible encontrar elementos contradictorios de este proceso, como que la región es la más desigual del mundo. En algunos países, los niveles de pobreza aún superan el 40% de la población (CEPAL, 2012). Además, la región enfrenta problemas tan graves como la violencia y el crimen, que generan la inseguridad y falta de convivencia. La UNODC (2012)[46] muestra una creciente alza en las tasas de delitos en la región, entre los años 2000 y 2010 aumentó en 12% la tasa de homicidios. De hecho, 10 de cada 20 países con las mayores tasas de homicidios del planeta se encuentran en este hemisferio (UNODC, 2013).

Para la Organización Panamericana de la Salud (OPS)[47] un índice bajo de criminalidad es el que se halla entre 0 y 5 homicidios por cada 100.000 habitantes por año. Ese puede ser tratado con los mecanismos convencionales. Cuando el índice de homicidios está entre 5 y 8 la situación es delicada, pero cuando excede de 8 nos encontramos frente a un cuadro de criminalidad “epidémica”. No puede ser tratada por las vías usuales. Han demostrado ser insuficientes. A pesar de las diferencias nacionales, la región se encuentra con violencia letal alta, con tasas de homicidios en niveles casi epidémicos[48] y una muy baja percepción de seguridad. Tales características están asociadas a dos tipos de delitos con alta presencia en América Latina el homicidio y el narcotráfico. Los países que más han sufrido la incidencia de los delitos, las violencias y las conflictividades según muestreo del 2000 al 2012 de datos recabados por The United Nations Office on Drugs and Crime (UNODC), son Colombia, en segundo lugar, Honduras, en tercer lugar, El Salvador, seguidos de Jamaica, Venezuela, Guatemala y Bahamas en su orden, este análisis no considera los incrementos de la incidencia criminalista del 2013 al 2015, se fundamenta en el análisis del impacto del delito homicidio.

[46] http://www.unodc.org/gsh/en/data.html

[47] http://www.paho.org/mex/index.php?option=com_content&view=article&id=206%3Asituacion-salud-americas&Itemid=319

[48] http://www.sicasalud.net/sites/default/files/INDICADORES%20BASICOS%202013_0.pdf

3.1 Selección de casos de éxito mundiales

Considerando la tecnología como un medio que aporta, diferentes soluciones en áreas vitales de la Seguridad Pública. Por ejemplo:

- La proximidad que brinda el Internet, que permite, mantener actualizados de forma permanente al personal policial, sobre órdenes de comando estratégicas sea esto en centros de operaciones o a través de unidades móviles de comunicaciones en medios móviles de respuesta ciudadana.
- Soluciones posicionadas y referenciadas, que tienen como objetivo suministrar información cartográfica relacionada con investigación estadística y documental, que se usa en áreas de inteligencia criminal para la elaboración de mapas del delito caracterizando zonas de delitos, violencias y conflictividades.
- Tanto el desarrollo de sitios vinculados a la seguridad pública como el posicionamiento global determinado por satélite (GPS) para unidades móviles. cámaras de vídeo de alta definición con trasmisión simultánea para controlar el movimiento de sectores geográficos determinados.
- El acceso de telefonía satelital y celular 3G y 4G con conexión a Internet para lugares inhóspitos.
- Integración de bases de datos con huellas dactilares digitalizadas que pueden ser consultadas mediante scanner de alta seguridad, así como
- Los sistemas de identificación facial son ahora comunes en aplicaciones para la Seguridad Pública.

Según Cellular Telephone Industries Association (CTIA)[49][50] desde la necesidad de compartir textos, imágenes, video y voz, sobre servicios inalámbricos que mejoran el enfoque de cómo ser los primeros en responder y manejar las emergencias. Es esencial que las funciones de seguridad pública estén suficientemente financiadas, incluyendo actualizaciones y mejoras a la tecnología, en este sentido en base a la alta experiencia de CTIA en este campo los criterios básicos para poder examinar casos de éxito radican en tres grandes ejes:

1) Los estándares operacionales.
2) Los estándares técnicos.
3) Los estándares de formación.

Se pueden considerar dentro de los estándares antes mencionados:

1) **Los estándares operacionales que facilitan:**
   a. La disposición para el intercambio común de datos
   b. Prácticas de gerencia y despliegue
   c. Criterios de capacidad de servicio
   d. Despliegue de respuesta para emergencias
   e. Capacidad de respuesta a grupos vulnerables: como Desaparecidos, Secuestrados y niños explotados sexualmente
   f. Nomenclatura de uso de Canales estándares para la Interoperabilidad
   g. Requisitos funcionales mínimos asociados al despacho (Computer Aided Dispatch CAD)
   h. Prácticas para el uso de los medios sociales en comunicaciones de seguridad pública
   i. Códigos de estado Común para el Intercambio de Datos

[49] CTIA - The Wireless Association , originalmente conocida como la Asociación de Industrias de teléfono celular
[50] http://www.ctia.org/policy-initiatives/policy-topics/911

j. Establecimiento de un Programa de Garantía de Calidad y Mejora de la Calidad de los puntos de respuesta de seguridad pública

2) **Los estándares técnicos como ser:**
   a. El protocolo automatizado de alarma
   b. Tipos de comunicaciones comunes en Seguridad Pública, de incidentes que facilitan el intercambio de datos.
3) **Los estándares de formación:**
   a. Para el desarrollo de competencias básicas y normas mínimas de formación de Oficiales de Entrenamiento en Comunicaciones para la Seguridad Pública.

3.2 Determinación de mejor práctica en la efectividad social

Las Tecnologías de la Información y la Comunicación (TICs) ofrecen una variedad de herramientas y aplicaciones capaces de abrir nuevas posibilidades para la Seguridad Pública y Nacional de los países. En particular, las TICs pueden ayudar a adaptar el proceso de prevención de las violencias, los delitos y conflictividades principalmente urbanas, a las necesidades individuales de los ciudadanos, en sus comunidades, sus entornos en una posibilidad desde lo local a lo nacional y viceversa sin desvincular lo global, ya que muchas de las necesidades de coordinación son de carácter transnacional y global.

La solución para una utilización eficaz de las TICs en los temas de Seguridad, sin embargo, no solo reside en la propia tecnología. Se debe considerar el garantizar el acceso universal a las TICs, para lograr un éxito considerable, en este entorno es deseable que existan marcos regulatorios y legales que deberían dirigirse a avanzar en la comprensión sobre cómo emplear eficazmente las nuevas tecnologías y sobre donde existen obstáculos en el camino participativo hacia el éxito de una interoperabilidad técnica y social de las TICs.

3.3 Análisis de tendencias

Según la Unión Internacional de Telecomunicaciones en su artículo "Banda[51] ancha móvil, teléfonos inteligentes, aplicaciones y redes fijas" se presentan cuatro desafíos para los organismos de reglamentación con relación a la cuarta generación

i. **Banda ancha móvil**
   La mitad de la población mundial disponía en 2013 de cobertura de red de banda ancha móvil de tercera generación (3G). La migración a la tecnología denominada "evolución de red a largo plazo" o "Long-Term Evolution" (LTE) se está desarrollando a una velocidad mucho mayor que la migración anterior de las redes 2G a 3G. En 2013 existían redes LTE comerciales en 88 países (según la Asociación GSMA), o en 101 países (según la Asociación mundial de fabricantes de sistemas móviles), cuando hace tres años sólo existían redes LTE en 14 países. Ericsson estima que el 65% de la población mundial tendrá cobertura de LTE en 2019, comparado con el 10% en 2012.

   En 2013 se vendieron más de 1.000 millones de teléfonos móviles inteligentes, con un 38% de crecimiento, superando la cifra de ventas de teléfonos comunes.

ii. **Aplicaciones y tráfico de servicios de datos móviles**
   El mercado de las aplicaciones ("apps") superó las 100.000 millones de descargas en 2013, representando un 50% de crecimiento respecto al año anterior. La estimación de ingresos totales ha sido de unos 26.000 millones de USD en 2013, aunque las aplicaciones gratuitas fueron el 91% del total de descargas.

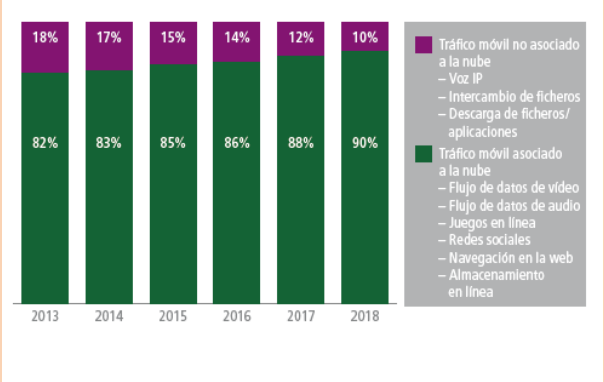
[51] https://itunews.itu.int/Es/5086-Banda-ancha-movil-telefonos-inteligentes-aplicaciones-y-redes-fijas.note.aspx

El tráfico de vídeo en la red móvil supuso a finales de 2013 más del 50% del tráfico de datos móviles y es previsible que crezca hasta representar casi el 70% en 2018. En ese momento es probable que las aplicaciones en la nube lleguen a representar el 90% del tráfico de datos móviles.

iii. Redes fijas de banda ancha

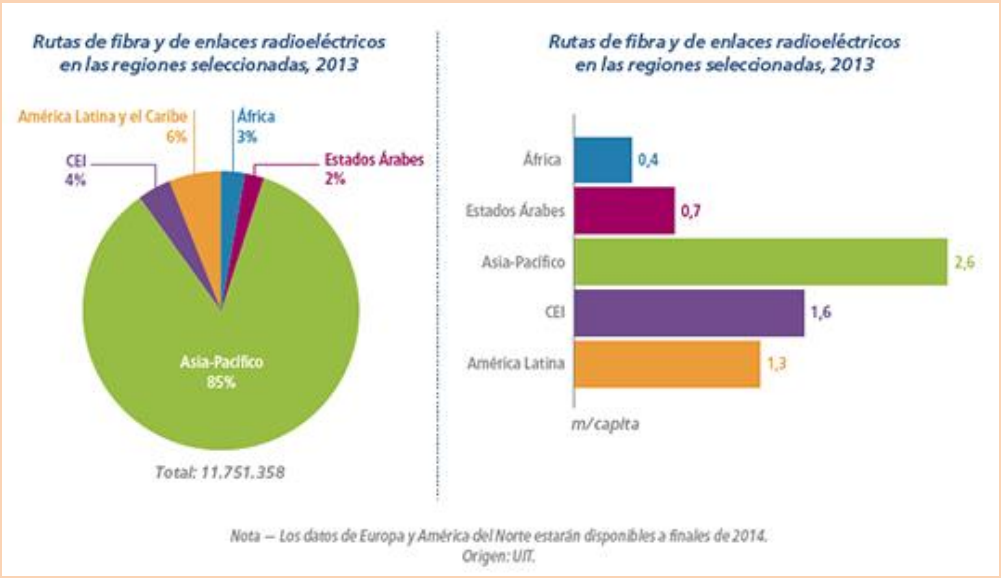
A finales de 2013 existían más de 11,7 millones de kilómetros de redes troncales de fibra y por medios radioeléctricos en cinco zonas del mundo: África, Estados Árabes, Asia-Pacífico, Comunidad de Estados Independientes (CEI) y América Latina y el Caribe. La recopilación de datos de estas regiones es parte del proyecto de la UIT de disponer de un mapa de la conectividad mundial.[52]

Figura 9: Tráfico móvil según asociación a la nube



Fuente: *UIT en base a datos de la propia UIT, Gartner, Cisco VNI, Telegraphy e IDC*

Figura 10: Rutas de fibra y enlaces radioeléctricos en África, Estados Árabes, Asia-Pacífico, CEI y América Latina



Fuente: *Tomado, de la Unión Internacional de Telecomunicaciones (UIT), Tendencias en el mercado de las TIC, Banda ancha móvil, teléfonos inteligentes, aplicaciones y redes fijas, Cuatro desafíos para los organismos de reglamentación de cuarta generación, Redes fijas de banda ancha.*

[52] https://itunews.itu.int/Es/5086-Banda-ancha-movil-telefonos-inteligentes-aplicaciones-y-redes-fijas.note.aspx

iv. Aprovechamiento de Líneas de cobre

Entre tanto, es importante aprovechar al máximo las líneas de cobre existentes para que los ciudadanos se beneficien de los servicios de banda ancha de alta velocidad. Ello puede proporcionar una solución alternativa, al menos a corto plazo, que permita aumentar la velocidad de acceso a hasta 1 Gbit/s en los últimos cien metros de la red.

3.4 Análisis de características

Según el Informe, con la recomendación UIT-R SM.2015, "Los gobiernos nacionales y locales, así como las fuerzas armadas, tendrán necesidades de espectro para satisfacer futuros sistemas de radiocomunicaciones. Aunque los servicios comerciales pueden satisfacer una parte de estas necesidades, muchos pueden ser singulares y requerirán espectro y sistemas radioeléctricos especiales dedicados para estos fines. Es probable que algunos de los sistemas puedan exigir seguridad nacional[53] en la medida que su conocimiento no debe estar en el dominio público, y deben ser protegidos por la entidad reglamentaria".

Avanzando en las regulaciones y tendencias, la Recomendación UIT-T E.161.1[54] ofrece orientación a los Estados Miembros que se encuentran en el proceso de selección de un número de emergencia único por primera vez, o de un número de emergencia secundario alternativo para las redes públicas de telecomunicaciones. Según esta recomendación **una llamada de emergencia** [b-UIT-T Q-Sup.47] se define como la: "Llamada que solicita servicios de emergencia. Se ofrece a la parte llamante una forma rápida y fácil de comunicar información relativa a una situación de emergencia a la organización competente (por ejemplo, bomberos, policía, ambulancias). Las llamadas de emergencia se encaminarán a los servicios de emergencia de conformidad con los reglamentos nacionales".- **Un número de emergencia** se define como el: "número de tipo distinto al E.164 atribuido en el **plan nacional de numeración** para efectuar llamadas de emergencia. Por regla general, el número de emergencia suele ser un código abreviado".- En este sentido UIT recomienda a todo Estado Miembro que tenga previsto introducir un segundo número de emergencia alternativo podría considerar la posibilidad de utilizar el 112 o el 911, o ambos, el cual debería encaminarse hacia el número de emergencia vigente. El segundo número de emergencia alternativo resulta útil, por ejemplo, para las personas que se encuentran visitando al país y desean efectuar una llamada de emergencia.

Complementario a lo anterior la CTIA[55] sitúa dos escenarios alrededor de la gestión de emergencias en sistemas tipo 911

- El demoninado Enhanced 911 (E-911): tecnología que complementa la interacción entre los primeros sistemas de atención pública asegurando que todas las llamadas se desvían a un centro de llamadas y permiten transmitir información, incluyendo la ubicación, a un "punto de respuesta de seguridad pública" (PSAP en inglés)
- Next Generation 911 (NG911): las acciones conjuntas con la seguridad pública, la industria inalámbrica y la iniciativa de los formuladores de políticas para actualizar la infraestructura de 911 para permitir que los PSAP sean capaces de recibir voz, texto, vídeo y mensajes multimedia.

En Estados Unidos de Norte América, según CTIA-The Wireless Association más de 38 por ciento de los hogares estadounidenses cuentan con teléfonos inalámbricos, no es sorprendente que más de 400 mil llamadas al 911 se realizan desde dispositivos inalámbricos todos los días. CTIA sigue apoyando a la regla de

[53] Métodos para la determinación de estrategias nacionales a largo plazo para la utilización del espectro radioeléctrico (Cuestión UIT-R 205/1), Informe UIT-R SM.2015

[54] Directrices para seleccionar el número de emergencia en redes públicas de telecomunicaciones (Recomendación UIT-T E.161.1), Sector de Normalización de las Telecomunicaciones de la UIT (09/2008).

[55] http://www.ctia.org/policy-initiatives/policy-topics/911

la FCC "todas las llamadas" para los 911 y E-911 servicios, que asegura todas las llamadas se desvían a un PSAP[56]

Recuadro 1: ¿Cómo identificar casos de éxito?

En este contexto la buena práctica para identificar casos de éxito, redunda alrededor de:

1. Las aplicaciones políticas, normas y regulaciones sobre las TICs considerando los modelos existentes para la Seguridad Pública.
2. La consideración de recomendaciones internacionales de UIT en los vinculado a las recomendaciones UIT-T E.161.1 y el UIT-R SM.2015, sobre la planificación espectral el uso de los números de emergencia, lo vinculado a los planes nacionales de numeración y las consideraciones.
3. La consideración de experiencias de organizaciones como CTIA que habiendo llevado a la practica las recomendaciones de la UIT, que han logrado incidir en un sistema ordenado de emergencia a la población y ejecuta facilidades de despacho y desplazamiento coordinado y oportuno.
4. La facilidad de la "conexión e interoperabilidad" que permite la regulación, su aplicación, el ordenamiento para que las TICs tomen un valor preponderante para atender las emergencias cotidianas y de Seguridad Pública, está vinculado a que puedan trabajar unos con otros.

Mientras "Text-to-911" representa una herramienta de seguridad pública de gran valor en USA, siempre se prefieren las llamadas de voz ya que transmite la mejor información de forma rápida, y la mayoría de las zonas todavía no admiten mensajes multimedia, como textos, vídeos e imágenes. Similares escenarios son recurrentes en el resto del continente americano.

"En el Reglamento de las Telecomunicaciones Internacionales (RTI) se afirma que las administraciones o los operadores pertinentes del sector privado deberían alcanzar acuerdos para proporcionar conectividad internacional. Y la promoción de la interoperabilidad es uno de los objetivos estratégicos de la UIT. Existe un consenso entre todos los miembros de la UIT en cuanto a la importancia fundamental de la interoperabilidad, lo que debe considerar la compleja combinación actual de normas legales, prácticas y normas técnicas patentadas aplicables a los sistemas y equipos. Incluso cuando dos redes están conectadas, ello no garantiza que todo aparato o servicio pueda funcionar sin interrupción en ambas."[57]

3.5 Análisis de cumplimiento de normas APCO 25

APCO[58], es la Asociación de Funcionarios de Seguridad Pública de comunicaciones con sede en los Estados Unidos, tiene un papel en el desarrollo de normas que afectan la industria.- En resumen APCO permite a las agencias acceder y compartir información crítica cuando y donde sea necesario. Esto ayuda a responder eficazmente a los desafíos diarios, a la creación de respuestas tácticas para mantener servicios vitales operativos en situaciones exigentes de Seguridad Pública y de Situaciones Cotidianas de Emergencias.

En el mundo superconectado de hoy, el intercambio de datos entre los dispositivos de consumo es casi instantáneo. Los primeros en responder son las instituciones como bomberos, la policía y las agencias de respuesta de emergencia, sin embargo, saben que el intercambio de información dentro de una organización no siempre es fácil, y mucho menos a través de múltiples agencias con diferentes competencias

[56] **Punto de Respuesta de Seguridad Pública (PSAP):** Un centro responsable de responder a llamadas 911 de emergencia de personas que despacha los servicios de emergencia tales como la policía, los bomberos y otros socorristas llamada.

[57] Información sobre los antecedentes de la CMI, Interconexión e interoperabilidad, UICT, 2012, Dubai, EAU,

[58] https://www.apcointl.org/

y equipos, diferentes tipos de tecnología y una marcada diferencia de disponibilidad de recursos, con sistemas de comunicaciones en algunas ocasiones con o ninguna información operativa.

La interoperabilidad se mantiene como el estándar de oro en las comunicaciones de seguridad pública, y muchos ya han hecho grandes avances en el logro de este objetivo. Por ejemplo el conocido Project 25 y APCO-25, se trata de un estándar de comunicaciones digitales por radio. Esta tecnología es un estándar de TIA (Telecommunications Industry Association) y está apoyada por APCO (Association of Public Safety Communication Officials – Project 25). Es ampliamente usada en Estados Unidos y Canadá, su estándar equivalente en Europa es el TETRA.

Una aplicación efectiva 911, según APCO debe cumplir:

Requisitos técnicos

- Cumplir con las normas de la industria.
- Operar en cualquier país.
- Ser tan fiable como el sistema existente 911.
- Mantener la sencillez de marcación 911.
- Facilidad de conectividad (ruta) de usuarios al PSAP apropiado.
- Uso y control Eficiente.

Requisitos operativos

- Trabajar sin demora, independientemente de cualquier novedad el sistema operativo del dispositivo o la aplicación en sí.
- El Sistema 911 debe estar libre para ser utilizado por el público. -En algunos estados de la Unión Americana su acceso puede implicar costos.
- No imponer costos irrazonables a un punto de respuesta de seguridad pública (PSAP)
- Cumplir con las normas de la FCC, los reglamentos estatales y locales, y las mejores prácticas de la industria
- Ser dispositivo y sistema operativo sin tendencias religiosas
- Requisitos de seguridad cibernética
- Conocer de seguridad pública

Requisitos de Formación

- Requisitos indispensables contar con un programa de formación de personal seguridad pública, enfocado a a la respuesta a la ciudadanía y a la administración de la seguridad

Hoy coexiste la sociedad real con la virtual. La cibercultura, surgida de la utilización de las nuevas tecnologías de la información y comunicación como ser el internet fomenta aspectos que facilitan las polaridades, el anonimato, la libertad absoluta, la circulación de la información sin barreras de tiempo y espacio, con universalidad; transmisión de información al infinito, con fuentes confiables y fuentes ficticias, así como con informaciones ciertas e informaciones adulteradas, que los usuarios principalmente deben saber distinguir.

Un campo de sembrado para la propagación de una nueva modalidad criminal, que afecta a todos los ciudadanos y a la cual las fuerzas policiales de américa latina luchan con desigualdad de capacidades y diversidad de medidas, principalmente en delitos contra la extorsión.

Desde este firmamento tecnológico se abre una perspectiva diferente para el ámbito de la Seguridad Pública. Que demanda la solución a problemas técnicos y operativos en el ámbito de dicha seguridad, con el empleo de estas nuevas tecnologías y en el área de la aplicación a nuevos ámbitos delictivos, que están incidiendo en la Seguridad y Convivencia Ciudadana a nivel global.

3.6 Aplicaciones especiales de IP Radio

La interoperabilidad de las comunicaciones es un imperativo reconocido para la seguridad nacional, seguridad pública, la seguridad interna, el cumplimiento de la ley o cualquier otra organización que deba compartir inteligencia, coordinar planes y montar operaciones conjuntas exitosas con otros organismos que operen en sistemas en frecuencias dispares o que necesiten integrarse a un sistema. Organismos locales, estatales y nacionales con sistemas de voz incompatibles pueden comunicarse con un radio utilizando una solución de interoperabilidad con protocolo de internet (IP), para que dos terminales IP puedan establecer una comunicación es necesaria una señalización**,** que facilite el intercambio de información entre los usuarios y la red, a fin de que la llamada pueda ser establecida y posteriormente, terminada. Esta señalización se puede efectuar mediante diferentes protocolos, pero hoy en día el protocolo más utilizado es SIP, cuyo significado es Session Initiation Protocol o protocolo de inicio de sesiones.

Como las tecnologías evolucionan, basadas en IP de voz, vídeo y sistemas de datos están proporcionando superiores rendimientos e información más rica en comparación con los enfoques tradicionales de aplicaciones de misión crítica o táctica.

Muchas redes de comunicaciones de seguridad pública están evolucionando y combinando IP multiprotocolo (Multiprotocol Label Switching MPLS) y estándares del Proyecto 25 (APCO 25), así como los basados en los protocolos TETRA (Terrestrial Trunked Radio) basado en sistemas de video vigilancia y finalmente, de Long Term Evolution (LTE) y Land mobile radio (LMR).

El sistema tradicional TETRA, está basado en nodos de conmutación y estaciones base que permiten:

- La gestión del sistema reduce los tiempos de espera y garantiza cortos periodos de establecimiento de llamadas (500ms)
- Los usuarios comparten automáticamente los recursos del sistema de manera organizada
- Alta funcionalidad en servicios de emergencia y la Seguridad en transmisión de voz y datos
- Sus funcionalidades permiten comunicaciones
    - Half Duplex: tipo de llamada con dos o más abonados. La comunicación se realiza en ambos sentidos con solo un abonado por turno. Sólo es utilizado un canal.
    - Simplex: tipo de llamada con dos o más abonados. La comunicación se realiza en ambos sentidos con solo un abonado por turno. Sólo es utilizada una frecuencia
    - Llamada de emergencia: mediante grupos selectivos
    - Llamadas de difusión: abriendo todas las terminales conectadas a la red
    - Redundancia de conmutación: de red, estaciones base, conexión con componentes externos
    - Integración de puestos de despacho
    - Localización automática de vehículos
    - Modelos de estados estándar OSI (ITU-T X.731)
    - Clases estándar de alarmas ITU-T M.3100
    - Grabador digital de voz

Las redes evolucionadas permiten mejorar la interoperabilidad una mejor integración con las aplicaciones de TICs. Debido a que muchas de estas aplicaciones son informáticas, de recursos intensivos y ricos en medios, requieren mucho más ancho de banda de misión crítica actual tráfico de voz y sensores. Los operadores de red pueden efectivamente hacer frente a las necesidades actuales y futuras de comunicaciones IP de seguridad pública.

3.7 Integración e Interoperabilidad de TICs para la Seguridad Ciudadana

La capacidad de las autoridades de implantar comunicaciones en tiempo real es crítica para organizar el centro de operaciones y control en la escena de una emergencia por eventos naturales o situaciones cotidianas de inseguridad, para mantener niveles óptimos de comprensión del entorno, y en general para

operar con efectividad dentro de un amplio rango de posibles situaciones. Las comunicaciones inalámbricas (incluyendo radio comunicaciones) son el medio más efectivo de transmitir y recibir información en una situación de emergencia adonde el área afectada puede no tener una infraestructura adecuada para apoyar al personal de emergencia, o la infraestructura existente puede haber sido destruida a causa del evento o en su defecto la conectividad se requiere en zonas aisladas o remotas específicamente sobre tres facilidades demandas

1. **Las necesidades operacionales:** consisten en la posibilidad de que autoridades como la policía o bomberos entre otros, establezcan y mantengan comunicaciones en apoyo de las operaciones de una gestión de inseguridad de forma coordinada.
2. **Necesidades de Interoperabilidad**: La capacidad de que el personal en un evento de diferentes competencias (ejemplo policía y bomberos) se pueda comunicar entre sí, que pueda también comunicarse personal de disciplinas diferentes (policía, cuerpos de investigación, medicina forense), y de niveles diferentes del gobierno (policía, gobierno de la ciudad), utilizando una variedad de bandas de frecuencia, según sea necesario y autorizado se conoce como "Interoperabilidad".
3. **Continuidad de las Comunicaciones:** La habilidad de que las agencias públicas de respuesta para emergencias e inseguridad puedan mantener sus comunicaciones en el caso de daño o destrucción de la infraestructura pública es lo que se conoce como "Continuidad de las Comunicaciones".

El caso del desarrollo IP de Raytheon

Según Raytheon y JPS Communications en Handbook of Pachwork Interoperability[59], la interoperabilidad puede considerarse en pocas líneas como "La capacidad de un funcionario público y la seguridad para hablar con quien sea que necesiten, cuando lo necesiten, cuando está debidamente autorizado."

Se requiere interoperabilidad porque sin ella, el gran número de diferentes tipos de sistemas de comunicaciones actualmente en uso no pueden trabajar con los demás, por lo que es muy difícil para los usuarios de los diferentes sistemas conversar y establecer coordinaciones interagenciales. Normalmente, un tipo de la radio hace caso omiso de las señales de todos los demás tipos de radio, y un usuario de teléfono por lo general no puede hablar sobre un radio.

La Interoperabilidad se logra mediante la estandarización de equipos, coordinaciones de frecuencia, y utilizando sistemas que permitan la conectividad simultánea por ejemplo de diferentes redes de radios (Sistemas de radio VHF vs UHF, AM vs FM, etc.), que conecten sistemas de radio a sistemas telefónicos (Celulares o sistemas satelitales) que conecten los sistemas de radio con circuitos de VoIP (voz sobre IP).

Raytheon ha desarrollado el dispositivo transportable TPR-1000 que puede contener múltiples radios, una radio para cada organización involucrados en los esfuerzos de respuesta (HF, VHF, UHF) que puede ser programada rápidamente a cada organización siendo capaz de transmitir y recibir de los operadores en una zona especifica.

Las radios pueden ser interconectadas por la inteligencia del TPR-1000 en una variedad de maneras, incluyendo una mezcla de radios de 2 vías y conferencias conversaciones, así como una mezcla de conexiones móviles permanentes y temporales a incluir de radios, teléfonos y celular.

Aunque TPR-1000 de Raytheon es personalizable, un sistema típico consta de dos casos transportable. Los casos primarios albergan la Raytheon ACU-1000, 2 radios (Uno UHF, uno VHF), una fuente de alimentación radio, y los paneles de interconexión para interconectar el caso primario al mundo exterior y al chasis secundario. El TPR-1000 secundario contiene una caja 8 radios adicionales (4 cada UHF y VHF), energía de radio suministros, y los paneles de interconexión. El TRP 1000 incluye un ordenador portátil y software especial para controlar todo el sistema, cables de interconexión necesarios, de salida de RF cables y antenas

[59] http://www.countyradio.us/Interop/Handbook_of_Patchwork_Interop.pdf

necesarias para operar el sistema. TPR-1000 puede interconectar radios en cualquier banda incluyendo banda HF, VHF, UHF, P25, 800Mhz, y tecnologías celulares

Este proyecto fue apoyado por el Departamento de Justicia de EE.UU[60], a través de la Oficina de Programas de Justicia al asociado de investigación de la Comunidad, la Oficina de Estadísticas de Justicia, Instituto Nacional de Justicia, Oficina de Justicia Juvenil y Prevención de la Delincuencia, y la Oficina para Víctimas del Delito y la Comunidad de Investigadores Asociados.

El caso del desarrollo IP MOTOBRIGDE de Motorola

Sistema de interoperabilidad avanzada IP que permite la capacidad del operador para extender su cobertura de la red de radio a través de la red IP, para llevar a cabo la transición a la red de radio de forma transparente. Motobridge[61] considera los factores de operatividad sobre:

- Interoperabilidad: como facilidad de interoperar a través de gran variedad de redes dispares (HF-VHF, VHF-UHF u otra combinación de bandas) y dispositivos de usuario. Extendiendo la cobertura de red de radio a través de la red IP
- IP de Despacho: sobre IP despacho y control, con interfaz gráfica de usuario simple y funciones de control avanzadas. despacho remoto
- Sobre-IP Radio Voting: para comunicarse eficientemente con destino necesario y ahorrar recursos del sistema cubriendo aquellos "puntos muertos", sin cobertura con la facilidad de múltiples tecnologías
- Calidad de audio: Rápido PTT y audio fiable sobre IP, con cifrado de audio y la señalización de voz
- Altamente escalable - Fácilmente ampliable a partir de una solución portátil, en el lugar del siniestro a una ciudad, operativos de seguridad y soluciones de estado.
- Seguridad: cifrado digital y cortafuegos opcional

Soporta conectividad sobre

- Radio (P25, analógica, convencional, concentración de enlaces, ASTRO, MOTOTRBO, TETRA, radios de otras marcas (TX (transmisión), RX (recepción) y PTT (push to talk))
- Voz sobre IP : VoIP (incluyendo SIP)
- Celular: 3G/4G
- Computadoras y Smartphones sobre IP, WiFi
- Móviles Satélite
- línea de cobre
- Red Telefónica Conmutada (Public Switched Telephone Network PSTN)

	Video demostrativo MOTOBRIDGE	https://www.youtube.com/watch?v=Db42GksT3TM https://www.youtube.com/watch?v=rVur21WktjQ

[60] Bajo el proyecto Developing Multi-Agency Interoperability Communication Systems , http://bussafety.fta.dot.gov/uploads/resource/3898_filename

[61] http://www.anfer.com/productos_motorola_MOTOBRIDGE.asp

3.8 Sistema ejemplares de despacho: El caso de Montgomery County, MD USA

El condado de Montgomery, Maryland cuenta con un Centro de Comunicaciones de Emergencias 911 (9-1-1 ECC Emergency Communications Centre) es un centro reconocido a nivel nacional y mundial, el más grande de Maryland, y uno de los 50 más grandes de los Estados Unidos.

El Condado de Montgomery inauguró un nuevo Centro de 9-1-1 en julio de 2003 que incorpora todos los sistemas nuevos de tecnología. El equipo incluye: a una información gráfica (mapeo), Sistema de Emergencias 9-1-1 y el sistema de atención de NO emergencias por teléfono, un sistema de despacho asistido por computadora, un sistema de radio troncalizado de 800 MHz, una localización automática de vehículos a través de Global Position System satélite, un móvil sistema de terminal de datos y otros sistemas auxiliares.

El sistema de respuesta para emergencias y la seguridad pública de Montgomery county[62] forma parte de todo un sistema tecnológico para la seguridad humana de las personas y está integrado y habilitado para múltiples socios por:

Tabla 4: Componentes y Funciones del sistema de seguridad pública del condado de Montgomery

COMPONENTE	FUNCIÓN
Los centros de operación de transporte	que manejan las operaciones de tráfico aéreo
Las fuerzas de cumplimiento de la ley	conformada por la policía del Estado y la policía nacional de parques de los Estados Unidos de Norte América
El Sistema de Mantenimiento de carreteras	carreteras de alta velocidad, secundarias y terciarias
El Sistema de Operaciones de Emergencias	integrado por los centros de operaciones de emergencia, la agencia de gestión de emergencias del estado, los centros de E-911, los centros PD/FIRE-911 (policía y bomberos)
El laboratorio de información compartida	manejado por universidad de Maryland
Equipos de Mantenimiento	conformado por el centro de operaciones en red, el centro de reparación de señales de tráfico, el centro de reparaciones de cámaras y radio, el centro de reparación de mensajes dinámicos
Centros de operaciones de las ciudades en el estado de policía y 911	

La dinámica se desenvuelve principalmente alrededor del desarrollo de:

- Planes de Respuesta a Emergencias,
- Planes de Comunicaciones para la Crisis
- Reunificación Familiar (entre otros temas).

[62] Focus on how agencies are effectively using or planning to use technologies to improve operations (approach is to determine what is needed for better operations, then determine the optimum technologies; also using technologies as a "bridge" between agencies), Maryland Transportation Operations Summit 2008

Sus servicios van enfocados a

- **Servicios de patrulla**: comunitarios, altos comandantes y oficiales de escuelas
- **Servicios de campo**: tráfico, especiales, animales e información pública
- **Servicios de investigación**: crímenes mayores, investigación penal, investigaciones especiales e investigación de victimas de grupos vulnerables y discapacitados
- **Servicios de administración**: 911 ECC, recuperación de vehículos, servicios legales y laborales, academia de entrenamiento, planificación de políticas, sistema de reducción de alarmas falsas

Este sistema multiplataforma de patrullaje, campo, investigación y administración de la seguridad permite coordinar acciones que van enfocadas a las acciones de "Seguridad Ciudadana" y también al respecto de la "Convivencia Ciudadana" , expresados en la operatividad en:

- Un sistema de transparencia con reportes anuales.
- El programa Crime Solvers diseñado para obtener la ayuda de la comunidad para ayudar a la Policía del Condado de Montgomery a resolver crímenes. Cuando una persona llama, envía textos, o presente una denuncia a través de Internet, esta información se transmite a la agencia de policía con jurisdicción primaria. Si esta información conduce a un arresto y / o acusación, la persona que llama tiene derecho a una recompensa de hasta $ 10,000
- Políticas definidas para interacción ciudadana
  - Video grabación de los abordajes ciudadanos
  - Seguimiento vehicular por CCTV y bases de datos
  - Motor de colisiones vehiculares
  - Asistencia a automovilistas
  - Uso de la fuerza
- Denuncias y control de armas en línea
- Oficina de información para el manejo del estress
- Abordajes de grupos vulnerables con problemas de salud
- Seguridad para la tercera edad (KSS Keeping Seniors Safe) para:
  - Los hábitos de compra ilícita y seguridad de estacionamiento
  - Seguridad en el hogar y la preparación personal para una emergencia
  - El fraude y las estafas
  - El robo de identidad identificación y prevención
  - A quién llamar para las necesidades de emergencia y no de emergencia
- Registro de Delincuentes Sexuales
- Asistencia a victimas
  - Intervención en Crisis: propietarios, acreedores, empleadores
  - Referidos: alimentos de emergencia y refugio, ayuda financiera, asesoramiento
  - Ayuda Directa: asistencia en la presentación de la ayuda financiera (es decir: las facturas médicas, facturas de funerales), ayuda con las opciones de seguridad personal (es decir: / órdenes de paz protectores, pantallas de seguridad para el hogar), que proporciona información sobre el p
- Ley de armas (Montgomery County Maryland- Weapons Law)
- Open data: informes semanales, mensuales, trimestrales y anuales abiertas y de acceso público para todos los ciudadanos

El estándar CALEA[63] en Montgomery County

El Departamento de Policía del Condado de Montgomery ha sido acreditado a nivel internacional a través de la Comisión de Acreditación para Agencias Policiales (CALEA)[64] desde el 31 de julio de 1993. El Director de Acreditación, adscrito a la División de Políticas y Planificación, es responsable de asegurar que el departamento mantiene el cumplimiento de los estándares de acreditación de CALEA.

El Departamento revalido con éxito en 1998, 2001, 2004, 2007, 2010 (Meritorius Flagship), y 2013.

La Comisión de Acreditación para Agencias Policiales (CALEA) es una organización sin fines de lucro que acredita internacionalmente a las agencias de aplicación de la ley. Las normas se desarrollaron para ayudar a las fuerzas del orden a alcanzar los siguientes:

- capacidad de agencia aumento para prevenir y controlar la delincuencia;
- mejorar la eficacia de la agencia y la eficiencia en la prestación de los servicios encargados de hacer cumplir la ley;
- mejorar la cooperación y coordinación con otros organismos encargados de hacer cumplir la ley y otros componentes del sistema de justicia penal;
- aumentar la confianza de los ciudadanos y el personal de las metas, objetivos, políticas y prácticas de la agencia.

CALEA tiene tres ejes esenciales:

- Acreditación de Comunicaciones de Seguridad Pública
- Acreditación de Cumplimiento de la Ley
- Acreditación de la Academia de Capacitación en Seguridad Pública

En el caso de la Acreditación de Comunicaciones de Seguridad Pública

El Programa de Acreditación de Comunicaciones para la Seguridad Pública CALEA ofrece un centro de comunicaciones, o de la unidad de comunicaciones de una agencia de seguridad pública, con un proceso para revisar sistemáticamente y evaluar internamente sus operaciones y procedimientos. Desde el primer Premio de Comunicación Acreditación de CALEA fue concedida en 1999, el programa se ha convertido en el método principal para una agencia de comunicación para demostrar voluntariamente su compromiso con la excelencia.

Las normas en que se basa el Programa de Acreditación de Comunicaciones de Seguridad Pública reflejan el pensamiento actual y la experiencia de los ejecutivos de las comunicaciones de seguridad pública y expertos de acreditación. APCO Internacional (Association of Public-Safety Communications Officials International, Inc.), es la principal asociación de miembros de comunicaciones, fue socio en el desarrollo de estándares de CALEA para Seguridad Agencias de Comunicación Públicos y su Programa de Acreditación. Esta relación continúa hoy y APCO reconoce los logros de los organismos públicos de comunicaciones de seguridad y apoya la acreditación sobre las siguientes consideraciones:

a) Es uno de los métodos más eficaces para alcanzar los objetivos administrativos y operativos, mientras que también proporciona orientación al personal.
b) Los Estándares de acreditación de CALEA proporcionan los informes necesarios y analizan como se tiene que tomar decisiones de gestión informadas basadas en la evidencia del estatus de los Sistemas de Comunicaciones.

[63] http://www.calea.org/, Commission on Accreditation for Law Enforcement Agencies (CALEA)
[64] http://www.calea.org/content/programs

c) Requiere un programa de preparación, de modo que un centro de comunicaciones este listo para hacer frente a los acontecimientos inusuales naturales o hechos cotidianos de inseguridad.
d) La acreditación es un medio para el desarrollo o la mejora en la relación de un centro de comunicaciones con la comunidad o de las agencias de servicios de TICs en su conjunto.
e) Fortalece la rendición de cuentas de una agencia, tanto dentro de la agencia y la comunidad, a través de un uso continuo de estándares que definen claramente la autoridad, el rendimiento y responsabilidades.
f) Permite limitar la responsabilidad y el riesgo de exposición de un centro de comunicaciones, ya que demuestra que se han cumplido las normas internacionalmente reconocidas para las comunicaciones de seguridad pública, según lo verificado por un equipo de evaluadores externos CALEA entrenados independientes.
g) Facilita consolidación de agencias con excelencia profesional.

La elegibilidad para participar en el Programa de Acreditación de la Academia de Formación de Seguridad Pública se limita a las organizaciones gubernamentales, colegios y universidades acreditadas y otras organizaciones que están autorizadas por una autoridad competente para proporcionar programas integrales básicos de formación seguridad pública, capacitación avanzada o en servicio.

“Casos exitosos del uso de TIC en seguridad pública en América Latina”

Parte IV: Casos de éxito en la Región.

4. Casos de éxito en la región.

La seguridad ciudadana (PNUD) es la condición personal, objetiva y subjetiva, de encontrarse libre de violencia o amenaza de violencia, o despojo intencional por parte de otros. Es el derecho natural e inalienable de la persona que le debe permitir el ejercicio pleno de todos los derechos humanos sin perturbaciones ni afectaciones por parte de terceros.

Observar casos de éxito en la región conlleva, analizar y estudiar como las TICS, inciden en la protección de ciertas opciones u oportunidades de las personas en su vida, su integridad, su patrimonio contra un tipo específico de riesgo (el delito) que altera en forma 'súbita y dolorosa' la vida cotidiana de las víctimas, pero también sobre las violencias y las conflictividades urbanas que forman parte de este triángulo de inseguridad.

"La Seguridad Ciudadana implica que al ciudadano hay que asegurarle las condiciones que hagan posible un desarrollo humano sostenible, se necesita desmitificar el uso de las TICs en la dimensión ciudadana lo cual conlleva cumplir las necesidades vitales del ser humano (seguridad humana) en todas sus dimensiones (Seguridad alimentaria, educativa, ambiental, de salud, económica, etc.) limitando a través del uso de las TICs la naturalización del crimen(Daniel Luz PNUD-RLAC)".

Por las razones expuestas, la inseguridad no queda reducida únicamente a los problemas de criminalidad, es una problemática compleja: está atada a los problemas de sanidad, de marginalidad, de exclusión, de medio ambiente, de urbanismo, de educación; es el resultado de desigualdades crecientes. La inseguridad es un riesgo al que hace falta darle respuestas multidisciplinarias, en este sentido las facilidades que puedan establecerse a través de Observatorios, Centros de Estudio y Análisis para la Seguridad y Convivencia ciudadana, o entidades académicas principalmente en un ecosistema de actores donde participen los gobiernos locales permite generar facilidades de políticas públicas y recomendaciones que forman parte las facilidades programáticas incluidos en la planificación y presupuestos locales.

La seguridad de los habitantes tiene que comprender no solo la tranquilidad de no ser víctima de hechos delictivos, sino también la de vivir en un Estado constitucional de Derecho y la de participar de los beneficios del desarrollo en materia de salud, educación, vivienda, ocio y todos los ámbitos de bienestar social. El concepto es el del desarrollo humano sostenible, que tiene la equidad como principio, debe también a través del uso de las TICs promover espacios para una adecuada respuesta a los ciudadanos en su demanda de previsión, prevención y control de la violencia, los delitos y las conflictividades.

4.1 Aplicación de Instrumentos a nivel Regional

La aplicación de instrumentos a nivel regional con la cooperación de la Oficina de la Unión Internacional de Telecomunicaciones (UIT) y la Comisión Técnica Regional de Telecomunicaciones (COMTELCA[65]) permitió recolectar información de los países bajo un instrumento de consulta que consta de cinco secciones sobre:

- Sección 1: Datos generales
- Sección 2: Políticas Públicas
- Sección 3: Implementaciones de TICs
- Sección 4: Regulación, innovación y agendas
- Sección 5: Recomendaciones

[65] http://www.comtelca.org/

La demanda de información del instrumento está encaminada a rescatar información sobre las acciones para:

I. Consolidar un sistema único de control de delitos, violencias y conflictividades en tiempo real que reciba todas las denuncias (llamadas, mensajes, correos electrónicos y redes sociales),
II. Actividades que faciliten gradualmente consolidar una agenda electrónica y permita generar movilizaciones para beneficio de la ciudadanía bajo la gestión de conocimiento sobre la evidencia de contextos y necesidades centrados en las ciudadanas y los ciudadanos.
III. Concentrar sistemas informáticos que ayuden a evaluar las tendencias y patrones con la participación interinstitucional que incluya instituciones como los entes reguladores, mesas de seguridad ciudadana, universidades, observatorios, centros de estudio y análisis, así como gobiernos locales.
IV. Vincular los sistemas de información que proporcionan datos sobre antecedentes penales, registro de vehículos, de infracciones administrativas con las bases de datos no delictivas de identificación personas y socio económicas.
V. Consolidar la innovación de equipos de radiocomunicación principalmente de instituciones policiales a través de la sustitución de los radios analógicos y digitales con una tendencia gradual hacia dispositivos que tengan la capacidad de transporte de datos, imágenes, videos y voz en tiempo real.
VI. Analizar y estudiar las facilidades de nuevas tecnologías de redes como LTE que no sólo optimizan el transporte de datos y la integración de otros servicios de multimedia, sino que facilitan la comunicación con otros países en materia de Seguridad Pública y las capacidades de interoperabilidad regional.
VII. Obtener de los países sus recomendaciones para el estudio y sus referencias de casos de éxito a nivel de país.
VIII. Conocer sobre las iniciativas para contrarrestar delitos y estados de violencias emergentes que afectan a la región

4.2 Análisis de Información de instrumentos aplicados

4.2.1 El Caso de Costa Rica

SECCIÓN 1: DATOS GENERALES

Tabla 5: Datos generales del Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

	Datos de contacto general:	
	Nombre de la institución	Ministerio de Ciencia, Tecnología y Telecomunicaciones.
	Nombre del Contacto	Elidier Moya Rodriguez

SECCIÓN 2: POLITICAS PUBLICAS

El análisis del instrumento indica que en Costa Rica, a julio del 2015**,** Las políticas de Seguridad Pública o Ciudadana, **NO** están vinculadas al marco regulatorio de TICs existente en el país y que **NO** existe un plan de interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs. Sin embargo, es de reconocer que Costa Rica presenta avances importantes desde el año 2,000 que rescatan la consolidación y

las facilidades de interoperabilidad vinculadas a sus políticas, así como su operatividad en la Seguridad y la Justicia, un ejemplo de esto es el Sistema de Costarricense de Información Jurídica (SCIJ)

El objetivo fundamental de este Sistema fue diseñar, probar e implantar los mecanismos organizacionales y de gestión, que permitieran un mejoramiento sostenido de la productividad de los despachos judiciales, apoyados por soportes tecnológicos especializados, de modo que el Poder Judicial[66] logre la capacidad de brindar a sus usuarios un servicio de alta calidad, a fin de coadyuvar con su misión constitucional de brindar una justicia pronta y cumplida" (Mora y Solís; 2002).

El software Sistema de Gestión de Despachos es totalmente integrado, de tal manera que permite dar seguimiento a un expediente judicial desde que ingresa al despacho o al Sistema de Recepción de Documentos, donde se le asigna automáticamente un número único, hasta que finaliza e la corriente judicial. El software también es flexible, de tal manera que permite ajustar su orden y contenido de acuerdo con cambio de leyes, procedimientos jurídicos o administrativos. También permite la exportación de información a Intranet e Internet, lo cual facilita la accesibilidad y promueve la transparencia acerca de la tramitación de las causas a los usuarios y litigantes.

Se resalta que la Política de Estado en Seguridad Ciudadana para la Gobernabilidad Democrática y la Paz Social (POLSEPAZ) en Costa Rica, supone el desarrollo de acciones en los ámbitos de competencia de cada uno de los poderes del Estado, atendiendo al marco de la Constitución Política y las leyes de la República. La mayoría de esas acciones son interdependientes y, por tanto, su ejecución requiere de altos grados de coordinación[67]. Si bien NO existe un plan de interoperabilidad, El Comité consultivo funciona como un espacio de diálogo, comunicación e información con miras a conocer el avance de la implementación de la POLSEPAZ.

La Contraloría General de la República de Costa Rica cuenta con "Normas técnicas para la gestión y el control de las Tecnologías de Información"[68], esta normativa establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado.

SECCIÓN 3: IMPLEMENTACIONES DE TICS

Las aplicaciones de TICs **vinculadas a la Seguridad Pública** que se han implementado con éxito se describen a continuación:

- Centros de operaciones de la Policía en los niveles locales y nacionales.
- Sistemas de radiocomunicación de Seguridad Ciudadana para la Policía.
- Sistemas de información de Seguridad Ciudadana para la Policía.
- Sistemas de operaciones de Organismos de Emergencia.
- Sistemas de información y posicionamiento geográfico para emergencias, con posicionamiento geográfico, pero no específicamente para emergencias.
- Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV)
- Sistemas de dactiloscopia.
- Observatorios de Seguridad Ciudadana.
- Centros integrados con interoperabilidad con las soluciones anteriores tipo 911[69].- Con integración del sistema Automated Fingerprint Identification System (AFIS).
- Sistema de Identificación de Vehículos, de patrullas.

[66] http://www.poder-judicial.go.cr/
[67] Modelo de coordinación y concertación de la POLSEPAZ
[68] http://www.ocu.ucr.ac.cr/Leyes/Nuevas%20normas%20de%20TI%20-CGR%20N-2-2007-CO-DFOE.pdf
[69] http://www.911.go.cr/quienes-somos/resena-historica/

Implementaciones en progreso en Costa Rica

- Sistema Integrado de Identificación Balística (IBIS).
- Sistema de Identificación Aeroportuaria.
- Sistema de Identificación y reconocimiento facial.
- Sistemas de Radio Comunitarios.
- Sistemas de Inteligencia Forense.
- App contra Cibercrimen[70].

Sistema de Emergencias 911

Tabla 6: Datos del sistema de Emergencia 911 de Costa Rica

	Datos de la experiencia de éxito regional:	
	Nombre de la institución	Sistema de Emergencias 911
		Inaugurado: el 21 de Enero de 1994
		Contacto: Tel:+ (506) 2522-2700, E-mail: info@911.go.cr

De la consulta se rescata la experiencia del 911, que comienza en 1990, cuando el entonces presidente de la Comisión Nacional de Emergencias Dr. Humberto Trejos Fonseca (1990–1994), convocó a una reunión a diferentes instituciones. Proponiéndose la meta de un 9-1-1 para Costa Rica, se iniciaron los contactos con los organismos que atendían las emergencias, con el objetivo de mejorar los tiempos de respuesta en la atención de eventos de emergencia de los habitantes de la gran área metropolitana, procurando mejorar también la administración de los recursos disponibles de las Instituciones involucradas.

El 21 de enero de 1994 se inaugura la central única de atención de llamadas, funcionando en un edificio en terrenos donados por la Comisión Nacional de Emergencias, frente al Aeropuerto Tobías Bolaños en Pavas. Este novedoso Sistema de Emergencias colocó a Costa Rica a la vanguardia en América Latina y se vio el fruto del esfuerzo de tres años de arduo trabajo de coordinación inter-institucional, respaldados por la firme voluntad del Gobierno de la República. El sistema por razones técnicas, comenzó a funcionar con el número **1-2-2**, pero a partir del 30 de abril de 1994, se dio paso al conocido número **9-1-1.**

Actualmente es la institución que por medio de un único número recibe y tramita las llamadas de Emergencia en Costa Rica[71]. Reuniendo y coordinando con todas las instituciones de respuesta (Cruz Roja, Bomberos, Fuerza Pública, Policía de Tránsito, Comisión Nacional de Emergencias y Organismo de investigación Judicial) y además de las instituciones asesoras en Violencia intrafamiliar (PANI, INAMU e Instituto del hombre WEM) del país para brindar la ayuda que se necesita, cuenta con 68 operadores y 10 supervisores que atienden estas llamadas en tres turnos, cada operador recibe un salario base de 460,000

[70] http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0910-PA-IXP/9%20Viernes%20PANI%20Caso%20Memes%20Memes%20Everywhere.mp4

[71] https://www.youtube.com/watch?v=RX_Yj0B_Ceg

mil colones, el presupuesto anual del 911 es de alrededor de 4 mil millones de colones se financia con el 1% de la facturación de los servicios de telefonía fija y celular, el 80% de las llamadas corresponden a incidentes a no corresponden a una emergencia.

Servicio de Multas del 911

- Procedimiento de multas

El procedimiento para cobro por llamadas indebidas al "9-1-1" tiene como propósito reducir el uso incorrecto de este servicio, y además de educar y concientizar a la población sobre el uso correcto de las facilidades que brinda el Sistema de Emergencias 9-1-1[72]. Para ello dispone el artículo 16 de Ley del Sistema de Emergencias 9-1-1, una prohibición expresa de realizar llamadas que no corresponden a una emergencia. Debe quedar claro, que la sanción es para la persona, física o jurídica, a nombre de quien aparece registrado el derecho telefónico, por su deber de cuidado, y no para quien realice la llamada.

- Procedimiento administrativo

Se hace del conocimiento del usuario, que desde su número telefónico se ha realizado una o varias llamadas al 9-1-1 y que han sido calificadas como "indebidas".

El o la concesionaria del número telefónico puede apersonarse a escuchar la grabación o visitando el sitio web de la Institución, según datos suministrados en el documento de notificación, donde se introduzca el número de cedula, el número de expediente y la clave que se le ha brindado previamente para interponer su escrito de defensa. Puede hacerse acompañar de un abogado si así lo considera, no es obligatorio.

Es importante aclarar que la grabación, o cualquier otro dato relacionado con el expediente pueden ser consultados en cualquier etapa procesal. El interesado(a) presentar todo tipo de prueba, documental, testimonial o cualquier otra que considere oportuna. La multa por llamadas bromistas cuesta 94 mil colones por llamada. La contraloría del 911 recibe entre 12 y 17 quejas formales por mes.

El 9-1-1 cuenta con un total de 11 instituciones adscritas, de las cuales 10 son responsables de dar atención y seguimiento a los reportes de emergencia que se reciben:

1. Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE).
2. Patronato Nacional de la Infancia (PANI)
3. Instituto Costarricense de Electricidad (Grupo ICE)
4. Instituto Nacional de la Mujer (INAMU)
5. Benemérito Cuerpo de Bomberos de Costa Rica
6. Cruz Roja Costarricense
7. Ministerio de Seguridad Pública (Fuerza Pública)
8. Organismo de Investigación Judicial (OIJ)
9. Caja Costarricense de Seguro Social (CCSS)
10. Dirección General Policía de Tránsito
11. Instituto WEM

El Sistema de Emergencias 9-1-1, órgano del Estado con desconcentración máxima, adscrito al Instituto Costarricense de Electricidad, con cédula jurídica No. 3-007-213928, domiciliado en San José, programa, tramita y ejecuta todas las contrataciones que se requieren, tanto para su operación, como en inversión de la Institución, lográndolo con sus propios recursos presupuestarios, que se recaudan a través de la factura telefónica de cada uno de los operadores telefónicos.

En las aplicaciones de TICs vinculadas **en la administración de Justicia en centros penitenciarios NO** se rescatan avances significativos sobre:

- Seguridad perimetral.

[72] http://www.911.go.cr/quienes-somos/resena-historica/

- Vigilancia y Monitoreo.
- Control de Acceso.
- Sensores y Dispositivos.
- Sistemas de posicionamiento.
- Sistemas de pánico celular.

Sobre la consulta de TICs vinculadas **en la Seguridad Pública y la Inteligencia** se resaltan las **Plataformas de información en inteligencia para el:**

- análisis y estudio de personas desaparecidas[73]

CSIRT-CR

La Presidencia de la República y el Ministerio de Ciencia y Tecnología consideraron importante para crear el CSIRT:

- El conjunto de amenazas concretas derivadas del uso malicioso de las tecnologías digitales y de sus limitaciones y vulnerabilidades intrínsecas, cuyo fin último es lesionar la integridad individual en favor del crimen organizado en diferentes formas y que lleva al Estado a extender las nociones de derecho, jurisprudencia y soberanía hacia el espacio tecnológico para definir de manera integral el concepto de bienestar social.
- Que el Estado tiene como uno de sus objetivos fundamentales el aumentar el aprovechamiento de las oportunidades que brinda la ciencia y la tecnología para incrementar el nivel de desarrollo del país, incluyendo la protección del capital de información del país y de manera última al ciudadano con el fin de garantizar las condiciones suficientes y necesarias para la competitividad.
- Que la Ley de Promoción del Desarrollo Científico y Tecnológico en su artículo 4º, inciso e), contempla como un deber y una responsabilidad del Estado "Establecer las políticas de desarrollo científico y tecnológico, supervisar su ejecución y evaluar su impacto y resultados, en el marco de la estrategia de desarrollo nacional".
- Que la Ley Nº 7169 de Promoción del Desarrollo Científico y Tecnológico en su artículo 4º, inciso k), establece el deber del Estado de impulsar la incorporación "Selectiva de la tecnología moderna en la Administración Pública a fin de agilizar y actualizar, permanentemente, los servicios públicos, en el marco de una reforma administrativa, para lograr la modernización del aparato estatal costarricense, en procura de mejores niveles de eficiencia".
- Que el Ministerio de Ciencia y Tecnología tiene como acciones el apoyar los programas de transformación y modernización del sector estatal, así como establecer áreas temáticas estratégicas, dentro de las que se haya la formulación y ejecución de políticas y estrategias relacionadas con la seguridad en las Tecnologías de la Información y la Comunicación en el ámbito del Sector Público costarricense, con el objetivo de alcanzar mayores niveles de eficiencia en los servicios del Estado, y a la vez contribuir a crear una infraestructura de las tecnologías de la información y la comunicación que potencien al sector productivo nacional.

Según La Gaceta Nacional de Costa Rica, publicó el 13 de abril del 2012 el Decreto Nº37052 por el que se constituye el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) con sede en las instalaciones del Ministerio de Ciencia y Tecnología. Dicho Decreto señala al CSIRT-CR con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de

[73] http://www.latinoamericanosdesaparecidos.org/costa_rica/default.php

expertos en seguridad de las tecnologías de la información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

Sus objetivos, fijados en el artículo 2 del Decreto, son:

- Promover a nivel nacional la cultura de la seguridad cibernética e informática.
- Coordinar, a nivel nacional acciones que permitan el mejoramiento general de la seguridad cibernética e informática.
- Apoyar a las autoridades administrativas y judiciales en los casos que corresponda para la investigación y procesamiento de perpetradores de delitos cibernéticos e informáticos.
- Coordinar con el Comité Interamericano contra el terrorismo (CICTE), y otras entidades nacionales e internacionales sobre el diseño y aplicación de políticas, estrategias y lineamientos en la adquisición de bienes y servicios en materia de la seguridad de las tecnologías de la información y la comunicación, con los estándares que observen las normativas vigentes internacionales para la implementación y/o aplicación en el sector público.
- Incentivar, orientar y promover las iniciativas públicas y privadas conducentes a lograr un adecuado desarrollo del país en el campo de la seguridad de las tecnologías de la información y la comunicación, esfuerzos orientados a lograr una mayor protección del ciudadano.
- Promover la adopción de políticas públicas que promuevan la mayor eficiencia y eficacia en los recursos informáticos de las entidades públicas.
- Promover y velar por el establecimiento de planes de contingencia en materia de seguridad de las tecnologías de la información y la comunicación en el sector público.
- Proponer las guías para la evaluación de los programas interinstitucionales en materia de seguridad de tecnologías de la información y la comunicación.
- Asesorar y proponer a la Presidencia de la República la normativa en materia de seguridad de las tecnologías de la información y la comunicación, que se requiera para el cumplimiento de las políticas en la materia.
- Promover proyectos y actividades de investigación, capacitación y difusión en materia de seguridad de tecnologías de la información y la comunicación.
- Impulsar entre las entidades públicas y privadas el desarrollo y ejecución de políticas y estrategias nacionales en el campo de la seguridad de las tecnologías de la información y la comunicación.

El CSIRT-CR comenzó brindando tres servicios, el primero de ellos la atención inmediata de situaciones como ataques a páginas web, algo que ha sido frecuente en los últimos años en el país, el segundo capacitaciones de personal, la tercera función principal es generar normativa técnica para garantizar un grado mínimo de seguridad en las instituciones y empresas que manejan datos personales.

Sobre las TICS vinculadas a los **Sistemas de Información Ciudadana y las Redes Sociales** se resalta: **App para la Justicia**[74]

El poder Judicial de Costa Rica cuenta con una Apps disponible para Android e IOS[75], gratuita y disponible para la ciudadanía.Esta aplicación es presentada por el Poder Judicial de Costa Rica como una nueva forma para promover el acceso a la justicia.En ella encontrará un conjunto de servicios tales como:

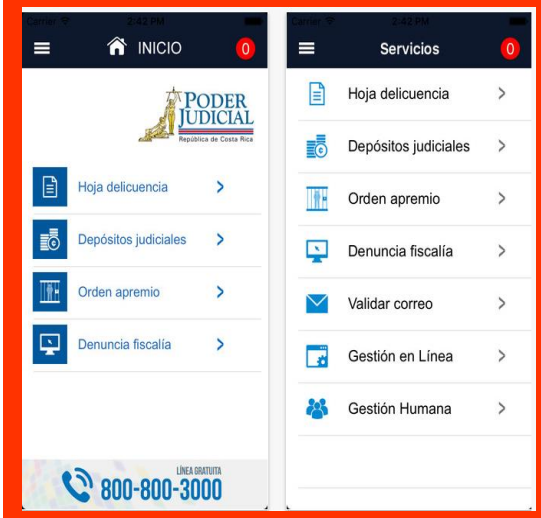
- Trámites judiciales.
- Solicitud de la hoja de delincuencia.
- Consulta de órdenes de apremio.
- Consulta de depósitos judiciales.

[74] http://www.poder-judicial.go.cr/

[75] https://itunes.apple.com/cr/app/poder-judicial/id762885040?mt=8

- Consulta de expedientes del Sistema de Gestión en Línea.
- Consulta de personas sentenciadas en fuga.
- Mapa de las sedes judiciales con números de teléfono y horarios.
- Consulta de concursos y convocatorias para Jueces y Juezas.
- Información de como realizar diversos trámites judiciales.

Figura 11: Pantalla de la app del poder judicial de Costa Rica



4.2.2 El Caso de Guatemala

SECCIÓN 1: DATOS GENERALES

Tabla 7: Datos del Ministerio de Gobernación de Guatemala

	Datos de contacto general:	
	Nombre de la institución	Ministerio de Gobernación.

SECCIÓN 2: POLITICAS PUBLICAS

El análisis del instrumento recibido de Guatemala nos indica, a julio del 2015**,** que las políticas de Seguridad Pública o Ciudadana, **NO** están vinculadas al marco regulatorio de TICs existente en el país y que **NO** existe un plan de interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs. Guatemala presenta avances importantes, resaltando la activación de la Ley del Sistema de Alerta Alba Kenneth, este mecanismo fue establecido bajo el Decreto 28-2010, Ley del Sistema y reformado según el Decreto 5-2012 que ha permitido localizar a más de mil infantes, con la Defensoria de los derechos de la niñez y la adolescencia de la Institución del Procurador de los Derechos Humanos, con casi el triple de denuncias por niñez desaparecida [76]. Funciona bajo mando de la Coordinadora Nacional del Sistema de Alerta Alba-Keneth, la cual articula e integra las acciones de instituciones públicas, siendo ellas las siguientes: Procuraduría General de la Nación, a través de la Unidad de Alerta Alba-Keneth, quien la preside, Policía Nacional Civil, Dirección General de Migración, Secretaría de Comunicación Social

Figura 12: Alerta Alba-Keneth

[76] http://www.pdh.org.gt/component/allvideoshare/video/ley-alba-kenneth-ha-permitido-localizar-a-mas-de-mil-infantes.html

de la Presidencia de la República, Ministerio Público de Guatemala, Ministerio de Relaciones Exteriores, Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas

La Ley del Sistema de **Alerta Alba-Keneth**[77], se origina por la trágica muerte de **Alba Michelle** y **Keneth Alexis**[78], debido a la inexistencia de un procedimiento que permitiera dar respuesta de forma inmediata y adecuada a las sustracciones y desapariciones de niños, niñas y adolescentes, ya que para ese entonces las autoridades policiales esperaban de 24 a 48 horas para iniciar la búsqueda y localización de una persona desaparecida. Cuenta con una nueva sede a partir de julio del 2014[79], atiende las 24 horas y están interconectados con la Policía Nacional Civil y la Dirección de Migración. El 86% de las alertas **Alerta Alba-Keneth** activadas se han resuelto positivamente con el apoyo del Ministerio Público, su sistema de registro y control se implemento a partir del 2014, a la fecha esta pendiente la desactivación de la alerta con los expedientes que ya están en investigación, el éxito de las **Alerta Alba-Keneth** consiste en la coordinación interinstitucional, la alianza con organizaciones de sociedad civil y organismos internacionales.

La Política Nacional de Seguridad[80] se orienta a construir las condiciones para que las personas se sientan seguras, libres de violencia y temor, confiadas en alcanzar sus aspiraciones individuales y colectivas. Asimismo, tiene como fin integrar los esfuerzos de todo el país en un propósito común: lograr el desarrollo integral, fortalecer la democracia y superar las desigualdades sociales, para edificar una *"Guatemala Segura y Próspera".* La Política, considera como eje de transformación y lineamiento estratégico: "La tecnología[81]", la define como conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos, que debe estar al servicio del país, de manera que colabore en la consecución de los Objetivos Nacionales. En el campo de la seguridad, cobra especial relevancia para la convivencia pacífica, la tranquilidad y la estabilidad nacional, así como en la prevención de situaciones de emergencia o desastres, apoyo al Sistema de Seguridad y Justicia para prevenir y mitigar, con productos y sistemas de alta tecnología.

SECCIÓN 3: IMPLEMENTACIONES DE TICS

Aplicaciones de TICs **vinculadas a la Seguridad Pública** que se han implementado con éxito

- Centros de operaciones de la Policía en los niveles locales y nacionales.
- Sistemas de radiocomunicación de Seguridad Ciudadana para la Policía.
- Sistemas de información de Seguridad Ciudadana para la Policía.
- Sistemas de operaciones de Organismos de Emergencia. Existe convenio con el 911.
- Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV)
- Sistemas de dactiloscopia.
- Sistema de Identificación de Vehículos.
- Sistema de Identificación y reconocimiento facial.
- Observatorios de Seguridad Ciudadana.
- Centros integrados con interoperabilidad con las soluciones anteriores tipo 911, a través de la línea 110[82] principalmente de atención de emergencias de la Policía.

[77] http://www.pgn.gob.gt/acerca-de-procuraduria-general-de-la-nacion/alerta-alba-keneth/

[78] **https://www.youtube.com/watch?v=0njhRFPITq4** , quinto aniversario

[79] https://www.youtube.com/watch?v=wESD565Rluk

[80] http://www.segeplan.gob.gt/downloads/clearinghouse/politicas_publicas/Seguridad/Politica_Nacional_de_Seguridad.pdf

[81] La Política Nacional de Seguridad , Capitulo V Páginas 25 y 27,

[82] http://noticias.emisorasunidas.com/noticias/nacionales/anuncia-propuesta-para-regionalizar-numero-telefono-110-crear-911

Sistema de CCTV Ciudad de Guatemala

Tabla 8: Datos del sistema de CCTV en Ciudad de Guatemala

	Datos de la experiencia de éxito regional:	
	Nombre de la institución	Sistema de CCTV Ciudad Guatemala
		Inaugurado: 2014

Este sistema fue instalado bajo el caso de excepción No. ECE-DCPNC-01-2013, denominado Arrendamiento con opción a compra, instalación y puesta en funcionamiento de un sistema de transmisión de video en tiempo real para vigilancia de la zona 18 y áreas adyacentes, para uso de la Policía Nacional Civil**.-**El arrendamiento consistió en el suministro de equipo y servicios integrales consistentes en: 1018 cámaras de video vigilancia, equipo activo de transmisión, sistema almacenamiento y gestión con 20 operadores, que ha venido a fortalecer los proceso instiyucionales que se comenzaron a inicios del 2012**,** que ha incidido en que los índices de violencia en los sectores con bajo vigilancia disminuyan en hasta 40%[83] desde que las autoridades policiales instalaron las cámaras de video con un costo de $150 millones de dólares (USD) en un proceso de fortalecimiento. Dicho proceso de ha venido fortaleciendo el 2014 con 1,200 camaras instaladas en el municipio de Villa Nueva, al sur, 1,133 en el municipio de Mixco y 80 en la ciudad colonial de la Antigua Guatemala

Los componentes del sistema de video vigilancia considerados son los siguientes:

1. Infraestructura de conectividad y transmisión de datos.
2. Cámaras de video vigilancia de alta resolución.
3. Botones de emergencia.
4. Solución Tecnológica de Almacenamiento Digital.
5. Software de Gestión, Administración de Cámaras, Analítica de Video, Reconocimiento de placas y Reconocimiento facial.
6. Centro de Monitoreo.

Agentes policiales monitorean los videos desde sus estaciones y en tiempo real alertan a los agentes de las patrullas sobre posibles actividades delictivas. Las cámaras los han ayudado a responder ante los delitos de manera suficientemente veloz como para capturar a los sospechosos antes de que puedan escapar. “Las fuerzas policiales tienen más ‘ojos’ para la vigilancia, lo que impide que los delincuentes cometan delitos”, dijo Carlos Argueta, Viceministro de Tecnología de Información y Comunicaciones del Ministerio de Gobernación (MINGOB). “Es una novedad el que los agentes que patrullan las calles tengan apoyo del centro. Esto les ha permitido realizar algunas capturas en flagrancia, con las manos en la masa”.

Las cámaras tienen diferentes capacidades. La mayoría de ellas cerca del 80% son estacionarias y están enfocadas hacia una lugar fijo. La policía puede mover cerca del 20% hacia la derecha o hacia la izquierda, hacia arriba y hacia abajo. Y el 10% de las mismas poseen capacidad de reconocimiento facial, lo que significa que pueden identificar delincuentes por su rostro a través de su conexión a una base de datos que mantiene el Registro Nacional de Personas (RENAP). La policía también puede comparar tomas de las matrículas de

[83] Revista Militar Digital, http://dialogo-americas.com/es/articles/rmisa/features/2014/10/20/feature-01

los autos con la base de datos de la Superintendencia de Administración Tributaria (SAT) para determinar si los autos que están siendo vigilados han sido reportados como robados o están sujetos a incautación.

En la actualidad, las cámaras han sido instaladas en varios puntos estratégicos en toda la ciudad, con especial énfasis en la Zona 18, la cual tenía una tasa de 72 homicidios por 100.000 habitantes a principios de 2012. En comparación, el país en su totalidad tiene una tasa de homicidios de casi 40 por 100.000 habitantes, de acuerdo con un informe presentado por las Naciones Unidas en abril del 2015.

Según PNUD[84], sobre las valoraciones de impacto, un agente de policía encargada de la edición de videos solicitados por el Ministerio Público en el Centro de Monitoreo de la Comisaría 12 en la zona 18 explicó que tras la inauguración del Centro en Julio de 2014, por 19 días consecutivos hubo cero homicidios en la zona gracias a la video-vigilancia y a la respuesta efectiva de las patrullas. Los datos obtenidos por medio de video-vigilancia permiten una mejor formulación de cargos para la acusación y condena penal. La tecnología, de la mano de una respuesta rápida de la policía, generan mayor confianza de la población en la policía nacional. Como resultado, los vecinos de la zona 18 se han acercado a la policía para pedir ayuda en casos de familiares desaparecidos, de objetos perdidos en el transporte público y otras situaciones en las que los 'ojos' de la policía podrían haber detectado algo. "No es fácil tener que rechazar muchos de estos pedidos debido a las prioridades para atender el crimen y violencia", explicó un agente de la policía. Según el grupo de apoyo mutuo[85] la zona que constantemente reporta la mayor cantidad de víctimas es la zona 18, pero en 6 meses del 2015 la zona que nos sorprende es la zona 5 la que se coloca en el primer lugar con 36 víctimas. En segundo lugar se coloca la zona 18 con una víctima menos y en tercer lugar la zona 21 con 26 víctimas, la tendencia de a la estabilización y a la baja principalmente en la zona 18 donde se implemento con más fortaleza el proyecto, es evidente al 2015. Sin embargo a nivel de municipios Guatemala, Mixco y Villanueva mantienen sus altos indices de violencia a nivel de país.

www.alertos.org

Es una plataforma de observación ciudadana que busca que quienes viven, trabajan o visitan Guatemala, asuman un rol protagónico en el combate contra la delincuencia, poniendo a su disposición una herramienta tecnológica de fácil utilización, que permite dar seguimiento a la labor del Estado, y requiere, permanentemente, del compromiso de los propios ciudadanos, de las autoridades y de los medios de comunicación.

Figura 13: Pantalla del sistema "Alertos"

El objetivo de ALERTOS [86] es **mejorar seguridad ciudadana** recuperando zonas públicas, fortaleciendo instituciones, cultivar la prevención, mejor seguridad pública, facilitar turismo e incentivar inversión extranjera a través de medidas de prevención orientadas a reducir el crimen y mejorar medidas de seguridad pública. Ciudad Segura incluye entre sus intervenciones un sistema de video vigilancia, cuyas grabaciones son admisibles en las cortes como parte de programas de prevención del delito en el país.

En las aplicaciones de TICs vinculadas **en la administración de Justicia en centros penitenciarios** se rescatan avances sobre:

[84] http://www.gt.undp.org/content/guatemala/es/home/ourwork/democraticgovernance/successstories/PTI.html#
[85] http://areadetransparencia.blogspot.com/2015/07/informe-de-monitoreo-de-violencia-y_21.html
[86] http://www.mejoremosguate.org/cms/es/que-estamos-haciendo/alertos

Seguridad perimetral:

- Sistemas de observación móviles y aéreos (drones)[87].
- Radio comunicadores en vehículos de patrulla y para guardias penitenciarios.
- Sistema de Bloqueo de Comunicaciones a través de servicios de Internet, WI-Fi, telefonía satelital y otros sistemas.

Vigilancia y Monitoreo:

- Monitoreo mediante brazalete electrónico.

Control de Acceso:

- Dispositivos de detección de metales u otro tipo de artículos no permitidos,

Sensores y Dispositivos:

- Botones de pánico.

Sistemas de inhibición celular:

- Inhibición de Tráfico de Telecomunicaciones Móviles en Centros Penitenciarios (Decreto 12-2014)[88].

Sobre las regulaciones de las TICs para la Seguridad Pública y Ciudadana:

- La disposición para el intercambio común de datos.
- Requisitos funcionales mínimos asociados al despacho (Computer Aided Dispatch CAD).

Sobre la consulta de TICs vinculadas **en la Seguridad Pública y la Inteligencia** se resaltan las **Plataformas de información en inteligencia para el:**

- Análisis y estudio de personas desaparecidas[89].
- Sistemas Información con el uso de drones para recopilar información de voz, data y/o imágenes.

CSIRT-GT GUATEMALA

Un CSIRT (Computer Security Incident Response Team) de Guatemala90 es un equipo de respuesta ante Incidencias de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

[87] http://www.pnc.gob.gt/index.php?option=com_k2&view=item&id=1686:%E2%80%9Cdrones%E2%80%9D-y-c%C3%A1maras-de-alta-definici%C3%B3n-ser%C3%A1n-los-ojos-de-la-polic%C3%ADa&Itemid=414
[88] http://www.plazapublica.com.gt/sites/default/files/decreto_numero_12-2014.pdf
[89] https://www.facebook.com/Alerta-Alba-Keneth-493384187343854/
[90] http://www.csirt.gt/

Un CSIRT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

El CSIRT-GT nació a instancias de la convocatoria del Comité Interamericano de Lucha contra el Terrorismo, CICTE, quien invitó a los países que integran la OEA a conformar sus Equipos de Respuesta a Incidentes de Seguridad Cibernética (Computer Security Incident Response Team, CSIRT), para combatir amenazas a la seguridad cibernética.

El Ministerio de Relaciones Exteriores ha facilitado el proceso de conformación del Equipo Nacional, por lo que desde junio del 2006 comenzó a convocar a diversas instituciones públicas, privadas y académicas, para diseñar y cumplir con un plan de trabajo que permitiera seguir los pasos básicos de creación del CSIRT remitidos por el CICTE. Se recomendó utilizar la Metodología de la Universidad Carnegie Mellon.

Figura 14: Pantalla de la App "PNCMÓVIL"

Entre junio y noviembre del 2006 se realizaron alrededor de 12 reuniones las cuales al final permitieron que, con el apoyo de la Superintendencia de Telecomunicaciones, el Clúster de Tecnologías de la Información, el Ministerio de la Defensa Nacional y el resto de entidades públicas y privadas se completara una primera etapa en la que se definió el contenido y ámbito de aplicación; así como la nominación oficial del Equipo Nacional ante el Comité Interamericano contra el terrorismo.

Actualmente el equipo coordinador lo conforman: Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional y 2 Asesores de seguridad de la información.

Guatemala no cuenta con legislación especial[91] que regule normas relativas a los delitos informáticos cometidos a través de sistemas que utilicen tecnologías de la información, únicamente se encuentran algunas normas que fueron adicionadas a nuestro actual Código Penal, mismas que no responden a las necesidades actuales, debido a la irrefutable variación de las tecnologías de la información.

Sobre las TICS vinculadas **a los Sistemas de Información Ciudadana y las Redes Sociales** se resalta:

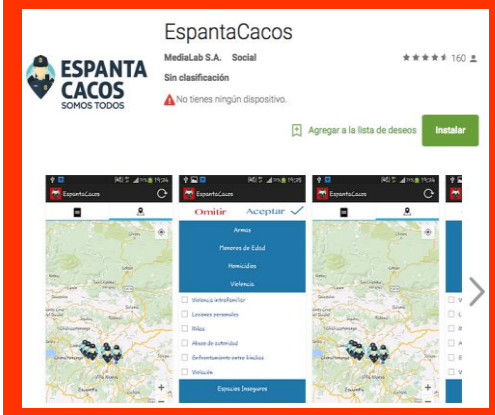
El Proyecto "EspantaCacos[92]"

El proyecto nació en el 2012, como una respuesta social para promover la denuncia pública de los puntos en los que frecuentemente ocurren actos delictivos. Este Proceso fue acompañado de la Campaña "No más Asaltos" que alcanzó un alto número de ciudadanos impactados en la ciudad de Guatemala y notas en los medios de comunicación a nivel nacional e internacional.

Guatemala tambien resalta la ejecucion del patrullaje inteligente mediante:

- Patrullaje inteligente mediante APPs
- Patrullaje inteligente mediante radio

Figura 15: Pantalla de la app "Espantacacos"



[91] http://www.csirt.gt/?q=node/5
[92] https://play.google.com/store/apps/details?id=gt.DigitalHulahoop.anticacos&hl=es_419

PNC MOVIL[93]

Lanzada en marzo del 2015, con el apoyo de Reforma Policial, PNCmóvil es la primera aplicación móvil cuyas características de gobierno electrónico, favorecen al ciudadano para realizar consultas en tiempo real.

En esta primera versión, PNC MÓVIL trae a los usuarios la consulta de vehículos, en las cuales, con la introducción del tipo y número de placa, podrá establecer las características principales del vehículo, así como estado de solvente o reportado como robado.

Esto permite a ciudadanía interesada en su propio vehículo o en la compra de uno, establecer la solvencia o no del mismo, extendiéndose el beneficio a talleres de mecánica, compañías aseguradoras, predios de compra-venta de carros, etc.

Finalmente, la función para reporte de vehículos sospechosos, para lo cual el ciudadano deberá, por una sola ocasión, ampliar sus datos personales de registro, como su número de DPI, nombres, apellidos y fecha de nacimiento. Esto, una vez validado, permitirá al ciudadano reportar vehículos inusuales en su vecindario, sospechosos de estar involucrados en posibles acciones ilícitas, entre otros.

Una segunda versión, traerá la prestación para denuncia de vehículos robados, la cual integrará en tiempo real a las unidades, como el 110 y el sistema de cámaras LPR (detectoras de placas de circulación) para facilitar un seguimiento inmediato de acontecimientos relacionados a robo de vehículos, en tiempo real.

SECCIÓN 4: REGULACIÓN, INNOVACIÓN Y AGENDAS

Se resalta la aplicación de regulaciones sobre

- La disposición para el intercambio común de datos
- Requisitos funcionales mínimos asociados al despacho (Computer Aided Dispatch CAD)

Sobre a la innovacion que está en estudio, analisis o implementación por parte del organismo regulador se destaca:

- Política de Interoperabilidad que promueva intercambiar información del gobierno en aspectos: organizacionales, técnicos, operacionales y de gobernanza.
- Plan o estrategia para el desarrollo de Sistemas informáticos que ayuden a evaluar las tendencias y las probabilidades
- Plan o estrategia para desarrollar un sistema único de control de delitos en tiempo real que reciba todas las denuncias (llamadas, correos electrónicos y redes sociales),
- Plan o estrategia para desarrollar aplicaciones móviles para extender las opciones de denuncias por medio de texto, imagen, video y audio
- Plan o estrategia para el uso de los medios sociales en comunicaciones de seguridad pública

A nivel general en cuanto al impacto de las TICs en la Seguridad Ciudadana y Pública no se ubicaron datos y estudios complementario más profundos.

4.2.3 El Caso de Honduras

SECCIÓN 1: DATOS GENERALES

[93] http://www.1mobile.es/gt-digitalhulahoop-pncmovil-134054.html

Tabla 9: Datos generales de la Comisión Nacional de Telecomunicaciones de Honduras

	Datos de contacto general:	
	Nombre de la institución	Comisión Nacional de Telecomunicaciones (CONATEL)

SECCIÓN 2: POLITICAS PÚBLICAS

El análisis del instrumento recibido de Honduras indica, a julio del 2015**,** que Las políticas de Seguridad Pública o Ciudadana, **SI** están vinculadas al marco regulatorio de TICs existente en el país y que **NO** existe un plan de interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs.- Honduras presenta avances importantes, resaltando la activación de la Politica Integral de Convivencia y Seguridad Ciudadana para Honduras 2011-2022[94], que vincula el uso de la TICs y aspectos como el desarrollo del "Sistema Información de Violencia y Delincuencia" para atender el problema de la inseguridad ciudadana y la violencia, orientar políticas de prevención y control y asegurar el seguimiento y evaluación de las mismas, es necesario asegurar la capacidad de recolectar y analizar datos de una manera confiable y oportuna.

Además, rectora el mejoramiento del Sistema de Comunicaciones para la puesta en funcionamiento de una central única de comunicaciones, dirigida a la creación de una Central Única de Emergencias y Seguridad, donde además de la policía hagan presencia y operatividad los servicios de bomberos, Salud, Policía de tránsito, Cruz Roja, prevención y atención de emergencias y todas aquellas instituciones que por sus funciones puedan contribuir a atender una emergencia.

Una central única de Emergencias y Seguridad que:

- Mejore la capacidad de repuesta de cada agencia para atender más incidentes con los mismos recursos de personal y equipos,
- Permita identificar y suplir los cuellos de botella de personal, infraestructura y equipos de cada agencia.
- En el corto plazo permita atender las emergencias en menor tiempo y en forma más efectiva.
- En el mediano plazo y con fundamento en las estadísticas de atención y acciones de prevención, mejore la seguridad de los ciudadanos.
- Mejorar la capacidad del país para responder a las catástrofes naturales, o situaciones de orden público

En materia de centros penitenciarios también rectora:

- Mejorar los sistemas de seguridad de los centros carcelarios, para lo cual se requiere, capacitar al personal existente en materia de seguridad carcelaria,
- Implementar seguridad electrónica interna y perimetral,
- Desarrollar sistemas de comunicación especiales,
- Desarrollar sistemas independientes y autónomos de energía e iluminación y desarrollar procesos de control, administración y automatización centralizado de los sistemas de seguridad.

[94]http://www.hn.undp.org/content/dam/honduras/docs/publicaciones/Politica_Integral_Convivencia_Seguridad_2011_2022.pdf

- Fortalecer el sistema de comunicaciones de cada uno de los centros carcelarios y a su vez con todo el Sistema Penitenciario a partir de establecer una red de comunicaciones que permita mantener el contacto de los administrativos y la guardia,
- Contar con equipos que permitan la transferencia de información confidencial en forma segura,
- Manejo de bases de datos de reclusos con archivos centralizados para mayor veracidad y como método de respaldo.
- Fortalecer los sistemas de movilidad y traslado reclusos.
- Crear y aplicar manuales con estándares internacionales de disciplina y comportamiento interno de los reclusos, personal administrativos y guardia.

La Política Nacional de Prevención de Violencia[95] hacia Niñez y juventud, aprobada el 13 de febrero del 2013, rescata en su segundo principio que "La política de prevención de la violencia hacia la niñez y la juventud se basa en una estrategia que garantice a la niñez y juventud el acceso a la capacitación técnica, el conocimiento tecnológico adecuado, y la realización de sus potencialidades, permitiendo su inserción satisfactoria al trabajo digno en su vida productiva."

En su inciso 5.1, que La Prevención de la Violencia, delincuencia y los conflictos se orientará por los siguientes lineamientos generales: Difusión, promoción y articulación de programas que promuevan la promoción del Desarrollo Positivo de Jóvenes Vulnerables, Promoción y Reorientación del Desarrollo Humano de Población en Riesgo, Empleabilidad y Habilidades para la Vida, Fomento de Cultura Ciudadana, Fortalecimiento, creación y Rescate de Espacios Públicos, Acceso a centros deportivos, artísticos, tecnológicos e informativos, otros procesos innovadores y sostenibles a nivel de las comunidades

SECCIÓN 3: IMPLEMENTACIONES DE TICS

Aplicaciones de TICs **vinculadas a la Seguridad Pública** que se han implementado con éxito

- Centros de operaciones de la Policía en los niveles locales y nacionales.
- Sistemas de radiocomunicación de Seguridad Ciudadana para la Policía.
- Sistemas de información de Seguridad Ciudadana para la Policía.
- Sistemas de operaciones de Organismos de Emergencia. Existe convenio con el 911.
- Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV)
- Sistemas de dactiloscopia.
- Sistema de Identificación de Vehículos,
- Sistema de Identificación y reconocimiento facial.
- Observatorios de Seguridad Ciudadana
- Centros integrados con interoperabilidad con las soluciones anteriores tipo 911,
- Sistema Integrado de Identificación Balística (IBIS).
- Sistema de Identificación Aeroportuaria
- Sistemas de Radio Comunitarios

Implementaciones en progreso en Honduras

Sistema de Inteligencia Forense que facilita la gestión de conocimiento y la investigación forense de:

- Patología,
- Clínica y

[95] http://www.pnp.gob.hn/Archivos%20Para%20Descarga/PNPV%20RESUMEN%20EJECUTIVO%20Y%20PNPV%20AL%2012%20DE%20FEBRERO%20DEL%202013%20(1).pdf

- Laboratorios de drogas, armas y explosivos, daños al medio ambiente, etc.

Sistema desarrollado para mejorar la habilidad del departamento de Medicina Forense eficientando la recolección de información que permite compartir de forma confiable la información concerniente a la investigación criminal con otras instituciones ,ONGS y el público en general.- Lo que demandó implementar e integrar un sistema de gestión de información para ser aplicado por la Dirección de Medicina Forense a Nivel Nacional y el correspondiente lanzamiento de una revista en línea con el análisis de estadísticas y datos de crimen para el público.

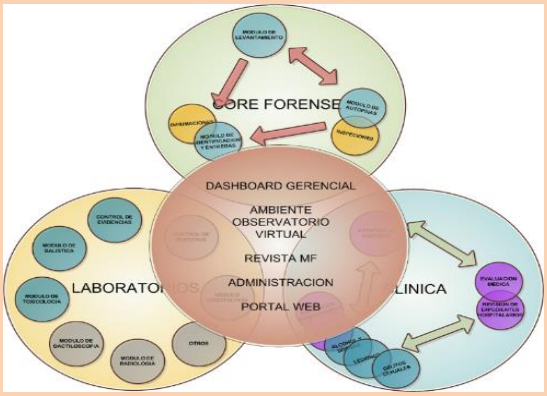
Su levantamiento de línea base comenzó en enero del 2014, a junio del 2014 ya se contaba con los documentos de análisis y diseño, entrando en una fase de desarrollo en agosto del 2014, su implementación inicial se dio a partir de abril del 2015, está siendo financiado por USAID, permitió por las exigencias de la Dirección Forense trabajar todos la documentación de sustento bajo formatos protocolares y normas ISO-9001.[96]

El sistema es la base de gestión de conocimiento de la mesa interinstitucional que conforman el Observatorio de la Violencia, la Secretaria de Seguridad, el Ministerio Público a través de Medicina Forense. La solución técnica fue desarrollada con software libre: Microsoft Windows 7 o 8

- Servidor web Apache 2.4
- Base de datos PostgreSQL 9.3
- EDI de Programación NetBeans 8.O
- Pentaho
- Framework de programación Synfony 2.4

Considera los siguientes módulos operativos:

Figura 16: Módulos Operativos del Sistema de Inteligencia Forense

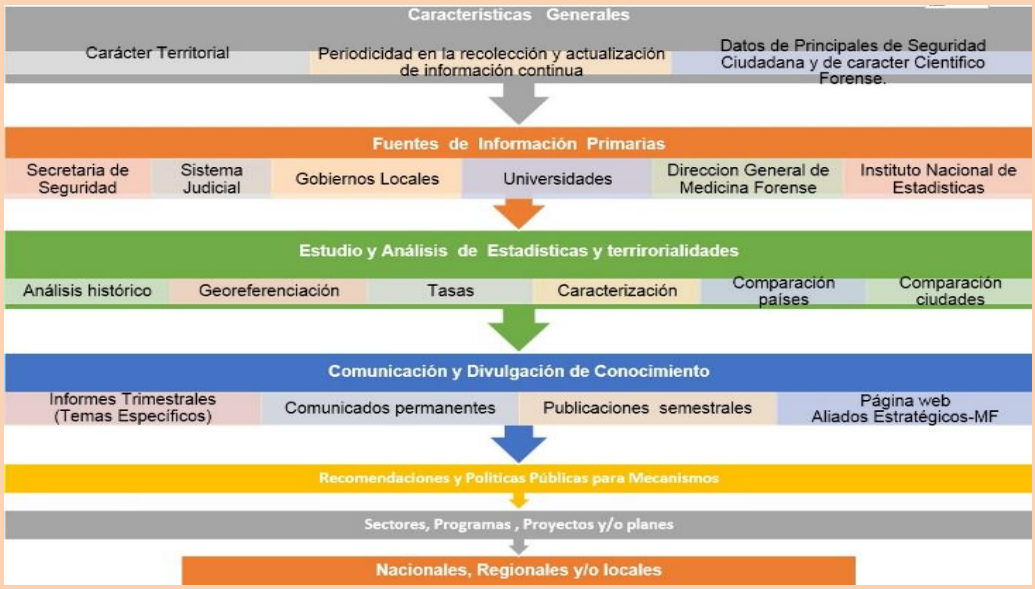


Fuente: *Revista Forense de Honduras*

El sistema fue concebido sobre la base de gestión de conocimiento basado en la evidencia, que se perfilará gradualmente bajo mecanismos de investigación definidos considerando un marco integral de Observatorio Forense que se consolidará gradualmente bajo lo siguiente:

[96] https://www.mp.hn/Forense/revista-2/

Figura 17: Marco integral del observatorio forense



Fuente: *Elaboración propia*

Este sistema forma parte del plan estratégico[97] 2015-2020 del Ministerio Público de Honduras.

Sistema de 911 Honduras

Tabla 10: Datos del sistema 911 de Honduras

	Datos del Sistema de 911 Honduras	
	Nombre de la institución	Sistema 911 Honduras
	Dirección Internet	www.seguridad.gob.hn
	Inaugurado:	Nace como linea 199 Evoluciona a 911 mayo 2013

Como una medida más para contrarrestar los altos índices de violencia que azotan a Honduras, la noche del jueves 25 de abril del 2013 se anunció la implementación del número 911, para que la población haga sus denuncias de emergencia.

> **"El anuncio se hizo en cadena de radio y televisión, todos los números de emergencia quedan concentrados en el 911. Habrá equipos de respuesta para atender inmediatamente las emergencias denunciadas."**

[97] https://www.mp.hn/index.php?option=com_content&view=category&layout=blog&id=142&Itemid=304

La medida trata de fortalecer la seguridad ciudadana y los sistemas de respuesta inmediata como los de llamadas de emergencia de la Policía Nacional.

"Tengo a bien informar que, a partir de esta fecha, hemos puesto a disposición el número de emergencias 911 de la Policía Nacional, el que, sin duda, contribuirá a que combatamos la delincuencia y la violencia con mayor efectividad", dijo el titular de Seguridad, Pompeyo Bonilla en esa fecha.

Al número 911, que es parte del proyecto de Ciudades Seguras, se puede llamar, tanto desde teléfonos fijos, como desde teléfonos celulares, todo con el fin de felicitarle a la ciudadanía la poderosa herramienta de la denuncia.

Figura 18: Sistema de Emergencias 911 – Honduras

Este nuevo servicio del 911, sustituye a todos los números de emergencia existentes como el 100 de la Emergencia Municipal, el 101 de Dirección Nacional de Servicios Especiales de Investigación, el 112 de la Dirección Nacional de Investigación Criminal, el 114 para casos de Violencia Domestica y el 199 de la Policía Nacional.

La Comisión Nacional de Telecomunicaciones (CONATEL) aprobó la normativa necesaria para sancionar a quienes efectúen llamadas inadecuadas, con penas que van desde sanciones económicas, hasta la suspensión definitiva del número telefónico.

A partir del primero de mayo del 2013, la Policía Nacional y las Fuerzas Armadas tienen equipos de reacción inmediata en los diferentes cuadrantes de Tegucigalpa y San Pedro Sula, lo que ha permitido la atención oportuna a las denuncias al 911.- San Pedro Sula desde el año 2004 opera bajo la estructura de ocho(8) sectores Nor oeste, Nor este, Sur oeste, Sur este, Sub urbano Este, Sub urbano Nor Este, Sub Urbano, Sur Este para abordajes en seguridad y convivencia ciudadana, aunque su organización territorial comenzo bajo esta estructura desde 1994.

El sistema del 911 está integrado por un centro de comando y control, además de moderna tecnología con cámaras de video seguridad para prevenir y esclarecer diferente tipo de situaciones que puedan afectar la seguridad ciudadana. Con la misión de apoyar, dirigir, controlar, administrar la plataforma tecnológica inteligente para la oportuna actuación e intervención de las unidades operativas, fortalecer la prevención y combate del crimen común y organizado, los procesos investigativos de la Policía y la interoperabilidad con los organismos de emeregencia.

En las aplicaciones de TICs vinculadas **en la administración de Justicia en centros penitenciarios** se rescatan avances sobre:

Seguridad perimetral:

- Radio comunicadores en vehículos de patrulla y para guardias penitenciarios,
- Ampliación de marcos jurídicos con la Ley de Limitación de Servicios de Telefonía Móvil Celular y Comunicaciones Personales (PCS) en los Centros Penales [98] y otros sistemas.-

[98] http://www.congresonacional.hn/index.php/2014-02-10-22-24-42/congreso/item/920-cn-amplia-a-wi-fi-bloqueo-de-llamadas-desde-carceles-e-impone-hasta-siete-anos-de-prision-a-los-infractores

Vigilancia y Monitoreo:

- Monitoreo mediante brazalete electrónico
- Cámaras de circuito cerrado de televisión,
- Seguimiento e interferencia telefonía celular.

Control de Acceso:

- Dispositivos de detección de metales u otro tipo de artículos no permitidos,

Sistemas de limitación de servicios de telefonía móvil celular y comunicaciones personales:

- Ley de limitación de servicios de telefonía móvil celular y comunicaciones personales (PCS) en centros penales a nivel nacional.(Decreto 255/2013[99])

Esta ley demandó de CONATEL el establecimineto de los mecanismos técnicos, administrativos, regulatorios, financieros, así como la coordinación y cooperación interinstitucional que posibilite el cumplimiento de la Ley[100] de Limitaciones de Servicios de Telefonía Móvil Celular y Comunicaciones Personales (PCS) en Centros Penales, Penitenciarias Nacionales y Centros de Internamiento de Menores a nivel Nacional contenidas en el Decreto Legislativo 255-2013.- La Creación de la Comisión Interinstitucional de Seguridad de las Telecomunicaciones (CISTEL) para dar cumplimiento a la limitación de brindar o prestar servicios de Telefonía Móvil Celular y de Comunicaciones Personales

Sobre la consulta de TICs vinculadas **en la Seguridad Pública y la Inteligencia** se resaltan las

Plataformas de información en inteligencia:

- Locales nacionales y transnacionales de inteligencia para recabar "indicios" como los manejados por los cuerpos de Fiscalía,
- Sistemas de Información para la Gestión Pericial Forense

Pero existe poco o ninguna implementación sobre

- Seguimiento de la "Ruta" de la delincuencia común y organizada,
- La delincuencia económica y financiera,
- Inteligencia criminal,
- Análisis y estudio de casos de drogas y
- Análisis y estudio de casos de terrorismo
- Análisis y estudio de crimen organizado
- Análisis y estudio del crimen cibernético
- **Sistemas de información Especializados:**
  - Sistemas Satelitales de captación de imágenes.
  - análisis y estudio de personas desaparecidas

SECCIÓN 4: REGULACIÓN, INNOVACIÓN Y AGENDAS

Sobre las regulaciones de las TICs para la Seguridad Pública y Ciudadana, en lo referente a los criterios en las regulaciones de las TIC para la Seguridad Pública y Ciudadana que son consideradas:

- Estándares operacionales
- Estándares técnicos

[99] http://sitae.conatel.gob.hn/centrospenales/Ley_Decreto_255-2013.pdf
[100]http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20de%20Limitaci%C3%B3n%20de%20Servicios%20de%20Telefon%C3%ADa%20Movil%20Celular%20en%20Centros%20Penales%20a%20nivel%20nacional.pdf

- Nomenclatura de uso de canales estándares para la Interoperabilidad
- La disposición para el intercambio común de datos

Sobre a la innovacion está en estudio, analisis o implementación por parte del organismo regulador

- Política de Interoperabilidad que promueva intercambiar información del gobierno en aspectos: organizacionales, técnicos, operacionales y de gobernanza.
- Plan o estrategia para desarrollar un sistema único de control de delitos en tiempo real que reciba todas las denuncias (llamadas, correos electrónicos y redes sociales),
- Plan o estrategia para desarrollar aplicaciones móviles para extender las opciones de denuncias por medio de texto, imagen, video y audio
- Plan o estrategia para el uso de los medios sociales en comunicaciones de seguridad pública

NO se ha contemplado (i) el estudio de estándares de interoperabilidad para reforzar el transporte de datos, imágenes, videos y voz en tiempo entre el policía, las patrullas, los ciudadanos y los centros con equipos base o tipo sistemas de despacho ni un (ii) Plan o estrategia para el desarrollo de Sistemas informáticos que ayuden a evaluar las tendencias y las probabilidades

Agenda Digital de Honduras (ADH)[101] 2014-2018

Ésta iniciativa busca crear una Red de Información Regional para romper la brecha digital y tecnológica que existe a nivel nacional, impulsando el acceso a la información y las comunicaciones de las regiones para desarrollar el acceso a los servicios de educación, salud y seguridad, entre otros, así como el potencial productivo, de manera que coadyuve a la mejora de las condiciones y nivel de vida de sus ciudadanos.

Considerando el Decreto PCM 047-2010 del Poder Ejecutivo el Gabinete de Telecomunicaciones[102] (GT), es la autoridad política en relación con los procesos vinculados a la implementación de la ADH, gabinete que debería de integrarse según esta disposición, por los Secretarios de Estado del Despacho Presidencial que lo coordina, de Finanzas, Defensa, Seguridad, Planificación y Cooperación Externa y un ciudadano nombrado por el Presidente de la Republica, con funciones de:

- Impulsar políticas que incentiven el desarrollo de la infraestructura para el uso de tecnologías de la información.
- Promover la puesta en funcionamiento del Fondo Social de Telecomunicaciones que permita proveer servicios de telecomunicaciones y tecnologías de la información a nivel nacional.
- Coordinar la implementación, seguimiento y evaluación de la ADH, con las diferentes instituciones del Estado y actores no gubernamentales.
- Conocer y aprobar los lineamientos de políticas, programas y proyectos relacionados con la ADH y las TIC en general.
- Conocer y aprobar el presupuesto plurianual y presupuesto anual para la implementación de la Agenda.
- Establecer las orientaciones para la gestión de recursos internos y externos, para el financiamiento requerido.

En la actualidad las actividades vinculadas a la coordinación y gestión de la Secretaria de Coordinacion General del Gobierno (SCGG-HN), a través de la Unidad de Gobierno Digital[103], de la Dirección Presidencial de Transparencia, Modernización y Reforma del Estado

La agenda si bien representa una facilidad política y operativa, no ha facilitado avances sobre la Seguridad Ciudadana del país, donde existen brechas de normativa y regulación sobre:

[101] http://agendadigital.hn/wp-content/uploads/2013/10/AgendadigitalCOR.pdf
[102] http://melarayasociados.com/legislacion/nuevo-pagina-3/nuevo-pagina-12/
[103] http://www.scgg.gob.hn/sites/default/files/organigrama-general.jpg

- Ley de Tecnologías de la Información y Comunicación
- Ley de Comercio electrónico
- Plan nacional de banda ancha
- Ley de protección de la información
- Ley de Gobierno Digital
- Ley de delito Cibernético.

4.2.4 El Caso de Panamá

SECCIÓN 1: DATOS GENERALES

Tabla 11: Datos de la Autoridad para la Innovación Gubernamental de Panamá

	Datos de contacto general:	
	Nombre de la institución:	Autoridad para la Innovación Gubernamental

SECCIÓN 2: POLITICAS PÚBLICAS

El análisis del instrumento recibido de Panamá indica, a julio del 2015**,** que las políticas de Seguridad Pública o Ciudadana, **SI** están vinculadas al marco regulatorio de TICs existente en el país y que **SI** existe un plan de interoperabilidad[104], que considera integraciones para la Seguridad Pública de las TICs.

La Autoridad Nacional para la Innovación Gubernamental (AIG), es la entidad responsable de la modernización del Estado, mediante el uso de las Tecnologías de Información y Comunicaciones (TICs). Para lograr esto, la AIG ha orientado sus esfuerzos en alcanzar desde el 2011, tres grandes hitos importantes que son:

Infraestructura Digital: Consiste en la implementación de los componentes necesarios que constituirán el vehículo tecnológico para la construcción de la plataforma digital requerida para poder desarrollar los proyectos de modernización tecnológica del Estado. Entre estos están la Nube Computacional, Interoperabilidad del Estado, CSIRT, y NOC.

- **Conectividad:** Consiste en la implementación de tecnologías apropiadas y de última generación para lograr el acceso y la conectividad de la mayor cantidad de ciudadanos y entidades a nivel nacional. Entre estos están La Red Nacional de Acceso Universal Internet, Plataforma Multiservicios de Comunicaciones, Red de Gobiernos Locales y Centro de Atención Ciudadana 311.

[104] http://www.innovacion.gob.pa/descargas/PSP-Propuesta-Ley-y-Marco-de-Interoperabilidad.pdf

- **Desarrollo de Proyectos Institucionales**: Consiste en la planeación e implementación de proyectos con la colaboración de otras instituciones del Estado, con visión integrada de Gobierno y clasificados en diferentes áreas como e-salud, e-educación, e-seguridad, e-pagos sociales, e-tierras, e-tránsito, e-finanzas públicas, e-banca pública, e-justicia, e-exportaciones, e-Gobiernos Locales y Panamá sin Papel.

Figura 19: Panamá Inteligente. Visión única del Ciudadano

SECCIÓN 3: IMPLEMENTACIONES DE TICS

Aplicaciones de TICs **vinculadas a la Seguridad Pública** que se han implementado con éxito en Panamá sobre lo siguiente:

- Centros de operaciones de la Policía en los niveles locales y nacionales.
- Sistemas de radiocomunicación de Seguridad Ciudadana para la Policía.
- Sistemas de información de Seguridad Ciudadana para la Policía.
- Sistemas de Información y posicionamiento geográfico para emergencias.
- Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV)
- Sistemas de dactiloscopia.
- Sistema de Identificación de Vehículos.
- Sistemas de Identificación aeroportuaria.
- Sistema de Identificación y reconocimiento facial.
- Observatorios de Seguridad Ciudadana.
- Sistemas de Inteligencia Forense: que facilita la gestión de conocimiento y la investigación forense de Patología, Clínica y Laboratorios de drogas, armas y explosivos, daños al medio ambiente, etc.
- Observatorios de Seguridad Ciudadana.
- Centros integrados con interoperabilidad con las soluciones anteriores tipo 911.
- Centros de Respuesta para incidentes informáticos (Computer incident report).
- Sistema de Identificación Aeroportuaria (Migratoria y para reconocimiento facial).

Sistema de Video Vigilancia, Panamá

Tabla 12: Datos del sistema de video vigilancia de Panamá

	Datos del Sistema de Video-Vigilancia, Panamá	
	Nombre de la institución	Sistema de Video Vigilancia
	Dirección Internet	http://www.policia.gob.pa/
	Datos de Contacto:	+(507) 511-7000

Desde 2007 Panamá comienza la instalación de cámaras, llegando a 564 cámaras en el 2009. Como una medida más para contrarrestar la Inseguridad Cable & Wireless Panamá entregó a la Policía Nacional la plataforma tecnológica para el Proyecto de Video Vigilancia Ciudadana, contribuyendo de esta manera con los estamentos de seguridad del estado orientados a garantizar la seguridad de los panameños.

Actualmente el proyecto de Video Vigilancia contará con un total de 264 cámaras más, de las cuales 95 estarán listas en el mes de septiembre y las mismas serán ubicadas en los Corregimientos de Bella Vista, Calidonia, San Felipe y el Chorrillo. Para el mes de noviembre 169 cámaras suplementarias vendrán a complementar lo que constituirá una verdadera muralla virtual al servicio de la los agentes de la Policía Nacional. Estas cámaras estarán en los corregimientos de Parque Lefevre, San Francisco, Pueblo Nuevo y Bethania. Las inversiones iniciales, con fondos nacionales del sistema fueron de 3 millones de dólares con fortalecimientos posteriores de 4 millones de dólares en ciudad de Panamá, desde mediados del 2015 el Ministerio de Seguridad de Panamá ha comenzado un fortalecimiento para instalar 5,000 cámaras en ciudad Panamá a un costo de 20 millones de dólares, bajo el programa Barrios seguros con más oportunidades y mano firme, el mismo programa ha contemplado un presupuesto de 2 millones de dólares para la compra de brazaletes para la administración de Justicia, específicamente para el proyecto contra la violencia domestica, que coordina el ministro de Seguridad Pública, Rodolfo Aguilera.

Este sistema de Video Vigilancia en ciudad Panamá cuenta con la facilidad "ShotSpotter"[105], que permite detectar con exactitud si se realizó un disparo desde una arma de fuego, el calibre del arma y su posicionamiento en la cámara más cercana, mediante el proceso de sensar los decibeles de ruido y gestionarlos a través de bases de datos ya existente, se puso a prueba el sistema en la cumbre de las Américas de Panamá[106] con más de 300 cámaras en abril del 2015, para la protección de mandatarios a nivel continental, 300 policías están directamente involucrados en la gestión, coordinación de los centros de operaciones 24/7 y respuesta a la ciudadanía bajo este sistema.

En las aplicaciones de TICs vinculadas **en la administración de Justicia en centros penitenciarios** se rescatan avances significativos sobre:

Seguridad perimetral:

- Radio comunicadores en vehículos de patrulla y para guardias penitenciarios.
- Sistema de Bloqueo de Comunicaciones a través de servicios de Internet, WI-Fi, telefonía satelital y otros sistemas.

[105] http://www.shotspotter.com/
[106] http://www.telemetro.com/cumbredelasamericas/videos/camaras-vigilancia-instaladas-perimetro-Cumbre_3_794350618.html

Vigilancia y Monitoreo:

- Monitoreo mediante brazalete electrónico.
- Cámaras de circuito cerrado de televisión.
- Seguimiento e interferencia telefonía celular.

Control de Acceso:

- Dispositivos de detección de metales u otro tipo de artículos no permitidos.
- Dispositivos de detección de explosivos.
- Escáneres de vehículos y personal.

Sistemas de posicionamiento

- Monitoreo y traslado de recursos a centros judiciales u otro reclusorio .

Sobre la consulta de TICs vinculadas **en la Seguridad Pública y la Inteligencia** se resaltan las

Plataformas de información en inteligencia para el:

- La delincuencia y economía financiera
- Análisis y estudio del crimen cibernético (CSIRT)

Sobre el CSIRT[107] PANAMÁ (*Computer Security Incident Response Team*)

Es el equipo nacional de respuesta a incidentes de seguridad de la información de Panamá. Entre sus objetivos están la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá.

Tiene como misión coordinar, colaborar, y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas y de comunicaciones de las entidades gubernamentales.

Figura 20: Sede del CSIRT, Panamá

Este proyecto se propone fortalecer la difusión, el conocimiento y atención de suceso de Seguridad Informática del Estado. Con la coordinación y colaboración de los estamentos para la resolución de incidentes de seguridad de la información y comunicación. Se crea mediante decreto ejecutivo 709, del 26 de Septiembre del 2011[108], cuenta actualmente con un equipo de 4 personas involucradas directamente en los procesos del CSIRT financiados bajo presupuesto nacional de la AIG.

[107] http://www.innovacion.gob.pa/csirt
[108] http://www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf

Sobre la consulta de TICs vinculadas **a los Sistemas de Información Ciudadana y las Redes Sociales** se resalta:

- El patrullaje inteligente mediante radio

SECCIÓN 4: REGULACIÓN, INNOVACIÓN Y AGENDAS

Sobre las regulaciones de las TICs para la Seguridad Pública y Ciudadana, en lo referente a los criterios en las regulaciones de las TIC para la Seguridad Pública y Ciudadana que son consideradas:

- Estándares técnicos
- La disposición para el intercambio común de datos
- Criterios de capacidad de servicio

Sobre a la innovacion está en estudio, analisis o implementación por parte del organismo regulador

- Política de Interoperabilidad que promueva intercambiar información del gobierno en aspectos: organizacionales, técnicos, operacionales y de gobernanza.
- Plan o estrategia para el desarrollo de Sistemas informáticos que ayuden a evaluar las tendencias y las probabilidades.
- Plan o estrategia para desarrollar un sistema único de control de delitos en tiempo real que reciba todas las denuncias (llamadas, correos electrónicos y redes sociales).

NO se ha contemplado (i) el estudio de estándares de interoperabilidad para reforzar el transporte de datos, imágenes, videos y voz en tiempo entre el policía, las patrullas, los ciudadanos y los centros con equipos base o tipo sistemas de despacho (ii) Plan o estrategia para desarrollar aplicaciones móviles para extender las opciones de denuncia por medio de texto, imagen, video y audio ni un (iii) Plan o estrategia para el uso de medios sociales en comunicaciones de seguridad pública

En Control de Acceso: se enuncia un avance en:

- Dispositivos de detección de metales u otro tipo de artículos no permitidos,
- Dispositivos de detección de explosivos
- Escáneres de vehículos y personal con tecnología de Rayos X

Agenda Digital Panamá

Con un plan ambicioso, que supone un cambio importante en la forma de gobernar los recursos del país, con una fuerte renovación política y ética, con una fuerte descentralización de la gestión y la reforma legal y constitucional, que ha puesto su foco de acción en el crecimiento económico que ayude en la distribución y la inclusión social que a su vez retroalimente el crecimiento (“Incluir para Crecer y Crecer para Redistribuir”).

El Plan identifica 5 palancas de crecimiento:

1. Infraestructura y Servicios para la Competitividad del país (Sectores Motores) o Sectores Motores: Logística, Agricultura, Turismo y Minería
2. Infraestructura para los Servicios Sociales.
3. Generación de Capacidades para la Competitividad (Educación, reducción de la Brecha Digital, y fortalecimiento institucional)
4. Seguridad Jurídica y Transparencia
5. Medio-ambiente y planificación para el ordenamiento territorial

El presupuesto estimado necesario solo para la contratación de 35 personas asciende a un valor de B/.832,000 por año. La agenda rescata algunas ideas y mejores experiencias [109] de Chile, Colombia y España para el cambio de normas y leyes, entre primeras 4 líneas como ser:

Figura 21: Agenda Digital Panamá

Ley de Privacidad de Datos

Ley de privacidad de datos que fortalezca la interoperabilidad y la posibilidad de implementar estrategias de cloud computing tanto a nivel gubernamental como a nivel de entorno empresarial:

- Para efectos de interoperabilidad, apoya la generación de certezas jurídicas para las instituciones a la hora de compartir datos personales, uno de los principales frenos en la implementación de estrategias de interoperabilidad. - Similar cuestión aplica para la implementación de nubes gubernamentales, donde al centralizar información de instituciones con diferente alcance legal, se requiere de certezas de protección de información para proteger los ámbitos legales de acción de las instituciones involucradas en una estrategia de este tipo. -
- Finalmente, en lo relativo a entorno empresarial, una buena ley de protección de datos, permite el establecimiento de negocios basados en datos por parte de empresas extranjeras que ofrezcan servicios basados en la nube, y que les permita entregar certezas jurídicas a sus usuarios en relación al uso de sus datos, como es el caso de Irlanda, donde la ley de protección de datos, ha facilitado la instalación de grandes empresas como Microsoft y Facebook.

Ley de Ciberseguridad

La AIG tratará de dar cumplimiento a los retos de seguridad, por medio de la acción coordinada de su Centro de Respuesta (C-SIRT), el desarrollo de medios tecnológicos y la apropiada normativa, de conformidad con el Plan Nacional de Ciberseguridad que se está implementando.

- Ataques a los sistemas de información.
- Retos relacionados con la difusión de los dispositivos móviles y de los servicios basados en la utilización de redes móviles.
- Retos relacionados con el advenimiento de los "entornos inteligentes". Estos "entornos inteligentes" suponen un punto importante dentro de la sociedad de la información.
- Retos relacionados con la sensibilización de los usuarios. Uno de los problemas a los que se enfrenta Panamá y su entidades de gobierno es la extendida infravaloración que otorgan los usuarios a los riesgos que corren. El reto es conseguir presentar la seguridad como un activo y no como un coste de manera que los usuarios no lo consideren un aspecto negativo como viene sucediendo, en cierta medida, hasta el día de hoy.

[109] http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf , página 33

8.2.3 Marco de Interoperabilidad

Desarrollar un marco de interoperabilidad que incluya protocolos, definiciones técnicas, metodologías y patrones al estilo del esquema desarrollado por Brasil denominado e-Ping.

8.2.4 Decreto de Software Libre

Sobre el uso de software libre y neutralidad tecnológica informada para la implementación de TI al interior del Gobierno que incluya normas sobre licenciamiento a la hora de contratar desarrollos privados, disponibilidad de software en repositorios, evaluación no sesgada de soluciones abiertas y privativas, promoviendo el uso de tecnologías abiertas, entre otros.

Se rescata la iniciativa de Panamá de contar con un equipo gestión estratégica interinstitucional o multisectorial para consolidar políticas, planes, proyectos para promover acciones de impacto en las TICs para la Seguridad Pública.

4.2.5 El Caso de República Dominicana

SECCIÓN 1: DATOS GENERALES

Tabla 13: Datos del Instituto Dominicano de las Telecomunicaciones

	Datos de contacto general:	
	Nombre de la institución	Instituto Dominicano de las Telecomunicaciones (INDOTEL)

SECCIÓN 2: POLITICAS PÚBLICAS

El análisis del instrumento recibido de República Dominicana indica, a julio del 2015**,** que las políticas de Seguridad Pública y Ciudadana, **SI** están vinculadas al marco regulatorio de TICs[110] existente en el país y que **SI** existe regulaciones que se enrutan hacia un plan de interoperabilidad[111], que considera integraciones para la Seguridad Pública de las TICs.

INDOTEL es el organismo creado por la Ley General de Telecomunicaciones (153-98) que regula y supervisa el desarrollo del mercado de las telecomunicaciones. Su misión es "regular y promover la prestación de servicios de telecomunicaciones en beneficio de la sociedad, en un marco de libre, leal y efectiva competencia".

Según la ley no.126-02 sobre Comercio electrónico, documentos y firmas digitales. -

INDOTEL considera en la agenda Regulatoria "Un aspecto relevante a tener en cuenta es la interoperabilidad inherente a las transacciones digitales, la cual se logra mediante la adopción de estándares tecnológicos

[110] www.indotel.gob.do/index.php/uploads/2199/Res079-08-pdf

[111] Normas complementarias a la Ley No.126-02 , www.indotel.gob.do/index.php/uploads/3563/87-pdf

internacionalmente aceptados, y mediante el establecimiento de normas compatibles con la legislación internacional y las leyes modelo."

SECCIÓN 3: IMPLEMENTACIONES DE TICS

Las aplicaciones de TICs **vinculadas a la Seguridad Pública** que se han implementado con éxito en República Dominicana se describen a continuación:

- Centros de operaciones de la Policía en los niveles locales y nacionales.
- Sistemas de radiocomunicación de Seguridad Ciudadana para la Policía.
- Sistemas de operaciones de Organismos o instituciones de Emergencia.
- Sistemas de Información y posicionamiento geográfico para emergencias.
- Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV).
- Sistemas de dactiloscopia.
- Sistema de Identificación de Vehículos.

No se describen avances sobre

- Sistemas de Identificación aeroportuaria
- Sistema de Identificación y reconocimiento facial.
- Sistemas de Inteligencia Forense: que facilita la gestión de conocimiento y la investigación forense de Patología, Clínica y Laboratorios de drogas, armas y explosivos, daños al medio ambiente, etc.
- Centros integrados con interoperabilidad con las soluciones tipo 911.
- Centros de Respuesta para incidentes informáticos (Computer incident report)
- Sistema Integrado de Identificación Balística (IBIS).
- Sistemas de Radio Comunitarios.

Sistema Nacional de Atención a emergencias y seguridad 9-1-1

Tabla 14: Datos del Sistema Nacional de Atención a emergencias y seguridad 9-1-1, República Dominicana

	Datos de Sistema Nacional de Atención a emergencias y seguridad 9-1-1, República Dominicana	
	Nombre de la institución	911 República Dominicana
	Sitio Internet	www.911.gob.do

Figura 22: 911 – República Dominicana

El Sistema 911 [112] de República Dominicana atiende emergencias de Seguridad y Convivencia Ciudadana, así como las emergencias y urgencias cotidianas de la población

El Ministerio de la Presidencia, a través del Sistema Nacional de Atención a Emergencias y Seguridad 911 informa diariamente [113] de las atenciones del sistema 911, como una facilidad de transparencia y acceso de información a la población.

El Sistema Nacional de Atención a Emergencias y Seguridad 911 trabaja para brindar un servicio de calidad y para ello, mantiene una campaña educativa permanente para que la población sepa en qué situaciones debe marcar el número. Por lo tanto, conocer la diferencia entre los términos "emergencia" y "urgencia" es importante no solo para el personal de seguridad o para el equipo médico, sino también para toda la población en su conjunto.

Una una inversión de unos 2 mil millones de pesos, de los cuales el 40% se logro gracias a las donaciones de equipos hechas por países como Estados Unidos, Corea del Sur y Taiwán se realizó en este sistema[114].

Emergencia[115] es toda situación imprevista que requiere atención o tratamiento inmediato porque pone en peligro la vida de una persona o sus bienes. Mientras que una "urgencia" una situación de salud que también se presenta repentinamente, pero sin riesgo de vida y puede requerir asistencia médica dentro de un período de tiempo razonable (2 o 3 horas después de ocurrido el hecho).

Atendiendo[116] a la necesidad de atender las emergencias de manera oportuna, es importante hacer uso responsable del Sistema para seguir brindando un buen servicio a la ciudadanía y continuar salvando vidas.

El Sistema 911 cuenta con una facilidad educativa interactiva e innovadora, que permite a los ciudadanos de forma sencilla orientarse, sensibilizarse y educarse sobre los servicios prestados. Como sistema nacional de atención de emergencias y seguridad ciudadana también tiene bajo coordinación las operaciones del cuerpo de bomberos[117]. Opera con un presupuesto con fondos del estado de RD$ 2500 millones (Pesos RD) a partir del año 2014.

La policía[118] para integrarse a este sistema incorporo 230 radio patrullas, 502 motocicletas, la dotación de 200º estaciones de radiocomunicación, con 5324, agentes requirió preparar 112 destacamentos (puestos de policía) y 5 destacamentos móviles, la instalación de 1200 cámaras

Si bien las respuestas al formulario no referencian el Observatorio de Seguridad Ciudadana de República Dominicana [119] (OSC-RD).- El Observatorio, órgano dependiente del Consejo Nacional de Seguridad

[112] https://www.youtube.com/watch?v=hslMvEwFmoQ
[113] http://minpre.gob.do/
[114] https://www.youtube.com/watch?v=T_eNQcIa368
[115] http://911.gob.do/#3
[116] http://911.gob.do/#4
[117] http://911.gob.do/#10
[118] https://www.youtube.com/watch?v=jimOKYyQziw
[119] http://mip.gob.do/Portals/0/docs/Publicaciones%20Docs/2014/19-08-2014/Boletines/Boletin%20Enero-Junio%202014.pdf

Ciudadana es un esfuerzo interinstitucional bajo la coordinación del Ministerio de Interior y Policía[120] para realizar análisis sobre la situación de violencia y criminalidad en el país. Se realiza una mirada descriptiva de los datos estadísticos, documentando la dimensiones y caracterización de los hechos ocurridos con la finalidad de que esta aproximación al fenómeno contribuya a un mejor entendimiento de la realidad y permita avanzar en la búsqueda de soluciones efectivas.

Figura 23: Observatorio de Seguridad Ciudadana de la República Dominicana

El objetivo principal del boletín es documentar la situación de violencia, criminalidad y accidentalidad a fin de que las autoridades gubernamentales, los sectores de seguridad, salud, educación y justicia, con la participación del sector académico, así como la sociedad civil, ONGs y medios de comunicación, tengan los elementos que les permitan impulsar la formulación de estrategias y políticas, así como evaluar la pertinencia y sostenibilidad de las estrategias que actualmente funcionan en el país. El Ministerio de Interior y Policía destaca la gran colaboración en este ejercicio conjunto, de los equipos técnicos de todas las fuentes de información, así como el apoyo técnico del Programa de las Naciones Unidas para el Desarrollo (PNUD). Sus

Se rescata[121] de esta experiencia que al igual que el

- Centro de Estudio y Análisis para la Convivencia y Seguridad Ciudadana de Bogotá, Colombia (CEACSC)[122] los observatorios de:
- Seguridad Ciudadana de la CCIAP de Panamá[123]
- Seguridad Ciudadana de República Dominicana (OSC-RD)[124]

cuentan con una facilidad "protocolar" que rige y guía su actuar institucional.

En las aplicaciones de TICs vinculadas **en la administración de Justicia en centros penitenciarios NO** se rescatan avances significativos sobre:

- Seguridad perimetral.
- Vigilancia y monitoreo.
- Control de acceso.
- Sensores y dispositivos de alarma.
- Sistemas de posicionamiento.
- Sistema de pánico celular.

[120] http://mip.gob.do/mip.gob.do/ObservatoriodeSeguridadCiudadana/tabid/285/Default.aspx
[121]http://mip.gob.do/Portals/0/docs/Plan_de_Seguridad/Observatorio/MANUAL%20OPERATIVO%20DEL%20OBSERVATORIO%20DE%20SEGURIDAD%20CIUDADANA.pdf
[122] http://www.ceacsc.gov.co/index.php/que-hacemos
[123] http://www.seguridadcciap.com/wordpress/estado-de-situacion-y-lineas-de-trabajo/
[124]http://mip.gob.do/images/docs/Programas/Observatorio/MANUAL%20OPERATIVO%20DEL%20OBSERVATORIO%20DE%20SEGURIDAD%20CIUDADANA.pdf

Sobre la consulta de TICs vinculadas **en la Seguridad Pública y la Inteligencia** se resaltan las **Plataformas de información en inteligencia para:**

- La delincuencia y economía financiera sobre
- Inteligencia criminal.
- Análisis y estudio de casos de drogas.
- Análisis y estudio de casos de terrorismo.
- Análisis y estudio de crimen organizado.
- Análisis y estudio del crimen cibernético.

Pero existe poca implementación sobre

- Sistemas de información Especializados:
  - locales nacionales y transnacionales de inteligencia para recabar "indicios" como los manejados por los cuerpos de Fiscalía.
  - Sistemas de Información para la Gestión Pericial Forense.
  - Sistemas Satelitales de captación de imágenes.
  - Sistemas Información con el uso de drones para recopilar información de voz, data y/o imágenes.
  - Sistemas de información Especializados:
    - Sistemas Satelitales de captación de imágenes.
    - análisis y estudio de personas desaparecidas.

Sobre la consulta de TICs vinculadas **a los Sistemas de Información Ciudadana y las Redes Sociales** se resalta:

- El patrullaje inteligente mediante radio.

SECCIÓN 4: REGULACIÓN, INNOVACIÓN Y AGENDAS

Sobre las regulaciones de las TICs para la Seguridad Pública y Ciudadana, en lo referente a los criterios en las regulaciones de las TIC para la Seguridad Pública y Ciudadana que son consideradas:

- Estándares técnicos.
- Estándares operacionales.
- Estándares de formación.

Sobre los criterios en las regulaciones de las TIC para la Seguridad Pública y Ciudadana en República Dominicana se considera de alta importancia

- Criterios de capacidad de servicio.

Sobre la innovación está en estudio, análisis o implementación por parte del organismo regulador

- Política de Interoperabilidad que promueva intercambiar información del gobierno en aspectos: organizacionales, técnicos, operacionales y de gobernanza.
- Plan o estrategia para el desarrollo de Sistemas informáticos que ayuden a evaluar las tendencias y las probabilidades
- Plan o estrategia para desarrollar un sistema único de control de delitos en tiempo real que reciba todas las denuncias (llamadas, correos electrónicos y redes sociales),
- Plan o estrategia para desarrollar aplicaciones móviles para extender las opciones de denuncias por medio de texto, imagen, video y audio

- Plan o estrategia para el uso de los medios sociales en comunicaciones de seguridad pública
- El estudio de estándares de interoperabilidad para reforzar el transporte de datos, imágenes, videos y voz en tiempo entre el policía, las patrullas, los ciudadanos y los centros con equipos base o tipo sistemas de despacho

Agenda Digital República Dominicana 2014-2016

La Agenda Digital de la República Dominicana 2014-2016[125] es considerada una hoja de ruta que ofrece una visión clara de los desafíos que enfrenta el país para acelerar su proceso de Desarrollo Sostenible y su inserción hacia una sociedad de la información basada en el uso intensivo de las tecnologías de la información y comunicación, y de las acciones que se propone emprender en los próximos tres años en esta dirección.

Figura 24: Agenda Digital de la República Dominicana

La Ley Orgánica de la Estrategia Nacional de Desarrollo 2030 y su reglamento de implementación 134-15 constituyen el plan de Desarrollo Sostenible para la República Dominicana. Adicionalmente, se ha creado un portal donde se monitorean los Objetivos del Milenio (ODM) y su impacto en el desarrollo sostenible del país

La Agenda está organizada en cinco ejes estratégicos, con un total de cinco objetivos generales, 17 objetivos específicos, 39 líneas de acción y 115 iniciativas, tomando como horizonte los desafíos que requiere el avance del país hacia una economía digital. Los ejes estratégicos se enmarcan con los objetivos del Plan de Acción de Ginebra de la Cumbre Mundial para la Sociedad de la Información (CMSI), así como con áreas prioritarias de la CMSI post 2015, surgidas del proceso de consulta de la CMSI+10. De igual modo, con el Plan Regional para la Sociedad de la Información para América Latina y el Caribe (eLAC 2018).

El Marco Legal, Normativo y Políticas TIC del Gobierno Dominicano es utilizado para impulsar las TIC y el Gobierno Electrónico e incrementar los servicios ofrecidos a los ciudadanos por las diferentes instituciones del Gobierno. La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) es el órgano encargado de la estrategia de Gobierno Electrónico.

Las políticas gubernamentales sobre tecnologías de punta son fijadas por la OPTIC. Según el Decreto No. 229-07 que ratifica el Decreto No.1090-04, que creó la OPTIC. Son funciones de la OPTIC establecer políticas relacionadas con asuntos TIC y de Gobierno electrónico. El mismo decreto coloca la OPTIC como dependencia directa del Poder Ejecutivo, y establece los ámbitos en los cuales se desarrollará el Gobierno Electrónico.

Artículo 3. Del Decreto 229-05 sobre funciones de la OPTIC:

3.4 Formulación de políticas y la implementación del proceso de desarrollo e innovación tecnológica para la transformación y la modernización del Estado hacia la sociedad de la información, promoviendo la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y estandarización en materia de las Tecnologías de la Información y Comunicación (TIC).

[125] http://www.gob.do/index.php/politicas/2014-12-16-20-55-59

3.8 Velar, asistir y supervisar las normas, estándares y políticas relativos a la seguridad y privacidad de la información digitalizada y electrónica en el sector público.

3.9 Establecer los estándares, normas y criterios que permitan integrar los sistemas de las Tecnologías de la Información y Comunicación (TIC) de la Administración Publica.

3.13 Presentar al Poder Ejecutivo propuestas normativas que contribuyan al mejor desarrollo de las políticas de las Tecnologías de la Información y Comunicación (TIC) de la Administración Publica.

El Marco Legal, Normativo y Políticas TIC del Gobierno Dominicano[126] consta de las siguientes partes:

- Agenda Digital Dominicana, Estrategia (e-strategy), Sostenibilidad (e-sustainability)
- Medio Ambiente y e-Waste
- Marco legal de Gobierno Electrónico en la República Dominicana
- Normativas TIC

Los temas principales para el desarrollo sostenible de la República Dominicana en los próximos años se centran en varios ejes estratégicos:

- **Eje estratégico 1: infraestructura y acceso.**
  El desarrollo de una economía digital que beneficie a la población, al gobierno y al sector productivo se sustenta en la disponibilidad de una infraestructura de telecomunicaciones y banda ancha de calidad, accesible en todo el territorio nacional y asequible a toda la población.

  En la República Dominicana, el sector privado y el gobierno han trabajado en el desarrollo de esta infraestructura, a lo largo de la última década; con iniciativas público-privadas, que han hecho posible el aumento considerable de las suscripciones de Internet y de los servicios ofrecidos a través de esta red, así como el masivo uso de los teléfonos celulares.

  El gobierno, a través del Fondo de Desarrollo de las Telecomunicaciones (FDT), bajo la responsabilidad del Instituto Dominicano de las Telecomunicaciones (INDOTEL), ha implementado el programa de Banda Ancha Rural en más de 500 comunidades rurales y urbanas; se han habilitado más de 900 salas digitales que han beneficiado a diferentes sectores de la sociedad, incluyendo a las personas con discapacidad y 96 centros tecnológicos comunitarios, cubriendo todas las provincias del país. Se instalaron servicios de Wi-Fi en más de 100 municipios; para el acceso gratuito a Internet, se han dotado de computadoras a miles de estudiantes de escasos recursos económicos y se ha implementado el programa de la Excelencia Académica, en coordinación con el Instituto Tecnológico de las Américas (ITLA).

- **Eje estratégico: gobierno electrónico y servicios digitales.**
  Un componente estructural de la Sociedad de la Información y el Conocimiento lo constituye la oferta de un conjunto de servicios digitales, por parte del Estado, para el uso de la población, las empresas, el propio Gobierno y sus empleados, denominado Gobierno Electrónico (GE).

  En los procesos de reforma y modernización del Estado, el desarrollo del Gobierno Electrónico, a nivel central y local, posibilita la entrega de servicios públicos de manera ágil y directa, promueve la participación ciudadana y la transparencia de la gestión pública, contribuyendo al desarrollo de un Gobierno abierto y participativo.

  Desde el año 2004, el Gobierno dominicano inició la formulación de una estrategia de Gobierno Electrónico con la creación de la Oficina Presidencial de Tecnologías de la Información y

[126] http://www.gob.do/index.php/politicas/2014-12-16-20-56-34

Comunicación (OPTIC), mediante la cual se han implementado importantes iniciativas con el objetivo de incorporar el uso de las TIC al proceso de modernización de la administración pública en República Dominicana.

Uno de los avances, obtenidos a través de la OPTIC, es el Centro de Contacto Gubernamental (*GOB) que ofrece información a toda la población dominicana, por vía telefónica, concerniente a los diferentes servicios que las instituciones gubernamentales necesiten dar a conocer. Asimismo, en la actualidad el 100% de la administración pública central tiene presencia web, y es posible disponer de diversos trámites y servicios transaccionales en línea.

Contar con los sistemas interconectados a nivel del Estado; representa otro importante desafío; es necesario agotar una agenda profunda y sostenida en materia de interoperabilidad, requisito indispensable para la centralización y unificación de los servicios.

- **Eje estratégico 3: creación de capacidades.**
  La educación y la formación de ciudadanos y ciudadanas, además de ser una vía de inclusión social y de inserción laboral, constituyen un factor para desarrollar la innovación y apoyar el crecimiento de las economías. Es de reconocimiento universal que el manejo de las TIC, por parte de las personas, es fundamental y aquellos que no logren adquirir las capacidades básicas para utilizarlas podrían quedar excluidos del nuevo paradigma socioeconómico.

  Aspirar a una economía digital como parte del desarrollo implica la mejoría significativa del nivel educativo de la población, para dominar las nuevas tecnologías y convertirlas en herramientas útiles para su desarrollo personal y laboral, y para que el país disponga de una masa crítica de técnicos y profesionales con formación en las especialidades requeridas para impulsar el desarrollo de los contenidos, servicios y aplicaciones que el nuevo entorno digital demanda. Del mismo modo, sería posible generar una amplia cultura y habilidades digitales en la población que posibiliten el desarrollo de las innovaciones que el sector productivo requiere incorporando las TIC.

  A nivel de la educación inicial, básica y media, además de los desafíos de accesibilidad y equidad, el país tiene el gran reto de mejorar la calidad de la enseñanza y, de manera especial, los niveles de aprendizaje de los estudiantes en matemáticas y ciencias, áreas de conocimiento requeridas para impulsar una economía digital con sentido para el desarrollo nacional.

  El Ministerio de Educación de la República Dominicana (MINERD) ha impulsado diferentes iniciativas TIC que han contribuido a la inclusión digital de estudiantes y docentes del sistema escolar público dominicano como parte de los diferentes Planes de Educación en la última década.

- **Eje estratégico 4: desarrollo productivo e innovación.**
  Las tecnologías de la información y las comunicaciones (TIC) se han convertido en un instrumento imprescindible para los sectores productivos, puesto que contribuyen a la organización, la gestión empresarial, la adopción de innovaciones productivas y el acceso a nuevos mercados, nacionales e internacionales, incidiendo en el crecimiento económico y productivo de los países, ya que viabilizan el desarrollo de sectores económicos de alto valor agregado, generan empleos de calidad y elevan el poder adquisitivo de los ciudadanos.

  Reconociendo la importancia de lo anterior, el Gobierno dominicano ha definido, en el artículo 25 de la Estrategia Nacional de Desarrollo (END) 2030, objetivos y líneas de acción orientadas a fomentar el desarrollo y la innovación de la industria nacional TIC, procurando el progresivo

aumento del valor agregado nacional, e incentivar el uso de TIC como herramienta competitiva en la gestión y operaciones de los sectores público y privado.

Con el objeto de iniciar el proceso de transformación productiva, en el año 2000, el Gobierno dominicano construyó el Parque Cibernético de Santo Domingo y el Instituto Tecnológico de las Américas (ITLA).

En el 2010 se establece el Clúster de Empresas de Desarrollo de Software y la Incubadora de Negocios Tecnológicos (EMPRENDE), auspiciada por el Ministerio de Educación Superior, Ciencia y Tecnología (MESCyT). Ese mismo año surge la Cámara Dominicana de las Tecnologías de la Información y la Comunicación (Cámara TIC-RD) cuya misión es impulsar iniciativas desde el sector privado para el fomento del Sector TIC.

La comunidad de emprendedores Developers Dominicanos, iniciativa del sector privado, en el año 2012 desarrolló acciones destinadas a promover el crecimiento de la Industria de Bienes y Servicios TIC, aunque con un alcance limitado.

Con el apoyo del Sistema de la Integración Centroamericana (SICA), en 2014, se lanzó la Estrategia Nacional de Emprendimiento, que define los lineamientos a seguir para el impulso de esta actividad en el país.

- **Eje estratégico 5: entorno habilitador.**
  Gobernanza de Internet
  Como resultado de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), se adoptó la Agenda de Túnez, en su segunda fase, que estableció la Gobernanza de Internet como parte esencial de la agenda de la Sociedad de la Información a nivel mundial. Se acordó que la gestión de Internet debe ser multilateral, transparente y democrática, con la plena participación de todas las partes interesadas: gobiernos, sector privado, sociedad civil, academia, comunidad técnica y las organizaciones internacionales.

  A fin de lograr lo anterior, a través de la Agenda Digital Dominicana se propone establecer un mecanismo nacional de Gobernanza de Internet con el enfoque de partes interesadas, para abordar las cuestiones fundamentales de política y toma de decisiones sobre los recursos críticos de Internet (nombres de dominio, protocolos, direcciones, seguridad y estabilidad de la red) y los temas relacionados con la neutralidad de la red, derechos humanos en Internet, libertad de expresión, privacidad, delitos informáticos, ciberseguridad, incluyendo un marco regulatorio para estimular el uso eficiente de los servicios de Internet en la República Dominicana.

  Ciberseguridad.
  La República Dominicana, al igual que el resto de los países, está expuesta a los ciberataques que, además de generar elevados gastos, ocasionan la pérdida de confianza de ciudadanas y ciudadanos en los sistemas críticos que son esenciales para el funcionamiento de la sociedad.

  En materia de ciberseguridad, en los últimos años el Estado dominicano ha dado pasos positivos a partir de la creación y promulgación de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología y la subsecuente creación de la Dirección de Investigación de Crímenes de Alta Tecnología (DICAT) de la Policía Nacional.

4.3 Análisis y estudio de tendencias, características y cumplimiento de normas

El análisis y estudio de instrumentos delimita la necesidad de un Espacio Regional interactivo que facilite a través de una agenda en el entorno COMTELCA los temas siguientes:

I. Consolidar un PROTOCOLO interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs, bajo una visión de aprovechamiento de los avances regionales y nacionales.
II. Se detecta que existen BRECHAS de desarrollo en la implementación de TICs vinculadas principalmente en Identificación Balística, dactiloscopia, sistemas de Inteligencia Forense, Identificación y reconocimiento facial, Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV) con facilidad de posicionamiento de eventos, así como de detección de objetos por medios no invasivos (scanners) en puertos y fronteras que supere los rayos x tradicionales.
III. En materia de OBSERVATORIOS no es una práctica la gestión de conocimiento basada en la evidencia bajo la operatividad de "protocolos" definidos y las facilidades de OPEN DATA que facilite la orientación y comprensión de resultados en cada uno de los países y a nivel regional.
IV. Existe un vacío Regional en materia de Centros de respuesta para incidentes informáticos (Computer Incident Response), existen avances en Guatemala, Costa Rica y Panamá, lo que puede facilitar que el resto de países de la región puedan asistirse de estos países, de UIT y COMTELCA para comenzar sus labores para consolidar los CSIRT nacionales.
V. El uso de sistemas de Vigilancia y Monitoreo mediante Brazalete Electrónico, para el seguimiento de los reclusos y dispositivos de control de presencia interna en las cárceles, así como el uso de sistemas de pánico no tienen aplicaciones en la región.
VI. NO se detecta a nivel regional una experiencia integradora que permita el considerar una PLATAFORMA de seguimiento de la "Ruta" de la delincuencia común y organizada, incidente en la administración de Justicia, es decir una plataforma que integre los Sistemas de Justicia, Seguridad, Ministerio Público y observatorios al menos en un país.
VII. NO existen Sistemas de Información para la Gestión Pericial Forense locales nacionales y transnacionales de inteligencia que faciliten obtener "indicios" como los manejados por los cuerpos de Fiscalía online.
VIII. A nivel regional se debe masificar y considerar la experiencia de Panamá y Guatemala para el análisis y estudio de casos de drogas y terrorismo, crimen organizado y crimen cibernético (Análisis y estudio del crimen cibernético - Computer Security Incident Response Team CSIRT)
IX. Considerar la experiencia de Guatemala con la Alerta Alba Keneth en la gestión de personas desaparecidas, así como el desarrollo de APPs (ALERTOS, ESPANTA CACOS, PNC MOVIL) para la Seguridad Ciudadana, como una facilidad de replica para los países de la región.
X. Sistematizar rápidamente la experiencia de Honduras en cuanto a la normalización de bloqueo Celular en Centros Penitenciarios, puede facilitar una incidencia en el nivel regional sobre el tema.
XI. Facilitar el intercambio de experiencias sostenido del 911 de Costa Rica y la práctica innovadora de República Dominicana sobre la atención de emergencias y urgencias, así como de una gestión transparente de sistemas 911 que vincula la educación de los diversos estratos de población.
XII. Estudiar la facilidad de RECOMENDACIONES sobre la integración del sistema Automated Fingerprint Identification System (AFIS), de Identificación y reconocimiento facial y de CCTV con la integración sensorial de audio (ShotSpotter), así como la migración de escaners de rayos x hacia escaners de rayos gamma.
XIII. NO se detecta a nivel regional una gestión de Agendas Digitales con una visión para ser considerada como una hoja de ruta que ofrece una visión clara de los desafíos que enfrentan los países y que incluye la Seguridad Ciudadana con sus retos a nivel regional.

4.4 Tendencia de mejor práctica en la efectividad social

4.4.1 La efectividad de los esfuerzos T4D, de Creative Associates

Esta iniciativa es implementada por Creative Associates International[127] Inc., con recursos de la Agencia Internacional para el Desarrollo de los Estados Unidos (USAID), institución que ha realizado programas similares en Honduras, Guatemala, El Salvador y Panamá, habiendo establecido en este proceso más de 100 Centros de Alcance en toda la región. Se concentra comunidades altamente vulnerables a las violencias, los delitos y los conflictos, realiza sus actividades en asociación con Municipalidades, Patronatos, Instituciones Basadas en la FE y ONGs. Los Centros de Alcance (CDA)[128] son un instrumento clave de prevención de la violencia juvenil implementados mediante una metodología de 8 componentes:

1. Uso Creativo del Tiempo Libre,
2. Capacitación para el Trabajo,
3. Reforzamiento Escolar y Homologación Educativa,
4. Formación en Valores y Virtudes,
5. Voluntariado,
6. Gestión de Oportunidades,
7. Proyecto de Vida, y
8. Microempresa como alternativa para su sostenibilidad.

Estos CDAs cuentan con 15 computadores en un InfoLab, que gradualmente están contando con conectividad de internet y convirtiéndose en una red de información donde se abordan temas vinculados al emprendedurismo, la construcción de Paz y Convivencia y otros temas vinculados a la gestión de la Seguridad Ciudadana en las diferentes comunidades a nivel regional. Los CDAs actualmente son altamente influyentes en territorios críticos e inseguros y permiten gestar información con la escucha activa de las comunidades sobre los problemas de inseguridad. Solo en el caso de Honduras se ha implementado 50 CDAs y ha demandado la capacitación de más de 800 voluntarios causando un alto impacto en zonas vulnerables[129] donde el proceso ha llegado a los ámbitos familiares[130] permitiendo que Jóvenes a punto de unirse a pandillas violentas, en una facilidad de prevención secundaria dirigida a las familias, llega al corazón del problema, ayudando a las familias, a niños, a niñas y jóvenes para alejarlos del centro de la violencia mediante aplicaciones de ICTD4[131]. En El Salvador esta dinámica permitió el lanzamiento de 10 Academias TI Microsoft[132], en 10 de los municipios más violentos del país, 2.000 jóvenes en riesgo obtuvieron las habilidades de tecnología que necesitan para tener éxito, proceso que actualmente se esta comenzando a replicar en Honduras. Las Academias son parte de una asociación del sector privado Salvadoreño llamado "ESTAMOS con vos" ("Estamos con ustedes"). En Panamá 9,795 jóvenes recibieron beneficios, en las Ciudades de Panamá, San Miguelito, Colón, Arraiján, La Chorrera y el Darién. Estos Centros de Alcance están siendo gestionados por grupos comunitarios. Sirven como los únicos centros extraescolares de recursos para los jóvenes entre las edades de 12-29 años. También ofrecen una plataforma para fortalecer las alianzas entre la comunidad, el público y el sector privado para trabajar juntos evitando que los jóvenes participen en el crimen y la violencia, y sirven como un modelo de prevención eficaz del delito en las comunidades donde el centro de sus acciones van alrededor del uso de TICs y actividades de uso positivo para la prevención de violencia.

[127] http://www.creativeassociatesinternational.com/citizen-security/
[128] http://www.alcancepositivo.org/centros-de-alcance-y-el-poder-de-5/
[129] http://www.creativeassociatesinternational.com/feature-story/outreach-centers-hope-in-the-storm-for-honduran-youth/ (ver VIDEO de Medición de Impacto)
[130] http://www.creativeassociatesinternational.com/multimedia/honduras-targeted-prevention-brings-kids-back-from-the-brink/
[131] http://www.creativeassociatesinternational.com/technology-for-development/
[132] http://www.creativeassociatesinternational.com/news/microsoft-academies-to-train-salvadoran-youth-for-tech-careers/

Creative ha sido pionero en estrategias de vanguardia para llegar a las personas con mayor riesgo con la prestación de servicios individualizados y comunitarios de los CDAs, involucrando a las familias y los jóvenes. Estos programas de prevención secundaria han producido resultados medibles en algunas de las comunidades más violentas del triángulo norte de la región Centro Americana y la República de Panamá.

Esta iniciativa forma parte del Proyecto Global T4D [133] (Technology for Development) que facilita la integración de TICs con un enfoque que privilegia en primera instancia la Seguridad Humana, lo cual gradualmente esta vinculando la seguridad ciudadana en los diferentes países a través de la integración gradual de los InfoLab de los diferentes Centros de Alcance. Creative también utiliza teléfonos móviles, televisión y medios de comunicación social para ayudar a las comunidades a aumentar su conocimiento de los procesos de seguridad ciudadana, electorales y de participación de la comunidad. Estas intervenciones han sido especialmente útiles para las mujeres y los jóvenes en países como los de América Central, en África en países como Nigeria, Tanzania, Yemen, y Zambia.

T4D Innovation Lab anima y amplia la experimentación con el uso de TICs que producen resultados, con énfasis en:

- Las tecnologías móviles.
- Sistemas de Instrucción.
- Sistemas tales como la energía solar y Habilitación de comunicación inalámbrica.
- Recolección y mapeo de datos para la Seguridad y Convivencia Ciudadana.

Estas áreas T4D permiten investigar cómo la tecnología puede aprovechar el cambio social positivo ante la inseguridad existente, maximizar la rendición de cuentas, y transformar vidas en y con las comunidades.

Según Michael MacCabe[134], Director de T4D en Creative, el compromiso de los actores comunitarios y voluntarios, y la dificultad de acceso a estos lugares inseguros permite que las iniciativas T4D tengan acogida no solo para la enseñanza, sino también para acciones de Seguridad y Convivencia Ciudadana en las comunidades. Según MacCabe las tendencias de uso las aplicaciones T4D en Centros de Alcance (CDA) establecen mediciones preliminares de participación y usos en 62% de hombres y un 38% en mujeres.

4.4.2 La Iniciativa SparkLab.

Una entrevista con Miguel Raimilla, Director Ejecutivo de Telecentre Foundation (mraimilla@telecentre.org)

SPARKlab es una iniciativa creada y coordinada por la Fundación Telecentre[135] la Generalitat de Cataluña, y la Unión Internacional de Telecomunicaciones (UIT), en estrecha colaboración con un grupo selecto de organizaciones y profesionales desde los mundos público y privado de la academia. Tiene los siguientes objetivos:

- Crear una red global de centros especializados en la innovación, la inclusión digital y de alto impacto socio-económico en empresas de la comunidad;
- Coordinar una plataforma de cooperación internacional que facilite la participación y la cooperación internacional de diferentes comunidades, académicos, organizaciones públicas y privadas;
- Estimular la innovación entre los individuos y las organizaciones comunitarias;
- Desarrollar soluciones TIC de alto valor social y tecnológico añadido para las comunidades, empresas y público y entidades privadas;
- Construir el talento sociales, proyectos y empresas;
- Promover el establecimiento de espacios cívicos de servicios múltiples para el trabajo colaborativo, la discusión, aprendizaje y un mejor uso de las TIC;
- Avanzar y ampliar los productos y servicios a nivel regional y mundial;

[133] http://www.creativeassociatesinternational.com/wp-content/uploads/2014/05/ED_Technology.pdf
[134] Michael MacCabe es director de T4D en Creative Associates International, Email: michaelmc@creativedc.com
[135] http://www.telecentre.org/

- Facilitar el acceso a los intercambios tecnológicos, la cultura y el conocimiento multisectorial a nivel nacional, regional y global
- Facilitar la experimentación y puesta a prueba de conceptos, aplicaciones, servicios y soluciones de TIC a nivel nacional, regional, y el nivel mundial;
- Crear tendencias de las TIC para el desarrollo

En entrevista con Miguel Raimilla, director ejecutivo de Telecentre Foundation, los telecentros, son hoy por hoy una RED con tendencias globales, con alianzas estratégicas con la Comisión de Banda Ancha para el Desarrollo Digital, la Alianza para el acceso a Internet, su inversiones son basadas en ICT4D (Information and Communication Technologies for Development) se centra en aplicar directamente las TICs para la reducción de la pobreza, su uso beneficia a la población desfavorecida y en un sentido indirecto, donde las TIC asisten a organizaciones cooperantes, ONGs, gobiernos o negocios para mejorar las condiciones socioeconómicas.

Según Raimilla, "el ICT4D está proporcionando información, análisis, experiencia y otros recursos especializados que favorecen a las comunidades, para desarrollar y ofrecer recursos pertinentes, servicios y soluciones para apoyar el crecimiento y la sostenibilidad a largo plazo de los telecentros y otros modelos de acceso de computación", es decir los telecentros facilitan la comunicación eficiente y eficaz , colaboración entre el sector privado, las organizaciones internacionales, los innovadores y emprendedores con la comunidad global de telecentros.- En esta entrevista Raimilla considera que siguen siendo un reto recopilar datos pertinentes y fiables sobre el impacto de las iniciativas de TICs, aplicaciones de Internet y APPs móviles en todo el mundo.

El concepto SPARKlab es la evolución del modelo tradicional de una TIC espacio o telecentro público, convertido en un laboratorio de innovación cívica y la inclusión social que facilite la participación local, multisectorial y más su uso avanzado y eficiente de las TICs y los recursos de comunicaciones móviles. El telecentro, donde la comunidad colabora, aprende, experimenta, y trae consigo innovación, empresas, servicios, contenidos y soluciones de una manera dinámica, participativa, y ampliable.

Según Raimilla los telecentros además de ser un espacio de "Coworking", comenta la experiencia de la buena práctica de Panamá, donde el 70% de las personas que asisten son mujeres, rescata que el enfoque de género, es un seguimiento de la Cumbre Empresarial de la Américas 2012, para la Formación y Empleabilidad y rescata la facilidad de atención durante el 2014 de 1 millón 300 mil mujeres a través de la red de Telecentros como un impacto importante.

"Si bien la cultura de formación y empoderamiento cívico, para el emprendimiento y generación de empleo, son los ejes principales, hoy en día los telecentros también se utilizan con enfoque de Seguridad Humana, en una mirada que garantiza acciones de Seguridad Ciudadana. Nos comenta que "no es suficiente la tecnología para lograr coordinarse, sino existe la cohesión social alrededor de las TICs cualquier iniciativa de formación enfocada al desarrollo económico o al seguridad ciudadana será frágil".

SPARKlab facilita la exploración y experimentación participativa sobre los usos alternativos y aplicaciones de las TICs en diferentes contextos y ecosistemas, en este sentido su implementación ha fomentado la:

- Demostración y experimentación de nuevas tecnologías, software, aplicaciones y plataformas para el intercambio de contenidos.
- Demostración y prueba de nuevos métodos para la enseñanza y la formación.
- El desarrollo constante de las clases básicas y avanzadas de las TICs sobre diversos: temas y áreas de desarrollo humano un través de cursos con la participación de socios globales.
- La incubación de talento y empresas de TICs.
- El desarrollo de nuevas soluciones y aplicaciones de las TICs.
- Prestación de servicios especializados para la inclusión digital y TICs para el desarrollo.

4.4.3 Visita Ciudad Bogotá, Colombia

Comisión de Regulación de Comunicaciones (CRC), Colombia.

En entrevista con Hugo Romero de la Comisión de Regulación de Comunicaciones (CRC) con sede en la ciudad de Bogotá, Colombia nos comenta sobre su experiencia en materia de gestión listas "positivas" y "negativas" de celulares a nivel ciudadano, así como también en bloque celular también denominado "Inhibición de tecnología celular" en centros penitenciarios de la República de Colombia.

Esta iniciativa forma parte de la agenda digital de país, "vive digital" y "vive digital 2". - El Plan responde al reto de alcanzar la prosperidad democrática gracias a la apropiación y el uso de la tecnología. **Vive Digital** le apuesta a la masificación de Internet. En una correlación directa entre la penetración de Internet, la apropiación de las Tecnologías de la Información y las Comunicaciones (TICs), la generación de empleo, la reducción de la pobreza y el incremento de la Seguridad Ciudadana. El plan **Vive Digital** conlleva entonces importantes beneficios sociales y económicos, en los que CRC, en Colombia viene implementando una estrategia público-privada para combatir el hurto de celulares, ha participado activamente en materia de regulación, y en dicho proceso evidenciando la necesidad de contar con el apoyo de todos los países de la región para que los equipos hurtados sean bloqueados para su uso en las redes de todos los países y no solo de Colombia, ante el trasiego de terminales robadas hacia otros países.

Desde el 2012 hasta la fecha la CRC ha continuado el seguimiento a la implementación y operatividad de las listas "positivas" y "negativas" de celulares. Como parte de dicho seguimiento se amplió hasta el 1 de marzo de 2013[136] la fecha máxima para que los usuarios propietarios de equipos terminales móviles realizaran el registro de los mismos ante el proveedor con el cual tiene contratado su servicio. Una vez finalizado dicho plazo, los usuarios que hacen uso de equipos terminales no registrados continúan en un monitoreo por parte del operador, a fin de identificar cuándo dicho usuario cambia la SIM del equipo y de esta manera proceder a informarle su obligación de registrar el equipo o de lo contrario proceder al bloqueo del mismo.

La estrategia se basa en tres ejes esenciales que son:

1. Reducir las vulnerabilidades del mercado: con controles en la importación, activación, venta, exportación y generación de acuerdos de cooperación con otros países
2. Atacar la economía criminal: desmantelando estructuras criminales y
3. Concientizar sobre el perjuicio: con campañas masivas de comunicación

CRC también a profundizado en marcos regulatorios para generar:

- Medidas para combatir el hurto, falsificación y mercado gris de dispositivos móviles.
- Medidas con los operadores celulares para definir parámetros de diseño y simulación del bloqueo de celulares en cárceles de Colombia, lo que permite reducir la afectación de los entornos poblacionales adyacentes a los centros penitenciarios en Colombia y centrar el bloqueo en el interior de los centros penitenciarios.

Ministerio de TICs, Bogotá Colombia

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTICs), según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones y a sus beneficios.

[136] https://www.crcom.gov.co/recursos_user/Normatividad/Resoluciones/2013/00004119.pdf

El MinTIC, fomenta actualmente la consolidación del Sistema Integrado de Emergencias y Seguridad (SIES), que es soportado por el Fondo Nacional de Seguridad y Convivencia Ciudadana (FONSECON).- Según decreto 4366 de 2006, el Sistema Integrado de Emergencias y Seguridad (SIES) está conformado por los siguientes subsistemas:

1. **Número Único Nacional de Seguridad y Emergencias (123[137]).**

Subsistema integrado en un número único liderado por las fuerzas de reacción del Estado, para la atención de requerimientos de la ciudadanía en cuanto a eventos de seguridad, convivencia ciudadana, emergencias y desastres. Dicho subsistema debe ser de funcionalidad avanzada, tecnología de punta y escalable, para garantizar la respuesta en el menor tiempo posible.

2. **Sistema de vídeo vigilancia mediante circuitos cerrados de televisión (CCTV).**

Compuesto por cámaras de vídeo ubicadas estratégicamente en los distritos o municipios, las cuales estarán controladas por la Policía Nacional desde un centro de monitoreo, que permite observar y grabar los diferentes escenarios de convivencia ciudadana.

3. **Centros de Información Estratégica Policial (CIEPS).**

Observatorios del delito a nivel departamental y municipal ubicados en los comandos de Policía, los cuales contarán con herramientas tecnológicas para el análisis de las diferentes problemáticas que afectan la convivencia y seguridad ciudadana, generando un espacio de participación de las autoridades político-administrativas, los organismos de seguridad y judiciales del Estado del orden nacional y local.

4. **Alarmas Comunitarias (A-C).**

Es un instrumento de alerta de los Frentes de Seguridad Local organizados por la Policía Nacional (alarmas, pitos, luces, sirenas, reflectores), que se activa frente a una situación anómala, que permite a la comunidad y a las autoridades reaccionar de acuerdo a parámetros que se establezcan.

5. **Sistemas de radio comunicaciones para redes de Cooperantes.**

Son redes de radio comunicaciones en VHF y UHF, que el Ministerio de Defensa, en coordinación con la Fuerza Pública, las Gobernaciones y las Alcaldías, ha instalado en sitios donde no hay ningún tipo de comunicación, para facilitar la transmisión de cualquier situación de emergencia de forma directa entre los Ciudadanos y la Fuerza Pública.

6. **Otros Sistemas de Seguridad, como controles de acceso, localización automática, georreferenciación, monitoreo y bloqueo de vehículos, entre otros.**

Estos 6 elementos que componen en SIES están permitiendo generar intervenciones y respuestas multisectoriales, integrándose en la facilidad de gestión de ciudades inteligentes a nivel de Colombia, lo que está facilitando gradualmente un mayor nivel de organización para la respuesta territorial ante situaciones de emergencias y de seguridad ciudadana.

MinTIC impulsa el El Plan Vive Digital buscando el gran salto tecnológico a través de la masificación del uso Internet con el fin de reducir la pobreza y generar empleo. Para lograrlo el Plan impulsa el ecosistema digital del país conformado por 4 grandes componentes:

- **Infraestructura:** La infraestructura corresponde a los elementos físicos que proveen conectividad digital. Algunos ejemplos son las redes de fibra óptica nacionales, las torres de telefonía celular con sus equipos y antenas, y las redes de pares de cobre, coaxiales o de fibra óptica tendidas a los hogares y negocios.
- **Servicios:** los servicios ofrecidos por los operadores hacen uso de la infraestructura y permiten desarrollar la conectividad digital. Algunos ejemplos de servicios son el servicio de Internet, el servicio de telefonía móvil o el servicio de mensajes de texto (SMS).
- **Aplicaciones:** Las aplicaciones son herramientas informáticas que le permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar

[137] http://www.123bogota.gov.co/

una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores, tabletas o celulares.

- **Usuarios:** Los usuarios hacen uso de las aplicaciones e indirectamente de los servicios e infraestructura para consumir y producir información digital. Los usuarios en este ecosistema somos todos los que usamos Internet, telefonía celular o cualquier otro medio de comunicación digital.

El Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana (CEACSC)

El Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana[138] (CEACSC) de la Secretaría Distrital de Gobierno es la instancia asesora de la Alcaldía Mayor en materia de convivencia y seguridad ciudadana. El CEACSC participa de la formulación, seguimiento, análisis y evaluación de políticas públicas mediante la generación de estudios que comprenden las dinámicas urbanas a través de la caracterización de las conductas incívicas, las conflictividades, violencias y delitos, a través de análisis estadísticos y espaciales, metodologías de investigación social como estudios etnográficos, cartografía social y trabajo de campo, cuenta con un equipo de 8 personas para su gestión.

Los productos del CEACSC son los resultados de las investigaciones realizadas, la producción de información para la toma de decisiones de acciones públicas, la elaboración de informes en materia de balances y monitoreo de muertes violentas, delitos de mayor impacto y conductas que afectan la convivencia, y la elaboración y conceptualización de formulación de políticas públicas.

En su visión provee metodologías innovadoras para sistematizar y transformar la información existente en nuevas mediciones que permiten, gestionar conocimiento para la sociedad basado en la evidencia. Considerando que trabajar con información basada en la evidencia demanda acciones estudio y análisis, que vinculan el proceso básico de la investigación aplicada: observando, estudiando y analizando; su dinámica considera como un mecanismo de estudio y el análisis, el uso de TICs que facilitan acciones públicas para la Seguridad Ciudadana, la Justicia y específicamente sobre buenas prácticas con gobiernos locales y centrales.

El Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana (CEACSC) [139], fue creado en el 2008 mediante Resolución 708 de la Secretaría Distrital de Gobierno. Sus actividades retoman el trabajo realizado desde 1995 a través del Sistema de Información de Violencia y Delincuencia del Observatorio de Cultura Urbana; el cual funcionaba en el entonces Instituto Distrital de Cultura y Turismo y el Sistema Unificado de Información de Violencia y Delincuencia (SUIVD).

Así la determinación de diseño conceptual, variables y aplicativos con visión amplia en este nuevo marco operativo y conceptual del CEACSC (de un observatorio a un centro de estudio y análisis) conlleva conservar sus características generales de estudio y análisis en lo siguiente:

1. Carácter Territorial: zonas críticas, redefiniendo sus características generales en el ámbito de interacción con aliados y la institucionalidad.
2. Los “Datos de Principales problemáticas que atendía anteriormente vinculados a delitos” a “Datos de Principales problemáticas que atenderá, observará, estudiará y podrá analizar en materia de delitos, violencias y conflictividades urbanas”.
3. La “Periodicidad en el tratamiento de información Trimestral, Semestral o anual”, a la “Periodicidad en el tratamiento de información continua”, que permite gestionar conocimiento al CEACSC considerando la información actual e histórica existente, para abordajes de carácter permanentes y socialmente continuos.
4. Estudio y Análisis de estadísticas aplicadas a los territorios, en la gestión del conocimiento para la edición de revistas y reportes científicos indagando bajo criterios de investigación aplicada definidos sobre:

[138] http://www.ceacsc.gov.co/
[139] http://www.ceacsc.gov.co/index.php/quienes-somos/institucionalidad/historia

- Caracterización del Homicidio
- Sistema de Responsabilidad Penal para Adolescentes
- Violencia Familiar y delitos sexuales
- Mediatización de Conflictividades, violencias y delitos
- Caracterización de personas reportadas como desaparecidas en la Ciudad de Bogotá
- Caracterización de conductas contravencionales y querellables
- Caracterización de micro tráfico
- Seguimiento y caracterización de los ataques con agentes químicos
- Seguimiento y caracterización del suicidio
- Seguimiento y caracterización del embarazo en adolescentes
- Seguimiento y caracterización de trata de personas

Esto permite su intervención, mediante el apoyo de líneas base en proyectos como:

- Estrategia de jóvenes en Paz.
- Caracterización de la captura por civil.
- Jóvenes construyen ciudad.
- Caracterización y georeferenciación de la población afro descendiente en 20 localidades de Bogotá.
- Informes sobre la base información del 123.
- Caracterización de delitos en el sistema de Transmilenio.

Los mecanismos de sistematización de los datos se procesan en tablas de análisis estadístico para la producción de información; junto con los análisis de tipo cualitativo recolectados en los instrumentos para tal fin, y con un marco metodológico de investigación definido, se procesan por parte de los investigadores y analistas para la generación de recomendaciones de política pública, mecanismos de evaluación, seguimiento y monitoreo de las ya existentes o la conceptualización, diseño y formulación de nuevas acciones públicas.

Frente a este producto de políticas públicas, el principal desafío es la sostenibilidad institucional de las recomendaciones que se realizan por parte del CEACSCS y que deben ser adoptadas por la Secretaría de Gobierno. Se requiere para superar este aspecto, una mayor inversión en los rubros de investigaciones de temáticas específicas que afectan la convivencia y la seguridad ciudadana en el distrito capital. Se refuerza de nuevo la necesaria articulación entre el CEACSC, la Secretaría de Gobierno y su Subsecretaría de Asuntos para la Convivencia y Seguridad Ciudadana, la Dirección de Seguridad, la Subsecretaria para Asuntos Locales y la Dirección de Derechos Humanos.

Estas acciones han sido la base, para desarrollar bajo la gestión de información y conocimiento basado en la evidencia[140] e investigaciones por objetivos, el Plan Integral de Convivencia y Seguridad Ciudadana (PICSC) [141], lo que facilita una gestión pública de la Seguridad y Convivencia Ciudadana y sus programaciones en los presupuestos del gobierno de la Ciudad de Bogotá.

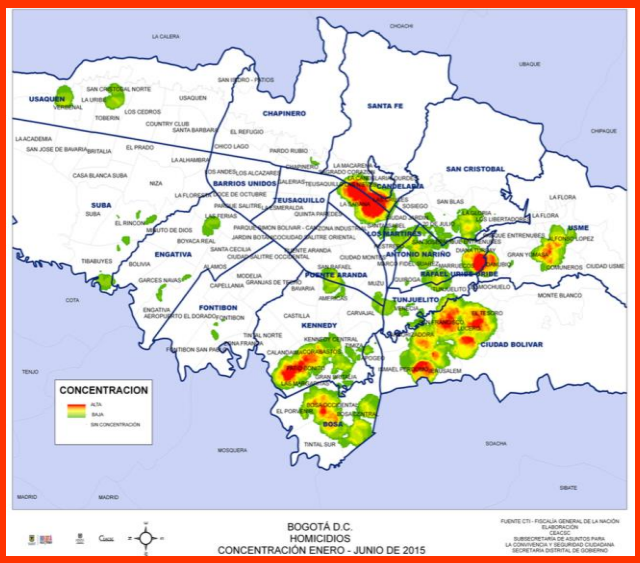
Para el CEACSC su enfoque territorial y de abordaje en campo se encuentra sustentado en metodologías de investigación social como los estudios etnográficos, cartografía social, investigaciones cualitativas, grupos focales, aplicación de encuestas, diarios de campo, bitácoras de registro socio espacial, la metodología de los diálogos dinámicas de ciudad. Los análisis de los diferentes tipos de instrumentos se realizan bajo la concepción de integralidad y multicausalidad propuesta y definida por el Plan Integral de Convivencia y Seguridad Ciudadana (PICSC), Bogotá Humana y Segura 2013 – 2023.

[140] http://www.ceacsc.gov.co/index.php/que-hacemos
[141] http://issuu.com/ceacsc/docs/libro_picsc_bogot___2013_-_2023_opt

El trabajo continuo lleva al CEACSC a presentar en base a la gestión de conocimiento basado en la evidencia, el PLAN INTEGRAL DE CONVIVENCIA Y SEGURIDAD CIUDADANA (PICSC) 2013-2023 "BOGOTÁ HUMANA Y SEGURA[142]" en cumplimiento de las disposiciones legales, abordando las problemáticas de conflictividades, violencias y delitos a partir de un diagnóstico objetivo.

Cada una de las investigaciones que realiza el CEACSC poseen un enfoque diferencial aplicado, puesto que los instrumentos de caracterización socio espacial implementados cuentan con variables demográficas que permiten conocer las realidades sociales de los diferentes grupos poblacionales. Además, el CEACSC posee permanentes líneas de investigación en: Violencia Intra Familiar, Jóvenes en Conflicto con la Ley, Sustancias Psicoactivas con especial énfasis en población drogo dependiente habitante de calle y actualmente apoya técnicamente y metodológicamente a la Dirección de Asuntos Étnicos en la elaboración de la caracterización de la población Afrodescendiente en el Distrito Capital.

Figura 25: Investigaciones por objetivos del CEACSC



Los productos del CEACSC se materializan a la fecha en 27 políticas públicas adoptadas por la Alcaldía de Bogotá como acciones públicas para la reducción de las conflictividades, violencias y delitos, dentro de las que se cuentan: el PICSC, el Plan 75 100 Seguridad Humana, la Estrategia Intersecciones, Estrategia Jóvenes de Paz, la estrategia de articulación público – privada del sistema de video vigilancia de Bogotá, entre otros.

Esto le permite proponer y emprender acciones públicas de convivencia y seguridad ciudadana a corto, mediano y largo plazo. Bajo la pregunta ¿Cómo encarar los desafíos en materia de convivencia y seguridad ciudadana en una megaciudad como Bogotá D.C. con una población de 7.674.366 habitantes en 2013, con proyección para el 2020 de 8.380.801 habitantes?

Conociendo que no existen ciudades de "riesgo cero" en conflictividades, violencias y delitos; sin embargo, desde un enfoque integral de la Seguridad Humana y la Seguridad Ciudadana, resulta imprescindible conocer los factores multicausales de las violencias, los delitos y las conflictividades, el grado de identidad de la sociedad con la ciudad, el nivel de confianza en la administración pública, la cohesión social fundamentada en la solidaridad y no en el miedo, así como los contextos globales, locales y microterritoriales para avanzar eficiente y eficazmente en la reducción de los riegos de los ciudadanos(as) de ser víctimas de violencias y delitos. Los retos que se tienen en materia de (in)seguridad lleva al CEACSC a profundizar en otras formas de pensar y actuar mediante la formulación de nuevos paradigmas.

La información producida junto con las investigaciones realizadas se articula y tiene como usuarios estratégicos al Alcalde Mayor de Bogotá, al despacho de la Secretaria de Gobierno, insumo en los Consejos de Seguridad y Gobierno; y a las diferentes dependencias y secretarías que solicitan información detallada y particular que abarca las temáticas de conflictividades, violencias y delitos. AFTER

[142]http://www.gobiernobogota.gov.co/images/stories/Servicios/observatorios/PICSC_BOGOTA_2013_2023_CON_MODIFICACIONES.pdf

Definiendo los principales ejes del PICSC al 2023 sobre lo siguiente:

La información que se recopila estadísticamente es dinámica y depende su actualización de las entidades productoras de la misma.

Los mecanismos de sistematización de los datos se procesan en tablas de análisis estadístico para la producción de información; junto con los análisis de tipo cualitativo recolectados en los instrumentos para tal fin, y con un marco metodológico de investigación definido, se procesan por parte de los investigadores y analistas para la generación de recomendaciones de política pública, mecanismos de evaluación, seguimiento y monitoreo de las ya existentes o la conceptualización, diseño y formulación de nuevas acciones públicas.

Figura 26: **Ejes principales del PICSC al 2023**

Fuente: *Plan Integral de Convivencia y Seguridad Ciudadana (PICSC)*

El Centro de Estudio y Análisis en Convivencia y Seguridad Ciudadana (CEACSC) ha acumulado un conocimiento calificado, permitiendo definir y evaluar políticas públicas fundamentadas en la objetividad y bajo la gestión de evidencias. A nivel nacional e internacional este "Centro de Pensamiento" tiene un reconocimiento positivo, prueba de ello son las constantes visitas y solicitudes de apoyo en materia de convivencia y seguridad ciudadana a nivel continental.

Cada una de las investigaciones que realiza el CEACSC poseen un enfoque diferencial aplicado, puesto que los instrumentos de caracterización socio espacial implementados cuentan con variables demográficas que permiten conocer las realidades sociales de los diferentes grupos poblacionales. Además, el CEACSC posee permanentes líneas de investigación en: Violencia Intra Familiar, Jóvenes en Conflicto con la Ley, Sustancias Psicoactivas con especial énfasis en población drogodependiente habitante de calle y actualmente apoya técnicamente y metodológicamente a la Dirección de Asuntos Étnicos en la elaboración de la caracterización de la población Afrodescendiente en el Distrito Capital.

Sistema de Reconocimiento Facial Transmilenio

El Sistema TransMilenio también tiene un costo de 12.500 millones de pesos colombianos, alrededor de 4.25 millones de dólares americanos cuenta con un Centro de Control de la Operación que permite supervisar forma permanente la operación y cada uno de los buses de los buses troncales del Sistema. Esto hace posible controlar la velocidad, la frecuencia, los horarios y las rutas de los vehículos, y lo más importante, permite una prestación adecuada del servicio en cada uno de sus recorridos. Para el funcionamiento del Sistema, cada vehículo de los servicios troncales está equipado con tres elementos:

1. Un equipo de GPS (Sistema de Posicionamiento Global, por sus siglas en inglés) que reporta la ubicación del bus.
2. Un computador de abordo (CIBOR) en el bus que permite intercambiar información operativa entre el Centro de Control y el bus y generar toda la información operativa y el cumplimiento por parte de cada uno de ellos.
3. Un Sistema de comunicaciones (TETRA, Terrestrial Trunked Radio) por medio del cual se envía y recibe información entre el Centro de Control, Buses y con el personal de inspección y control de la operación.

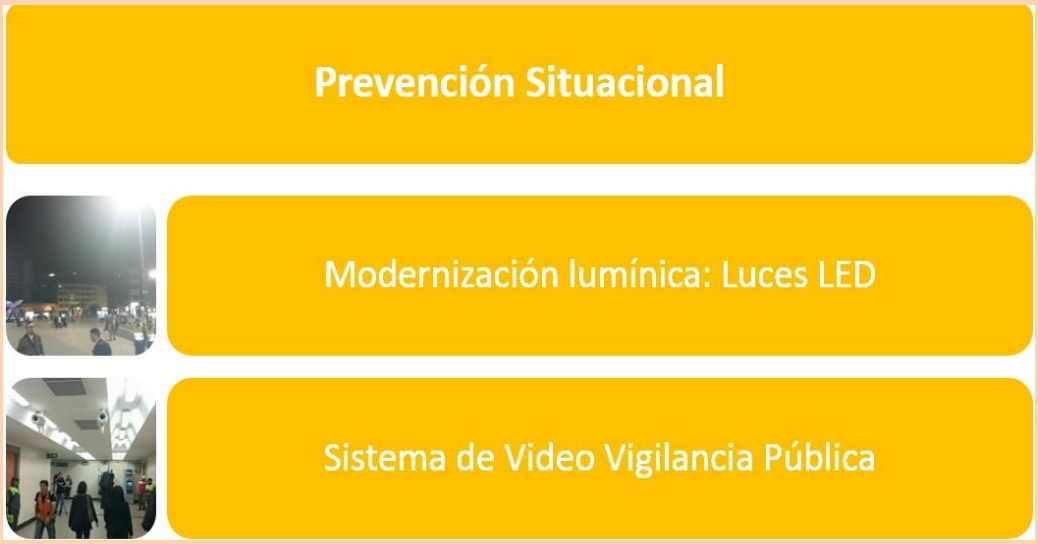
Este monitoreo constituye la base del Sistema de control de la operación, así como el fundamento de toda la estadística en cuanto al cumplimiento por parte de las empresas operadoras Troncales. TRANSMILENIO S. A. cuenta con un circuito cerrado de televisión provisto de 300 cámaras (269 fijas y 31 móviles), interconectadas al Centro de Control. Conexión de cámaras de Seguridad con el CAD. Con el propósito de mejorar los índices de seguridad en el Sistema y disminuir el tiempo de respuesta a las necesidades y expectativas de la ciudadanía, el Sistema TransMilenio cuenta con 226 cámaras del circuito cerrado de televisión, operadas y monitoreadas constantemente por el Centro Automático de Despacho (CAD) de la Policía, y el centro de operaciones de TransMilenio.

Mediante la implementación de este Sistema de monitoreo, la Policía Metropolitana y la incorporación del sistema de Reconocimiento Facial el centro de operaciones mantiene un control directo y permanente sobre las estaciones y portales del Sistema TransMilenio las 24 horas; el sistema de reconocimiento facial permite identificar principalmente a quienes protagonizan los actos de inseguridad y acoso dentro del sistema.

El sistema Face First[143], empleado con éxito en Inglaterra, esta siendo implementado en principio en las estaciones más concurridas, como Jiménez, Ricaurte y Héroes, y en varios articulados en la ciudad de Bogotá

Este sistema de Reconocimiento Facial forma parte del PLAN INTEGRAL DE CONVIVENCIA Y SEGURIDAD CIUDADANA (PICSC) 2013-2023 “BOGOTÁ HUMANA Y SEGURA, en su eje de prevención Situacional, alrededor del eje de sistema de Video Vigilancia Pública

Figura 27: **Sistema Face First**



Fuente: *Plan Integral de Convivencia y Seguridad Ciudadana (PICSC)*

En Inglaterra, donde ya está siendo empleado con éxito, el sistema Face First revolucionó la forma de buscar delincuentes en sitios de alta aglomeración de público como estaciones de transporte masivo de buses y trenes, y es considerado el más efectivo hasta ahora. Se trata de cámaras que reconocen al instante los rostros de multitud de personas que pasan simultáneamente sobre el campo de visión del lente. Esos rostros posteriormente son identificados a través de un banco de datos previamente recopilado por los mismos equipos y que estará en poder de la Policía.

[143] http://www.facefirst.com/

El sistema permite millones de comparaciones de rostros en cuestión de segundos, en la medida en que están siendo captados en vivo. El software localiza la posición y el tamaño de la cara, el centro de los ojos y así la imagen facial es alineada, logrando que la imagen sea llevada al banco de datos.

Ventajas del sistema

1. Brinda a los agentes de la ley una forma de aumentar su identificación y aprehensión de los delincuentes conocidos y otras personas de interés.
2. Logra la velocidad y precisión nunca antes disponibles a los oficiales en el campo.
3. Elimina la necesidad de llevar a los sospechosos a la estación para su identificación.
4. Pone fin a la posibilidad de que los delincuentes buscados están usando una identificación falsa.
5. Aumenta las detenciones y la capacidad de identificar y detener a los terroristas y otros individuos.
6. Supera las dificultades y el tiempo involucrados en el logro de una identificación precisa con las huellas dactilares.

Cómo funciona.

- En primer lugar, las fotos y los datos de delincuentes y personas de interés locales, regionales, nacionales e incluso internacionales existentes se cargan en la base de datos FaceFirst.
- Cuando un oficial detiene a alguien por una infracción de tráfico u otra violación, los oficiales pueden utilizar una aplicación en su teléfono inteligente para escanear la cara de la persona y, en segundo, aprender si esa persona es un individuo buscado.
- Este registro exacto de cada delincuente, puede ser transmitido a tabletas, computadores portátiles y teléfonos inteligentes que llevan a la mano los agentes ubicados en las estaciones y articulados.

El sistema Face First permite, además, enviar alertas a otros sitios a donde el señalado delincuente podria a asistir, por ejemplo, estadios de futbol y terminales de transporte; lugares que podrían ser objetivos de sus ataques o incursiones.

El Gobierno de la Bogotá Humana, por intermedio del Fondo de Vigilancia y Seguridad, con el apoyo de Transmilenio, implementó este moderno e innovador Sistema Integrado de Video Vigilancia Inteligente, pionero en el Transporte Público de Latinoamérica, con el fin de brindarle más seguridad a los ciudadanos que a diario usan Transmilenio. El Sistema Integrado de Video Vigilancia Inteligente para Transmilenio (SIVIT[144]) es una solución de alta tecnología en seguridad, que integra cámaras fijas y móviles, servidores y un desarrollo informático de avanzada, provisto de motores biométricos brindando resultados para el reconocimiento facial de personas con requerimientos judiciales y alertar a las autoridades para facilitar su control y captura, la implementación del sistema de reconocimiento facial se realiza a partir de marzo del año 2015.

4.4.4 Visita en Ciudad Panamá, Panamá

Visita a Autoridad Nacional de los Servicios Públicos ASEP

La Autoridad Nacional de los Servicios Públicos (ASEP) es un organismo autónomo, dirigido y administrado por una Junta Directiva, compuesta por tres Directores, que se encargan del control y fiscalización de los servicios públicos de Telecomunicaciones, Electricidad, Agua Potable y Alcantarillados Sanitarios, y los Servicios de Radio y Televisión.

[144] https://www.youtube.com/watch?v=bmBPpokifLc

Las Telecomunicaciones en la República de Panamá constituyen un servicio público, y como tal, se encuentran reguladas por la Ley No. 31 de 8 de febrero de 1996, la cual tiene el objetivo fundamental de acelerar la modernización y el desarrollo del sector, promover la inversión privada en el mercado, extender su acceso, mejorar la calidad de servicios provistos, promover tarifas bajas al usuario y la competencia leal, en la provisión de los servicios de telecomunicaciones.

Las telecomunicaciones incluyen toda transmisión, emisión o recepción de los signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por medio de líneas físicas, emisiones radioeléctricas, medios ópticos o por cualquier otro sistema o medio de transmisión existente o que exista en el futuro. De manera similar los servicios públicos de Radio y Televisión se encuentran regulados por la Ley No. 24 de 30 de junio de 1999, la cual establece el fundamento legal y técnico para la operación de estos servicios y adicionalmente señala las funciones que tendrá la Autoridad Nacional de los Servicios Públicos (ASEP) como organismo regulador en esta materia. Esta Autoridad, a través de la Dirección Nacional de Telecomunicaciones, tiene la finalidad de regular, ordenar, fiscalizar y reglamentar eficazmente, entre otros, la operación y administración de los servicios de telecomunicaciones, los de radio y televisión, así como el espectro radioeléctrico; y se manifiesta a través de las resoluciones que dicta de conformidad a las disposiciones legales que regulan la materia.

La Autoridad Nacional para la Innovación Gubernamental (AIG) en cooperación con la Autoridad de los Servicios Públicos (ASEP), realiza con éxito intervenciones de nuevas tecnologías de punta, para ir cerrando la brecha digital a través del uso de las Tecnologías de la Información y Comunicaciones (TICs) en Panamá en diferentes campos, a través del Fondo de Servicio Universal, lo que puede permitir a instituciones de Panamá coordinar con ASEP y AIG facilidades para el uso de TICs en aplicaciones para la seguridad y convivencia ciudadana , el fortalecimiento institucional y acciones de previsión y prevención de violencias, delitos y conflictividades.

Observatorio de Seguridad Ciudadana (OSC) de la Cámara de Comercio, Industrias y Agricultura de Panamá[145] (CCIAP)

El Observatorio de Seguridad Ciudadana está bajo la supervisión y coordinación de la Dirección de Asuntos Jurídicos, Cabildeo y Seguridad Ciudadana. Es una iniciativa, que desde el sector privado, busca aportar a la solución de la (in) Seguridad Ciudadana a través de la gestión del conocimiento de una manera integral.

Se define como un espacio de articulación intersectorial e interdisciplinario donde se recopilan datos e información que puede orientar el análisis y estudio de información necesaria, relevante, confiable y oportuna sobre los diferentes tipos de violencia, lesiones, delitos y toda aquella dinámica social negativa que afecte la seguridad ciudadana; permitiendo de forma continua la definición de indicadores, políticas, intervenciones y procesos.

Primeros pasos del Observatorio[146]

El observatorio comienza (i) consolidando el equipo de trabajo inmediatamente (ii) generando las condiciones para la recolección de la información afrontando los obstáculos institucionales y la falta de datos , (iii) Comienza la realización del Informe Histórico 2005-2009 (iv) El diseño e implementación de la primera encuesta en Panamá sobre la que no hay antecedentes comparativos nacionales de este tipo (v) Logra consolidar en los primeros seis meses del 2010 la Mesa de Dialogo Estadístico como espacio de reflexión y debate sobre las tendencias y los avances del Observatorio.

Continuando su acelerada intervención en los temas vinculantes a la Seguridad y Ciudadana se generan los primeros resultados de estudio e históricos por parte del observatorio. Mediante una acción

[145] http://www.cciap.net/
[146] http://www.seguridadcciap.com/wordpress/

complementaria el OSC lanza el segundo informe de Victimización y Percepción de la Seguridad Ciudadana en octubre del 2011 bajo una:

- Investigación cuantitativa con alto rigor científico con una muestra a nivel nacional (excluyendo las comarcas Indígenas) de 3,001 cuestionarios aplicados, a razón de 1 entrevista por hogar (cara a cara, agosto a diciembre de 2010).
- Como marco de referencia para la distribución esperada de la muestra según sexo, edad, nivel socioeconómico, provincia y zona (urbano/rural), se utilizaron las estimaciones de población a julio del 2010 de la Contraloría General de la República.
- El informe también presenta algunos registros proporcionados por el Sistema Nacional Integrado de Estadística Criminales/SIEC, la Policía Nacional y la Dirección de Investigación Criminal /DIJ

En un esfuerzo conjunto de la Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP) , el liderazgo del Programa de las Naciones Unidas para el Desarrollo (PNUD-PANAMA) y el Apoyo técnico el Programa Conjunto "Ventana Temática Prevención de Conflictos y Construcción de Paz", bajo el auspicio del Fondo para el Logro de los Objetivos de Desarrollo del Milenio ONU-España. Se formalizan los apoyos con el Programa para la Naciones Unidas (PNUD), el 25 de abril 2009 según memorándum de entendimiento entre PNUD y la CCIAP y avalado por Peter Ghotmann director de País de PNUD y Adolfo Linares Presidente de la CCIAP en ese entonces, memorando que cuenta con una vigencia inicial hasta el 24 de Abril del 2014 (vigencia de 5 años a partir de su firma) y que establece un marco global de actuación conjunta entre PNUD y la CCIAP.

El Observatorio cuenta con las siguientes alianzas estratégicas:

- Ministerio de Seguridad Pública
- Procuraduría General de la Nación
- Instituto de Medicina Legal y Ciencias Forenses
- Universidad de Panamá
- Policía Nacional
- Diarios La Estrella de Panamá y El Siglo

Dichas alianzas, han permitido que la operatividad del Observatorio se haya desarrollado con altos niveles de sostenibilidad, hacia una gestión de conocimiento continua y objetiva. Brindando herramientas accesibles para la toma de decisión con base a conocimiento y evidencias que permiten una mejora en las condiciones de la Seguridad Ciudadana en el País.

El observatorio cuenta con grupo de notables que componen el *Consejo Asesor de Seguridad y que son parte de los accionares de estudios y análisis*, para sus principales acciones, su interacción y papel como medio nacional incidente en la Seguridad Ciudadana de Panamá.

Se resaltan las caracterizaciones realizadas por el personal del Observatorio, pero también se resalta que a raíz de la demanda de información confiable, el observatorio implementa un instrumento de encuesta , que hoy en día permite el conocimiento de los factores de riesgo para determinar factores protectores que tiene que prevenir y potenciar Panamá respectivamente, así como los comportamientos que influyen en la Seguridad , Convivencia y facilidades de previsión y prevención de violencias, delitos y conflictividades para los ciudadanos en el país.

Innovación y Desarrollo (I+D) para la gestión de conocimiento en la Seguridad Ciudadana, el observatorio ha realizado procesos Investigaciones aplicadas en las que se resalta la:

- **Innovación radical**: con caracterizaciones a nivel local de las zonas criticas *o inseguras* ya conocidas, sus consecuentes recomendaciones de mejora y abordajes, así como el análisis y estudio de toda la información vinculada a los delitos, las violencias y los conflictos.
- **Innovación incremental**: sobre la mejora en la *presentación visual de las encuestas y su tratamiento posterior al tiempo de publicación de forma desagregada y programada* valiéndose del apoyo de empresas privadas encuestadoras.
- **Innovación abierta:** escritos de profesionales sobre la formalidad de reconocimiento de la opinión y la participación por ejemplo en la revista electrónica CONVIVIR.
- **Innovación en gestión**: con la integración del Consejo Asesor de Seguridad Ciudadana constituido por personas notables del país, quedando pendiente subsanar la brecha de la participación en los procesos de los niveles locales al menos en carácter de invitados.
- **Desarrollo**: de instrumentos científicos electrónicos como ser encuestas de precepción de la Victimización (delitos), Vulnerabilidad (Violencias) y Convivencia (Conflictos), y sus correspondientes facilidades de salida de Cultura Ciudadana, Espacios Públicos, y abordajes de institucionalidad caracterizan los abordajes nacionales que ejecuta el observatorio de la CCIAP.

Este accionar de innovación y desarrollo (I+D) le permite contar con nuevos elementos, que introducidos de forma institucional en la CCIAP con la intención de beneficiarla totalmente, una parte de ella y a la sociedad Panameña en su conjunto, hoy por hoy se constituyen en un contrapeso social en el abordaje de la seguridad ciudadana.

Espacios técnicos sobre temas relacionados a la Seguridad Ciudadana (desayunos temáticos[147])

Nacen en el marco y como producto del Observatorio de Seguridad Ciudadana de la Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP) en el marco del Programa Conjunto Ventana de Paz como espacio para la promoción del dialogo destinados al intercambio entre actores relacionado con temas sobre seguridad ciudadana.

El Observatorio de Seguridad Ciudadana organizo y ha coordinado alrededor de 14 “Desayunos Temáticos” desde el 2010 a la fecha, donde se exponen temas enfocados en la seguridad ciudadana y los derechos humanos. Se invita a especialistas nacionales e internacionales en temas que promueven un espacio de intercambio, reflexión y conocimiento con el objeto de mejorar los niveles de desarrollo humano en la sociedad panameña.

Entre los temas que se han presentado en la Cámara de Comercio se pueden mencionar: “Derechos Humanos y Seguridad Ciudadana”, “Crimen Organizado: Trata de Personas”, “¿Cómo se mide la Seguridad Ciudadana?”, “Medios de Comunicación y Seguridad Ciudadana”, “Niños, Niñas y Adolescentes: Seguridad Ciudadana y Derechos Humanos”, “Prevención de la violencia juvenil”, entre otros.

Entre los beneficiarios, se encuentran las instituciones públicas, la policía nacional, gobiernos locales y/o municipales, sociedad civil, miembros de la Cámara de Comercio, Industria y Agricultura de Panamá, entre otros. La convocatoria se hace de manera amplia sin exclusiones con ello se construye espacios legítimos de dialogo que permiten la transmisión de parámetros mínimos en el tratamiento de la seguridad ciudadana a nivel nacional.

Entre sus resultados, se resalta una amplia participación de los diferentes miembros de las instituciones, transmisión de conocimiento en temas de seguridad, por ejemplo la “relación de los medios de comunicación con la seguridad ciudadana”, y como incide el trabajo de medios en la construcción de la percepción ciudadana.

[147] http://www.seguridadcciap.com/wordpress/category/noticias/

Democratización conceptual y estadísticas de la Seguridad Ciudadana (informes, revistas, boletines del OS de la CCIAP)

Es así que los principales hallazgo del primer informe dan cuenta de las deficiencia en materia conceptual y de registro de la información que es manejada por las instituciones de seguridad y que sirven de sustenta en algunos casos para la toma de decisiones. Con recomendaciones puntuales, se da paso a la puesta en práctica de acciones como la mesa de diálogo estadístico, así como reuniones consultivas con las principales instituciones de seguridad (Policía Nacional).

Existiendo vínculos con las instituciones de Seguridad, el OSC gestiona la Primera Encuesta de Victimización y Percepción Social de la Seguridad Ciudadana en Panamá. Ello, constituye el segundo informe del Observatorio de Seguridad Ciudadana, denominado "Victimización y Percepción Social de la Seguridad Ciudadana en Panamá".

Aunado a ello, avanzar en un posicionamiento en la sociedad en su conjunto a través de la implementación de una campaña de prevención con sustento en los hallazgos de la Primera Encuesta de Victimización y Percepción Social de la Seguridad.

En Octubre del 2012 se lanza el **tercer informe** de

Seguridad Ciudadana, denominado: **Democratizando las Cifras sobre Seguridad Ciudadana en Panamá**.

El Observatorio desarrolla su **Segunda Encuesta de Victimización y Percepción Social de la Seguridad;** ello representa el Cuarto informe que publica esta instancia. La misma, al igual que la anterior tiene alcance nacional y representatividad étnica al incluirse por primera vez en un estudio sobre víctimas del delito a las Comarcas Indígenas.

Figura 28: Acciones de Sensibilización del Observatorio de Seguridad Ciudadana de la CCIAP, Panamá.

Adicional, ha generado la primera **revista o cuaderno especializado** en Seguridad Ciudadana denominada **Convivir**; la misma se puede denominar como un espacio democrático que apuesta a la participación sin exclusiones temáticas de plasmar de una manera profesional los pareceres frente a las diferentes dimensiones o particularidades de la seguridad ciudadana.

También produce de manera frecuente **boletines temáticos publicados** en el Portal del Observatorio, el mismo se denomina el **Observador**[148], aborda de manera puntual temas que resultaría complejo y extenso en abordarse; es decir una apuesta por cifras y textos explicativos cortos. El 2015, su último producto es el **V Informe sobre Seguridad Ciudadana, desde una perspectiva de médico legal** con análisis y estudio de datos 2012-2013. El VI Informe sobre Seguridad Ciudadana sobre Seguridad Ciudadana fue presentados el 09 de septiembre del 2015[149].

El observatorio cuenta con un equipo de tres técnicos y un presupuesto anual de 150 mil dólares americanos.

[148] http://www.seguridadcciap.com/wordpress/el-observador-edicion-5/
[149] http://www.seguridadcciap.com/wordpress/el-observatorio-de-seguridad-ciudadana-de-la-cciap-e-ipsos-panama-presentan-los-resultados-del-sexto-informe-de-seguridad-ciudadana/

Sistema de Información de Estadísticas Criminales (SIEC)

Con el fin de conocer la situación objetiva de la delincuencia en la República de Panamá, en el año 2007 se crea la Dirección del Sistema Nacional Integrado de Estadística Criminal *DNSIEC*, que sustituye en sus funciones a la CONADEC.

La misión y funciones de esta Dirección, dependiente del Ministerio de Seguridad Pública, son: *"[…] diseñar, normar, recolectar, procesar, analizar, investigar y realizar estudios con base en la información delictiva del país recabada por instituciones involucradas […]*" (sic. DECRETO 471 del año 2007).

La norma involucra en la obligación de informar, a la DNSIEC, los incidentes criminales o faltas administrativas registrados por los organismos del estado encargados de la prevención, procesamiento judicial y cumplimiento de penas.

Para el adecuado desempeño de su rol de administrador, la DNSIEC, diseñó e implementó un nuevo sistema informático denominado *SIEC*. Esta aplicación, que funciona *"on line"*, recibe el flujo de información de los organismos obligados, procesa los datos, genera mapas que geo-referencian los ilícitos y elabora estudios estadísticos.

Además, por ser un sistema de información dinámico, ofrece a los organismos participantes, la posibilidad de contar con una fuente alternativa para el monitoreo constante de los casos registrados, protegiendo la información aportada mediante la implementación de estrictos protocolos de acceso.

El Sistema Integrado de Estadísticas Criminales (SIEC) es una herramienta que ofrece a las entidades gubernamentales y a los usuarios autorizados, información de actualidad sobre el crimen y la violencia ciudadana en Panamá.

Esta herramienta permite recoger, procesar, ordenar e informar a todas las instancias del gobierno con responsabilidad en el área de seguridad ciudadana, con el fin de contribuir a la reducción de los problemas de inseguridad, mediante el uso de datos, estadísticas y mapas que indiquen las características y magnitud de los hechos delictivos que ocurren en el país.

De este modo, el Sistema Integrado de Estadísticas Criminales (SIEC) se orienta a satisfacer dos necesidades complementarias, aunque diferenciadas (IFPC 2009):

1. Contar con un sistema dinámico que permita el seguimiento de los casos criminales desde el momento en que se produce una falta o delito hasta las diferentes instancias en las que se practican intervenciones por parte de Estado a partir de la comisión de esa falta o delito.
2. Contar con un sistema de estadísticas que permita una visión global del problema de la seguridad. Estas necesidades se complementan con un Subsistema de Información Geográfica (SIG), como componente central del SIEC, cuyo objetivo es la georreferenciación de los hechos delictivos y la producción de mapas de violencia que, al evidenciar la dimensión espacial, permiten el análisis de la situación de la violencia y contribuyen a la definición de políticas y programas de seguridad integral para la prevención y reducción de los hechos delictivos.

El Sistema Integrado de Estadísticas Criminales centra la información que producen todas aquellas áreas del Estado con competencia en la prevención, procesamiento judicial y condena de las faltas administrativas que establezca la normativa vigente y los delitos tipificados en el Código Penal.

Así, el sistema debe capturar información en cuatro niveles:

1. Primer Nivel: Ocurrencia de falta y delitos;
2. Segundo Nivel: Desarrollo de Procesos de Instrucción;
3. Tercer Nivel: Desarrollo de Procesos Judiciales; y
4. Cuarto Nivel: Desarrollo de Procesos de Cumplimiento de Penas.

Figura 29: Esquema del Sistema Integrado de Estadísticas Criminales

Fuente: *Sistema Integrado de Estadísticas Criminales*

Los usuarios clave del sistema, con competencia en la producción de información en los cuatro niveles previamente mencionados, son la Dirección del Sistema Integrado de Estadística Criminal (SIEC), la Policía Nacional, la Policía Técnica Judicial, el Ministerio Público, el Órgano Judicial y el Servicio Penitenciario.

Esta herramienta, facilita la toma de decisiones a las instancias responsables de la seguridad ciudadana ya que posibilita el conocimiento de los problemas en tiempo real. El uso de datos, estadísticas e información geo-referenciada (mapas: incluyendo el mapa del delito) que indican con veracidad las características y magnitud de los hechos delictivos en el territorio nacional, es un factor fundamental a la hora de determinar la adopción de políticas y/o medidas de acción adecuadas que permitan reducir la inseguridad, real y percibida.

El SIEC centraliza información criminal producida por áreas del Estado con competencia en la prevención, detección, procesamiento judicial y condena de faltas administrativas y delitos tipificados, con el objetivo de proveer información estadística y estratégica para la toma de decisiones.

Los objetivos generales de la Dirección del Sistema Nacional Integrado de Estadísticas Criminales (SIEC) son: diseñar, normar, recolectar, procesar, analizar, investigar y realizar estudios con base en la información delictiva del país recabadas por las siguientes instituciones:

1. Autoridades de Policía: a) Presidente de la República; b) Gobernadores; c) Alcaldes; d) Corregidores y e) Jueces Nocturnos.
2. Fuerza Pública: a) Policía Nacional; b) Servicio Marítimo Nacional y c) Servicio Aéreo Nacional[150].
3. Ministerio Público: a) Fiscalías; b) Personerías y c) Policía Técnica Judicial[151]
4. Órgano Judicial: a) Corte Suprema de Justicia; b) Tribunales Superiores; c) Juzgados de Circuito y d) Juzgados Municipales.
5. Otros Organismos de Investigación Científica o Criminal.

El sistema cumple con el objetivo de delimitar y precisar el registro y la transmisión de información en cada una de las entidades, el equipo de trabajo del SIEC es de 9 personas y cuenta con un presupuesto de apoyo de fondos estatales y el apoyo del BID para la Creación del Instituto de Estadísticas e Investigaciones Estratégicas de Seguridad y Convivencia Ciudadana (IEIESC), ampliación del SIEC y fortalecimiento del

[150] El Servicio Marítimo Nacional y El Servicio Aéreo Nacional, se unifican mediante el Decreto Ley 7 del 2008 y se crea el Servicio Nacional Aeronaval.

[151] La Policía Técnica Judicial, se convierte en la Dirección de Investigaciones Judiciales, por Decreto Ley 69 del 2007.

Observatorio de la Violencia (OV) con 8.962 millones de dólares de Programa PROSI-BID y de la Unión Europea de 6.874 millones de Euros a través de la ampliación del Programa de Seguridad Integral de Panamá – APROSI.

4.5 Análisis de innovación tecnológica México, América Central y República Dominicana

4.5.1 El Caso de México

El 10 de junio de 2013, en México se aprueba el Decreto de Reforma a la Constitución Política de los Estados Unidos Mexicanos en Materia de Telecomunicaciones y Competencia Económica que considera:

i. La Transformación Gubernamental
ii. La Economía Digital
iii. La Educación de Calidad
iv. La Salud Universal y Efectiva
v. La Seguridad Ciudadana y un apartado sobre
vi. Los Habilitadores con contenidos de: Conectividad, Inclusión de Habilidades Digitales, Interoperabilidad, Marco Jurídico, Datos Abiertos.

El principal objetivo de la Reforma en materia de Telecomunicaciones, consistió en realizar diferentes cambios impulsados por los poderes Ejecutivo y Legislativo para establecer los fundamentos constitucionales y legales para crear una nueva arquitectura jurídica, institucional, regulatoria y de competencia en el sector de las telecomunicaciones y de la radiodifusión. Fundamentos basados en principios de efectividad, certidumbre jurídica, promoción de la competencia, regulación eficiente, inclusión social digital, independencia, transparencia y rendición de cuentas.

La reforma tuvo como propósito principal beneficiar a todos los mexicanos, por eso consideró dentro de sus principales objetivos, el permitir el acceso de la población a las tecnologías de la información y la comunicación (TICs), incluida la banda ancha, así como establecer condiciones de competencia y libre concurrencia en los servicios de telecomunicaciones y radiodifusión. Para que de esta forma, un mayor número de usuarios accediera a dichos servicios en mejores términos de calidad y precio.

La iniciativa recoge primordialmente las aspiraciones de los usuarios de los servicios de telecomunicaciones y radiodifusión. En ese sentido, una de las principales razones que sustentaron la iniciativa fue la de lograr la reducción de los costos de los servicios de telecomunicaciones para la sociedad mexicana, contar con más ofertas y buscar que los servicios se tradujeran en un beneficio concreto para toda la población.

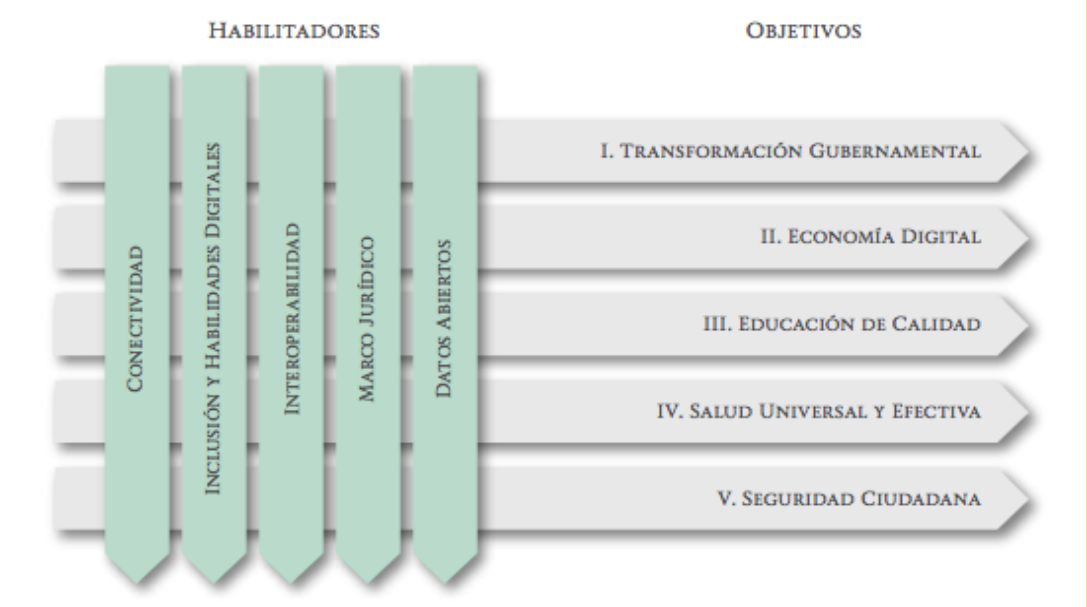
Según el presidente Enrique Peña Nieto “Gracias a esta Reforma, que fomenta la competencia y la inversión en el sector, habrá mayor disponibilidad y calidad en los servicios de telecomunicaciones, a menor costo. Además, establece que el Estado tiene la obligación de garantizar a los mexicanos el derecho de acceso a las Tecnologías de la Información y Comunicación (TIC).”. - Con esta reforma se busca democratizar el acceso a instrumentos como Internet y Banda Ancha, para aprovechar al máximo el sin fín de posibilidades que ofrecen.

El 14 de junio de 2014, se publicó en el Diario Oficial de la Federación la Ley Federal de Telecomunicaciones y Radiodifusión, que tiene por objeto regular, entre otros, el uso, aprovechamiento y explotación del espectro radioeléctrico el espacio que se utiliza para brindar los servicios de telecomunicaciones y radiodifusión, las redes públicas de telecomunicaciones, la prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión, la telefonía fija y móvil, los servicios y contenidos de televisión restringida y abierta, y la convergencia entre estos.

Los principales beneficios para los usuarios y las audiencias:

1. Prohibición de la discriminación.
2. Eliminación de la Larga Distancia Nacional.
3. Tarifa cero en terminación de llamadas.

Figura 30: Habilitadores y Objetivos de la Reforma a la Constitución Política de los Estados Unidos Mexicanos en Materia de Telecomunicaciones y Competencia Económica



Fuente: *Estrategia Digital Nacional de Mexico, Página 17,* *http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf*

4. Tarifas y planes con cobro por segundo.
5. Inclusión de apartado específico con derechos de los usuarios.
6. Inclusión de apartado específico para usuarios con discapacidad.
7. Culminación de la transición a la Televisión Digital Terrestre (TDT) el 31 de diciembre de 2015.
8. Multiprogramación en televisión radiodifundida.
9. Neutralidad de la red.
10. Prohibición de intervención de llamadas telefónicas.
11. Bloqueo de teléfonos reportados como robados o extraviados.
12. Confidencialidad de información de usuarios en redes públicas.

El Decreto de Reforma a la Constitución Política de los Estados Unidos Mexicanos en Materia de Telecomunicaciones y Competencia Económica, Esta contenido en el plan de Gobierno 2013-2018, con un enfoque de un Programa para un Gobierno Cercano y Moderno[152] , parte de la pregunta ¿**Cómo utilizar eficientemente los recursos públicos para incrementar la calidad de vida en México?**.- Se orienta con cada uno de los objetivos nacionales confluye con los mecanismos habilitadores de esta estrategia de país

Definiendo en materia de Seguridad Ciudadana utilizar a las TICs para prevenir la violencia social, articulando los esfuerzos de la ciudadanía y de las autoridades en torno a objetivos comunes para promover la seguridad, y también para prevenir y mitigar los daños causados por desastres naturales.

Con los siguientes objetivos secundarios

1. Generar herramientas y aplicaciones de denuncia ciudadana en múltiples plataformas.
2. Desarrollar instrumentos digitales para la prevención social de la violencia.
3. Impulsar la innovación cívica por medio de las TIC.

[152] http://www.dof.gob.mx/nota_detalle.php?codigo=5312420&fecha=30/08/2013

4. Prevenir y mitigar los daños causados por desastres naturales mediante el uso de las TIC.

Esto coincide con el Plan Nacional de Desarrollo y la iniciativa “México en Paz” que se enfoca en el avance de la democracia, la gobernabilidad y la seguridad de la población. Para alcanzar tales fines, la participación ciudadana se concibe como el eje de la relación entre gobierno y sociedad, ya que permite el desarrollo y fortalecimiento del tejido social que evita el quebrantamiento de la paz, y el mejoramiento de la transparencia y rendición de cuentas, reduciendo la corrupción.

A continuación se enuncian los aspectos habilitadores vinculados a la Seguridad Ciudadana:

Tabla 15: Habilitadores vinculados a la Seguridad Ciudadana

	Habilitadores	Contexto
1	**Conectividad**	La conectividad se refiere al desarrollo de redes, al despliegue de una mejor infraestructura en el territorio, a la ampliación de la capacidad de las redes existentes, y al desarrollo de competencia en el sector de las TICs para estimular la reducción de precios.
2	**Inclusión y Habilidades Digitales**	La inclusión y el desarrollo de habilidades digitales se relacionan con la necesidad de que todos los sectores sociales puedan aprovechar y utilizar las TIC de manera cotidiana, además de contar con el acceso a los servicios de telecomunicaciones
3	**Interoperabilidad**	La interoperabilidad se refiere a la capacidad de los sistemas para intercambiar información del gobierno con el fin de lograr objetivos comunes. La interoperabilidad tiene cuatro aspectos: **Técnico**: uso de soluciones tecnológicas que favorezcan la neutralidad e interoperabilidad. **Semántico**: uso de mecanismos que permitan que la información intercambiada se en- tienda sin ambigüedad. **Organizacional**: implementación de procesos organizacionales adecuados para la disponibilidad de la información. **Gobernanza**: desarrollo de componentes institucionales, espacios de diálogo y acuerdos necesarios para definir los estándares de interoperabilidad y su puesta en práctica.
4	**Marco Jurídico**	Se refiere a la armonización del marco jurídico con la finalidad de propiciar un entorno de certeza y confianza favorables para la adopción y fomento de las TIC, lo que implica el análisis del marco jurídico en torno a los diversos temas que contempla la Estrategia
5	**Datos Abiertos**	Los datos abiertos son un mecanismo fundamental para construir espacios de experimentación en los que ciudadanos participativos e innovadores puedan interactuar de manera cercana con servidores públicos para generar soluciones a problemas sociales e impulsar la transparencia y rendición de cuentas ante la ciudadanía

En este sentido, el uso de las TIC que promueve la Estrategia favorecerá la participación ciudadana para lograr un México en Paz, mediante

I. El acceso a datos abiertos con información pública del gobierno que resulte útil y valiosa para la seguridad ciudadana.
II. El acceso a canales de comunicación e interacción como redes sociales, blogs y wikis que permitan a la población convertirse en un actor más activo en el fortalecimiento de la cultura cívica y el seguimiento de la acción pública.
III. El acceso a la entrega de servicios públicos y trámites digitales, disponibles en todo momento y lugar, que acerquen al gobierno y al individuo.
IV. La generación de mecanismos de denuncia ciudadana de actos negativos o conductas delictivas que vulneren la seguridad de la población.

El impacto y seguimiento de estrategia esta disponible para su observancia en el sitio web http://www.presidencia.gob.mx/edn/indicadores/

Los ítem 20,21,22 y 23 son específicos[153] sobre la Seguridad Ciudadana en este sitio web para:

- 20. Generar herramientas y aplicaciones de denuncia ciudadana en multiples plataformas.
- 21. Desarrollar instrumentos digitales para la prevención social de la violencia.
- 22. Impulsar la innovación cívica por medio de TICs.
- 23. Prevenir y mitigar los daños causados por desastres naturales mediante el uso de las TICs.

4.6 Análisis de innovación tecnológica América del Sur

4.6.1 El Caso del ECU911 de Ecuador

El Servicio Integrado de Seguridad ECU 911 es un sistema integrado de comando control, comunicación, informática, inteligencia y vigilancia; es el proyecto en Ecuador con un concepto integral [154] de la seguridad[155]. Una plataforma tecnológica de punta que, en base a políticas, normativas y procesos, articula un servicio único para la recepción de llamadas y despachos simples o multidisciplinarios de emergencias, a partir de las capacidades y recursos provistos por instituciones de carácter público, a través de sus dependencias o entes a su cargo, para dar respuestas integrales a distintas peticiones de la ciudadanía en situaciones de emergencia en forma eficaz y eficiente. Con una inversión [156] de US$160 millones en tecnología y US$60 millones en infraestructuras tiene una cobertura de las principales ciudades del territorio ecuatoriano.

El Decreto Ejecutivo No. 988, del 29 de diciembre de 2011, evidencia en sus considerandos: “Que dentro de las instituciones del Estado no se ha creado un organismo que articule las acciones del Sistema de Seguridad Pública y del Estado con las del Sistema Nacional de Salud y los Gobiernos Autónomos Descentralizados, creando una sinergia entre las instituciones pertenecientes a los sectores indicados para dar una respuesta inmediata a temas como delincuencia común, desastres naturales o antrópicos, atención eficiente a peticiones de socorro, emergencias en salud, entre otros; Que para la correcta coordinación de los diferentes actores prestadores de servicios de emergencia, se hace necesaria la creación de una instancia de coordinación intersectorial que defina la política pública, la regulación, el licenciamiento, el control y la estrategia para dar una respuesta oportuna a las llamadas de emergencias[157].”

[153] http://www.presidencia.gob.mx/edn/objetivo/innovacion-civica-y-participacion-ciudadana
[154] https://www.youtube.com/watch?v=hNnTthFLeL4
[155] http://www.seguridad.gob.ec/wp-content/uploads/downloads/2012/12/revistaNS6final1.pdf
[156] https://www.youtube.com/watch?v=_-nvddDD_P4
[157] http://www.ecu911.gob.ec/estadisticas/

Este sistema integra las siguientes instituciones:

- Policía Nacional.
- Comisión de Tránsito de Ecuador.
- Ministerio de Salud Pública.
- Corporación Nacional de Electricidad.
- Cuerpo de Bomberos.
- Fuerzas Armadas.
- Secretaría Nacional de Gestión de Riesgos.

El Ecosistema de respuesta del ECU-911, considera:

- **Tiempo de atención de la llamada:** período empleado desde el reporte del incidente y su registro hasta el envío a la consola de despacho. Durante esta acción el operador levanta una ficha donde tipifica el ingreso de la emergencia.
- **Tiempo de despacho:** ciclo que comprende la asignación específica del recurso, de acuerdo al incidente, hasta su arribo al sitio de la emergencia.
- **Tiempo de respuesta**: lapso entendido desde el ingreso del incidente al sistema hasta que el recurso enviado por la institución atienda la emergencia.
- **Tiempo de solución del incidente**: fase que contempla el despacho del recurso pertinente, arribo al lugar de la emergencia hasta que finaliza o es atendido en su totalidad.
- **Tiempo de operación del incidente**: tiempo empleado desde el despacho del recurso hasta la solución definitiva de la emergencia.
- **Tiempo total del servicio**: espacio temporal empleado para atender un incidente. Desde el ingreso del reporte, sea a través de una llamada telefónica o mediante el sistema de videovigilancia hasta la finalización del incidente o su atención total.

El Ministerio Coordinador de Seguridad del Ecuador ha logrado sistematizar la respuesta a la ciudadanía del ECU911, y publica estos avances en la Revista ”Nuestra Seguridad[158]”, información que esta permitiendo acciones de estudio y análisis sobre la efectividad del ECU911.

Conformado por 132 consolas para llamadas, video vigilancia y despacho de las distintas instituciones de respuestas; 415 cámaras, 1200 GPS y 1210 dispositivos PDA, tecnologías informáticas y de comunicaciones que permiten ubicar el recurso más cercano y despacharlo. Un sistema nacional con módulos adicionales que brinda numerosas prestaciones técnicas: simulaciones de primer orden, predicción y análisis de simulacros de accidentes industriales, y a la vez, acceso y coordinación con todos los centros del Sistema Integrado de Seguridad ECU 911.

El desarrollo de sistemas integrados de investigación a fin de propiciar un entorno más seguro[159]; incorporando la informática y la electrónica para trabajar en prevención y seguridad vial. La implementación de radares es uno de los recursos científicos para el estudio de la movilidad, la vigilancia y control de velocidad, en vehículos livianos y pesados; un medio probado de examen e intervención que deviene un instrumento idóneo para el buen ejercicio de las actividades de entidades y agentes de tránsito y que, al mismo tiempo, legitima los procesos de indagación, transparenta los hechos y elimina la discrecionalidad. Estos radares pueden fotografiar al vehículo que infringe el marco normativo, registra y sistematiza la imagen, número, fecha, hora, tipo de vehículo, el sentido de la marcha, velocidad, población; información que abona a la veracidad de la infracción y a la aplicación justa de sanciones por contravenciones según los artículos 142 y 145 de la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial.

[158] http://www.seguridad.gob.ec/wp-content/uploads/downloads/2012/12/revistaNS6final1.pdf
[159] http://www.ecu911.gob.ec/biblioteca/ , Documentos, publicaciones y políticas

En artículo 396 del Código Orgánico Integral Penal de Ecuador castiga entre 15 y 30 días de prisión a las personas que hagan llamadas falsas al Sistema Integrado de Seguridad ECU 911. Esta es una contravención de cuarta clase que se decidió incorporar en la normativa debido al alto índice de llamadas malintencionadas. En el inciso número tres de ese artículo se dice que la sanción aplicará a "la persona que de manera indebida realice uso del número único de atención de emergencias para dar un aviso falso de emergencia y que implique desplazamiento, movilización o activación innecesaria de recursos de las instituciones de emergencia".

Sanciones inmediatas: cuando se reporta más de tres llamadas falsas al 911 se suspende 30 días la línea telefónica; cuando hay reincidencia se inhabilita por un año el servicio y si vuelve a ocurrir se elimina la línea telefónica de forma definitiva.

Observando resultados: las estadísticas [160] son una de las principales formas de medir la eficacia y funcionalidad del ECU 911, pueden ser observadas de forma mensual y anual. Esta herramienta ayuda a conocer la real magnitud de los incidentes y enriquecer la toma de decisiones, evaluar el sistema y mejorar acciones para eventos futuros, permitiendo proyectar acciones de mejora a la respuesta del sistema de emergencias sobre las evidencias de tiempos en la atención de incidentes.

4.7 Tendencias de nuevas tecnologías

Tecnología IGRIS, dispositivos para el escaneo.

La Detección por medios no invasivos, rápidos y fáciles de usar. No requiere una formación especial para operar o interpretar, se puede implementar en prácticamente cualquier lugar. La tecnología de escaneo IGRIS es capaz de determinar con 99.99% de precisión si el contrabando (armas, drogas, explosivos, etc) está presente [161]. La definición de contrabando se deja para el cliente, como sistemas IGRIS puede ser programado para detectar prácticamente cualquier sustancia de interés.

Las exploraciones de menos de 4 segundos tienen una exactitud cercana al 99,99% realizan la detección de todos los explosivos, líquidos o sólidos, material de contrabando y sus componentes y materiales de interés, tales como productos de contrabando, (es decir, los diamantes, los combustibles, dinero, alcohol, tabaco, drogas ilegales, y artículos sujetos a derechos de importación). Imágenes en 3D están disponibles para el personal de supervisión para identificar la ubicación de contrabando dentro de un contenedor de carga o vehículo, esta tecnología es más efectiva que el escaneo por rayos x que se limita a exploración dimensional 2D; IGRIS es un dispositivo de escaneo dimensional 3D eliminando los errores de identificación.

Las unidades de escaneo de rayos X puede indicar que una sustancia orgánica está presente, pero no puede identificar lo que la sustancia es. Los escáneres de rayos X convencionales sólo pueden distinguir entre los elementos de número atómico alto (es decir, hierro y mercurio) y el número atómico bajo (es decir, carbono, nitrógeno, y oxígeno).

Su tecnología, esta basada en la aplicación de rayos gamma, apoya la implementación de la LEY DE SEGURIDAD HR-1 (USA)[162], que demanda el escaneo del 100% de la carga marítima con destino USA en los puertos de origen, antes de ser cargados en el buque, mediante equipos de generación de imágenes no intrusivas y que detecten material radiactivo. Un informe de impacto económico de estas tecnologías esta disponible[163] y referencia el caso especifico de Puerto Limón en Costa Rica.

Superando a los sistemas de escaneo por rayos x que se fundamentan en

1. Como se identifican las sustancias en dos (2) dimensiones.

[160] http://www.ecu911.gob.ec/estadisticas/
[161] http://www.container-scan.com/index.php/features/igris-3d-rendering
[162] http://www.container-scan.com/index.php/features/video-igris-scanning-solutions/espanol
[163] http://www.container-scan.com/index.php/2015-07-24-20-38-42/u-s-aid-economic-impact-report

También en los siguientes puntos de importancia.

2. Tiempo de la Identificación de 3 a 5 segundos.
3. Exactitud de la identificación.
4. Escaneo en tres dimensiones (3D).
5. Contiene sistema computarizado de interpretación de resultados.
6. Detección de drogas, explosivos, armas, material nuclear.

“Casos exitosos del uso de TIC en seguridad pública en América Latina”

Parte V: Casos de éxito en el ámbito nacional y local.

5. Casos de éxito en Honduras en el ámbito nacional y local.

5.1. Una mirada al Plan Maestro de Gobierno Digital[164]

La República de Honduras comenzó las negociaciones para el abordaje de tecnologías de información y las comunicaciones con Corea en visita oficial de gobierno a Corea en febrero de 2011.- Esta iniciativa tecnológica inició el 27 de agosto del 2014 como parte de la modernización del aparato estatal y seguimiento de las acciones del anterior gobierno. El Plan Maestro fue elaborado por la Agencia Nacional de Promoción de la Industria de tecnologías de información y comunicación de Corea (NIPA). Así mismo la delegación coreana hizo entrega de un estudio de factibilidad para la implementación de un Centro de Datos Gubernamentales, que fue desarrollado con el apoyo de la Asociación Coreana de Consultoría e Ingeniería (KENCA).

Análisis económico de la iniciativa:

- Diseño detallado US$ 322,408
- Construcción de Edificios, Maquinaria / instalación eléctrica instalación, etc. US$ 10,516,358
- Redes: Router, Switch, Seguridad, IPTV, centro de datos, Software de Gestión US$ 12,416,661
- Operación del Centro: electricidad, sistema de aire acondicionado, generador, sistema contra incendios, seguridad física, etc. US$ 9,819,858
- Costo de contingencia US$ 982,586
- Impuesto al Valor Agregado (15%) US$ 5,108,681
- Sub total del proyecto[165] US$ 39,166,552
- Contrapartida del estado de Honduras$16,833,488
- Costo del proyecto US$ 56,000,000

El proyecto tiene como fin planificar de forma continua la transformación y mejora de las relaciones del Estado hondureño con empresas privadas, instituciones públicas y ciudadanos, mediante el uso efectivo de las tecnologías de la información y comunicaciones TICs, haciendo que cada situación pública se integre de forma funcional a la red, esta bajo la coordinación y gestión de la Secretaria de Coordinación General del Gobierno (SCGG-HN)

Además busca desarrollar las líneas de acción para el establecimiento del gobierno digital en el país, por medio de un trabajo conjunto con los actores claves y con el ejemplo del modelo coreano, que es líder a nivel mundial. El plan dispone de una visión y misión de gobierno digital a medio y largo plazo, a la vez propone estrategias para obtener un gobierno más eficiente, así como el marco legal y recursos humanos que son pertinentes a Gobierno Digital.

El plan busca desarrollar las líneas de acción para el establecimiento del gobierno digital en Honduras, por medio de un trabajo conjunto con los actores claves y con el ejemplo del modelo coreano, que es líder a nivel mundial.

El Plan de Gobierno Digital tiene como objetivos principales:

[164] http://www.scgg.gob.hn/content/plan-maestro-de-gobierno-digital-para-honduras
[165] Feasibility Study on Government Integrated Data Center (GIDC) for the Republic of Honduras

- Disponer de una visión y misión de gobierno digital a medio y largo plazo.
- Proponer las estrategias de implementación para realizar las tareas e iniciativas principales.
- Seleccionar las iniciativas importantes y preparar la hoja de ruta reflejando las prioridades para un gobierno más eficiente.
- Recomendaciones para la gestión del cambio incluyendo organización, marco legal y recursos humanos que son pertinentes a Gobierno Digital.

El marco para estudio de factibilidad se ejecuto en 5 etapas, y esta disponible a febrero del año 2015

i. Etapa de preparación, se organizo el equipo, establece ámbito de trabajo y realiza reunión de inauguración.
ii. Etapa de evaluación, se analiza estado actual a través de investigación, entrevista y datos.
iii. Etapa de desarrollo de estrategia, se establece visión y meta basado en estado analizado, y se desarrolla estrategias para obtener la visión y modelo de futuro.
iv. Etapa de estrategia de implementación, se desarrolla gestión de sistema y operación y estrategias para hoja de ruta. - Por último, la
v. Etapa de estrategia de gestión incluye análisis económico de inversión y búsqueda de recursos.

El equipo de proyecto se estructura con Korea Engineering & Consulting Association (KENCA[166]) de Corea y la Secretaria de Coordinación General SCGG[167] del Gobierno Honduras. El equipo coreano realiza estudio de factibilidad como análisis de centro de datos y estrategias de implementación y gestión, mientras Honduras ofrece información de localización para centro de datos, tamaño, y estado actual de centro de datos.

Además busca desarrollar las líneas de acción para el establecimiento del gobierno digital en el país, por medio de un trabajo conjunto con los actores claves y con el ejemplo del modelo coreano, que es líder a nivel mundial.

El plan dispone de una visión y misión de gobierno digital a medio y largo plazo, a la vez propone estrategias para obtener un gobierno más eficiente, así como el marco legal y recursos humanos que son pertinentes a Gobierno Digital. - Esta es una de las iniciativas más importantes que establece el plan y que servirá como base para el resto de proyectos que se deben implementar.

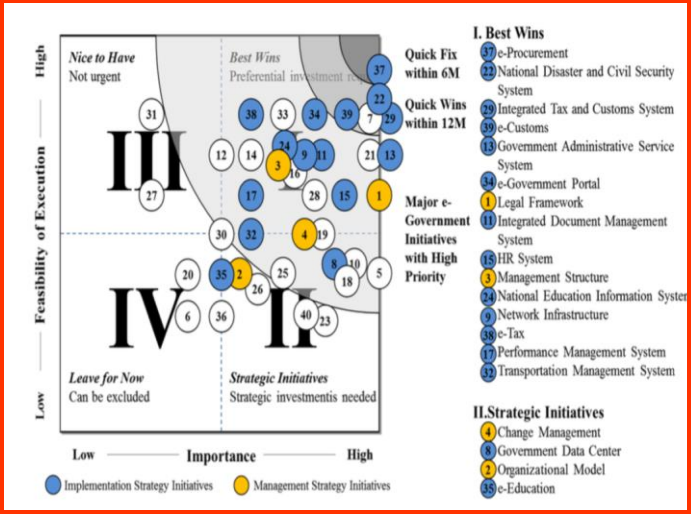
Según el documento elaborado por Korea, el principal desafío del gobierno de Honduras es la brecha digital; sólo el 17,8% de la población es usuario de Internet y Honduras clasificó en 116 de 148 países (con el valor de 3,24) publicado en el Networked Readiness Index (NRI) 2013 del World Economic Forum, implica que existe una considerable brecha digital no sólo en comparación con los países desarrollados, sino también en América Latina

El NRI comprende cuatro subíndices: estos índices miden el medio ambiente para las TIC; la disposición de una sociedad de usar las TIC; el uso real de todos los actores principales; y, por último, los impactos que generan las TIC en la economía y en la sociedad. Los primeros tres subíndices pueden ser considerados como los controladores que establecen las condiciones para los resultados de la cuarta subíndice, los impactos de las TIC. Estos cuatro subíndices se dividen en 10 pilares compuestos por 54 indicadores individuales en total, de acuerdo con la siguiente estructura

[166] http://www.kenca.org/index.jsp
[167] http://www.scgg.gob.hn/content/la-secretar%C3%ADa-de-coordinaci%C3%B3n-general-de-gobierno

Según el análisis de la cartera cuadrantes de TICS la fase de implementación, requiere ser iniciada a inicios del año 2016 con la más alta prioridad. Considerando la oficina de Desastres nacionales y el sistema de la seguridad civil, el sistema tributario y aduanero integrado y e-Aduanas tiene mayor prioridad que debe ser iniciado dentro de los 12 meses posterior a la presentación del estudio, así como portal de e-Gobierno también debe ser implementado con alta prioridad y tiene que estar alineado con la implementación del sistema de gobierno de un servicio administrativo.

Figura 31: Análisis de la cartera cuadrantes de TICS



La priorización final se sugiere como una hoja de ruta en la estrategia de ejecución después de definir cada iniciativa e-Gobierno elegido con el plan de acción y teniendo en cuenta la secuencia lógica basada en las interrelaciones de las iniciativas.

En los temas de Seguridad Ciudadana ha considerado[168] el estatus actual de los sistemas que se enuncian a continuación de:

- Sistema Estadístico Policial en Línea (SEPOL) para el registro de muertes por homicidios, registro de muertes, homicidios e incidentes
- Sistema de Identificación automatizado de huella digital (Automated Fingerprint Identification System AFIS)
- Localización automática de vehículos (Automatic Vehicle Location AVL)
- Sistema Integrado de Identificación Balística (Integrated Ballistics Identification System IBIS)
- Sistema Nacional de Registro de Licencias (Driver's License Registration System).
- Sistema de Registro Penal Nacional 911(Criminal Record System Nationwide 911 System).

En este estudio se considera la facilidad de sustituciones del Sistema Electrónico Digital (SEDI) de la Corte Suprema de Justicia, que es el sistema que permite el seguimiento de casos en el marco del sector de la justicia. Sin embargo, no existe un plan concreto para el desarrollo y ejecución por falta de presupuesto y recursos calificados.

[168] e-Government Master Plan for the Republic of Honduras, página 81

Los primeros resultados están enfocados alrededor de un reordenamiento de sitios web del Estado de Honduras, para lo cual ya se ha desarrollado un Manual para el desarrollo de Sitios Web de Gobierno, contiene la información requerida para la generación de espacios digitales para diferentes plataformas que utilicen Internet, cumpliendo con los requerimientos del Gobierno de Honduras y actualizado al año 2015.[169]

La División de Gobierno Digital dependiente de la Dirección Presidencial de Transparencia, Modernización y Reforma del Estado, adscrita a la Secretaría de Coordinación General de Gobierno, es el organismo encargado de promover el buen uso de las tecnologías de la información y comunicación (TICs) para aumentar la eficiencia de la gestión pública, ha establecido tambien las políticas para la administración y uso del correo electrónico en las instituciones del Gobierno de la República de Honduras con el propósito de normar el uso, unificar criterios técnicos y administrativos sobre el servicio de correo electrónico institucional, el cual constituye un medio oficial para la transmisión de mensajes y documentos digitales a través de la red institucional o vía web, asegurando y facilitando una eficiente comunicación tanto interna como externa.

Figura 32: División de Gobierno Digital

Asimismo, se incluyen las mejores prácticas internacionales para el uso apropiado del servicio de correo electrónico[170] de las Instituciones del Gobierno que buscan el mayor rendimiento y seguridad de la información de las cuentas de correo electrónico de los usuarios.

5.2. Tendencia de mejor práctica en la efectividad social

Sistema de 911 Honduras

Tabla 16: Datos del sistema de 911 de Honduras

	Datos del Sistema de 911, Honduras	
	Nombre de la institución:	Sistema 911 Honduras
	Sitio Internet:	www.seguridad.gob.hn
	Inaugurado:	Nace como linea 199 Evoluciona a 911 mayo 2013

[169] http://www.scgg.gob.hn/content/manual-de-desarrollo-de-sitios-web-de-gobierno-2015
[170] http://www.scgg.gob.hn/content/pol%C3%ADticas-para-la-administraci%C3%B3n-y-uso-del-correo-de-las-instituciones-del-gobierno-de-la

Como una medida más para contrarrestar los altos índices de violencia que azotan a Honduras, la noche del jueves 25 de abril del 2013 se anunció la implementación del número 911, para que la población haga sus denuncias de emergencia.

"El anuncio se hizo en cadena de radio y televisión, todos los números de emergencia quedan concentrados en el 911. Habrá equipos de respuesta para atender inmediatamente las emergencias denunciadas."

Figura 33: Sistema de Emergencias 911 - Honduras

La medida trata de fortalecer la seguridad ciudadana y los sistemas de respuesta inmediata como los de llamadas de emergencia de la Policía Nacional.

"Tengo a bien informar que a partir de esta fecha, hemos puesto a disposición el número de emergencias 911 de la Policía Nacional, el que sin duda, contribuirá a que combatamos la delincuencia y la violencia con mayor efectividad", dijo el titular de Seguridad, en ese entonces, el Sr. Pompeyo Bonilla. Al número 911, que es parte del proyecto de Ciudades Seguras, se puede llamar, tanto desde teléfonos fijos, como desde teléfonos celulares, todo con el fin de felicitarle a la ciudadanía la poderosa herramienta de la denuncia, es financiado por la tasa de seguridad.

Este nuevo servicio del 911, sustituye a todos los números de emergencia existentes como el 100 de la Emergencia Municipal, el 101 de Dirección Nacional de Servicios Especiales de Investigación, el 112 de la Dirección Nacional de Investigación Criminal, el 114 para casos de Violencia Domestica y el 199 de la Policía Nacional.

La Comisión Nacional de Telecomunicaciones (CONATEL) aprobó la normativa necesaria para sancionar a quienes efectúen llamadas inadecuadas, con penas que van desde sanciones económicas, hasta la suspensión definitiva del número telefónico.

A partir del primero de mayo del 2013, la Policía Nacional y las Fuerzas Armadas tienen equipos de reacción inmediata en los diferentes cuadrantes de Tegucigalpa y San Pedro Sula en un inicio, lo que ha permitido la atención oportuna a las denuncias al 911.

El sistema del 911 está integrado por un centro de comando y control, además de moderna tecnología con cámaras de video seguridad para prevenir y esclarecer diferente tipo de situaciones que puedan afectar la seguridad ciudadana. Con la misión de apoyar, dirigir, controlar, administrar la plataforma tecnológica inteligente para la oportuna actuación e intervención de las unidades operativas, fortalecer la prevención y combate del crimen común y organizado, los procesos investigativos de la Policía y la interoperabilidad con los organismos de emergencia.

El Congreso Nacional aprobó el 19 de mayo del 2015 la Ley del Sistema Nacional de Emergencias 911[171], como un servicio público y de seguridad nacional responsable de la atención de las llamadas de emergencia dirigidas al número 911 realizadas por cualquier persona desde cualquier parte del territorio nacional que

[171] http://www.observatoriodescentralizacion.org/download/leyes_vigentes/07-09-15%20(1).pdf%20LEY%20DEL%20SISTEMA%20DE%20EMERGENCIA%20911.pdf

requiera seguridad, atención prioritaria, extinción de incendios, salvamento o protección civil, procurando dar respuesta inmediata coordinada y de calidad.

En el proyecto se establece que la operación del sistema nacional de emergencias 911, será financiada con los fondos de la Tasa de Seguridad, fondos municipales y transferencias nacionales y extranjeras.

Servicio público y seguridad

El sistema se crea como un servicio público y de seguridad debidamente controlado por el Estado. Mediante este sistema, cualquier persona que requiera seguridad, atención prioritaria, extinción de incendios, salvamento o protección civil utilizará la línea del 911.

Con esta ley se reglamenta el procedimiento para la recepción de denuncias por parte de personas que enfrenten un peligro o denuncias una situación de inseguridad.

La ley contempla de tres a seis años de reclusión a quienes hagan llamadas falsas a esta línea. Además, se cargará en la factura o saldo disponible del usuario un costo equivalente del 500 por ciento del valor normal de la llamada.

El articulo cinco (5) de la ley del Sistema Nacional de Emergencias 911, define que esta está integrado por las siguientes instituciones:

- Secretaría de Estado en los Despachos de Seguridad.
- Secretaría de Estado en los Despachos de Defensa Nacional.
- Secretaría de Estado en los Despachos de Salud.
- Instituto Hondureño de Seguridad Social IHSS.
- Policía Nacional.
- Policía Militar y del Orden Público.
- Comisión Permanente de Contingencias (COPECO).
- Cuerpo de Bomberos.
- Instituto Nacional Penitenciario.
- Instituto Nacional de Migración.
- Instituto Nacional de la Mujer.
- Dirección Nacional de Transporte.
- Alcaldías municipales que integren al Sistema Nacional de Emergencias 911.
- Cruz Roja Hondureña.
- Ministerio Público.
- Otras instituciones Públicas o Privadas que se integren al Sistema Nacional de Emergencias 911.

Su artículo 6, define que El Sistema Nacional de Emergencias 911, opera jerárquicamente bajo la subordinación del Consejo Nacional de Defensa y Seguridad.

Su artículo 13.- define que El Sistema Nacional de Emergencias 911 funcionará a través de:

a) Centro de Emergencias y Coordinaciones de Operaciones de Tegucigalpa (CECOP-TEGUCIGALPA), como sede principal.
b) Centro de Emergencias y coordinaciones de operaciones de San Pedro Sula (CECOP-SPS), como centro de respaldo, pero con capacidad operativa igual a la sede principal.
c) Centros de Operaciones Institucionales, en cada una de las instituciones que integren efectivamente el Sistema Nacional de Emergencias 911.
d) Bases de Operación Institucional (BOI), que se instalen a nivel nacional.
e) Centros de Control y Mando Móvil (CCM), vehículo de intervención rápida.
f) Centro de Excelencia Formativa (CEF), como un centro de formación permanente para certificar al personal civil e institucional bajo el referente internacional y, donde se lleve a cabo el desarrollo y

evolución de las herramientas implementadas de tal forma que se conviertan en una fuente generadora de personal calificado y tecnología a exportar.

g) Otras unidades o dependencias que sean creadas en adelante mediante los reglamentos relacionados.

Para mayor coordinación y eficiencia operativa del Sistema Nacional de Emergencias 911 todos los cuerpos de seguridad y emergencias, deben integrar todos los sistemas de radio y compartir la misma sala y la misma plataforma tecnológica para la atención de llamadas, gestión de incidencias, comunicación de radio y cumplir todos los protocolos, como mínimo en el CECOP-TEGUCIGALPA y en el (CECOP-SPS).

Actualmente el 911[172] atiende diariamente alrededor de 3,000 llamadas, los tiempos de respuesta que manejan varían entre 5 a 15 minutos en la ciudades de Tegucigalpa y San Pedro, dependiendo de la zona donde se suscite el hecho. Durante el 2014 se recibieron 10.3 millones de comunicaciones, de esas un 76% fueron falsas, con la nueva ley aprobada en mayo del 2015 se espera que la efectividad del Sistema 911 de Honduras sea mayor.

5.3. Análisis de tendencias y proyecciones, TICs para promover de la Seguridad y Convivencia Ciudadana

Análisis de características Sistema Estadístico Policial en Línea (SEPOL)

Tabla 17: Datos del Sistema Estadístico Policial en Línea (SEPOL)

	Datos del Sistema Estadístico Policial en Línea (SEPOL)	
	Nombre de la institución	**Secretaria de Seguridad**
	Inicio:	Sistema Estadístico Policial en Línea (SEPOL) Creado mediante acuerdo Ministerial 1437-2010 como “Departamento de Estadisticas D-8

Es el Departamento, encargado de generar y difundir información estadística relacionada a la incidencia delincuencial y el accionar policial, a través del Sistema Estadístico Policial en Línea (SEPOL), con la finalidad de brindar datos confiables como insumo para la elaboración de Análisis y estrategias que conlleven a la implementación de políticas públicas de seguridad orientadas a la prevención y combate del delito, financiado con fondos nacionales del estado de Honduras.

Para el año 2015, el Departamento de Estadísticas desempeña su misión con calidad certificada y con procesos automatizados de explotación de información lo cual es un soporte para la evaluación y planeación del desarrollo, institucional, al diseñar estrategias y proporcionar datos objetivos, válidos y confiables de manera oportuna, así como la información estadística requerida por usuarios diversos.

Antecedentes

[172] https://www.youtube.com/watch?v=UA8SKwnWR1o

En el año 2010 y mediante el Acuerdo Ministerial 1437-2010, se creó el Departamento de Estadística de la Policía. Su misión es la de coordinar y unificar las estadísticas de las diferentes Direcciones y Unidades de la Policía Nacional así como formar parte de los sistemas de información interagencial. Al interior de la Policía, existen cuatro Direcciones de Policía: la Preventiva, la de Investigación, la de Servicios Especiales de Investigación y la Dirección de Tránsito, que procesan de manera independiente denuncias delictivas a nivel local y nacional, las cuales remiten a su vez al Departamento de Estadística.

Este Departamento registra y compila estadísticas referidas a incidencia delictiva y también a operatividad policial, que da cuenta de armas decomisadas, decomiso de drogas, detenidos por la policía, allanamientos, denuncias cumplidas, etc. Los usuarios de la información producida son a nivel nacional el Instituto Nacional de Estadísticas, diferentes Secretaría de Estado, la Corte Suprema, el Ministerio Público y el Observatorio de la Violencia de la Universidad Nacional Autónoma de Honduras.

Al Departamento le corresponde homologar entre sí las definiciones y variables correspondientes a los diversos delitos. Sin embargo, continúan habiendo diferencias respecto de diversos tipos penales al interior de la propia policía. Un informe reciente del Banco Mundial cita como ejemplos el secuestro, el trasiego de drogas, la violencia doméstica, entre otros crímenes que son documentados de manera diferenciada, a lo que se le suma la diferencia entre estos y los registros que lleva el Ministerio Público.

A pesar de que la creación del Departamento de Estadística en la Policía Nacional constituye un avance para el fortalecimiento institucional y debiera contribuir a la toma de decisiones mejor informadas y documentadas, el reto es superar el proceso rudimentario que sigue por ahora: las Jefaturas Departamentales registran los eventos en el formato de libro de novedades y a diario los envían al Centro de Operaciones Policiales quien los registra en un formato de novedades en archivo de Word; y seguidamente es enviado al Departamento de Estadísticas para su Digitación en formato Access y Excel. Esto da lugar a que se produzcan problemas de confiabilidad en el dato, que ocurren al momento de digitar la información en la base de datos.

En línea con lo anterior, y previo al funcionamiento del actual SEPOL, entre las conclusiones del "Diagnóstico de sistemas de información de la Policía Nacional y el MP de Honduras[173]" destacan las siguientes: (i) hay diversos sistemas de información para el manejo de los datos en cada institución; (ii) existe la necesidad de obtener datos de calidad que sean proporcionados por cada sistema en tiempo real; (iii) no hay un dato único unificado a nivel superior; (iv) se observan debilidades en el proceso de validación y verificación permanente de los sistemas de información que permitan evitar duplicidad de datos y minimizar errores en la entrada de la información; y (v) se presenta la ausencia de documentación de procesos en los sistemas de información actuales, entre otros.

SEPOL en la actualidad[174]

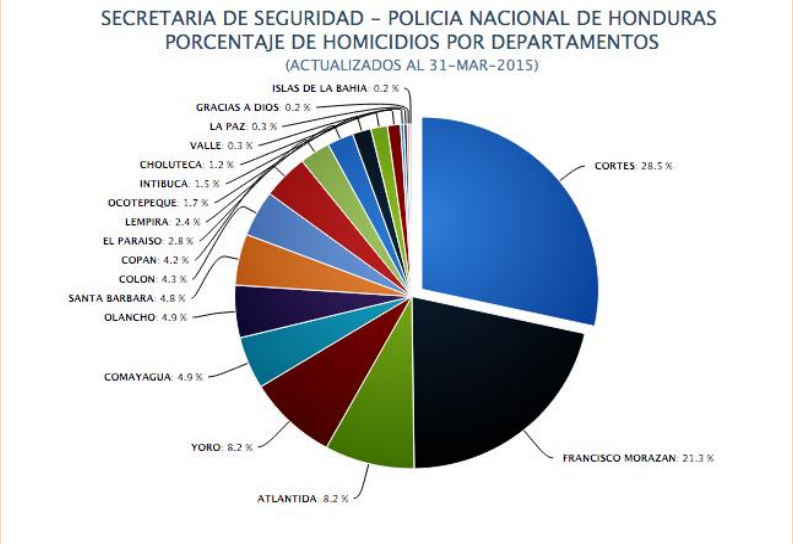
En el 2011 los aspectos que resaltaban como necesidades fundamentales a fin de construir un sistema que entregue información actualizada y oportuna que permita guiar y orientar adecuadamente el accionar policial:

- El primero es fortalecer la capacidad técnica del equipo profesional que participa en todo el proceso de producción de datos, desde aquel que se encuentra a nivel de las Jefaturas Departamentales, hasta aquel que produce los informes y analiza los datos. A nivel de Dirección debe crearse una capacidad de análisis del crimen que entregue análisis procesados de utilidad para las diversas Direcciones de la Policía.
- En segundo lugar, se requiere invertir a fin de modernizar fuertemente los sistemas de software con los que cuenta la Policía, adquiriendo un sistema de información estadístico para centralizar la

[173] **Nota Técnica para el Sector de Seguridad Informe Final,** HO- L1063 Programa de Apoyo a la Implementación de la Política Integral de Convivencia y Seguridad Ciudadana**,** Febrero 2011
[174] https://www.sepol.hn/index.php

información. Paralelamente debe procederse a georreferenciar la información delictual y de operaciones policiales a fin de guiar la actividad de la Policía.

Figura 34: Porcentaje de Homicidios por Departamentos. Secretaría de Seguridad – Policía Nacional de Honduras



Fuente: *SEPOL, Secretaría de Seguridad Honduras*

Esta visión inicial ha facilitado que al 2015, la SEPOL facilite datos que son de acceso público[175] para cualquier organización a través. Permitiendo a los usuarios seleccionar sus propias categorías de estudio y análisis y generar[176] sus propios gráficos.

[175] Idem
[176] https://www.sepol.hn/sepol-estadisticas-incidencia-delito-municipio.php

El estilo del Departamento de Estadística, se enmarca en políticas institucionales que son la pauta que orienta las acciones estratégicas hacia un entorno dinámico, el mismo que presenta nuevas potencialidades y nuevos desafíos a la vez, haciendo necesario el saber discernir la prioridad de las diversas actividades estadísticas. -Estas políticas institucionales se las puede resumir en las siguientes:

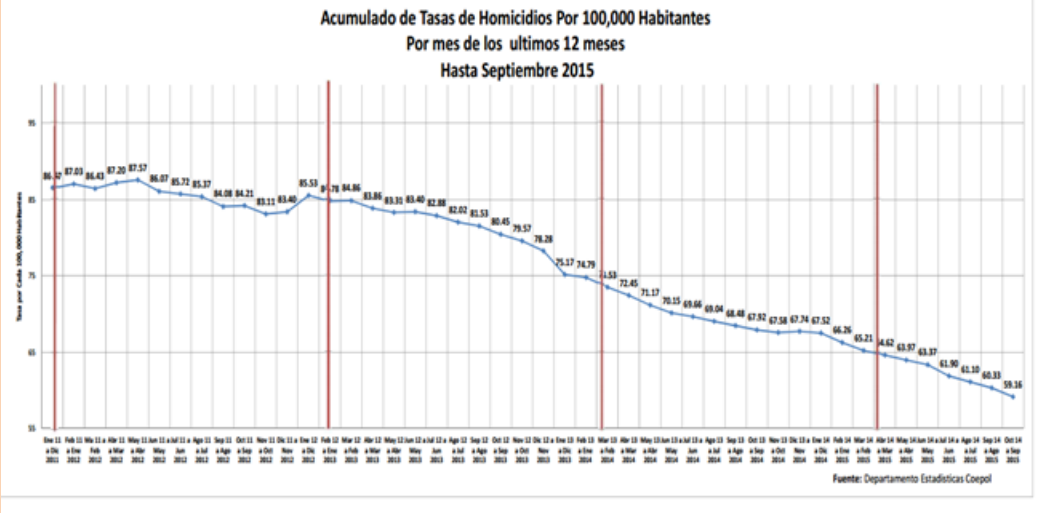
Figura 35: Sistema Estadístico Policial en Línea (SEPOL)

- Impulsar la participación de las comisiones interinstitucionales que garanticen el funcionamiento y fortalecimiento del Departamento de Estadísticas.
- Concienciar y mejorar el conocimiento entre los usuarios, informantes y población en general sobre la naturaleza, importancia y utilidad de la información estadística policial, así como la preservación del secreto estadístico a través de la reserva de información con resoluciones de Instituto de acceso a la información pública.
- Fortalecer la capacidad de gestión interna y de gerencia institucional.
- Vigorizar la imagen de este departamento a nivel institucional interno y externo.
- Dar énfasis a la investigación estadística en temas de actualidad.
- Definir los procesos nuevos y rediseño de los actuales que deben ejecutarse en el Sistema de Información de la Secretaría de Seguridad.
- Ofrecer una propuesta de modelo conceptual y funcional de la manera en que debería funcionar el Sistema de Estadística Policial en Línea (SEPOL).
- Realizar una construcción teórica de un esquema conceptual que permita desarrollar un marco de referencia a partir del cual se pueda plantear la construcción del sistema integrado de estadísticas delictivas (denuncias- Flagrancia)
- Establecer una definición conceptual de toda la información solicitada y la metodología para la organización y funcionamiento de la oficina responsable en la administración del Sistema de Estadístico Policial en Línea (SEPOL)

Fuente[177] SEPOL Policía Nacional de Honduras[178]

[177] https://www.sepol.hn/sepol-estadisticas-honduras.php?id=140
[178] https://www.sepol.hn/artisistem/images/sepol-images/files/Acumulado%20Tasas%20de%20Homicidios%20hasta%202015.pdf

Figura 36: Acumulado de tasas de homicidios por 100,000 habitantes por mes de los últimos 12 meses hasta septiembre de 2015



Fuente: *SEPOL. Policía Nacional de Honduras*

5.4. Análisis de cumplimiento de normativas

Las políticas de Seguridad Pública o Ciudadana, **SI** están vinculadas al marco regulatorio de TICs existente en el país , sin existir un plan de interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs.- Honduras presenta avances importantes, resaltando la activación de la Política Integral de Convivencia y Seguridad Ciudadana para Honduras 2011-2022[179], que vincula el uso de la TICs y aspectos como el desarrollo del "Sistema Información de Violencia y Delincuencia" para atender el problema de la inseguridad ciudadana y la violencia, orientar políticas de prevención y control y asegurar el seguimiento y evaluación de las mismas, es necesario asegurar la capacidad de recolectar y analizar datos de una manera confiable y oportuna.

Además rectora el mejoramiento del Sistema de Comunicaciones para la puesta en funcionamiento de una central única de comunicaciones, dirigida a la creación de una central única de emergencias y seguridad, donde además de la policía hagan presencia y operatividad los servicios de bomberos, Salud, Policía de tránsito, Cruz Roja, prevención y atención de emergencias y todas aquellas instituciones que por sus funciones puedan contribuir a atender una emergencia.

Una Central única de emergencias y Seguridad que:

- Mejore la capacidad de repuesta de cada agencia para atender más incidentes con los mismos recursos de personal y equipos,
- Permita identificar y suplir los cuellos de botella de personal, infraestructura y equipos de cada agencia.
- En el corto plazo permita atender las emergencias en menor tiempo y en forma más efectiva.
- En el mediano plazo y con fundamento en las estadísticas de atención y acciones de prevención, mejore la seguridad de los ciudadanos.
- Mejorar la capacidad del país para responder a las catástrofes naturales, o situaciones de orden público

[179] http://www.hn.undp.org/content/dam/honduras/docs/publicaciones/Politica_Integral_Convivencia_Seguridad_2011_2022.pdf

Al 2015 después de la aprobación de esta política la central única[180] cuenta con una facilidad de ley que esta permitiendo de forma gradual consolidar un solo sistema[181] de emergencias y seguridad, a través del sistema 911 de Honduras.

En materia de centros penitenciarios también rectora:

- Mejorar los sistemas de seguridad de los centros carcelarios, para lo cual se requiere, capacitar al personal existente en materia de seguridad carcelaria,
- Implementar seguridad electrónica interna y perimetral,
- Desarrollar sistemas de comunicación especiales,
- Desarrollar sistemas independientes y autónomos de energía e iluminación y desarrollar procesos de control, administración y automatización centralizado de los sistemas de seguridad.
- Fortalecer el sistema de comunicaciones de cada uno de los centros carcelarios y a su vez con todo el Sistema Penitenciario a partir de establecer una red de comunicaciones que permita mantener el contacto de los administrativos y la guardia,
- Contar con equipos que permitan la transferencia de información confidencial en forma segura,
- Manejo de bases de datos de reclusos con archivos centralizados para mayor veracidad y como método de respaldo.
- Fortalecer los sistemas de movilidad y traslado reclusos.
- Crear y aplicar manuales con estándares internacionales de disciplina y comportamiento interno de los reclusos, personal administrativos y guardia.

En materia de centros penitenciarios hasta el momento existen la ley de limitación[182] de servicios de telecomunicaciones en centros penitenciarios, granjas penales y centros de internamiento de menores de niños y niñas a nivel nacional, orientada al bloqueo de llamadas, al 2015 el sistema penitenciario no cuenta con una facilidad de implementación de TICs, que lo fortalezca de forma integral, para que su gestión sea incidente en la seguridad y justicia del país.

5.5. Principales Marcos Regulatorios de Honduras

Tabla 18: Principales marcos reguladores de Honduras

Marcos Regulatorios	Referencias
Política Integral de Convivencia y Seguridad Ciudadana para Honduras 2011-2022[183]	Que vincula el uso de la TICs y aspectos como el desarrollo del "Sistema Información de Violencia y Delincuencia" para atender el problema de la inseguridad ciudadana y la violencia, orientar políticas de prevención y control y asegurar el seguimiento y evaluación de las mismas, considerando que es necesario asegurar la capacidad de recolectar y analizar datos de una manera confiable y oportuna.

[180] http://www.observatoriodescentralizacion.org/download/leyes_vigentes/07-09-15%20(1).pdf%20LEY%20DEL%20SISTEMA%20DE%20EMERGENCIA%20911.pdf
[181] [181] https://www.youtube.com/watch?v=UA8SKwnWR1o
[182]http://www.tsc.gob.hn/leyes/Ley_de_Limitacion_de_Servicios_de_Telecomunicaciones_en_Centros_Peniteciarios.pdf
[183]http://www.hn.undp.org/content/dam/honduras/docs/publicaciones/Politica_Integral_Convivencia_Seguridad_2011_2022.pdf

Marcos Regulatorios	Referencias
Ley de limitación de servicios de telefonía móvil celular y comunicaciones personales (PCS) en centros penales a nivel nacional.(Decreto 255/2013[184])	Esta ley demandó de CONATEL el establecimiento de los mecanismos técnicos, administrativos, regulatorios, financieros, así como la coordinación y cooperación interinstitucional que posibilite el cumplimiento de la Ley de Limitaciones de Servicios de Telefonía Móvil Celular y Comunicaciones Personales (PCS) en Centros Penales, Penitenciarias Nacionales y Centros de Internamiento de Menores a nivel Nacional contenidas en el Decreto Legislativo 255-2013.- La Creación de la Comisión Interinstitucional de Seguridad de las Telecomunicaciones (CISTEL) para dar cumplimiento a la limitación de brindar o prestar servicios de Telefonía Móvil Celular y de Comunicaciones Personales
Ley Especial de intervención de las comunicaciones privadas (Decreto 243/11)	El proceso de intervención de las comunicaciones estaba autorizado desde antes en el artículo 223 del Código Procesal Penal pero no había tenido mucho desarrollo normativo ni operativo. En esta Ley desarrolla de manera clara el procedimiento de la intervención telefónica, los supuestos a cumplir, las formalidades, las garantías para los ciudadanos y los requisitos a cumplir por todos los participantes en el proceso. Lo más destacado es que se crea la Unidad de Intervención de Comunicaciones (U.I.C), la cual dependerá de la Dirección Nacional de Investigación e Inteligencia, dependencia del Consejo Nacional de Defensa y Seguridad, como órgano encargado de ejecutar a través de su personal especializado, la intervención de las comunicaciones que el Órgano Jurisdiccional autorice. El Gobierno tiene 30 días para reglamentar esta Ley y la U.I.C. para empezar a operar.
Acuerdo Ministerial 1437-2010, se creó el Departamento de Estadística de la Policía. SEPOL	Su misión es la de coordinar y unificar las estadísticas de las diferentes Direcciones y Unidades de la Policía Nacional así como formar parte de los sistemas de información interagencial. Al interior de la Policía, existen cuatro Direcciones de Policía: la Preventiva, la de Investigación, la de Servicios Especiales de Investigación y la Dirección de Transito, que procesan de manera independiente denuncias delictivas a nivel local y nacional, las cuales remiten a su vez al Departamento de Estadística.
Ley del Sistema Nacional de Emergencias 911[185],	El Congreso Nacional aprobó el 19 de mayo del 2015 la ley, como base para un servicio público y de seguridad nacional responsable de la atención de las llamadas de emergencia dirigidas al número 911 realizadas por cualquier persona desde cualquier parte del territorio nacional que requiera seguridad, atención prioritaria, extinción de incendios, salvamento o protección civil, procurando dar respuesta inmediata coordinada y de calidad.

[184] http://sitae.conatel.gob.hn/centrospenales/Ley_Decreto_255-2013.pdf
[185] http://www.observatoriodescentralizacion.org/download/leyes_vigentes/07-09-15%20(1).pdf%20LEY%20DEL%20SISTEMA%20DE%20EMERGENCIA%20911.pdf

5.6. Gestión Pública y las soluciones de TICs para la Seguridad Ciudadana el caso de Puerto Cortes, departamento Cortes en Honduras.

Comisión Comunitaria de Seguridad Ciudadana

Un modelo para la Seguridad Ciudadana

Figura 37: Centro de monitoreo en Puerto Cortés

El área urbana de Puerto Cortés [186] se sitúa en el extremo sur de una pequeña península en el noreste de Honduras. La principal actividad económica de la ciudad gira en torno a las operaciones del puerto, el más importante del país la agricultura, el comercio, los servicios y el turismo. Pese a que goza de una posición geográfica privilegiada, la población no está exenta de los serios problemas de seguridad que aquejan a la región centroamericana.

En Puerto Cortés se ha desarrollado un modelo de atención ciudadana con el concepto de concertación. Un Cabildo Abierto dio pistas acerca de lo que sería la estrategia que vendría a responder a las demandas de seguridad de la población. Durante la administración del alcalde Allan David Ramos Molina[187] , el gobierno local ha trabajado para reducir los índices de violencia e incrementar la seguridad ciudadana.- Gracias a la Tasa de Seguridad que aportan los ciudadanos y a la firma de varios convenios con la Secretaria de Seguridad que significan solidas alianzas interinstitucionales, la ciudad ha llegado a convertirse en un modelo a seguir, en cuanto a iniciativas de seguridad que ha impulsado con el apoyo de la tecnología.

La acción conjunta entre el gobierno local y los diversos actores del territorio de puerto cortes acuerdan generar una Visión de Ser el Municipio líder en Honduras en Seguridad Ciudadana. Con una Misión de Disminuir los índices de violencia e inseguridad ciudadana para convertir el Municipio de Puerto Cortés altamente atractivo para los inversionistas nacionales y extranjeros.

Se aprueba en mayo del 2012 el artículo 37 para la compensación de fideicomisos municipales a nivel de gobierno local y se constituye un fideicomiso por L.7,170,626.06[188] para comenzar acciones contra la inseguridad, que venían siendo implementadas desde el año del 2007 mediante el cobro de la tasa de seguridad a la población, cuando el gobierno local no tenía presupuestos ni medios logísticos para enfrentar el problema y se llevo a esta facilidad con la participacion de la ciudadania, empresa privada y otros actores en el territorio con las siguientes actividades:

1) La decisión de implementar un plan de seguridad, apoyado por la ciudadanía.
2) Que el plan de seguridad Municipal sea certificado por la Secretaría de Estado en el Despacho de Seguridad.
3) Que se constituya un fideicomiso para la administración de los recursos destinados al plan de seguridad municipal.

[186] http://www.ampuertocortes.com/cms/
[187] http://www.ampuertocortes.com/cms/index.php/admon/corporacion-municipal
[188] http://www.ampuertocortes.com/cms/images/stories/seguridad_ciudadana/seguridad_cabildo_2013_parte1.pdf

Estrategia implementada en Puerto Cortés para reducir la criminalidad

Existen dos líneas estratégicas generales que orientan las acciones para enfrentar este problema para atacar las causas y los efectos de la delincuencia. Para ambas líneas la alcaldía crea:

1. El manual de Seguridad Ciudadana, un documento didáctico y motivador que permite esclarecer en detalle la organización y el funcionamiento de la Comisión Local de Seguridad Ciudadana. Con funciones, atribuciones y responsabilidades que les corresponde asumir a sus miembros, proporcionándoles información complementaria sobre los procedimientos y los aspectos que deben tomarse en cuenta para asegurar la construcción de elevados niveles de seguridad ciudadana.
2. La comisión Local de Seguridad Ciudadana, con su respectivo programa de capacitación y entrenamiento.
3. La implementación del programa de seguridad, incluyendo la integración entre recursos humanos, equipos técnicos y el manual de Seguridad Ciudadana. Parte de este programa consiste en diseñar un sistema de seguridad ciudadana municipal, con una estructura administrativa, logística y operativa, donde se integran y se coordinan todos lo operadores de justicia, autoridades civiles, militares y organizaciones de la sociedad civil. El propósito es combatir la delincuencia mediante la creación e instalación de un sistema electrónico de seguridad y video vigilancia, comandado y controlado desde el Centro de Seguridad y Emergencia número único 100. Este número único esta compuesto por los siguientes subsistemas:

    - Subsistema de recepción y despacho de llamadas.
    - Subsistema de estadística.
    - Subsistema de video vigilancia.
    - Subsistema de alarmas.
    - Subsistema de base de datos (antecedentes)
    - Subsistema de radiocomunicación.
    - Subsistema de localización de vehículos(AVL)
    - Subsistema de grabación
    - Subsistema de potencia
    - Subsistema de huellas dactilares(AFIS)

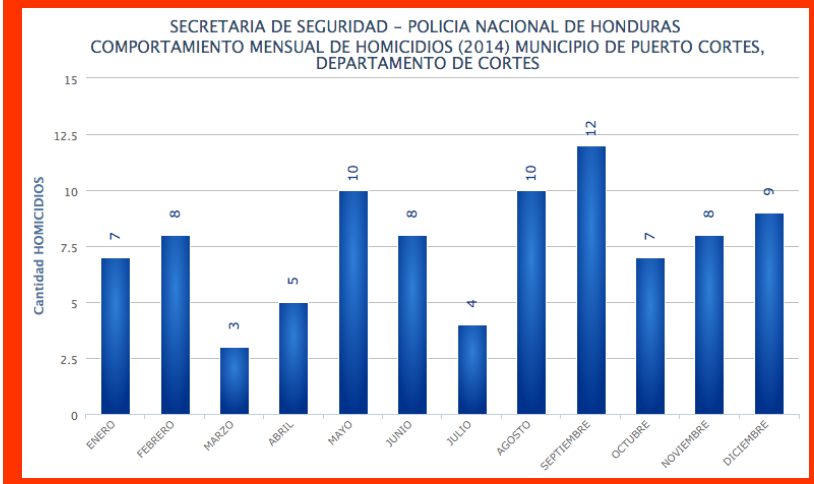
Destino de la Inversión

Los recursos de la tasa de seguridad se invirtieron de la siguiente manera:

- En un sistema electrónico de seguridad y video vigilancia.
- En apoyo logístico a los operadores de justicia y en organizaciones de emergencia, como el Cuerpo de Bomberos, la Cruz Roja y hospitales.
- En la construcción de polideportivos, infraestructura básica de calidad, alumbrado público en zonas oscuras de la ciudad, apoyo a la educación y a la salud de la población.

Según reportes de transparencia de la municipalidad de Puerto Cortes[189], la situación en Puerto Cortes ha mejorado desde la implementación de la nueva estrategia de seguridad de acuerdo con los datos que provee el observatorio de la violencia de la Universidad Nacional, hace tres años comenzaron a operar con una línea base de 102 homicidios, por cada 100,000 habitantes. Al 2014 según reportes La Universidad Nacional Autónoma de Honduras (UNAH) y el Instituto Universitario en Democracia, Paz y Seguridad (IUDPAS) [190] a través del Observatorio Nacional de la Violencia la tasa es de 92.9 (hpccmh), datos de SEPOL [191] confirman las tendencias de baja sobre el delito homicidio, a nivel del municipio se realizan medidas que completan el análisis y estudio comparativo que facilitan medir impacto [192] sobre las tendencias altas en temporalidad y discriminación territorial en el municipio de Puerto Cortes.

Figura 38: Comportamiento de homicidios (2014). Muncipio de Puerto Cortés



¿Cómo reaccionó la ciudad en el momento que propuso la implementación de la nueva tasa de seguridad?

Cuando el problema de la violencia delictiva se incrementó y la población demandaba respuesta inmediata de los operadores de justicia, estos carecían del recurso humano, el equipo y la logística y el presupuesto del operativo necesario para hacerle frente al problema. Mediante reuniones con representantes de diversos sectores de la sociedad, tales como la empresa privada, patronatos, medios de comunicación, sindicato y otros frentes populares, se les explicó que se necesitaba poner a práctica un programa de seguridad ciudadana que diese los resultados exigidos por la población; también se les indico que tal medida había que financiarla[193] con una tasa de seguridad municipal.

Por fortuna, ellos reaccionaron positivamente frente a la implementación de una nueva tasa, pues comprendieron que este era el medio ideal para recaudar los fondos destinados a ejecutar el programa. Se logró dialogar con la ciudadanía mediante asambleas con los patronatos de los barrios de la ciudad y los demás sectores de la sociedad civil, y a través de un cabildo abierto.

Video sobre la sistematización de la experiencia de Puerto Cortes puede verse en

http://www.ampuertocortes.com/cms/index.php/servicios-publicos/seguridad-ciudadana/item/294-video-amoprev-experiencia-puerto-cortes

Donde se describe como se comenzaron las acciones territoriales de:

1) Organización
2) Represión
3) Previsión

[189] http://www.ampuertocortes.com/cms/index.php/servicios-publicos/seguridad-ciudadana
[190] http://iudpas.org/pdf/Boletines/Choloma/CholomaEd13_EneDic2014.pdf
[191] https://www.sepol.hn/sepol-estadisticas-incidencia-municipio-delito-mensual.php
[192] http://www.ampuertocortes.com/cms/index.php/servicios-publicos/seguridad-ciudadana/item/294-video-amoprev-experiencia-puerto-cortes
[193] http://www.ampuertocortes.com/cms/index.php/servicios-publicos/seguridad-ciudadana

4) Prevención

Puerto Cortés por sus avances puede ser considerada su planificación, gestión y administración como un ejemplo a observar para una posible réplica.

Para consolidar una Agenda Local de Desarrollo (ADEL), bajo acciones participativas en cada zona de la ciudad, se realizo bajo el apoyo de los "manzaneros[194]", que son ciudadanos(as) responsables de la seguridad ciudadana y humana en cada manzana de la ciudad.

Figura 39: Programas de la Municipalidad de Puerto Cortes

Una ciudad emergente e inteligente

Allan Ramos: "Puerto Cortés será una ciudad digital[195]

Hacer de Puerto Cortés una ciudad modelo es una de las principales metas que se ha trazado el alcalde Allan Ramos, quien ya inició el proyecto de seguridad por medio de cámaras digitales, en los puntos más conflictivos del municipio.

Otro de los grandes proyectos que está por iniciar en la ciudad porteña es la "ciudad digital", con el propósito de conseguir un alto grado de tecnología en la administración municipal y dar mejor servicio a los pobladores. Ramos participó en el Noveno Programa de Gobiernos Locales Digitales del Siglo 21 y el 12 Encuentro de Ciudades Digitales, recién realizado en España. El alcalde porteño visitó las ciudades de Madrid y Bilbao y logró conocer los avances obtenidos en materia de modernización y construcción de sociedades digitales. El edil informó que en todo el mundo existen solo 128 ciudades digitales y Puerto Cortés podría convertirse en la 129 y la primera en Honduras.

¿Qué es una ciudad digital?

Es una ciudad que se consigue con alto grado de tecnología, en la prestación de sus servicios públicos y en casi toda la parte administrativa, más que todo las oficinas municipales sin papel, donde todos los datos de la ciudad estén en una base de datos y se pueda dar respuestas más eficientes a los ciudadanos.

¿Qué beneficios tiene para la Municipalidad pasar a ser una ciudad digital?

Tener la mayor agilización de trámites e información de los ciudadanos a través de un portal o una página web, para otorgar de forma más rápida permisos de operación, construcción, solvencias municipales y va permitir que todo el catastro del municipio esté totalmente digitalizado.

¿Está listo Puerto Cortés para convertirse en una ciudad digital?

[194] Idem Referencia 29

[195] http://www.laprensa.hn/honduras/valledesula/341558-98/allan-ramos-puerto-cort%C3%A9s-ser%C3%A1-una-ciudad-digital

Sí. Solo que necesitamos mucha capacitación del personal y una buena inversión económica, pero es algo necesario porque todas las ciudades que van creciendo se están enfocando en este nuevo modelo que viene a beneficiar a todo el municipio.

¿De dónde adoptó el modelo para convertir a Puerto Cortés en una ciudad digital?

Hemos estado observando el desarrollo de otros lugares y en Centroamérica ya existen algunos países que tienen ciudades digitales, como ejemplos la ciudad de Guatemala; en Costa Rica la ciudad de San José y en Panamá, San Miguelito, pero en Honduras, Puerto Cortés sería la primera ciudad en tener esta nueva dministración tecnológica, que vendrá a beneficiar a la Municipalidad y a la población.

¿Cuánto es la inversión municipal para tal fin?

Para una ciudad como Puerto Cortés se debe iniciar con una inversión de 350,000 dólares, pero para completar el proyecto se necesitan alrededor de 2.5 millones de dólares, en cuanto a mantenimiento y capacitaciones de los empleados.

¿Qué otros proyectos importantes se están realizando?

Estamos trabajando con las autoridades de la Secretaría de Seguridad para que podamos sacar el centro penal de la ciudad y trasladarlo a un lugar más seguro, donde exista espacio suficiente para las personas que están recluidas, porque actualmente lo que tenemos es una bomba de tiempo que se convierte en un peligro para el municipio.

Avances de una ciudad emergente e inteligente.

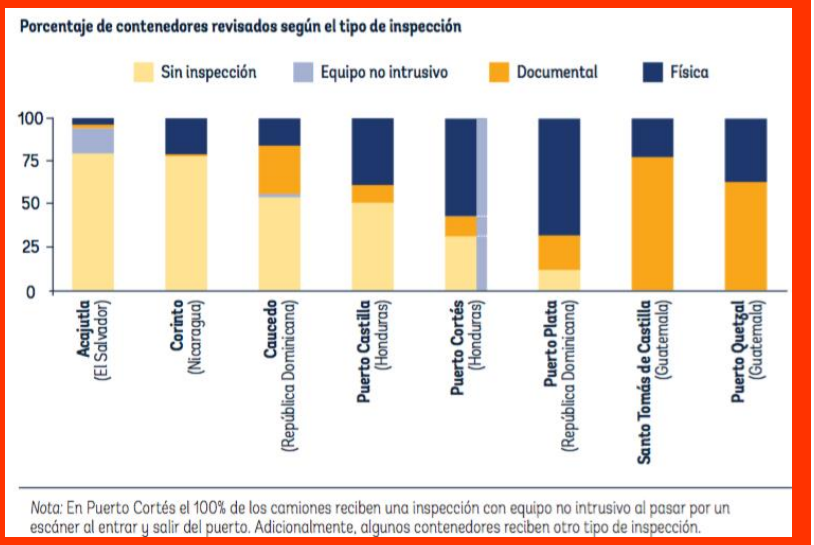
La ciudad más competitiva para las pequeñas y medianas empresas de Honduras es Puerto Cortés. Así lo revela el informe "Doing Business en Centroamérica y la República Dominicana", que fue presentado ayer por representantes del Banco Mundial (BM) a funcionarios, empresarios y delegados de sectores ligados a las Mipymes. El estudio preparado por los expertos Federic Bustello y Mario Nascimento es el primer documento subnacional que elabora el BM. El informe fue financiado por la Agencia de Estados Unidos para el Desarrollo Internacional (USAID) y el Departamento de Relaciones Exteriores, Comercio y Desarrollo de Canadá (DFATD).

Según este estudio[196] Puerto Cortés se situa en tecer lugar despues de Ciudad Panamá y Tegucigalpa con la menor composición de costos para apertura empresarial y puntualiza en que la observancia de esta experiencia puede orientar esfuerzos de reforma para reducir la carga para los emprendedores. La Alcaldía de Puerto Cortés redujo a 4 días la revisión preliminar mediante una ventanilla única que agrupa varias dependencias, como el Departamento Municipal Ambiental y las empresas de servicios públicos, situándola en la tercera ciudad dónde es más fácil obtener un permiso de construcción después de León (Nicaragua) y San Pedro Sula (Honduras). Considerando el fortalecimiento de la coordinación en la municipalidad y la promoción del intercambio de información entre dependencias a través de ventanillas únicas, la creación de ventanillas únicas representa un reto importante ya que se requiere de la participación de varias agencias. En la región sólo Puerto Cortés y Ciudad de Guatemala las han implementado eficientemente, lo que permite efectividad en una gestión pública local centrada en los ciudadanos y ciudadanas, fomentando facilidades participativas y de cohesión social.

[196] http://espanol.doingbusiness.org/~/media/GIAWB/Doing%20Business/Documents/Subnational-Reports/DB15-Central-America-and-the-Dominican-Republic-Spanish.pdf página 31

En materia de registros de propiedad Puerto Cortés se encuentras en el onceavo (11) lugar de las ciudades evaluadas por el Banco Mundial, después de San José (Costa Rica), San Salvador (El Salvador), Panamá (Panamá), Quetzaltenango (Guatemala), Ciudad de Guatemala (Guatemala), Escuintla (Guatemala), Cobán (Guatemala), San Miguel (El Salvador), Santa Ana (El Salvador), Soyapango (El Salvador) en su orden respectivamente.

Figura 40: Porcentaje de contenedores revisados según el tipo de inspección



En Puerto Cortés el 100%[197] de los camiones reciben una inspección con equipo no intrusivo al pasar por un escáner al entrar y salir del puerto. Adicionalmente, algunos contenedores reciben otro tipo de inspección. Esas acciones sobre la Seguridad y Convivencia Ciudadana, aplicadas al desarrollo humano en los territorios representan un activo invaluable, para la promoción de aspectos de Seguridad Humana como el desarrollo económico, la salud y la educación.

Ciudades inteligentes

Para el observatorio de la descentralización y la democracia local en América Latina y el Caribe, una 'Ciudad Inteligente[198]' es la respuesta a los retos del futuro, la respuesta que todo ciudadano busca, con una administración pública eficiente que genera nuevas respuestas sobre la base de la tecnología. En estas ciudades todo cobra importancia: desde la energía hasta los transportes, pasando por el mobiliario urbano. Todo ello ofrece una información al ciudadano y da respuesta a un nuevo entorno global.

Las 'Ciudades Inteligentes' representan el concepto de las urbes del futuro a través del uso intensivo de las tecnologías de vanguardia. De esta manera se consigue una gestión eficiente de los recursos económicos en la planificación, gestión y operación de los diferentes servicios municipales a los ciudadanos.

Tienen como objetivo mejorar la calidad de vida de sus habitantes, aumentar la eficiencia de los servicios públicos, incrementar la participación de los ciudadanos en ellos, mejorar las condiciones de sostenibilidad medioambiental y aumentar las oportunidades que la ciudad ofrece a las personas y a las empresas.

Para el desarrollo de una 'Smart City', contempla desde el plano tecnológico hasta la gestión e integración de la información, qué decisiones serán automatizadas, pasando por el plano de interacción con los ciudadanos como la movilidad, los servicios urbanos, la energía, el medio ambiente o la seguridad.

[197] http://espanol.doingbusiness.org/~/media/GIAWB/Doing%20Business/Documents/Subnational-Reports/DB15-Central-America-and-the-Dominican-Republic-Spanish.pdf

[198] http://www.observatoriodescentralizacion.com/index.php?option=com_content&view=article&id=246:ciudades-inteligentes-la-tecnologia-al-servicio-del-ciudadano&catid=35:inicio

Para poder llevar a cabo la 'Ciudad Inteligente' plantea una serie de retos de gestión y organización, una estrategia que ayuda a las administraciones a considerar cómo se organizan estas ciudades, pasando por los modelos de negocio públicos-privados que son necesarios seguir.

Ejemplos de aplicaciones en las ciudades inteligentes:

- Dispositivos que en tiempo real miden el tráfico sobre diferentes vías, con el fin de informar a los conductores (para mejor elegir su itinerario) y también para facilitar las decisiones públicas (políticas de urbanización, y de trazado y ampliación de vías de circulación).
- Dispositivos que marcan en tiempo real la ocupación de los estacionamientos públicos y de lugares para alquilar autos o bicicletas, para permitir un mejor servicio a los usuarios, y optimizar el uso de los espacios y de los vehículos de transporte.
- Geo localización en tiempo real de los vehículos de transporte colectivo, lo que permite una estimación fina de las horas de arribo a los distintos lugares, complementado con información en las distintas paradas.
- Dispositivos que miden los niveles de carga de los contenedores de basura, con el fin de optimizar la recolección.
- Medidas de los niveles de polución (CO2, ozono, calidad del agua) en tiempo real, para permitir alertas diferenciadas a la población, y para mejorar las políticas públicas en base a una cartografía dinámica y detallada.
- Medidas en tiempo real de alertas sobre peligros (inundaciones, incendios, tormentas, huracanes), para permitir una mejor respuesta de los servicios de socorro así como la evacuación preventiva de las poblaciones más amenazadas.
- Vídeo-vigilancia urbana.

5.7. Gestión Pública y las soluciones de TICs para la Seguridad Ciudadana el caso de Tegucigalpa AMDC, departamento Francisco Morazán en Honduras.

Observatorio de Convivencia y Seguridad Ciudadana en el Distrito Central.

La Alcaldía Municipal del Distrito Central aprobó el 23 de Octubre del 2014 en cabildo abierto, el Plan de Convivencia y Seguridad Ciudadana. -La propuesta contempla la creación de un Consejo Municipal de Seguridad, un Comité Municipal y un Observatorio Local de la Violencia para el Distrito Central. El documento fue elaborado en conjunto con el Programa de las Naciones Unidas (PNUD) y la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El plan incluye un diagnóstico de la inseguridad en el municipio, con un mapeo de principales problemas del 2013, cuando se reportaron 965 homicidios. El informe del año anterior destaca que las colonias de Tegucigalpa y Comayagüela con mayor incidencia de muertes violentas fueron: Villanueva, Flor del Campo, Nueva Suyapa, El Carrizal No. 1, Las Torres, Villa Cristina, Torocagua, Canaán, El Sitio y Zapote Norte. Con mayor número de femicidios se ubican: Campo Cielo, Villanueva, El Pedregal, La Peña y Las Brisas. Mientras que las colonias con más números de delitos relacionados con drogas fueron Villanueva, Kennedy, Nueva Suyapa, Hato de Enmedio y Oscar A. Flores.

Las autoridades de la Alcaldía Municipal y la Secretaría de Seguridad de Honduras suscribieron el 10 de diciembre del 2014 un convenio para implementar el Observatorio de Convivencia y Seguridad Ciudadana en el Distrito Central.

Esta herramienta, utilizada actualmente por el Instituto Universitario en Democracia Paz y Seguridad (IUDPAS), permitirá realizar evaluaciones para crear políticas para reducir los índices de violencia y criminalidad en la capital de Honduras.- Asimismo, el observatorio incluye actividades de monitoreo en áreas que tienen relación con el desarrollo del municipio para buscar los correctivos necesarios.- La firma se llevó a cabo entre los titulares de la comuna, el alcalde Nasry Asfura, y el ministro de Seguridad, Arturo Corrales, además que participaron los alcaldes de otros 29 municipios de Honduras. La iniciativa de un observatorio municipal se incluye en el Plan Local de Convivencia y Seguridad Ciudadana de la comuna.-Esta

propuesta fue aprobada hace dos meses en cabildo abierto y fue elevada a la Secretaría de Seguridad para su certificación y recibir fondos de la tasa de seguridad, reveló Asfura.- Cabe apuntar que tras la firma, la comuna recibió equipo de oficina para crear el observatorio.

Como parte de las acciones de organización y gestión de conocimiento de la Alcaldía Municipal, para el fortalecimiento de las acciones de planificación y gestión pública del Observatorio, realizará del 6 al 8 de Noviembre del 2015, **El hackathon de innovación ciudadana de Tegucigalpa**[199] es un evento para generar soluciones innovadoras para la ciudad usando datos abiertos. El objetivo es diseñar soluciones tecnológicas para abordar los principales desafíos de la ciudad, que a grandes rasgos son: saneamiento del río Choluteca, gestión de riesgos naturales, vivienda y comercio y seguridad ciudadana.

El evento está organizado de manera conjunta por el Municipio del Distrito Central y el Banco Interamericano de Desarrollo (BID). Está enmarcado dentro de la Iniciativa de Ciudades Emergentes y Sostenibles del BID, de la que la ciudad de Tegucigalpa forma parte, donde se trataran los temas de:

Figura 41: Ciudades Emergenges y Sostenibles

Fuente: *Banco Interamericano de Desarrollo (BID)*

El hackaton de innovación ciudadana de Tegucigalpa[200] es un evento para generar soluciones innovadoras para la ciudad usando datos abiertos. El evento está organizado de manera conjunta por el Ayuntamiento de Tegucigalpa y el Banco Interamericano de Desarrollo. Está enmarcado dentro de la Iniciativa de Ciudades Emergentes y Sostenibles del BID, de la que la ciudad de Tegucigalpa forma parte.

El objetivo del hackaton es abordar los desafíos de la ciudad identificados por la metodología de Iniciativa de Ciudades Emergentes y Sostenibles (ICES). A grandes rasgos son: saneamiento del río y las zonas aledañas, gestión de riesgos naturales y vivienda y comercio en el Distrito Central y seguridad ciudadana. El evento se presenta como un hackaton, y va precedido de un ciclo de conferencias y debates sobre los desafíos de la ciudad y el potencial del conocimiento abierto para resolverlos.

Audiencias meta

El hackaton pretende servir como un punto de encuentro para audiencias de distinta naturaleza y que normalmente no suelen interactuar. A continuación se describe quiénes son y qué pueden aportar al evento:

Policy Makers

Los policy makers son diseñadores de políticas y especialistas sectoriales que tengan un conocimiento avanzado sobre las problemáticas expuestas. Se espera que representen un 20% de la audiencia total.

[199] http://hacktegus.com/
[200] **http://hacktegus.com/index.php/2015/09/30/tegucigalpa-convoca-su-primer-hackaton-de-innovacion-ciudadana/#.Vi_Co3srKHs**

Hackers

Los *hackers* son desarrolladores informáticos que aportan al evento una capacidad de expresar tecnológicamente la solución diseñada. Se espera que representen el 60% por ciento de la audiencia.

Periodistas y comunicadores

Los expertos en comunicación y diseñadores gráficos se encargan de hacer trabajar en la descripción de la solución y en la adaptación del diseño de la aplicación para que sea fácilmente comprensible para la audiencia objetivo. Se espera que representen un 20% de la audiencia.

Productos y resultados esperados del hackaton

Este hackatón pretende incrementar la visibilidad del potencial de los datos abiertos[201] como medio para resolver problemas de las ciudades, e involucrar a los ciudadanos en el debate sobre el desarrollo sostenible de la ciudad. De manera secundaria, el evento servirá para dar a conocer la metodología de la Iniciativa de Ciudades Emergentes y Sostenibles, y la estrategia de la municipalidad para la promoción del emprendimiento y la innovación tecnológica en la ciudad.

Productos esperados

- Un mapeo del ecosistema abierto de Tegucigalpa.
- Un evento de colaboración multisectorial donde haya participantes del municipio, sector privado, organizaciones ciudadanas y ciudadanos a título individual, enfocado en el desarrollo de aplicaciones tecnológicas, web y móviles que resuelvan problemáticas de la ciudad y promuevan la innovación ciudadana.
- Un portal de datos abiertos con bases de datos municipales limpias y legibles para aplicaciones informáticas y para el público general.
- Prototipos de aplicaciones tecnológicas, web y móviles.
- Información para el observatorio.

[201] **http://hacktegus.com/index.php/2015/10/14/tres-retos-urbanos-en-tegucigalpa-y-el-potencial-de-los-datos-abiertos/#.Vi_Cp3srKHs**

Tabla 19: Socios organizadores del hackathon de innovación ciudadana de Tegucigalpa

Socios organizadores del hackathon de innovación ciudadana de Tegucigalpa	
Municipio	La ciudad de Tegucigalpa, a través de la Gerencia del Centro Histórico es la promotora principal del proyecto. El hackaton coincidirá con el lanzamiento de un portal de datos abiertos de la municipalidad. Aporta recursos humanos y financieros para la celebración del hackaton así como bases de datos del municipio.
Universidad Nacional de Honduras (UNAH)	La Universidad Nacional de Honduras apoyará al municipio en las tareas de limpieza y carga de bases de datos en el portal de datos abiertos, en la convocatoria y ejecución del evento. Durante el evento, apoyará a los jóvenes desarrolladores en el desarrollo de sus ideas. Colabora con la ciudad de Tegucigalpa para facilitar el contacto con las redes locales de hackers y aporta conocimiento técnico y apoyo para los desarrolladores
Banco Interamericano de Desarrollo (BID)	El BID, a través de la Iniciativa de Ciudades Emergentes y Sostenibles, dará apoyo metodológico y técnico para la celebración del evento y contribuirá a la financiación del evento y a la generación de alianzas con terceros.
Socios colaboradores	
Museo de la Identidad Nacional	Aporta el espacio para la organización del evento
Hondutel	Ancho de banda para la conectividad durante el evento
Tigo	Diseño de la estrategia de comunicación y convocatoria y premiación. Formar parte del jurado con acciones de comunicación y visibilidad de Tigo en el espacio del evento.
INFOP	Formar parte del jurado, con acciones de comunicación y visibilidad de INFOP en el espacio del evento.

Como facilidad de réplica e impacto un HACKTHON es una oportunidad, no solo para el levantamiento de información y desarrollo de herramientas para el gobierno local, permite realizar observancia para temas prioritarios de una ciudad emergente.

5.8. TICs en la Seguridad Ciudadana como prioridad para el Desarrollo comunitario y nacional

El caso de HONDURAS CONVIVE 202

Honduras Convive, nace con una visión de apoyar la reducción de la tasa de homicidios y crímenes violentos a través de alianzas entre ciudadanos y el estado. Con el objetivo de interrumpir patrones, sistemas y percepciones que fortalecen la violencia, estratégicamente trabajando para mejorar la seguridad comunitaria en zonas y sectores meta y aumentar la confianza ciudadana en las instituciones gubernamentales (Honduras Convive Strategy draft).

El Programa Honduras Convive, es un espacio que ha permitido abordar territorialmente la inseguridad ciudadana estableciendo redes locales de convivencia pacífica para desarrollar acciones enfocadas a la prevención de la violencia, la promoción de la paz y la seguridad ciudadana. Esta iniciativa considero dentro de sus prioridades atender a las personas adolescentes y jóvenes con necesidades de contar con sistemas locales de promoción de ambientes comunitarios seguros, herramientas para la resolución alternativa de conflictos y la atención temprana de situaciones de riesgos en sus comunidades, así como la atención de instituciones del estado de Honduras y de la Sociedad Civil.

Estos procesos fueron desarrollados mediante facilidades organización desde las y los jóvenes, a través de su organización en las redes locales de juventud, trabajando bajo metodologías participativas y vivenciales como “escucha activa” y el “trabajo de pares”, es decir escuchando el sentimiento de los y las jóvenes alrededor de sus intereses, su sueños y la conversión de sus “opciones” en “realizaciones” con un enfoque de desarrollo humano juvenil y fomento de género.

Redes Sociales en la Prevención de Violencia.

Proceso de Comunicación Social y Liderazgo financiada por Creative y USAID para crear una campaña de comunicación social basada en el uso de redes sociales y actividades comunitarias en las colonias La Era y La Travesía. Donde un grupo de 25 jóvenes hacen conciencia sobre la importancia del respeto a la vida y la paz, con su campaña denominada Yo Doy Paz[203].

Este proceso promueve, en la población la sensibilidad hacia las muertes y el dolor. La campaña promueve el respeto a la vida donde los jóvenes han realizado actividades comunitarias que van desde la creación de murales interactivos, el marcaje de calles, actividades comunitarias en Iglesias.

Figura 42: Foto campaña de comunicación social basada en el uso de redes sociales y actividades comunitarias en las colonias La Era y La Travesía

Fuente: *Elaboración propia*

[202] Contacto Honduras Convive, Sra Noy Villalobos, noyv@creahonduras.com
[203] http://www. libreexpresion.org/proyectos/

Hackathons para la Seguridad Ciudadana

Durante el 2014 y 2015, eventos apoyados por el pueblo y gobierno de los Estados Unidos de Norte América a través de la Agencia para el Desarrollo Internacional (USAID), así como por la oficina de Transición Internacional (OTI), a través de Honduras Convive, han patrocinado iniciativas de ICT4D (TICs para el desarrollo) que buscan crear actividades a favor de la comunidad, sobre el tema de seguridad ciudadana con aplicaciones que generan apoyo ciudadano a la Policía, como plataformas para reporte de robos, identificación de rostros y otras que puedan servir en la lucha por obtener seguridad y facilitar la respuesta de los operadores de Seguridad

Honduras 911 [204], es una APPs, que fomenta una comunidad donde las personas pueden reportar hechos delictivos o emergencias usando un Smartphone, que está en proceso de desarrollo y prueba para su integración al sistema oficial 911, potenciando iniciativas de ciudadaes y gobiernos emergentes e inteligentes en Honduras, que pueden tener una facilidad de réplica regional.

Figura 43: 911 - Honduras

Implementaciones de Sistemas de Inteligencia Forense en proceso de desarrollo en Honduras

Desde el 2014 Honduras Convive, apoya el proceso gestión de conocimiento y la investigación forense, a través del Sistema de Información para Gestión Pericial (SIGEP), con el Ministerio Público a través de la Dirección de Medicina Forense, en tres áreas:

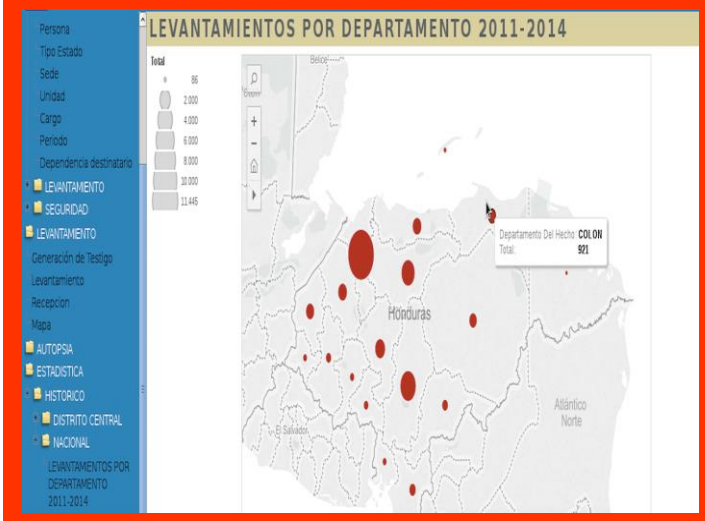
- Patología,
- Clínica y
- Laboratorios.

El Sistema en proceso de desarrollo, esta permitiendo de forma gradual mejorar la habilidad del departamento de Medicina Forense para eficientar la recolección de información, que permita compartir de forma confiable la información concerniente a la investigación criminal con otras instituciones, como ONGS, Observatorios y el público en general, bajo una facilidad de Gobierno Abierto(Open Government).- Lo que ha demandado integrar un sistema de gestión de información para ser gradualmente implementado por la Dirección de Medicina Forense.

[204] https://twitter.com/honduras911

Honduras Convive también ha facilitado el lanzamiento de una revista de Ciencias Forenses de Honduras que ha sido indexada en el portal de la Biblioteca virtual de Salud BVS de Honduras [205], que facilita el análisis de estadísticas y datos de crimen para el público, y su correspondiente tratado para publicación por diversos expertos en Seguridad Ciudadana.- Este Sistema de gestión de conocimiento también potencia de forma gradual el primer Observatorio Forense a nivel regional[206] con Componentes Permanentes de Investigación, Informes de históricos por oficinas regionales, Informes en base a la evidencia, Banco de Buenas Prácticas Forenses, Observatorio que estará funcional para la gestión de conocimiento a inicios del año 2016.

Figura 44: Sistema de Información para la Gestión Pericial de Honduras



5.9. TICs para Observatorios

El Instituto Universitario en Democracia Paz y Seguridad (IUDPAS)

El IUDPAS es el resultado del apoyo del Programa de las Naciones Unidas para el Desarrollo y de la Agencia de Cooperación Sueca para el Desarrollo Internacional, a través del Proyecto Armas Pequeñas y Seguridad y Justicia y en segunda etapa El Proyecto Seguridad Justicia y Cohesión Social, cuyo socio de implementación es la Universidad Nacional Autónoma de Honduras.

Figura 45: Gráfico de la biblioteca Instituto Universitario en Democracia, Paz y Seguridad (IUDPAS)

Fuente: *IUDPAS, UNAH*

El IUDPAS, Fue creado por la Comisión de Transición de la UNAH[207] (CT-UNAH) según el Punto N° 7 del Acta N° 157-2008, sesión celebrada el 22 de enero 2008, transcrito en oficio N° CT-UNAH-126-2008 con fecha 14 de febrero de 2008. En la actualidad, a través de la publicación de información estadística, desarrollo de investigaciones y la formación de capacidades a través de los diplomados universitarios y cursos especializados, se ha convertido en un referente confiable y objetivo en Honduras en materia de seguridad, paz y democracia. El IUDPAS, en alianza con el Instituto Nacional Demócrata (NDI), crea el repositorio Institucional de su biblioteca virtual cuya finalidad es la de poner a disposición de la población hondureña literatura en materia de derechos humanos, seguridad y democracia que permita generar conocimiento y mejorar la comprensión de las

[205] http://www.bvs.hn/RCFH/flash/1/#/0

http://www.bvs.hn/RCFH/html/RCFH.htlm

[206] https://www.mp.hn/Forense/estudio-y-analisis/

[207] http://www.tzibalnaah.unah.edu.hn:8080/handle/123456789/2

causas fundamentales de la violencia en Honduras a fin de propiciar el debate público e incidir en las propuestas que en materia de seguridad y justicia se implementan en el país.

La UNAH, en el marco de la reforma universitaria que actualmente impulsa, propicia la creación del IUDPAS que tiene como propósito central fortalecer los vínculos entre la investigación, la docencia y la Universidad-Sociedad. El instituto fue creado por la Junta de Transición de la UNAH mediante Oficio No. CT-UNAH-126-2008 de fecha 14 de febrero del año 2008, adscrito a la facultad de Ciencias Sociales.

Tabla 20: Datos del Instituto Universitario en Democracia Paz y Seguridad (IUDPAS)

	Datos **Instituto Universitario en Democracia Paz y Seguridad (IUDPAS)**	
	Nombre de la institución	**Instituto Universitario en Democracia Paz y Seguridad (IUDPAS)**[208]
	Redes Sociales:	Facebook: https://www.facebook.com/iudpas Blog: https://2013dmccc.wordpress.com/
	Datos de contacto	Teléfono: Tel: (504) 2292-1496 Email: info@iudpas.org Ciudad Universitaria, Edificio IUDPAS, Tegucigalpa

Sobre el Observatorio de la Violencia[209]

Su objetivo es sistematizar, clasificar, analizar y construir conocimiento sobre muertes violentas y no intencionales, y sobre lesiones de causa externa, que contribuya a mejorar los niveles de información de los funcionarios, tomadores de decisiones y diseñadores de políticas públicas; de académicos e investigadores del tema para contribuir a tener estudios de mayor calidad; a ONG para apoyar mejores formas de intervención; y a la ciudadanía para apoyar una mejor comprensión del problema.

Socios Estratégicos:

- Programa de las Naciones Unidas para el Desarrollo (PNUD)
- Agencia de los Estados Unidos para el Desarrollo Internacional (USAID)
- Agencia de Cooperación Española Internacional para el Desarrollo (AECID)
- Alianza Joven Regional (USAID/SICA)
- La Agencia Sueca de Desarrollo Internacional (ASDI)

Fuentes de Información:

- Medicina Forense
- Policía Nacional
- Dirección nacional de investigación Criminal
- Dirección nacional de transito

[208] http://iudpas.org/quienes-somos

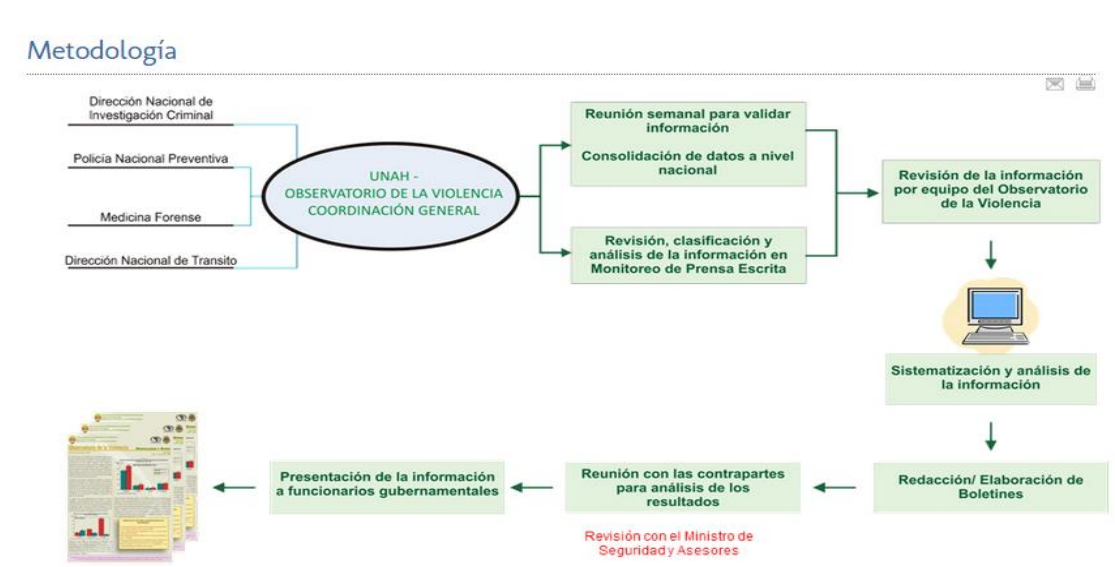
[209] http://iudpas.org/observatorio

Socios Estratégicos:

- Medicina Forense del Ministerio Público
- Gobiernos locales
- Secretaría de Seguridad
- Sociedad civil
- Centros universitarios Regionales
- Académicos
- Cooperación Extranjera

La metodología de estudio y análisis para gestión de conocimiento basado en la evidencia se describe a continuación:

Figura 46: Ejes principales del PICSC al 2023



Fuente: *IUDPAS, UNAH*

Historia de los Diplomados Universitarios

El problema de inseguridad, la injusticia y la falta de convivencia son problemas sociales que preocupan a los hondureños y hondureñas. El Estado y las organizaciones no gubernamentales han enfrentado el problema con una alta dosis de improvisación y empirismo ante la ausencia de investigaciones profundas que orienten el diseño de las políticas públicas. A falta de políticas públicas adecuadas para enfrentar los problemas, las respuestas tienen un carácter más reactivo orientado al control de la seguridad, que preventivo.

No existe en ninguna de las Universidades en el país, ni en las estatales ni en las privadas, centros de investigación que trabajen el tema de la violencia y la delincuencia, ni carreras con planes y programas de estudios orientados al tratamiento y comprensión de este problema, el trabajo del IUDPAS vinculado a la formación constante y reconocido por sus contenidos, actualmente los fondos que sostienen a IUDPAS en su mayoría son de fuente nacional, cuenta con la colaboración de cooperantes para proyectos locales y facilidades de investigación.

IUDPAS y la Prevención de violencias

Fortalece la capacidad de los actores educativos formando agentes de prevención de violencia en la escuela y la familia, mediante la

1. Formación de liderazgo juvenil en promoción de valores para la convivencia y la mediación escolar que permitan generar capacidades para la resolución de Conflictos.
2. Formar liderazgos en docentes, padres y madres de familia con el fin de crear estrategia destinada a disminuir y prevenir las expresiones de violencia en la escuela y la familia.
3. Establecer espacios de expresión artística, cultural y deportiva que permita a los involucrados el aprovechamiento del tiempo libre en el desarrollo de sus habilidades y destrezas.

La presente propuesta "Prevención de la Violencia en Centros Educativos" es parte del Proyecto Seguridad, Justicia y Cohesión Social que se desarrolla en tres departamentos del país mediante un convenio tripartito entre el Programa de las Naciones Unidas para el Desarrollo, la Secretaría de Educación y tres institutos públicos emblemáticos de los departamentos de Olancho, Choluteca y Comayagua, con fondos de la Agencia de Cooperación Sueca para el Desarrollo Internacional (ASDI).

Este proyecto se basa en la experiencia exitosa desarrollada desde el año 2005 en el Instituto Técnico "Luís Bográn", cuyas acciones se implementan en 35 centros educativos de la Capital de la República de Honduras , desde donde se han impulsado acciones de capacitación y formación de liderazgos en prevención de violencia y resolución pacífica de conflictos con todos los actores del área de educación.

Dado el éxito obtenido en dicho proyecto, los organismos cooperantes se han propuesto extenderlo a tres departamentos del país a través de la organización de un centro piloto en los institutos "León Alvarado" de Comayagua, "La Fraternidad" de Juticalpa y "José Cecilio del Valle" de Choluteca, con sus respectivos centros asociados.

Conclusiones del estudio

La Seguridad Ciudadana busca llevar a la ciudadanía una garantía de sus derechos y deberes, con una función incluyente de la sociedad y de las instituciones.- Esto es vinculante a una administración pública que no solo se sirva de las TICs para llegar a sus ciudadanos, sino que además sea capaz de idear los medios incluyentes para que los ciudadanos sean escuchados (sobre su protección personal, los abordajes prevención de violencias, delitos, conflictos, recepción y respuesta a denuncias, etc.) y puedan tener injerencia en la gestión pública de la Seguridad Humana (disuasión, formas de vigilancia comunitaria con el uso TICs, apoyo en emergencias cotidianas, respuestas vinculadas a la gestión de riesgos, sistemas de protección humana, etc), que permita consolidar bienes públicos locales, nacionales y regionales, para estos grandes males públicos existentes como la inseguridad, (principalmente con facilidades de participación, normativa y de inversiones en TICs), a continuación se enuncian una serie conclusiones vinculadas al análisis, el estudio y la recepción de información por parte de los países:

Tabla 21: Tabla de conclusiones

Sobre	Se concluye que:
1. Soluciones tecnológicas	Que se demanda fortalecimiento de normativa nacional y homologación regional de procesos para garantizar la: e) **Calidad**: procurando que los productos de las soluciones tecnológicas en base al uso de TICs desarrolladas o adquiridas, cumpliendo con los requerimientos especificados con calidad para uso y aplicación de la Seguridad Ciudadana y Pública. f) **Desarrollo**: de un marco de referencia para la construcción de soluciones tecnológicas en base a TICs, incluyendo la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios a nivel regional. g) **Definición de requerimientos**: para el desarrollo de soluciones mediante acciones coordinadas con las unidades responsables solicitantes como los operadores de Justicia y de Seguridad. h) **Administración**: definiendo compromisos y costos de servicios de TICs necesarios para mantener el adecuado funcionamiento de la Seguridad Ciudadana y Pública bajo facilidades predictivas de servicios. i) **Innovación**: para identificar iniciativas de creación de servicios de TICs susceptibles de aportar beneficios importantes en el cumplimiento de los objetivos estratégicos de la Justicia y la Seguridad Ciudadana en temas como Cibercrimen, desarrollo de Apps e Inteligencia de Observatorios.
2. Medición de Impacto	Se detecta una brecha en la medición de impacto de las TICs en la ciudadanía, que debe ser realizada considerando dos facilidades básicas: a) El monitoreo y evaluación de los resultados en la seguridad, alrededor de la respuesta que se demanda. b) El grado de efectividad en la atención de las emergencias cotidianas y riesgos por situaciones naturales, desagregando la eficiencia (institucional) y la eficacia(social).
3. Gestión de la Respuesta a la Ciudadanía	En el entorno actual la presentación de soluciones de tecnologías para la Seguridad Pública en la gestión de la respuesta a la Ciudadana se centra esencialmente en: a) **Generar herramientas y aplicaciones para la denuncia**: en múltiples plataformas, por medios digitales y análogos, a través de dispositivos fijos o móviles Los países deben considerar que en curso existen buenas prácticas regionales que consideran incluir los siguientes niveles b) **Innovación y Desarrollo de Instrumentos para la Prevención Social**: basado en la evidencia que permite la caracterización de patrones y tendencias para proveer información por medios digitales a los ciudadanos para desarrollar acciones preventivas para no ser víctimas de las violencias, los delitos y las conflictividades. c) **Gestión de Conocimiento para Sociedad:** aplicaciones principalmente para atender problemas de violencias, delitos y

Sobre	Se concluye que:
	conflictividades en niños, niñas y jóvenes, como población más vulnerabilizada. d) **Innovación Participativa:** con TICs que incrementan la capacidad de la ciudadanía para participar en los asuntos públicos en materia de Seguridad y emergencias cotidianas, incidiendo en bajar la incidencia de violencias, delitos y conflictividades mediante el incremento masivo de la denuncia
4. Gestión de Conocimiento social	Se necesita el fortalecimiento de facilidades de TICs en los Observatorios de Seguridad Ciudadana sobre aspectos importantes para su operatividad, considerando buenas prácticas regionales y continentales para: 1. **Conocer lo que sucede**: sobre la incidencia delictiva, de violencias y conflictividades accediendo a bases de datos de fuentes primarias para el conocimiento objetivo de la inseguridad. 2. **Conocer lo que siente la ciudadanía**: mediante encuestas e instrumentos de percepción de la seguridad y la convivencia, el miedo al delito y la percepción de la victimización, para el conocimiento subjetivo y de contexto de la inseguridad. 3. **Conocer lo que se hace**: seguimiento a la efectividad de las intervenciones en materia de seguridad de las políticas, modelos, y regulaciones vigentes y aplicadas principalmente por gobiernos (centrales y locales) en base al estudio y análisis realizado.
5. Estándares	Se necesita evaluar las facilidades del cumplimiento de estándares de instituciones como Cellular Telephone Industries Association (CTIA) [210][211] que orientan en las facilidades de compartir textos, imágenes, video y voz, sobre servicios inalámbricos para mejorar el enfoque de cómo ser los primeros en responder y manejar las emergencias con éxito considerando tres grandes ejes: 1) Los estándares operacionales 2) Los estándares técnicos 3) Los estándares de formación Que la CTIA [212] sitúa dos escenarios alrededor de la gestión de emergencias en sistemas tipo 911 • El denominado Enhanced 911 (E-911): tecnología que complementa la interacción entre los primeros sistemas de atención pública asegurando que todas las llamadas se desvían a un centro de llamadas y permiten transmitir información, incluyendo la ubicación, a un “punto de respuesta de seguridad pública” (PSAP en ingles) y

[210] CTIA - The Wireless Association , originalmente conocida como la Asociación de Industrias de teléfono celular
[211] http://www.ctia.org/policy-initiatives/policy-topics/911
[212] http://www.ctia.org/policy-initiatives/policy-topics/911

Sobre	Se concluye que:
	• Next Generation 911 (NG911): las acciones conjuntas con la seguridad pública, la industria inalámbrica y la iniciativa de los formuladores de políticas para actualizar la infraestructura de 911 para permitir que los PSAP sean capaces de recibir voz, texto, vídeo y mensajes multimedia. El estándar **CALEA**[213] de la Comisión de Acreditación para Agencias Policiales (CALEA) no es considerado a nivel regional para acreditar las comunicaciones de la Seguridad Pública CALEA tiene tres ejes esenciales: • **Acreditación de Comunicaciones de Seguridad Pública** • Acreditación de Cumplimiento de la Ley • Acreditación de la Academia de Capacitación en Seguridad Pública Se necesita de parte de UIT/COMTELCA un análisis y estudio para obtener una recomendación sobre las implicancias de las redes de comunicaciones de seguridad pública que deben y están evolucionando niveles IP multiprotocolo (Multiprotocol Label Switching MPLS) y con sus niveles comparativos de los estándares del Proyecto 25 (APCO 25), así como los basados en los protocolos TETRA (Terrestrial Trunked Radio), los basados sistemas de video vigilancia, de Long Term Evolution (LTE) y las ventajas de Digital Mobile Radio (DMR) que permita a los países acceder a mejores tecnologías para la Seguridad Pública.
6.Recomendaciones de UIT	Los países deben considerar aplicar en el inmediato plazo la Recomendación UIT-T E.161.1[214] que ofrece orientación a los Estados Miembros que se encuentran en el proceso de selección de un número de emergencia único por primera vez, o de un número de emergencia secundario alternativo para las redes públicas de telecomunicaciones. • Según esta recomendación **una llamada de emergencia** [b-UIT-T Q-Sup.47] se define como la: "Llamada que solicita servicios de emergencia. Se ofrece a la parte llamante una forma rápida y fácil de comunicar información relativa a una situación de emergencia a la organización competente (por ejemplo, bomberos, policía, ambulancias). Las llamadas de emergencia se encaminarán a los servicios de emergencia de conformidad con los reglamentos nacionales". - **Un número de emergencia** se define como el: "número de tipo distinto al E.164 atribuido en el **plan nacional de numeración** para efectuar llamadas de emergencia. Por regla

[213] http://www.calea.org/ , Commission on Accreditation for Law Enforcement Agencies (CALEA)
[214] Directrices para seleccionar el número de emergencia en redes públicas de telecomunicaciones (Recomendación UIT-T E.161.1) , Sector de Normalización de las Telecomunicaciones de la UIT (09/2008)

Sobre	Se concluye que:
	general, el número de emergencia suele ser un código abreviado".- En este sentido UIT recomienda a todo Estado Miembro que tenga previsto introducir un segundo número de emergencia alternativo podría considerar la posibilidad de utilizar el 112 o el 911, o ambos, el cual debería encaminarse hacia el número de emergencia vigente. El segundo número de emergencia alternativo resulta útil, por ejemplo, para las personas que se encuentran visitando al país y desean efectuar una llamada de emergencia.
7.Interoperabilidad	Las comisiones de regulación de los países deben de considerar la facilidad de la "conexión e interoperabilidad" que permite la regulación, su aplicación, el ordenamiento para que las TICs tomen un valor preponderante para atender las emergencias cotidianas y de Seguridad Pública, que permite estar vinculados y por consiguiente que instituciones puedan trabajar unas con otras.

Recomendaciones generales

Las Tecnologías de la Información y la Comunicación (TICs) ofrecen una variedad de herramientas y aplicaciones capaces de abrir nuevas posibilidades para la Seguridad Pública y Nacional de los países. En particular, las TICs pueden ayudar a adaptar el proceso de prevención de las violencias, los delitos y conflictividades principalmente urbanas, a las necesidades individuales de los ciudadanos, en sus comunidades, sus entornos en una posibilidad desde lo local a lo nacional y viceversa sin desvincular lo global, ya que muchas de las necesidades de coordinación son de carácter transnacional y global.

La solución para una utilización eficaz de las TIC en los temas de Seguridad, sin embargo, no reside en la propia tecnología. Se debe considerar el garantizar el acceso universal a las TICs, para lograr un éxito considerable, en este entorno es deseable que existan marcos regulatorios que permitan a avanzar en la comprensión sobre cómo emplear eficazmente las nuevas tecnologías y sobre donde existen obstáculos en el camino participativo hacia el éxito de una interoperabilidad técnica y social de las TICs.

Tabla 22: Tabla de recomendaciones

Se recomienda considerar las siguientes sugerencias
Considerar la integración de un comité regional con el apoyo de COMTELCA y UIT para que facilite el abordaje de una agenda conjunta de temas sobre TICs para la Seguridad Pública y Ciudadana, con temas de interés definidos por cada país y/o de forma conjunta vinculantes a nivel regional.
Facilitar una agenda regional a través de COMTELCA para el acceso ciudadano y las instituciones de seguridad pública a través de Apps (applications) para labores diarias y de gestión general de las actividades de Seguridad y Convivencia Ciudadana en los paises.
Considerar la facilidad de asociatividad abordada con la Cámara de Comercio, Industrias y Agricultura de Panamá (CCIAP) para consolidar a través de Centro de Estudios especializado en Banda Ancha para el Desarrollo (CEABAD) un Centro Virtual de Formación para la Seguridad Ciudadana

Se recomienda considerar las siguientes sugerencias

Se recomienda considerar la elaboración de un libro blanco, como base protocolar para la operatividad de un observatorio regional que permita brindar asistencia a los países sobre:

- **Interoperabilidad** sobre las capacidades técnicas, organizacionales, de gobernanza y de innovaciones, necesarias en las TICs para compartir información y conocimiento de forma consistente.
- **Desarrollo de Sistemas** informáticos que ayuden a evaluar las tendencias y las probabilidades.
- **Indicadores estandarizados** para control de delitos , violencias y conflictividades.
- **Desarrollo de aplicaciones móviles** para extender las opciones de denuncias por medio de texto, imagen, video y audio y el uso de los medios sociales en comunicaciones de seguridad pública.
- **Integración de estándares de interoperabilidad** para reforzar el transporte de datos, imágenes, videos y voz en tiempo entre el policía, las patrullas, los ciudadanos y los centros con equipos base o tipo sistemas de despacho.
- **Marcos Jurídicos y Regulaciones** para la armonización del marco político y jurídico con la finalidad de propiciar un entorno de certeza y confianza favorables para la adopción y fomento de las TICs para la Seguridad Ciudadana.
- **Datos abiertos** para el análisis y estudio de Problemáticas mediante la facilidad de observatorio y centros de estudio y análisis para la disponibilidad de información gubernamental y de la sociedad en general en formatos útiles y reutilizables por la población en general, para fomentar la "toma de decisiones" a través de la gestión de conocimiento sobre seguridad pública y ciudadana.
- **Conectividad** para el fortalecimiento y desarrollo de redes (gubernamentales y ciudadanas) y la ampliación de una mejor infraestructura en los territorios, la ampliación de la capacidad de las redes existentes, y el desarrollo de competencias en el sector de TICs para estimular aplicaciones principalmente en las redes celulares de forma masiva.
- **Participación Ciudadana y Destrezas Digitales** en un desarrollo equitativo de habilidades para desarrollar y operar tecnologías y servicios digitales, contemplando la cobertura social y el desarrollo de habilidades en sistemas comunitarios, a través de hackathons, barcamps, veture, etc
- **Comunicación digital y Redes Sociales**: como una facilidad de empoderamiento y Sensibilización social para el apoyo de estrategias digitales, una comunicación digital centrada en la ciudadanía y sus necesidades como demandante de Seguridad y Convivencia, que provea servicios digitales en base a gestión de conocimiento, y no solo información.

A los países considerar el análisis interno sobre aspectos importantes vinculados a la interoperabilidad como los siguientes

- **Interoperabilidad**: como facilidad de interoperar a través de gran variedad de redes dispares (HF-VHF, VHF-UHF u otra combinación de bandas) y dispositivos de usuario. Extendiendo la cobertura de red de radio a través de la red IP
- **IP de Despacho**: sobre IP despacho y control, con interfaz gráfica de usuario simple y funciones de control avanzadas. despacho remoto
- **IP Radio Voting**: para comunicarse eficientemente con destino necesario y ahorrar recursos del sistema cubriendo aquellos "puntos muertos", sin cobertura con la facilidad de múltiples tecnologías

Considerando que la dinámica de contrarrestar la Inseguridad se desenvuelve principalmente alrededor del desarrollo de 2 facilidades como lo son :

1. Planes de Respuesta a Emergencias,
2. Planes de Comunicaciones para la Crisis

Se recomienda considerar que las TICs deben incidir, como un tercer elemento en la

Se recomienda considerar las siguientes sugerencias
3. Reunificación Familiar y la Cohesión Comunitaria mediante acciones de sensibilización y educación en la previsión y prevención, para lograr empoderamiento en la participación ciudadana en la lucha contra las violencias, los delitos y las conflictividades.
Instrumentos de Consulta el análisis y estudio delimita preliminarmente la necesidad de una agenda regional sobre la consideración de los temas siguientes: I. Consolidar un PROTOCOLO interoperabilidad, que considere integraciones para la Seguridad Pública de las TICs, bajo una visión de aprovechamiento de los avances regionales y nacionales. II. El desarrollo de recomendaciones para la implementación de TICs vinculadas principalmente en Identificación Balística, dactiloscopia, sistemas de Inteligencia Forense, Identificación y reconocimiento facial, Sistemas de Vigilancia Ciudadana a través de Cámaras de video (CCTV) con facilidad de posicionamiento de eventos, así como de detección de objetos por medios no invasivos (scanners) en puertos y fronteras que supere los rayos x tradicionales. III. En materia de OBSERVATORIOS el fomento de la gestión de conocimiento basada en la evidencia bajo la operatividad de "protocolos" definidos y las facilidades de OPEN DATA que facilite la orientación y comprensión de resultados en cada uno de los paises y a nivel regional. IV. El acompañamiento de los Centros de respuesta para incidentes informáticos (Computer Incident Response) en Guatemala, Costa Rica y Panamá, y su replica en el resto de paises de la región para consolidar los CSIRT nacionales. V. El uso de sistemas de Vigilancia y Monitoreo mediante Brazalete Electrónico y dispositivos de control de presencia interna en las cárceles, así como el uso de sistemas de pánico para el seguimiento de reclusos. VI. NO se detecta a nivel regional una experiencia integradora que permita el considerar una PLATAFORMA de seguimiento de la "Ruta" de la delincuencia común y organizada, incidente en la administración de Justicia, es decir una plataforma que integre los Sistemas de Justicia, Seguridad, Ministerio Público y observatorios al menos en un país. VII. El fomento de Sistemas de Información para la Gestión Pericial Forense que faciliten obtener "indicios" como los manejados por los cuerpos de Fiscalía. VIII. Considerar la experiencia de Guatemala con la Alerta Alba Keneth en la gestión de personas desaparecidas, así como el desarrollo de APPs (ALERTOS, ESPANTA CACOS, PNC MOVIL) para la Seguridad Ciudadana, como una facilidad de replica para los paises de la región. IX. Sistematizar rápidamente la experiencia de Honduras en cuanto a la normalización e implementación del bloqueo Celular en Centros Penitenciarios, para facilitar una incidencia en el nivel regional sobre el tema. X. Facilitar el intercambio de experiencias sostenido del 911 de Costa Rica y la práctica innovadora de República Dominicana sobre la atención de emergencias y urgencias, así como de una gestión transparente de sistemas 911 que vincula la educación de los diversos estratos de población. XI. Estudiar la facilidad de recomendaciones sobre la integración de Sistemas de información y Tecnologías del sistema Automated Fingerprint Identification System (AFIS), de Identificación y reconocimiento facial y de CCTV con la integración sensorial de audio (ShotSpotter), así como la migración de escaners de rayos x hacia escaners de rayos gamma. XII. Considerar la Experiencia de Costa Rica, específicamente del PANI en la lucha contra la trata de niñez y juventud, sus desarrollos en redes sociales para la prevención de violencias, delitos y conflictividades y facilitación de la denuncia como una experiencia de réplica regional.
Sistemas de inteligencia especializados y forenses: la normatización y regulaciones es de inmediata necesidad a nivel regional como parte del abordaje de las agendas, en las mesas nacionales de Seguridad y Convivencia Ciudadana.
Comunidades inteligentes y emergentes: Se detectan algunas iniciativas que se apoyan en TICs para fortalecer su desarrollo local en un ámbito más holístico, que parte de un Plan en Seguridad y

Se recomienda considerar las siguientes sugerencias
Convivencia Ciudadana, hacia una Agenda para el Desarrollo Local (ADEL), convirtiendo el papel de las TICs en incidentes para el desarrollo de las comunidades.
Políticas Públicas y Recomendaciones: se recomienda observar la iniciativa de Panamá en la Agencia para la Innovación Gubernamental (AIG) de contar con un equipo gestión estratégica interinstitucional y multisectorial para consolidar políticas, planes, proyectos para promover acciones de impacto en las TICs para la Seguridad Pública, como una oportunidad de réplica regional.
Observatorio Regional de TICs: se recomienda evaluar la oportunidad para el establecimiento de un observatorio de TICs, como base de incidencia tecnológica para el desarrollo de comunidades, países y de forma regional, ante la gama de temas en agenda, el Centro de Estudios en Banda Ancha para el Desarrollo (CEABAD), puede contar con esta facilidad de apoyo con sede en uno de los paises que agrupa COMTELCA, permitiría incorporar un trabajo con universidades afiliadas a UIT mediante la realización de investigación aplicada de cara al fortalecimiento de comunidades inteligentes y emergentes, con una mirada sustentable.

Es importante que los especialistas en TICs consideren criterios sociales de Gestión del Cambio para consolidar la "Interoperabilidad Social", alrededor de una A,B,C básico donde confluyen las TICs, las

Figura 47: Criterios iniciales de Gestión del Cambio para Consolidar la Interoperabilidad

Fuente: *Elaboración propia*

necesidades sociales y los impactos generados por las TICs en un ambito de cultura ciudadana participativa.

Lecciones aprendidas y buenas prácticas

El objetivo principal de este apartado es, por tanto, la recopilación de buenas prácticas y lecciones aprendidas relacionadas con el estudio.

Se trata, también, de situar estas recomendaciones prácticas en una facilidad estructurada y con un componente de reflexión sobre el modelo de desarrollo que debe seguirse sobre el uso de las TICs en la seguridad pública y ciudadana. De esta forma, este apartado puede convertirse en una útil herramienta que sirva de guía para los responsables de vitalizar los procesos de seguridad y convivencia, podrán identificar soluciones que ya están funcionando con éxito en otros lugares, mantenerse alerta sobre procesos que están en desarrollo y nuevas tecnologías.

Tabla 23: Tablas de Lecciones aprendidas y buenas prácticas

a) Cumplimiento de estándares y recomendaciones APCO 25	
La Asociación de Funcionarios de Seguridad Pública de comunicaciones con sede en los Estados Unidos, tiene un papel en el desarrollo de normas que afectan la industria. - En resumen APCO permite a las agencias acceder y compartir información crítica cuando y donde sea necesario. Esto ayuda a responder eficazmente a los desafíos diarios, a la creación de respuestas tácticas para mantener servicios vitales operativos en situaciones exigentes de Seguridad Pública y de Situaciones Cotidianas de Emergencias. APCO ha desarrollado una serie de reursos para facilitar la operatividad de antiguos centros 911 y los actuales centros N-911	
Buenas prácticas observadas	9-1-1 Costa Rica. 9-1-1 República Dominicana.
Recomendaciones y lecciones aprendidas	Se sugiere analizar la facilidad de considerar las normas operativas, tecnicas y de formación de APCO 911 para aplicación regional. Se resalta la experiencia de Costa Rica en la implementación del 911, se resalta que en la implementacion de un nuevo sistema 911 (N911, Next 911) República Dominicana esta gradualmente implementando los estardandares y recomendaciones de APCO y facilidades de transparencia similares al ECU911.
Referencia	https://www.apcointl.org/ http://www.911.go.cr/ http://911.gob.do/ https://www.apcointl.org/resources.html http://www.ecu911.gob.ec/ http://www.123bogota.gov.co/

b) Cumplimiento de estándares : El estándar CALEA
La Comisión de Acreditación para Agencias Policiales (CALEA) es una organización sin fines de lucro que acredita internacionalmente a las agencias de aplicación de la ley. Las normas se desarrollaron para ayudar a las fuerzas del orden a alcanzar los siguientes: • capacidad de agencia aumento para prevenir y controlar la delincuencia; • mejorar la eficacia de la agencia y la eficiencia en la prestación de los servicios encargados de hacer cumplir la ley; • mejorar la cooperación y coordinación con otros organismos encargados de hacer cumplir la ley y otros componentes del sistema de justicia penal; • aumentar la confianza de los ciudadanos y el personal de las metas, objetivos, políticas y prácticas de la agencia.

CALEA tiene tres ejes esenciales: • Acreditación de Comunicaciones de Seguridad Pública • Acreditación de Cumplimiento de la Ley • Acreditación de la Academia de Capacitación en Seguridad Pública	
Buenas prácticas	Regionalmente no encontradas
Recomendaciones y lecciones aprendidas	Se recomienda considerar la adopción de facilidades que brinda CALEA para la Acreditación de Comunicaciones de Seguridad Pública, a nivel regional principalmente para sistemas 911.EL considerar su implementación a través de la plataforma CEABAD a nivel regional puede facilitar la sostenibilidad del proceso.
Referencia	http://www.calea.org/content/programs

c) Interoperabilidad por IP Radio	
Muchas redes de comunicaciones de seguridad pública están evolucionando y combinando IP multiprotocolo (Multiprotocol Label Switching MPLS) y estándares del Proyecto 25 (APCO 25), así como los basados en los protocolos TETRA (Terrestrial Trunked Radio), los basados sistemas de video vigilancia, de Long Term Evolution (LTE) y Land mobile radio (LMR).	
Buenas prácticas	Guatemala, Sistema LMR para la Seguridad Ciudadana.
Recomendaciones y lecciones aprendidas	Se recomienda a las agencias reguladoras de cara a los nuevos procesos de fortalecimiento tecnológico consideren la funcionalidad, alta penetración y flexibilidad de integración e interoperabilidad de los sistemas de Radiocomunicaciones LMR para aplicaciones en los cuerpos policiales. La existencia de aplicaciones tácticas de carácter móvil de alta penetración para uso en lugares donde existen puntos muertos de señal, así como las facilidades IP para integración de sistemas que comúnmente se realizan a través de radio enlaces, no se detecta una implementación en la región se recomienda observar la tecnología táctica de REDCOM y Raytheon para tales fines.
Referencia	https://www.apcointl.org/ http://blog.taitradio.com/2014/07/03/comparing-lmr-and-cellular-for-mission-critical-communications/ https://www.youtube.com/watch?v=Db42GksT3TM http://www.raytheon.com/capabilities/products/acu2000ip/ http://redcom.wpengine.com/media/REDCOM-TCP.pdf

d) Cumplimiento de estándares: Un número único de emergencia
Avanzando en las regulaciones y tendencias, la Recomendación UIT-T E.161.1 ofrece orientación a los Estados Miembros que se encuentran en el proceso de selección de un número de emergencia único por

d) Cumplimiento de estándares: Un número único de emergencia	
primera vez, o de un número de emergencia secundario alternativo para las redes públicas de telecomunicaciones.	
Buenas prácticas	9-1-1 Costa Rica 9-1-1 República Dominicana (N-911) 9-1-1 Honduras
Recomendaciones y lecciones aprendidas	Se recomienda trabajar una normativa regional homologada que fomente facilidades de respuesta para: 1. La aplicación política, normas y regulaciones sobre las TICs considerando los modelos existentes para la Seguridad Pública. 2. La consideración de recomendaciones internacionales de UIT en los vinculado a las recomendaciones UIT-T E.161.1, sobre la el uso de los números de emergencia, lo vinculado a los planes nacionales de numeración y sus consideraciones. 3. La consideración de experiencias de organizaciones como CTIA que habiendo llevado a la practicidad la Recomendaciones de IUT, han logrado incidir en un sistema ordenado de emergencias y seguridad a la población para ejecutar facilidades de despacho y desplazamiento coordinado y oportuno en USA. 4. La facilidad de la "conexión e interoperabilidad" que permite la regulación, su aplicación, el ordenamiento para que las TICs tomen un valor preponderante para atender las emergencias cotidianas y de Seguridad Pública, 5. Leyes que faciliten la vinculación interagencial, es decir a que los organismos vinculados a la seguridad y las emergencias puedan trabajar unos con otros.
Referencia	http://www.ctia.org/policy-initiatives/policy-topics/911 Directrices para seleccionar el número de emergencia en redes públicas de telecomunicaciones (Recomendación UIT-T E.161.1, Sector de Normalización de las Telecomunicaciones de la UIT (09/2008). http://www.observatoriodescentralizacion.org/download/leyes_vigentes/07-09-15%20(1).pdf%20LEY%20DEL%20SISTEMA%20DE%20EMERGENCIA%20911.pdf

e) Respuesta Ciudadana bajo alertas	
Guatemala presenta avances importantes, resaltando la activación de la Ley del Sistema de Alerta Alba Kenneth, este mecanismo fue establecido bajo el Decreto 28-2010, Ley del Sistema y reformado según el Decreto 5-2012 que ha permitido localizar a más de mil infantes, con la Defensoria de los derechos de la niñez y la adolescencia de la Institución del Procurador de los Derechos Humanos, con casi el triple de denuncias por niñez desaparecida	
Buenas prácticas	Guatemala: Alerta Alba Kenneth

Recomendaciones y lecciones aprendidas	Considerar esta práctica como una facilidad de réplica regional que ha tenido mucho éxito en USA, México y Guatemala, principalmente en el abordaje de casos de personas desaparecidas.
Referencia	http://www.pgn.gob.gt/acerca-de-procuraduria-general-de-la-nacion/alerta-alba-keneth/ http://www.amberalert.gov/ http://www.alertaamber.gob.mx/

f) Sistemas CCTV	
Agentes policiales monitorean los videos desde sus estaciones y en tiempo real alertan a los agentes de las patrullas sobre posibles actividades delictivas. Las cámaras los han ayudado a responder ante los delitos de manera suficientemente veloz como para capturar a los sospechosos antes de que puedan escapar.	
Buenas prácticas	CCTV, Ciudad Guatemala CCTV, Ciudad Panamá
Recomendaciones y lecciones aprendidas	Si bien las implementaciones en Guatemala y Panamá, presentan un impacto moderado en la reducción de violencia, conflictividades y delitos, se recomienda observar la experiencia de Panamá que incorpora cámaras con tecnología de posicionamiento (Shotspotter) y principalmente la experiencia de Ciudad Bogotá cuyo proyecto tecnológico nace de una línea base de problemáticas sociales vinculadas al desarrollo humano de las personas y es parte de un Plan Integral de Seguridad Ciudadana 2013-2023, que también incorpora ya tecnología de identificación facial.
Referencia	http://www.shotspotter.com/ http://www.telemetro.com/cumbredelasamericas/videos/camaras-vigilancia-instaladas-perimetro-Cumbre_3_794350618.html http://issuu.com/ceacsc/docs/libro_picsc_bogot___2013_-_2023_opt http://www.facefirst.com/ https://www.youtube.com/watch?v=bmBPpokifLc

g) APPs para la Seguridad y la Justicia	
Buenas prácticas	Guatemala Costa Rica
Recomendaciones y lecciones aprendidas	Exiten avances importantes en APPs para la seguridad ciudad en aplicaciones commo ALERTOS, PNCmóvil, EspantaCacos y APPs para la Justicia en el Poder Judicial en Costa Rica, se recomienda generar una protocolo de generacion de APPs que oriente a la región sobre las facilidades que permiten las APPs en la Seguridad y la Justicia de los paises.
Referencia	http://www.mejoremosguate.org/cms/es/que-estamos-haciendo/alertos https://play.google.com/store/apps/details?id=gt.DigitalHulahoop.anticacos&hl=es_419 http://www.1mobile.es/gt-digitalhulahoop-pncmovil-134054.html http://www.poder-judicial.go.cr/ https://itunes.apple.com/cr/app/poder-judicial/id762885040?mt=8

h) CSIRT	
Un CSIRT (Computer Security Incident Response Team) es un equipo de respuesta ante Incidencias de seguridad en tecnologías de la información	
Buenas prácticas	CSIRT Guatemala CSIRT Panamá CSIRT Costa Rica DICAT República Dominicana
Recomendaciones y lecciones aprendidas	Se recomienda a nivel regional el establecimiento de un grupo de trabajo la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos sobre las infraestructuras críticas de los países y el acceso a la información de los ciudadanos, en este sentido la experiencia de Guatemala, Panamá, Costa Rica y República Dominicana pueden apoyar a la región para su éxito con el apoyo de otros organismos como COMTELCA, UIT y OEA.
Referencia	http://www.csirt.gt/ http://www.innovacion.gob.pa/csirt http://pn.gob.do/v2/dicrim/departamentos/20110224-dicat.ashx http://www.csirtcv.gva.es/es/noticias/creaci%C3%B3n-del-csirt-cr-de-costa-rica.html

i) Procesos en desarrollo SIGEP Honduras	
Sistemas de Información para la Gestión Forense (SIGEP) que facilita la gestión de conocimiento y la investigación forense de Patología, Clínica y Laboratorios de drogas, armas y explosivos, daños al medio ambiente, etc.	
Buenas prácticas	Honduras
Algunas recomendaciones y lecciones aprendidas	Se recomienda a nivel regional el desarrollo en proceso que lleva Honduras sobre este sistema de inteligencia forense.
Referencia	https://www.mp.hn/Forense/

j) Observatorios para la Seguridad y Convivencia Ciudadana	
Buenas prácticas	Panamá (Cámara de Comercio, Industrias y Agricultura de Panamá CCIAP) República Dominicana (Secretaría de Seguridad) Honduras (Universidad Nacional Autónoma de Honduras UNAH) / Instituto Universitario en Democracia Paz y Seguridad (IUDPAS) Honduras (Sistema Estadístico Policial en Línea SEPOL)
Recomendaciones y lecciones aprendidas	En un ámbito diferenciado de operatividad privada (Panamá), sector seguridad (República Dominicana y Honduras) y académico (Honduras) se recomienda crear un grupo a nivel de COMTELCA que facilite sensibilización, formación e intercambio de experiencias a nivel regional, estas 4 experiencias la de Honduras con IUDPAS fundamentada en información principalmente forense y policial, la de Panamá en instrumentos de percepción, y la de República Dominicana y SEPOL de Honduras en información policial, necesitan observar el proceso del Centro de Estudio y Análisis de la Ciudad de Bogotá que es rectorado por un gobierno local, como la mejor práctica para un fortalecimiento regional y mejoras nacionales. Se recomienda a COMTELCA y UIT considerar esta línea de trabajo como un proceso innovador y valido para la región y el trabajo con gobiernos (central y local)
Referencia	http://www.ceacsc.gov.co/index.php/que-hacemos http://www.seguridadcciap.com/wordpress/estado-de-situacion-y-lineas-de-trabajo/ http://mip.gob.do/images/docs/Programas/Observatorio http://iudpas.org/

	https://www.sepol.hn/

k) Agendas digitales	
La inclusion y uso de las TICs como una forma de gobernar los recursos, con una fuerte renovación política y ética, con una fuerte descentralización de la gestión y la reforma legal y constitucional, un foco de acción en el crecimiento económico que ayude en la distribución y la inclusión social que a su vez retroalimente el crecimiento e incida en la Seguridad Pública y Ciudadana.	
Buenas prácticas	Panamá República Dominicana. Honduras
Recomendaciones y lecciones aprendidas	Se sugiere considerar las Agendas Digitales de la República Dominicana y Panamá como hojas de ruta que ofrecen una visión clara de los desafíos que enfrentan los países para acelerar su proceso de Desarrollo Sostenible y su inserción hacia una sociedad de la información, asi como la reciente experiencia de Honduras de planificar y gestionar un Plan Maestro de Gobierno Digital contra la experiencia de México que a nivel de país cuenta con un sistema en implementación y seguimiento transparente.
Referencia	http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf http://www.gob.do/index.php/politicas/2014-12-16-20-55-59 http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf http://www.presidencia.gob.mx/edn/indicadores/ http://www.scgg.gob.hn/content/plan-maestro-de-gobierno-digital-para-honduras

l) N-911	
El Sistema 911 de República Dominicana atiende emergencias de Seguridad y Convivencia Ciudadana, así como las emergencias y urgencias cotidianas de la población	
Buenas prácticas	911 República Dominicana
Recomendaciones y lecciones aprendidas	República Dominicana se presenta como la experiencia a observar para atención de emergencias de Seguridad y Convivencia Ciudadana y desastres naturales, contando con particularidad regional un sistema de transparencia con reportes diarios de sus atenciones. Se recomienda observar esta experiencia y vincularla con la experiencia del ECU911 de Ecuador que cuenta con sistemas protocolares de medición de respuesta como los sugeridos por APCO y CTIA en USA.
Referencia	www.911.gob.do http://www.ecu911.gob.ec/ http://www.ecu911.gob.ec/biblioteca/

	http://www.ecu911.gob.ec/estadisticas/ http://www.seguridad.gob.ec/wp-content/uploads/downloads/2012/12/revistaNS6final1.pdf

m) Iniciativas ICT4D	
Buenas prácticas	Centros de Alcance Esta iniciativa es implementada por Creative Associates International Inc., con recursos de la Agencia Internacional para el Desarrollo de los Estados Unidos (USAID), institución que ha realizado programas similares en Honduras, Guatemala, El Salvador y Panamá, habiendo establecido en este proceso más de 100 Centros de Alcance en toda la región Telecentros SPARKlab es una iniciativa creada y coordinada por la Fundación Telecentre la Generalitat de Cataluña, y la Unión Internacional de Telecomunicaciones (UIT), en estrecha colaboración con un grupo selecto de organizaciones y profesionales desde los mundos público y privado de la academia.
Recomendaciones y lecciones aprendidas	Observar las experiencias de los Centros de Alcance y de Telecentros como iniciativas de ICT4D (Information and Communication Technologies for Development) que están proporcionando información, análisis, experiencia y otros recursos especializados que favorecen a las comunidades, para desarrollar y ofrecer recursos pertinentes, servicios y soluciones para apoyar el crecimiento y la sostenibilidad a largo plazo sobre modelos de acceso de computación que sirven actualmente para el desarrollo humano y la seguridad ciudadana desde lo local.
Referencia	http://www.alcancepositivo.org/centros-de-alcance-y-el-poder-de-5/ http://www.creativeassociatesinternational.com/feature-story/outreach-centers-hope-in-the-storm-for-honduran-youth/ (ver VIDEO de Medición de Impacto) http://www.creativeassociatesinternational.com/citizen-security/ http://www.creativeassociatesinternational.com/news/microsoft-academies-to-train-salvadoran-youth-for-tech-careers/ http://www.telecentre.org/

n) Nuevas tecnologías	
Buenas prácticas	Tecnología IGRIS , dispositivos para el escaneo

n) Nuevas tecnologías	
	Las unidades de escaneo de rayos X puede indicar que una sustancia orgánica está presente, pero no puede identificar lo que la sustancia es. Los escáneres de rayos X convencionales sólo pueden distinguir entre los elementos de número atómico alto (es decir, hierro y mercurio) y el número atómico bajo (es decir, carbono, nitrógeno, y oxígeno). En estudio caso especifico de Puerto Limón en Costa Rica, Tecnología No implementada en la región
Recomendaciones y lecciones aprendidas	Su tecnología, esta basada en la aplicación de rayos gamma, apoya la implementación de la LEY DE SEGURIDAD HR-1 (USA), ya que su tecnología distingue entre los elementos de número atómico alto (es decir, hierro y mercurio) y el número atómico bajo (es decir, carbono, nitrógeno, y oxígeno), el escaneo en tres dimensiones, permite detectar elementos como drogas, explosivos, armas, material nuclear sin realizar una búsqueda invasiva en el interior de los contenedores, se recomienda a los países observar esta tecnología principalmente aplicada en puertos y fronteras.
Referencia	http://www.container-scan.com/index.php/features/igris-3d-rendering http://www.container-scan.com/index.php/features/video-igris-scanning-solutions/espanol http://www.container-scan.com/index.php/2015-07-24-20-38-42/u-s-aid-economic-impact-report

ñ) Sensibilización, formación y certificación de especialistas	
Recomendación	Se recomienda considerar la consolidación de un espacio regional que facilite la sensibilización, formación y certificación de personal regional a través de una plataforma como CEABAD con el apoyo de instituciones privadas, internacionales y de gobiernos, en temas vinculados a la Seguridad Ciudadana. Durante el estudio se identificó de parte de Cámara de Comercio, Industrias y Agricultura de Panamá CCIAP, el interés por establecer un Centro Regional de Formación mediante el uso de la plataforma de CEABAD.
Referencia	Formación y Certificación de Recursos humanos para la Seguridad Ciudadana

o) Ciudades emergentes	
Buenas prácticas	Bogotá, Colombia.

o) Ciudades emergentes	
	Medellín, Colombia
Recomendaciones y lecciones aprendidas	Se recomienda para una acción de fortalecimiento regional observar los casos de las ciudades de Bogotá y Medellín como ejemplos de planificación y gestión, y el recién estudio de Banco Mundial donde se describen los avances de ciudades a nivel de Centro America y el Caribe.
Referencia	http://www.ciudademergente.org/es/blog/2015/09/28/algunas-reflexiones-del-iv-foro-internacional-de-la-bicicleta-en-bogota/ http://www.ceacsc.gov.co/index.php/encuesta-de-felicidad-y-satisfaccion/i-encuesta-felicidad-y-satisfaccion-de-los-ciudadanos-en-bogota-2014 http://www.mdeinteligente.co/quienes-somos/gobierno-abierto/ http://espanol.doingbusiness.org/~/media/GIAWB/Doing%20Business/Documents/Subnational-Reports/DB15-Central-America-and-the-Dominican-Republic-Spanish.pdf

p) Redes Sociales **Uso positivo de FACEBOOK para prevención social y seguridad ciudadana.**	
Buenas prácticas	PANI Costa Rica, Presidenta Ana Teresa León Saenz Contacto Rodolfo Meneses López Email: Meneses@pani.go.cr +(506) 2523-0713
Recomendaciones y lecciones aprendidas	El Patronato Nacional de la Infancia ha realizado un trabajo para denunciar, abordar el problema de Cibercrimen contra niñez y juventud, el uso de MEMES para sensibilización ante de deserción infantil, bulling, abordaje trata de adolescentes y embarazo de adolescentes, peores formas de trabajo infantil, empoderamiento en redes sociales. Este tipo de trabajo con redes sociales en Facebook y Youtube, ha facilitado más de 300.000 visitas en 1 semana, se recomienda observarlo y estudiarlo como un caso para réplica regional.
Referencia	https://www.facebook.com/PatronatoNacionaldelaInfancia https://www.facebook.com/PANICR https://www.youtube.com/watch?v=gtkDBDIWBYc https://www.youtube.com/watch?v=mktboTdOcKQ https://www.youtube.com/watch?v=43GCqAl1i9s https://www.youtube.com/watch?v=-bFSVSJna00

Unión International de las Telecomunicaciones(UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y Jefe del Departamento de Administración y Coordinación de las Operaciones (DDR)
Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Departamento de Infraestructura, Entorno Habilitador y Ciberaplicaciones (IEE)
Correo-e: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento de Innovación y Asociaciones (IP)
Correo-e: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Apoyo a los Proyectos y Gestión del Conocimiento (PKM)
Correo-e: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía

International Telecommunication Union (ITU)
Oficina Regional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Etiopía

Correo-e: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún

Union internationale des télécommunications (UIT) Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des télécommunications (UIT) Oficina de Zona
19, Rue Parchappe x Amadou Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Senegal
Correo-e: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication Union (ITU)
Oficina de Zona de la UIT
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe
Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil

União Internacional de Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados
Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras
Correo-e: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Estados Árabes

Egipto

International Telecommunication Union (ITU)
Oficina Regional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egipto

Correo-e: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia

International Telecommunication Union (ITU)
Oficina de Zona
Thailand Post Training Center ,5th floor
111 Chaengwattana Road, Laksi
Bangkok 10210 – Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia

Correo-e: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Correo-e: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

Países de la CEI

Federación de Rusia

International Telecommunication Union (ITU)
Oficina de Zona
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120 – Federación de Rusia

Dirección postal:
P.O. Box 25 – Moscú 105120
Federación de Rusia
Correo-e: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europa

Suiza

Union internationale des télécommunications (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Unidade Europa (EUR)
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 5111

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int

Switzerland
Geneva, 2015
Photo credits: Shutterstock