

PRIMER DIAGNÓSTICO SOBRE CIBERDELINCUENCIA EN BOLIVIA

Una iniciativa de:



En coordinación con:



Financiado por:



Primer Diagnóstico sobre Ciberdelincuencia en Bolivia

Primera edición

2019

Esta publicación se desarrolla en el marco del proyecto “Participación Ciudadana en la Reforma para el Acceso Igualitario a la Justicia en Bolivia” CSO-LA/2018/403-733 desarrollado por Fundación CONSTRUIR, Asociación Un Nuevo Camino, Visión Mundial Bolivia, Fundación UNIR en coordinación con la Comunidad de Derechos Humanos, y el apoyo financiero de la Delegación de la Unión Europea en Bolivia.

El contenido y opiniones expresadas en esta publicación son de responsabilidad exclusiva de los autores y no reflejan necesariamente la opinión de las instituciones que desarrollan el proyecto y/o la Delegación de la Unión Europea.

Desarrollo del diagnóstico y redacción:

Fabian Espinoza Valencia

Equipo editorial:

Coordinación General

Susana Saavedra

Directora Ejecutiva

Fundación CONSTRUIR

Edición

Neyza Cruz

Fundación CONSTRUIR

Diseño y diagramación:

Diana Jimenez Valencia

Está permitido el uso, reproducción y difusión del material contenido en esta publicación sin fines comerciales, bajo la condición de que se cite la fuente. Esta publicación se distribuye sin fines de lucro.

La presente investigación está bajo el régimen de Creative Commons: Atribución-NoComercial (CC BY-NC), para conocer el código legal puede visitar: <https://creativecommons.org/licenses/by-nc/4.0/legalcode.es>

ÍNDICE

○	Presentación	7
○	Introducción	9
○	Ciberdelincuencia	10
○	Análisis Cuantitativo	11
○	Análisis Cualitativo	13
○	Resultados	15
○	Órgano Judicial	19
	La Paz	23
	El Alto	22
	Oruro	25
	Potosí	25
	Cochabamba	20
	Chuquisaca	30
	Tarija	30
	Pando	31
	Beni	19
	Santa Cruz	28
○	Órgano Ejecutivo	33
○	Conclusiones y Recomendaciones	47

ACRÓNIMOS

#: secuencia numérica correspondiente

T#S: Tribunal de Sentencia

T#SAC: Tribunal Anticorrupción de Sentencia

J#PS: Juzgado de Partido y de Sentencia

J#PLS: Juzgado de Partido Liquidador y de Sentencia

J#ACVM: Juzgado Anticorrupción y contra la Violencia de la Mujer

J#IPC: Juzgado de Instrucción Penal Cautelar

J#IMC: Juzgado de Instrucción Mixto Cautelar

J#SP: Juzgado de Sentencia Penal

J#IACVM: Juzgado de Instrucción Anticorrupción y Violencia
Contra la Mujer

J#PMS: Juzgado de Partido Mixto y de Sentencia

J#PMCCFNAPSSIP: Juzgado Público Mixto Civil y Comercial, de
la Familia, Niñez y Adolescencia de Partido y Seguridad Social e
Instrucción Penal

J#PMCC: Juzgado Público Mixto Civil y Comercial

J#PCCIP: Juzgado Público Civil y Comercial e Instrucción Penal

J#PFSP: Juzgado de Partido de Familia y Sentencia Penal

J#EP: Juzgado de Ejecución Penal

J#IEP: Juzgado de Instrucción y Ejecución Penal

J#PTCT: Juzgado de Partido de Trabajo, Coactivo y Tributario

J#PNA: Juzgado Público de la Niñez y Adolescencia

J#PNAIP: Juzgado público de Niñez y Adolescencia e Instrucción
Penal

J#PF: Juzgado Público de Familias

T#SJPTSSSP: Tribunal de Sentencia y Juzgado de Partido de
Trabajo y Seguridad Social y de Sentencia Penal

S#P: Sala Penal

PRESENTACIÓN

El primer diagnóstico sobre la situación de la ciberdelincuencia en Bolivia, es un estudio exploratorio para relevar información disponible en juzgados a nivel nacional sobre delitos informáticos, desarrollando un conjunto de recomendaciones para la reforma al sistema de justicia.

La investigación desarrollada como estudios de impacto sobre el eje Justicia Transparente e Independiente de la Agenda Ciudadana de Reforma a la Justicia, y la subcategoría “Estructura Organizacional” con el fin de proveer insumos para la ruta crítica de transformación de la justicia en el que la modernización de la gestión judicial es una cuestión necesaria para fortalecer el acceso a la justicia plural en Bolivia.

La primera versión de la Agenda Ciudadana de Reforma a la Justicia publicada en 2015, incluía un conjunto de propuestas para modernizar la gestión judicial entre ellos la consolidación de un sistema único de estadística, pero al mismo tiempo el desarrollo de tecnología que permita a cada institución contar con datos suficientes para la adopción de políticas públicas que con base en evidencia permitan mejorar los servicios judiciales y la respuesta oportuna a la demanda ciudadana de justicia.

Posteriormente tanto la “modernización de la gestión judicial” como la necesaria “promulgación de una ley de acceso a la información pública” fueron propuestos por la sociedad civil y aprobados como mandatos de la Cumbre Nacional de Justicia Plural en 2016.

La investigación (veeduría ciudadana) desarrollada provee insumos importantes que permiten evidenciar la precariedad de los sistemas informáticos en la administración de justicia, y consecuentemente, las barreras que impiden un adecuado abordaje a los delitos cibernéticos. Se trata de un tópico muy poco abordado en el país, por lo que los datos contribuirán no sólo a generar mayor debate público entre actores decisores, sino también permitirán fortalecer las propuestas de la sociedad civil en la Agenda Ciudadana de Reforma a la Justicia que actualmente está siendo actualizada a partir de diálogos ciudadanos en el marco del diseño del proyecto.

El análisis cuantitativo establece estadística descriptiva concentrada en el órgano judicial, recabando información concerniente a la existencia de procesos sobre

delitos informáticos y otros delitos relacionados con el uso del internet de manera directa e indirecta en los diferentes asientos judiciales tanto a nivel departamental y municipal desde el primer trimestre de la gestión 2014 hasta el último trimestre del año 2017. El análisis cualitativo concentra su atención en la información brindada por el órgano judicial, identificando desafíos para el tratamiento de ciberdelincuencia, en este sentido se ha podido constatar que los sistemas informáticos con los que cuenta el órgano judicial datan de alrededor de dos (2) décadas; así también se pudo evidenciar la falta de información en relación a la temática.

Asimismo, se recoge importantes apreciaciones en relación al acceso a la información como pilar fundamental para el desarrollo de procesos similares en los que, a la efectiva producción de datos y su disponibilidad, permitan identificar nudos críticos en la administración de justicia y de esta manera desarrollar políticas criminales que respondan a la situación actual y que vayan de acuerdo a los avances registrados en el uso de las nuevas tecnologías de la información.

Fundación CONSTRUIR

1.1. INTRODUCCIÓN

Es complejo abordar el fenómeno de la ciberdelincuencia a nivel global y local. En Bolivia, sin desmerecer los avances que existen en el área cibernética, la administración de justicia se delata arraigada en la capacidad de realizar una prosecución óptima cuando se trata de ilícitos relacionados con el internet.

Actualmente, en Bolivia a nivel nacional no existe un diagnóstico sobre la actividad delictiva en el ciberespacio desde y hacia la jurisdicción nacional. Es menester saber dónde estamos para saber hacia donde ir, y cómo.

A nivel cuantitativo, se han elaborado estadísticas de la cantidad de delitos informáticos y otros relacionados con las tecnologías de información y comunicación en los nueve departamentos de Bolivia, así como en otros juzgados rurales del país.

A nivel cualitativo, se han registrados hallazgos significativos que ponen de manifiesto las deficiencias del Órgano judicial y sus operarios en la administración de justicia de procesos relacionados con el internet.

En ese orden, la presente investigación, recoge estadísticas sobre la cantidad de delitos informáticos y otros relacionados con las tecnologías de información y comunicación en los nueve (9) departamentos de Bolivia¹, así como en juzgados del interior del país.

Asimismo, se tiene información y descripción correspondiente al Ministerio de Gobierno con información desde la Policía Boliviana Nacional, concatenando a información sobre el Órgano Ejecutivo (Ministerio de Relaciones Exteriores, de Gobierno, de Obras Públicas y Público).

Por último, a partir de toda la información se arriban a conclusiones y recomendaciones que plantean una ruta propuesta para que la administración de justicia boliviana siga en el ámbito cibernético jurídico procesal.

*“Quien no sabe lo que busca,
no entiende lo que encuentra” -Claude Bernard-*

¹ Se tiene en cuenta además la ciudad de El Alto como otro asiento judicial.

1.2. Y... ¿QUÉ ES CIBERDELINCUENCIA?

Ya no corresponde referirse a los delitos informáticos como un neologismo dentro de la rama del derecho penal, porque desde hace muchos años atrás que se combaten las consecuencias de actos delictivos en el internet. Cabe a tal efecto mencionar las siguientes nociones al respecto:

- Existen dos escuelas doctrinarias establecidas, una confirmatoria y otra negatoria de la existencia de esta tipología penal.
- El fenómeno de la ciberdelincuencia tiene una doble relevancia jurídico penal: como medio y como objeto para cometer ilícitos, con sus diversas particularidades.
- Es un fenómeno que produce disfuncionalidades sociales, con repercusiones que ocasionan un mayor daño por ser masivas y más difíciles de individualizar, y que nunca se habían registrado y con un cambio de paradigma en la prosecución judicial.

Establecido aquello, es pertinente partir de lo expresado por el profesor Chinchilla Sandí² quien define al delito informático como una:

“Acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas -hardware- o de los programas - software”

Esto, habilita a lo que fue en su momento un neologismo: la ciberdelincuencia, concebida como un fenómeno social que requiere adecuaciones, entre otras, normativa.

Conforme al informe *Ciberseguridad ¿estamos preparados en América Latina y el Caribe?*, publicado en 2016 por la Organización de Estados Americanos, Bolivia tiene un promedio de 2 sobre 5 en cuanto a la capacidad de abordar la ciberseguridad.

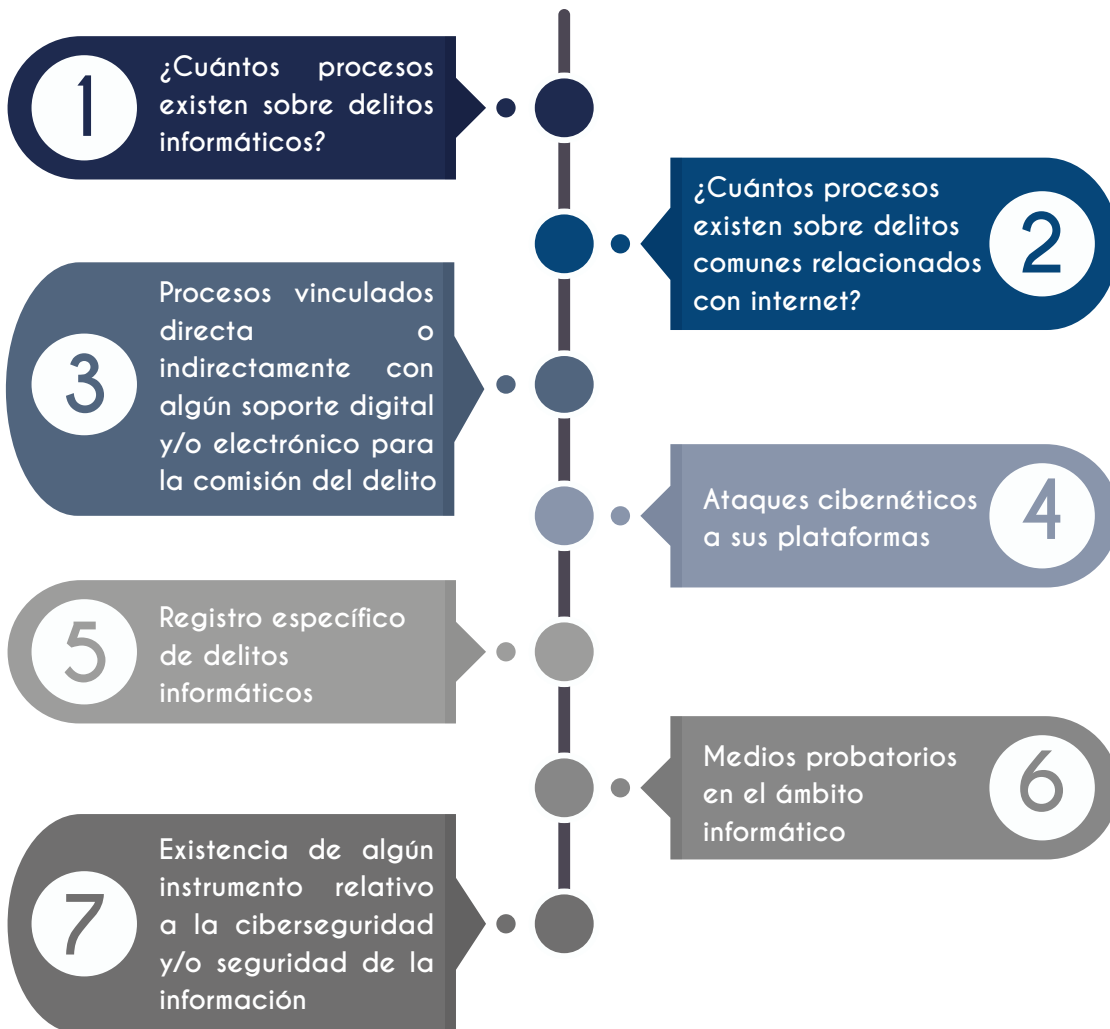
El informe, plantea que la respuesta idónea para combatir el cibercrimen es elaborar políticas criminales específicas y actualizadas que aborden la temática como corresponde. Para ello, debemos conocer cuál es nuestra situación, y a continuación abordaremos la temática.



2. Chinchilla, S. 2002. Delitos informáticos. San José, Costa Rica, Editorial IJSA

1.3. ANÁLISIS CUANTITATIVO

Se estableció una estadística descriptiva censal concentrada en el Órgano Judicial, recabando información de fuente primaria³ concerniente a la existencia de procesos sobre delitos informáticos⁴ y otros delitos relacionados con el internet de manera directa o indirecta en los diversos asientos judiciales⁵ a nivel departamental y municipal, desde el primer trimestre del 2014 al último trimestre del año 2017, a partir de los siguientes cuestionamientos base:



Cabe tomar en cuenta dos variables con respecto a los pronunciamientos de las autoridades judiciales:

- Hay casos en los que las autoridades consultadas no han provisto de ninguna información.

3 Autoridades judiciales y, en su caso auxiliares de los asientos judiciales de los 9 departamentos a nivel nacional y municipal.

4 Tipificados en el Código penal boliviano en los artículos 363 bis. - (Manipulación informática) y 363 ter. - (Alteración, acceso y uso indebido de datos informáticos)

5 Tribunales de sentencia y juzgados públicos, conforme a lo establecido por la Ley N° 025 del Órgano Judicial.

- Hay casos en los que las autoridades consultadas han provisto de información parcial.

Para ello, se han elaborado las siguientes tablas por ciudad, en las que se muestra en línea vertical los asientos judiciales, y en la línea horizontal, los bienes jurídicamente protegidos en base a los títulos del código penal boliviano en el Libro Segundo, Parte Especial:

1	Contra la seguridad interior y exterior del Estado (Título I; Capítulo I, II, III y IV)	11	Contra la libertad sexual (Título XI; Capítulo I, II, III y IV)
2	Contra la función pública Título II; Capítulo I y II)	12	Contra la propiedad (Título XII; Capítulo I, II, III, IV,V, VI, VII, VIII, IX, X, XI)
3	Contra la función judicial Título III; Capítulo I, II y III)	13	Delitos de trata y tráfico de personas
4	Contra la Fe pública (Título IV; Capítulo I, II, III y IV)	14	Delitos de pornografía infantil
5	Contra la seguridad común (Título V; Capítulo I, II y III)	15	Delitos contra derechos de autor (Capítulo X)
6	Contra la economía nacional, industria y comercio (Título VI; Capítulo I y II)	16	Delitos informáticos (Capítulo XI)
7	Contra la familia (Título VII; Capítulo I y II)	17	Delitos financieros (Capítulo XII)
8	Contra la vida, integridad corporal (Título VIII; Capítulo I, II, III y IV)	18	Fraude
9	Contra el honor (Título IX; Capítulo Único)	19	Crimen Organizado
10	Contra la libertad (Título X; Capítulo I, II, III y IV)		

Téngase presente que, del universo censal que corresponde a todos los asientos judiciales de los Tribunales Departamentales de Justicia del Estado, el motivo de la interrupción a la secuencia numérica del juzgado o tribunal es porque la autoridad judicial no ha provisto de datos.

1.4. ANÁLISIS CUALITATIVO

Los hallazgos fueron recabados en informes de fuente primaria, en los que se puede advertir que la administración de justicia boliviana padece de falencias al confrontar la ciberdelincuencia. Previamente, téngase presente lo siguiente:

1

La información provista por parte de cada estrado judicial no ha contemplado método de verificación alguno.

De algunos informes vertidos por personal del juzgado [5], se ha provisto de información registrada [6] en su base de datos informatizada, con la estimación de que el sistema IANUS ha sido instaurado hace más de 20 años atrás y otros del Sistema Integrado de Registro Judicial (SIREJ) pero de manera remanente.

2

3

Se puede evidenciar que en la mayoría de los casos la autoridad judicial deriva mediante proveído la provisión de información a la Secretaría del Juzgado.

Con respecto a la cuestión referencial 3.7. sobre algún instrumento de ciberseguridad el 96% de los asientos judiciales no cuenta con información al respecto. La respuesta más concreta se ha obtenido de la oficina correspondiente del Consejo de la Magistratura de Chuquisaca.

4

5

Se toman en cuenta procesos dentro del análisis cuantitativo no necesariamente porque el proceso haya tenido alguna relación con el internet en su comisión, sino por los medios probatorios de investigación posteriores.

Hay estrados judiciales que han concluido la inexistencia de procesos vinculados a las cuestiones base sin contemplar que existen procesos que versan sobre delitos tradicionales relacionados con internet.

6

7

Precítese que los Tribunales de Sentencia ha apuntado que la información provista excluye determinados delitos por razón de competencia de la pena mínima, Así como por otra parte se puede ver que ha habido casos relativos a delitos informáticos directos que han sido alcanzados por amnistía, extremo que muestra la baja sanción.

Téngase presente que, en la mayoría de los procesos sobre delitos informáticos tiene relación para un concurso real o ideal con los delitos contra la propiedad, contra la libertad sexual y la integridad física.

8

9

En el caso del departamento de Santa Cruz, no se pudo proceder a recabar la información correspondiente por la burocracia institucional de la presidencia del Tribunal Departamental de Justicia, así se puede evidenciar en el informe vertido [7], en el que afirma que debe procederse a una “estandarización mediante formato, debido a la complejidad del mismo y a la gran cantidad de datos que han sido requeridos.” Haciendo notar, que el resto de los Tribunales Departamentales de Justicia, han brindado toda la información correspondiente, inclusive los asientos judiciales del área rural.

En el análisis cuantitativo (tablas), cuando se señala únicamente con el dígito sin el numeral el tipo penal correspondiente, es porque no se ha especificado.

10

En ese entendido, a continuación de cada tabla cuantitativa expuesta por asiento judicial, se adjuntan documentos reales y originales de funcionarios judiciales (hallazgo del análisis cualitativo), habiendo removido nombres, domicilio u otro dato que pueda relacionar a cualquier persona, en estricto cumplimiento al régimen de protección de datos personales.



RESULTADOS ÓRGANO JUDICIAL

2.1. ÓRGANO JUDICIAL

En la presente tabla, se sistematizan las cifras más relevantes en los asientos judiciales de los 9 departamentos del país, incluyendo la jurisdicción de El Alto, así como ciudades del interior conforme a la información provista por las autoridades judiciales

	Delitos con vinculación a internet	Delitos informáticos
Beni	2	2
Cochabamba	299	4
El Alto	5	-
La Paz	93	42
Oruro	3	4
Potosí	5	1
Santa Cruz		
Sucre	25	1
Tarija	4	-
Pando	5	3

BENI

En el departamento de Beni no se ha podido recabar numerosa información, a partir de las 7 vocalías que conforman el Tribunal Departamental de Justicia.

Sin haber podido recabar tampoco algún hallazgo cualitativo significativo.

- ② Delitos informáticos
- ② Delitos vinculados a internet



COCHABAMBA

En el departamento de Cochabamba se destaca el alto índice de Delitos de violencia contra la mujer, contra la vida e integridad principalmente en los asientos jurisdiccionales en el área rural.

Asimismo se puede notar que hay una concurrencia de juzgados que proveen de información sin datos sobre algún proceso en el que haya tenido relación el internet.



4 Delitos informáticos

299 Delitos vinculados a internet

HALLAZGO CUALITATIVO

Un informe en el que se puede evidenciar las altas cifras en delitos vinculados con internet de naturaleza violenta.



ESTADO PLURINACIONAL DE BOLIVIA
 TRIBUNAL DEPARTAMENTAL DE JUSTICIA DE COCHABAMBA

INFORMA

DE: JUZGADO DE INSTRUCCIÓN
 PENAL NO. 1 DE SACABA

A: **F**
 DECANO EN EJERCICIO DE LA PRESIDENCIA DEL
 TRIBUNAL DEPARTAMENTAL DE JUSTICIA
 COCHABAMBA-BOLIVIA

REF.

FECHA:

En cumplimiento al llido por Presidencia del Tribunal
 Departamental de Justicia de Cochabamba se tiene a bien informar.

- A LA PREGUNTA 1 y 2: No se tiene ningún caso con referencia a este punto.
- ✓ A LA PREGUNTA 3: Se tiene 5 casos de falsedad ideológica y 2 de falsedad material.
- ✓ A LA PREGUNTA 4: Se tiene 15 casos de conducción peligrosa de vehículos.
- ✓ A LA PREGUNTA 5: No se tiene ningún caso con referencia a este punto.
- ✓ A LA PREGUNTA 6: Se tiene 1 caso de abandono de mujer embarazada.
- ✓ A LA PREGUNTA 7: Se tiene 11 casos de Homicidio y lesiones graves y gravísimas en accidente de tránsito, 2 casos de homicidio culposo, 1 caso de homicidio, 1 caso de asesinato, 2 casos de feminicidio, 3 casos de lesiones gravísimas, 42 casos de lesiones graves y leves, 56 casos de violencia familiar y doméstica.
- A LA PREGUNTA 8: No se tiene ningún caso con referencia a este punto.
- A LA PREGUNTA 9: Se tiene 3 casos de Amenazas.
- A LA PREGUNTA 10: Se tiene 6 casos de violación, 7 casos de violación de niño, niña o adolescente, 7 casos de abuso deshonesto.
- A LA PREGUNTA 11: Se tiene 10 casos hurto, 22 casos de robo, 18 casos de robo agravado, 15 casos de estafa y 4 casos de estelionato.
- A LA PREGUNTA 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23: No se tiene ningún caso con referencia a estos puntos.

Cabe aclarar que se informo tanto inicios como imputaciones

Sin otro particular, me despido de Usted con las consideraciones más distinguidas.

Es cuanto se informa

[Firma manuscrita]
 Causa N° 1 de Sacaba
 Cochabamba

EL ALTO

La Ley N° 025 del Órgano Judicial que tiene por objeto regular la estructura, organización y funcionamiento del Órgano Judicial, a la ciudad de El Alto no le asigna vocalías en la estructura del Tribunal Departamental de Justicia.

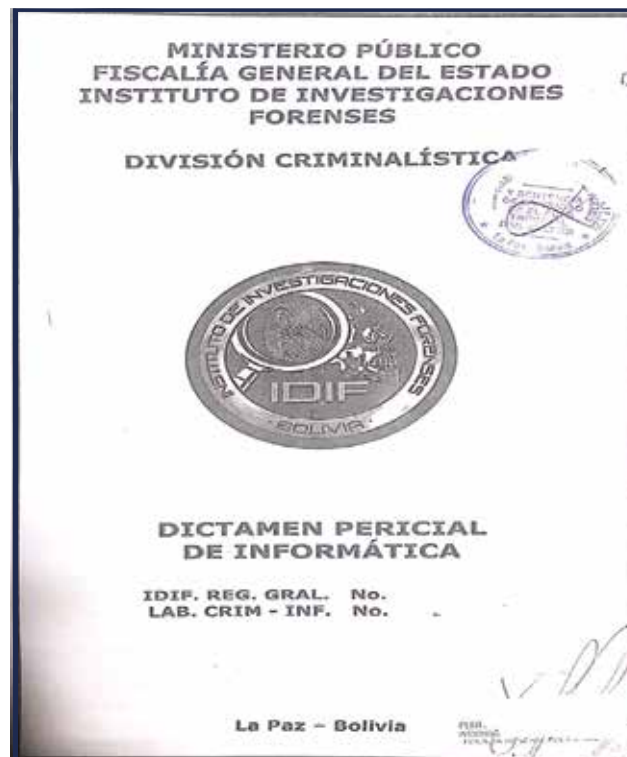
Un antecedente es que si bien no se registran delitos informáticos, sin embargo, fue proporcionado un caso de un peritaje informático forense.



- Delitos informáticos
- 5 Delitos vinculados a internet

HALLAZGO CUALITATIVO

A partir del análisis destaca la información provista por el Juzgado 4° de partido de Liquidación y Sentencia El Alto, que aporta con antecedentes en la temática con un dictamen pericial de informática.



LA PAZ

El Tribunal Departamental de Justicia de La Paz cuenta con 24 vocalías, y como ciudad sede, presenta una importante concurrencia de procesos judiciales vinculados directa o indirectamente con el internet.

42 Delitos informáticos

93 Delitos vinculados a internet



HALLAZGO CUALITATIVO

Un hallazgo cualitativo encontrado en el informe de un juzgado de instrucción cautelar penal permite identificar los delitos informáticos, a través de un listado detallado de procesos sobre este delito.

La información provista por el Juzgado 10º de Instrucción Penal Cautelar, destaca por la alta cantidad de procesos vinculados al delitos informático de manipulación informática (363 bis.).

La siguiente tabla muestra procesos vinculados con delitos informáticos un total de 25 casos, asimismo, se menciona el estado de cada causa.



DEPARTAMENTO DE JUSTICIA
ORGANO JUDICIAL
LA PAZ - BOLIVIA



JUZGADO DECIMO DE INSTRUCCIÓN EN LO PENAL CAUTELAR DE LA CIUDAD DE LA PAZ

En cumplimiento al INSTRUCTIVO C
remitir informar lo siguiente:

tengo a bien

- Con relación al punto 1, en el Juzgado Decimo de Instrucción se tramitan procesos por el delito de Manipulación Informática, adjuntándose el siguiente Formulario:

IANUS	SUJETOS PROCESALES	ESTADO DE LA CAUSA
	MP/LOS AUTORES	RECHAZO
20.	MP/LOS AUTORES	RECHAZO
2	MP/LOS AUTORES	RECHAZO
20	MP/LOS AUTORES	RECHAZO
20.	MP/LOS AUTORES	CONMINATORIA
		RECHAZO
2	MP/LOS AUTORES	RECHAZO
2	MP/LOS AUTORES	CONTROL JURISDICCIONAL
20	MP/LOS AUTORES	CONTROL JURISDICCIONAL
20.	M.	CONTROL JURISDICCIONAL
20.	MF	CONTROL JURISDICCIONAL
	C/.	
20	MP/LOS AUTORES	RECHAZO
20	MP/LOS AUTORES	CONTROL JURISDICCIONAL
2	MP/LOS AUTORES	RECHAZO
20	MP/LOS AUTORES	RECHAZO
20	MF	CONTROL JURISDICCIONAL
20	MP/LOS AUTORES	RECHAZO
20.	MP/LOS AUTORES	RECHAZO
20	MP/LOS AUTORES	CONTROL JURISDICCIONAL
20	MP/LOS AUTORES	CONTROL JURISDICCIONAL
2	MP/EL AUTOR	RECHAZO
20	MP/LOS AUTORES	RECHAZO
	MP/LOS AUTORES	RECHAZO
20	MP/P.	CONTROL JURISDICCIONAL
2	MP/LOS AUTORES	IMPUTACION FORMAL

ORURO

La estructura del Tribunal Departamental de Justicia Cuenta con 12 vocalías que registran delitos informáticos.

El hallazgo cualitativo relevante versa en el proceso judicial instaurado contra una docena de funcionarios públicos de la Oficina de Derechos Reales, que de manera premeditada y conjunta realizan manipulaciones irrumpiendo con varios controles de seguridad a nivel técnico así como logístico¹.



- 4 Delitos informáticos
- 3 Delitos vinculados a internet

POTOSÍ

El Tribunal Departamental de Justicia de Potosí cuenta con doce vocalías. Con relación a la recopilación de información sobre ciberdelincuencia, únicamente se pudo registrar la existencia de un proceso por delito informático.



- 1 Delitos informáticos
- 5 Delitos vinculados a internet

HALLAZGO CUALITATIVO

En el departamento de Potosí se recabó los hallazgos cualitativos más relevantes, que exponen la brecha digital existente entre los distintos Municipios en este departamento.

Un hallazgo relevante en el departamento de Potosí se ha relevado en el Juzgado 1º Público mixto Civil y Comercial, de Familia, Niñez y Adolescencia e instrucción, en la Provincia Alonso Ibañez en el Municipio de Sacaca, la autoridad judicial expide una

¹ Proceso instaurado en el juzgado 4to de instrucción penal, con imputación formal en contra de 13 personas y detención preventiva de 3 funcionarios públicos.


declaración inédita, que expone la brecha digital existente en Bolivia entre ciudades y áreas rurales, a su vez, como es que, el fenómeno del cibercrimen no se puede impetrar en razón de materia, por no contar con internet ni con entidades financieras.

Como resumen la cita del Juez: "(...) por su misma idiosincrasia, en este sector del país para la comisión de este tipo de delitos, no existen los servicios de las empresas telefónicas (...)"

ESTADO PLURINACIONAL DE BOLIVIA



ÓRGANO JUDICIAL
Tribunal Departamental de Justicia
Potosí - Bolivia



TRIBUNAL DEPARTAMENTAL DE JUSTICIA
POTOSÍ
SECRETARÍA DE PRESIDENCIA

RECIBIDO

HORAS

Sacaca, 12 de Abril de 2016

Señor:
Dra. Edith Rosario Peñaranda Ávila
PRESIDENTA DEL TRIBUNAL DEPARTAMENTAL DE JUSTICIA DE POTOSÍ

Ref.- Cumplimiento al Cite Pres N°

De nuestra mayor consideración:
En principio quiero hacerle llegar mi más sincero y cordial saludo a su digna autoridad.

Siendo de conocimiento de su autoridad y dando cumplimiento al Cumplimiento al Cite Pres N°
2017, tengo a bien de informarle de forma respetuosa lo requerido de manera siguiente:

Este órgano jurisdiccional, tiene competencia en la Provincia Alonso de Ibáñez - Sacaca, tanto en su primera sección y segunda sección abarcando áreas rurales en su totalidad, por su mismo idiosincrasia, en este sector del País para la comisión de este tipo de delitos, no existe los servicios de las empresas telefónicas de Viva y Tigo, siendo con excepción de la empresa nacional Entel, que brinda un servicio pésimo; Tampoco existe entidades financieras. Todo lo mencionado influyen en la no vinculación directa o indirecta, con algún soporte digital y/o electrónico para la comisión del delitos de los puntos solicitados y así mismo en la presente gestión en los otros puntos no se ha presentado los tipos de delitos requeridos en conclusión nos se ha registrado los puntos penales del 1 al 23, requeridos

Seguro de que entenderá mi posición y con las deferencias más distinguidas ante vuestra autoridad;

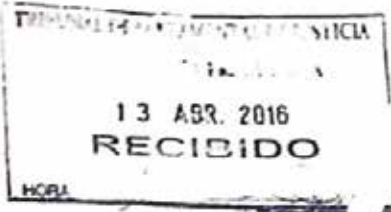

Atentamente,

c/c C.Ch.



JUZGADO PÚBLICO MIXTO CIVIL Y COMERCIAL DE FAMILIA, NIÑEZ Y ADOLESCENCIA E INSTRUCCIÓN PENAL N° 1
PROV. ALONSO DE IBÁÑEZ
POTOSÍ - BOLIVIA

Otro hallazgo relevado en el departamento de Potosí del Juzgado Público 1º Civil y Comercial de Uncía, el juez argumenta conforme al párrafo citado: "Por otra parte, hago conocer a Ud. que en este asiento judicial no se cuenta con el sistema de internet"



INFORME

A: PRESIDENTA DEL TRIBUNAL DEPARTAMENTAL DE JUSTICIA DE POTOSI

DE: JUZGADO PÚBLICO CIVIL Y COMERCIAL 1º DE UNCIA

CASO: Remite Informe

FECHA: 11 de abril de 2016

De mi mayor consideración.

Cumpliendo con el requerimiento de informe de fecha 04 de abril de 2016, al respecto tengo a bien informarlo siguiente:

Revisado los libros de ingresos de causas nuevas desde gestiones anteriores en materia penal, familia, niño, niña y adolescencia hasta la gestión de 2015, el juzgado a mi cargo no ha recibido ninguna causa directa e indirecta relativas a denuncias con algún soporte digital y/o electrónico con contenido delictivo.

Por otra parte, hago conocer a Ud. que en este asiento judicial no se cuenta con el sistema de internet

Es cuanto puedo informar en honor a la verdad.

Atentamente.-

Mano del Juez

JUEZA PÚBLICA CIVIL Y COMERCIAL 1º
UNCIA - POTOSI - BOLIVIA

JUEZA PÚBLICA CIVIL Y COMERCIAL 1º
UNCIA - POTOSI - BOLIVIA

SANTA CRUZ

El Tribunal Departamental de Justicia de Santa Cruz, está conformado con la mayor cantidad de vocalías veinte integrantes.

Por un lado, al haber solicitado información sobre cibercrimen a la Presidencia del TDJ, se remite un informe a la residencia del Tribunal Supremo de Justicia- TSJ, solicitando la *“estandarización mediante formato, debido a la complejidad del mismo y a la gran cantidad de datos que han sido requeridos”*, sin proveer información con respecto a lo solicitado.

Por otro lado, cabe destacar que el Tribunal Departamental de Justicia de Santa Cruz es el único asiento jurisdiccional que no ha provisto de ninguna información para la recopilación de esta investigación.



HALLAZGO CUALITATIVO

El siguiente informe de Presidencia del Tribunal Departamental de Justicia de Santa Cruz, solicita la *“estandarización mediante formato, debido a la complejidad del mismo y a la gran cantidad de datos que han sido requeridos.”*



710
162
16
F25

Santa Cruz de la Sierra, 06 de abril de 2016
CITE PDCIA - RRPP

Señor;
Dr. Pastor S. Mamani Villea
Presidente del Tribunal Supremo de Justicia
Presente.-

Ref. Solicitud de informe

De mi mayor consideración:

Por medio de la presente y con la finalidad de viabilizar la elaboración del informe solicitado mediante oficio ¹⁶²/2016 de fecha 31 de marzo de 2016, solicito a su autoridad ¹⁶² muy respetuosamente, que usted interponer sus buenos oficios ante la Presidencia de ¹⁶² ^{mb} a objeto de que se precisen los puntos del cuestionario ¹⁶²/2016-2017 de fecha 22 de marzo de 2016 y su estandarización mediante un formato, debido a la complejidad del mismo y a la gran cantidad de datos que han sido requeridos.

Con este motivo, reitero a usted mis consideraciones más distinguidas.

Atentamente,



PRESIDENTA
TRIBUNAL DEPARTAMENTAL DE JUSTICIA
SANTA CRUZ - BOLIVIA

GHR/RRPP
Adjunto: Lo indicado
Copia Archivo



Av. Uruguay esq. Monseñor Rivera · Telf. (3) 3365454 · Fax (3) 3362268 · www.organojudicial.gob.bo

Scanned with
CamScanner

CHUQUISACA

El Tribunal Departamental de Justicia de Chuquisaca cuenta con doce vocalías y en delitos informáticos los registros no son de alta concurrencia.

Asimismo, se ha podido recabar información más precisa con respecto al funcionamiento de los sistemas informáticos en la administración de justicia a través del relevamiento de información del Consejo de la Magistratura y del Tribunal Supremo de Justicia.

De igual importancia resaltar que el TDJ de Chuquisaca es el único asiento jurisdiccional que proporcionó información sobre ciberseguridad.



- 1 Delitos informáticos
- 25 Delitos vinculados a internet

TARIJA

El Tribunal Departamental de Justicia de Tarija cuenta con ocho vocalías, desde los asientos judiciales se ha registrado una alta cantidad de información provista por autoridades de juzgados.

Sin embargo, el análisis refleja que no se han registrado procesos relacionados a delitos informáticos u otros delitos comunes que hayan tenido relación con el internet.



- Delitos informáticos
- 4 Delitos vinculados a internet

PANDO

El Tribunal Departamental de Justicia de Pando está conformado por la menor cantidad de vocalías: cinco, conforme a la Ley N° 025.



HALLAZGO CUALITATIVO

En el TDJ de Pando el hallazgo encontrado fue la resolución judicial de un procedimiento abreviado con sentencia del Juzgado de instrucción penal cautelar N°3², caso que dentro de las medidas sustitutivas establecidas en el artículo 240 del Código de Procedimiento Penal, numeral 4 señala: “*Prohibición de concurrir a determinados lugares*” en el caso concreto, a cajeros automáticos dentro de un proceso sobre el delito informático de manipulación informática (363 bis.)

- 1.- La prohibición de cambiar de domicilio
 - 2.- La presentación ante el juzgado de ejecución penal cada 30 días.
 - 3.- Mantenerse en una fuente de trabajo, a tal efecto deberá acompañar contrato de trabajo ante el juzgado de ejecución penal en el plazo máximo de 15 días.
 - 4.- La prohibición de frecuentar los cajeros del Banco BISA
- Periodo de prueba que deberá ser cumplido durante 1 año, siendo que su incumplimiento dará lugar a su revocatoria y el condenado deberá cumplir la pena impuesta.
Regístrese y hágase saber.-

JUEZ DE INSTRUCCION
CAUTELAR N° 3
CÓBIZA - BOLIVIA

Ante mí

ABOGADA
JUZGADO PENAL CAUTELAR N° 3
Tribunal Departamental de Justicia de Pando



2. Seguimiento de Procesos en línea, en materia penal a través del IANUS, Caso N° 901-199201501965.

RESULTADOS ÓRGANO EJECUTIVO

2.2.1. MINISTERIO PÚBLICO

Fiscalía General del Estado

La información provista se refiere únicamente a datos estadísticos de los delitos de acción penal que son de competencia del Ministerio Público, y no así de los delitos de acción penal privada: delitos contra el honor.

El informe está circunscrito al periodo desde enero de 2013 hasta enero de 2017, en consideración a la promulgación de leyes que incorporaron nuevos delitos al Código Penal³. Se detalla la información, elaborada sobre la base de los informes que remitieron:

- Fiscalías Departamentales y
- Jefatura de Informática

TOTAL CASOS	
GESTIÓN	CASOS
2013	883
2014	1.455
2015	3.166
2016	1.045
2017	1.254
TOTAL	7.803

Datos Complementarios

Las siguientes cifras aborda los cuatro apartados puntuales que hacen a la prosecución de la ciberdelincuencia:

DESCUBRIMIENTO DE ORGANIZACIONES CRIMINALES		
Número de caso	Delito	Gestión
0	0	0

³ Ley 348, 393, 400, 477, 553, entre otras.

ATAQUES CIBERNÉTICOS A PLATAFORMAS DIGITALES ESTATALES

Número de caso	Delito	Gestión
0	0	0

ACTIVIDAD DEL CIBERCRIMEN EN REDES SOCIALES

GESTIÓN	CASOS
2013	1
2014	3
2015	19
2016	8
2017	13
TOTAL	44

RESOLUCIÓN DE CASOS CON MEDIOS PROBATORIOS DIGITALES

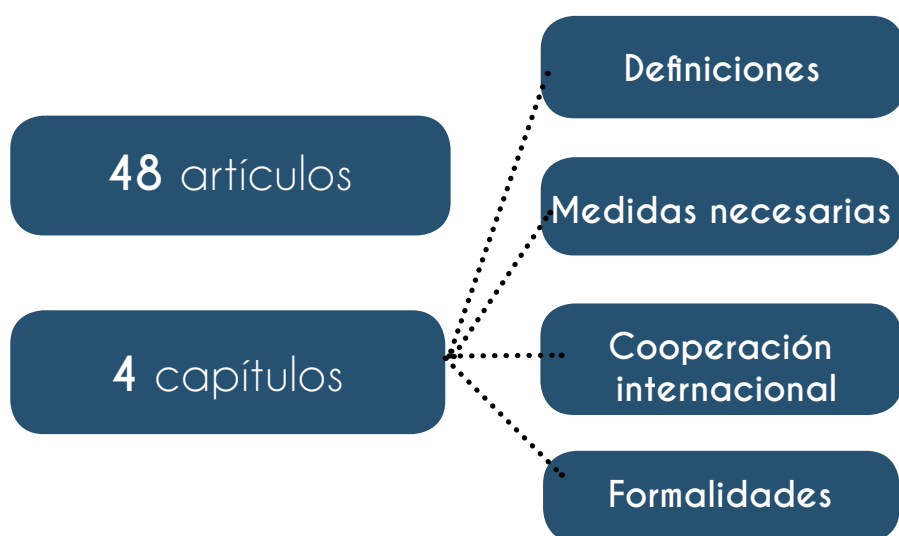
GESTIÓN	CASOS
2013	0
2014	3
2015	12
2016	5
2017	7
TOTAL	27

2.2.2. MINISTERIO DE RELACIONES EXTERIORES

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la protección de los derechos humanos y de las libertades fundamentales (1950), el Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, sin consideración de fronteras, así como el respeto de la vida privada⁴.

Los Estados miembros del Consejo de Europa y demás Estados signatarios han circunscrito el Convenio sobre Ciberdelincuencia en su Sesión N° 109 de 08 de noviembre de 2001, presentada para su firma en Budapest, Hungría el 23 de noviembre de 2001. El cuál entró en vigor el 1 de julio de 2004.

En el siguiente esquema se analiza el Convenio de Budapest principalmente con los delitos y otras normas relacionadas:



⁴ Párrafo 10 del preámbulo del Convenio sobre Ciberdelincuencia, firmado en Budapest, Hungría, 23.XI.2001

Con respecto a los Estados adheridos son 56 países de cinco continentes, trece de ellos son Americanos⁵.

Conforme al artículo 37 del Convenio, los Estados no miembros pueden adherirse al cuerpo normativo internacional por invitación del Comité de Ministros del Consejo de Europa, los Estados están sujetos a un posterior procedimiento específico preestablecido.

En el caso del Estado Plurinacional de Bolivia y la adhesión al Convenio sobre Ciberdelincuencia, la información oficial del Ministerio de Relaciones Exteriores, deberían cumplirse los siguientes parámetros:

- **Participación**

La autoridad entrevistada, para esta investigación, mencionó que: *“Bolivia no participó en la negociación del contenido referido Convenio sobre Ciberdelincuencia.”*

En la sesión participaron Estados no miembros del Consejo: Canadá, Japón, Sudáfrica y Estados Unidos de América. Asimismo, el Capítulo IV del Convenio establece las consideraciones necesarias para la adhesión así como ratificación de otros Estados, como legislación específica sobre delitos informáticos, sancionar las conductas ilícitas que afecten los sistemas informáticos, u otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de información o de la comunicación.

- **Solicitud**

En el caso del Estado Plurinacional de Bolivia, la Dirección General de Relaciones Bilaterales, como instancia operativa de las facultades dispuestas por el Viceministerio de Relaciones Exteriores, dependiente de esta cartera de Estado: *“(...) reportó que no se tiene registro o conocimiento de alguna gestión oficial realizada en tal sentido.”*

⁵ Argentina, Chile, Perú, Paraguay, Uruguay, Estados Unidos, Canadá, Panamá, República Dominicana, Panamá, Costa Rica, El Salvador y Colombia.

• Adhesión

La autoridad recurrida aclara el procedimiento para la incorporación de un Estado al Convenio de referencia, aludiendo a los artículos 36 y 37 del cuerpo normativo internacional⁶.

• Causal de no Adhesión

El Ministerio de Relaciones Exteriores a través de la emisión de un reporte: *“la referida Dirección General de Relaciones Bilaterales, esta Cartera de Estado no tiene registro o conocimiento de alguna gestión oficial realizada (...)”*

• Pasos a Seguir

En el caso de que el Estado Plurinacional de Bolivia se adhiera al Convenio sobre Ciberdelincuencia, la autoridad recurrida señala 10 pasos a seguir:

① **ADECUACIÓN** de normativa interna conforme al contenido del Convenio

② **SOLICITUD FORMAL DE ADHESIÓN** a través de comunicado oficial

③ **CONSIDERACIÓN** del Consejo de Europa de la solicitud formulada

④ **APROBACIÓN** mayoritaria conforme a sus estatutos y **POSTERIOR INVITACIÓN**

⑤ **VERIFICACIÓN** de cumplimiento de adecuación de la normativa interna

⑥ **ANÁLISIS JURÍDICO SOBRE RESERVAS** del Convenio

⁶ Artículo 36. Firma y entrada en vigor. 1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración. 2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa. 3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2. 4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37. Adhesión al Convenio. 1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros. 2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

7 **RATIFICACIÓN** del Convenio

8 Elaboración y firma del instrumento de **ADHESIÓN**

9 **DEPÓSITO** ante la secretaría general del Consejo de Europa

10 Determinación de la fecha de **ENTRADA EN VIGOR**

2.2.3. MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes

Una de las mayores dificultades en la prosecución del Cibercrimen radica en recabar los elementos probatorios suficientes y necesarios, que por lo general se realizan a través de pericias informáticas. De cualquier modo, siempre se debe acudir, en el ejercicio del derecho humano al acceso a la información, a solicitar datos a plataformas digitales que en la totalidad de los casos se encuentran establecidas en el exterior.

Para ello, conforme a la estructura organizativa del Órgano Ejecutivo del Estado Plurinacional de Bolivia⁷, es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), dependiente del Ministerio de Obras Públicas, Servicios y Vivienda, es la encargada de gestionar solicitudes concernientes al acceso a la información en plataformas digitales de telecomunicaciones.

En caso de requerir o solicitar datos e información con valor probatorio de origen o sede internacional, cumpliendo con el principio de legalidad de la prueba, téngase presente las siguientes consideraciones señaladas por la Autoridad de regulación y fiscalización de Telecomunicaciones y Transportes (ATT) en base a los siguientes planteamientos:

⁷ Decreto Supremo N° 29894, Estructura Organizativa del Poder Ejecutivo del Estado Plurinacional.

PROCEDIMIENTO/PROTOCOLO PARA SOLICITAR DATOS PERSONALES A CORPORACIONES DEL ÁMBITO INFORMÁTICO CON SEDE EXTRANJERA

1

No existe un procedimiento y/o protocolo para solicitudes de información y/o datos personales a corporaciones del ámbito informático con sede en países extranjeros, en caso de ser estas emanadas por autoridad competente con fines judiciales y adscritos a la normativa interna.

Pero, algunas veces llegan ciertos requerimientos fiscales ante esta autoridad, que coadyuva a dicho requerimiento, solicitando información puntual a corporaciones del ámbito informático con sedes en países extranjeros, obteniéndose en el marco de la política de privacidad de datos de las corporaciones mencionadas.

LA ATT ES LA INSTANCIA OFICIAL DEL ESTADO FALCULTADA PARA REALIZAR REQUERIMIENTOS OFICIALES A CORPORACIONES DEL ÁMBITO DIGITAL CON SEDE EXTRANJERA

2

Dentro de las competencias y atribuciones de la ATT definidas por el Decreto Supremo N°007 de 9 de abril de 2009, **no se menciona esta atribución o facultad, como una de sus potestades, para realizar requerimientos de manera oficial** ante corporaciones del ámbito digital con sede en países extranjeros.

INSTANCIA ESTATAL HABILITADA PARA REALIZAR REQUERIMIENTOS OFICIALES DE DATOS PERSONALES A CORPORACIONES DEL ÁMBITO DIGITAL CON SEDE EXTRANJERA

3

No se tiene conocimiento de la instancia oficial del Estado para requerir información y/o datos personales de empresas o corporaciones con sede en países extranjeros.

2.2.4. MINISTERIO DE GOBIERNO

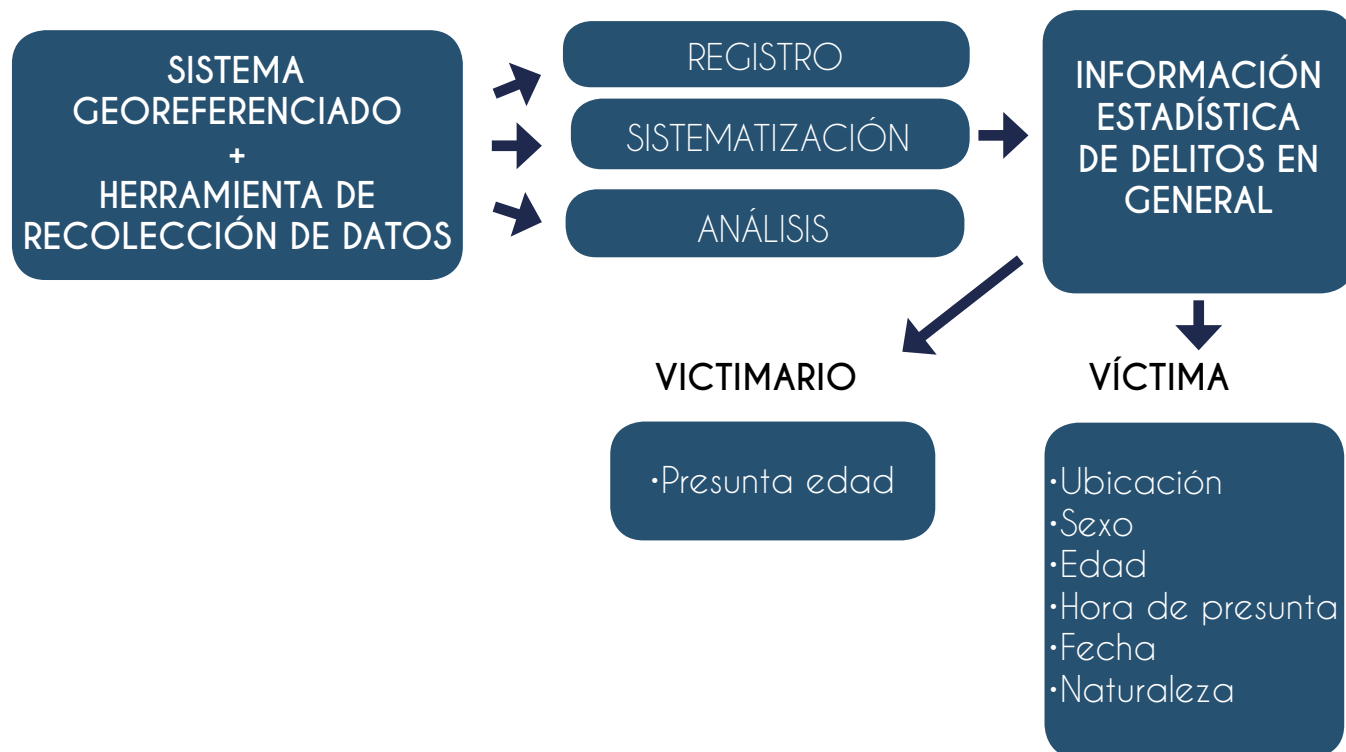
Observatorio Nacional de Seguridad Ciudadana

En el marco de lo establecido en la Ley N° 263 Integral de Lucha contra la Trata y Tráfico de Personas y su reglamento D.S. N° 1486, en su artículo 19, es importante conocer que la compilación de datos respecto a la trata y tráfico de personas y delitos conexos responde a un sistema de información.

El Ministerio de Gobierno, a través del Viceministerio de seguridad ciudadana cita:

Con relación al sistema de información y estadística de trata y tráfico de personas y delitos conexos, el Observatorio Nacional de Seguridad Ciudadana-ONSC, es la instancia nacional y oficial para la generación de datos propios y recopilar información de otras fuentes de información institucional.

Con tal cometido, ha implementado una de las tecnologías informáticas más destacables en la lucha contra el cibercrimen a través de un:



3. CONTEXTO NORMATIVO Y POLÍTICAS PÚBLICAS

Como parte de la metodología de investigación para la recopilación de información del diagnóstico sobre la ciberdelincuencia en Bolivia, se han realizados peticiones de acceso a información pública a distintas instituciones públicas, procediendo a solicitar información actualizada impulsando el derecho al acceso a la información.

Las instituciones a las que se solicitó información fueron: el Órgano Judicial, los Tribunales Departamentales de Justicia, por intermedio de la Presidencia del Tribunal Supremo de Justicia, el Órgano Ejecutivo y Ministerio Público por intermedio de la Fiscalía General del Estado.

Las siguientes cartas reflejan las respuestas de estas instituciones:



SALA PLENA
SECRETARIA DE SALA
Of. SP- SS - 805/2019
28 de agosto de 2019

Señor
Félix Fabián Espinoza Valencia
CONSULTOR
FUNDACIÓN CONSTRUIR
Nuestra Señora de La Paz.-

De mi mayor consideración:

A tiempo de expresarle un cordial y respetuoso saludo, mediante la presente, tengo a bien transmitir a su conocimiento conforme lo encomendado en Sesión Ordinaria de Sala Plena de la presente fecha 28 de agosto de 2019, con relación a la carta bajo referencia "Solicitud de información con fines académicos e investigación", lo siguiente:

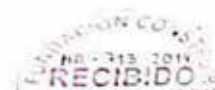
Luego de tomar conocimiento de la correspondencia señalada en la carta de referencia, se ha determinado sugerirle que en mérito a la calidad de la información requerida en el marco del proyecto "Promoviendo Debate Público y Compromisos en Derechos Humanos y Reforma del Sistema de Justicia" cuyos objetivos son laudables, sugerirle acudir ante el Consejo de la Magistratura, por cuanto cuentan con la Unidad Nacional de Estudios Técnicos y Estadísticos, a los fines requeridos.

Sin otro particular, hago propicia la ocasión para hacerle llegar a usted las seguridades de mi más alta distinción con toda atención.

Cordialmente,
smb/er archivo.

Srta. Susana María Murillo Espinoza
SECRETARIA DE SALA
OF. SP-SS
TRIBUNAL SUPLENTE DE JUSTICIA

La información solicitada no fue proporcionada y se hace la sugerencia de acudir a la Unidad Nacional de Estudios Técnicos y Estadísticos.





Sucre, 26 de agosto de 2019
OE.CITE: FGE/Stria. Gral N° 460/2019

Señor:
Felix Fabian Espinoza Valencia
CONSULTOR - FUNDACION CONSTRUIR.
Sucre.-

Ref.: Nota de fecha 20 de agosto de 2019

De mi mayor consideración:

Tengo a bien dirigirme a su persona, en virtud a nota enviada por el cual solicita datos estadístico sobre delitos informáticos y otros delitos relacionados con el Internet, al respecto el Ministerio Público no podrá proporcionarle la información solicitada, puesto que el Ministerio público no se rige a la Ley N° 025 y no tiene la información de las autoridades judiciales o asientos judiciales y menos la reglamentación correspondiente, asimismo hace conocer que el Ministerio Público tiene la pagina institucional www.fiscalia.gob.bo y la página del Facebook, pudiendo acudir a estas paginas con respecto a su solicitud.

Sin otro particular, saludo a usted con las consideraciones más distinguidas.

Atentamente,

Mg. Juan Quipe Mamani
FISCALÍA GENERAL DEL ESTADO

La respuesta a la petición de información señala que no podrá proporcionarse lo solicitado en virtud a la Ley 025 y por no tener la información, remitiendo a la página web y de facebook.

3.1. ACCESO A LA INFORMACIÓN PÚBLICA

Para el profesor Federico Vibes⁸ *“la gran cantidad de información almacenada en la red no tendría la virtualidad que tiene hoy en día si no contara con un sistema de comunicación tan eficaz como el que tiene. Esta modalidad de comunicación y **acceso a la información**, lejos de ser una cuestión pasajera o de moda, constituye un verdadero nuevo patrón de lo que serán las formas de interrelación de ahora en más. La cultura de las relaciones cara a cara ha sido cabalmente desplazada por la cultura de las telecomunicaciones, y en cuanto al modo de comunicarse con los demás, lo que décadas atrás era la excepción (comunicarse a través de telegramas, télex, teléfonos) ha pasado a ser una verdadera regla.”*

A partir de las respuestas de las peticiones de información realizadas, por ejemplo, la respuesta de la Fiscalía General del Estado signada por el secretario general se puede inferir una disociación entre el flujo de información: ciudadano-Estado, sin poder establecer con certeza cómo y qué información es la que la administración pública gestiona así como comparte, conforme a la política estatal de estándares abiertos, plasmada por un plan específico contenido en el Decreto Supremo N° 325 I de 9 de noviembre de 2015.

Por lo que debe concebirse el acceso a la información como un baluarte progresivo, la libertad de información consagrada como corolario de la libertad de expresión en instrumentos internacionales, como el Pacto Internacional de Derechos Civiles y Políticos (1966) y la Convención Americana sobre los Derechos Humanos (1969).

La legislación en materia de libertad de información refleja la premisa fundamental: *“que toda la información en poder de los gobiernos y las instituciones gubernamentales es, en principio, pública y solo podrá ser retenida si existen razones legítimas para no divulgarla, como suelen ser la privacidad y la seguridad.”*

En los últimos diez años, el derecho a la información ha sido reconocido por un cantidad de países, incluidos aquellos en desarrollo, a través de la adopción de numerosas leyes sobre libertad de información. En 1990 solo trece países habían adoptado leyes nacionales sobre libertad de información. En la actualidad hay más de 90 leyes aprobadas sobre Acceso a la Información Pública en países de todo el mundo y hay otras 30 en proceso de redacción, de acuerdo a datos de la Organización de Naciones Unidas.

⁸ Vibes, F. Vibes, Federico P. 18/08/2010. “Acceso a la cultura y derechos de autor”. Revista La Ley, p. 34.

3.2. LEY 1173

La Ley N°1173 de Abreviación Procesal Penal y de Fortalecimiento de La Lucha Integral Contra la Violencia a Niñas, Niños, Adolescentes y Mujeres, promulgada el 3 de Mayo de 2019, destaca por un abordaje integral de la ciberdelincuencia, esta norma tiene por objeto procurar la pronta y oportuna resolución de los conflictos penales, adoptando al efecto, medidas indispensables para profundizar varios aspectos del Código de Procedimiento Penal, implementando:

- a) Una oficina gestora, que unificará la información concerniente a la actividad procesal, permitiendo optimizar procedimientos y recaudación de datos estadísticos.
- b) Instaura y gestiona una comunicación electrónica que hace más efectiva la interacción interpartes así como agiliza plazos procesales, sin considerar las potenciales dificultades de orden informático que puede presentar en tanto la interoperabilidad⁹ y el consentimiento.

3.3. PROYECTO DE LEY MODIFICATORIO: ASPECTO TECNOLÓGICO

En los antecedentes del Informe N°010/2019-2020 de la Comisión de Justicia Plural, Ministerio Público y Defensa Legal de la Cámara de Senadores de la Asamblea Legislativa Plurinacional señala: "(...) la modificación que se realizó incorpora un fuerte componente tecnológico con el uso de las Tecnologías de la Información y Comunicación (TIC's) en la administración de justicia, por el cual se pondrá desarrollar las herramientas de la digitalización:

- a) la aplicación del buzón de notificaciones¹⁰ de ciudadanía digital
- b) la firma electrónica
- c) la digitalización de documentos
- d) el registro de las audiencias y
- e) la interoperabilidad.

Estas tareas estarán a cargo de las Oficinas Gestoras de Procesos. Asimismo, destaca lo señalado en la parte final de la **disposición final primera**: "las herramientas tecnológicas de información y comunicación referidas a las Oficinas Gestoras de Procesos, el buzón de notificaciones de ciudadanía digital y la digitalización

⁹ El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define interoperabilidad como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada (Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990)

¹⁰ El presente acápite cuenta con reglamentación específica

de las audiencias, entrarán en vigencia conforme al Plan de Implementación y funcionamiento progresivo a cargo del Órgano Judicial, que deberá efectivizarse hasta la inauguración del año judicial 2020”.

4. CONCLUSIONES Y RECOMENDACIONES

Todos los aspectos abordados en el diagnóstico permite conocer la situación y tomar acciones certeras desde todos los espacios que hacen a la administración de justicia.

4.1. ÓRGANO JUDICIAL

El Órgano Judicial tiene desarrollado nociones básicas sobre la ciberdelincuencia, descrito tanto con un análisis cuantitativo y cualitativo con el que se han plasmado tablas por estrado judicial de los nueve Tribunales Departamentales de Justicia.

Llegando a las siguientes conclusiones:

- Prácticamente la totalidad de los asientos judiciales ha negado la existencia de algún documento relativo a la **ciberseguridad**.
- No existe un mecanismo idóneo para el **registro de causas**.
- Existen autoridades judiciales que asumen que por el área competencial, no dan a conocer procesos relacionados directa o indirectamente con el ciberespacio.
- En muchos casos se puede divisar la **intervención** de las tecnologías de información así como de comunicación únicamente **en la etapa preliminar** de investigación y de manera complementaria a los medios probatorios tradicionales.
- En promedio la cantidad de delitos informáticos no supera el 30% de la carga procesal a nivel nacional. En cuanto al eje troncal:

La Paz cuenta con la mayor cantidad de procesos registrados relativos a delitos informáticos.

Cochabamba registra los más altos índices de violencia vinculados con el ciberespacio.

En **Santa Cruz** no se ha podido recabar información por negativa de Presidencia.

4.2. BRECHA DIGITAL

Existen hallazgos que permiten evidenciar que, existen jurisdicciones que no cuentan siquiera con acceso a internet. Se puede percibir a su vez que personal de la administración de justicia, entiende que no es parte de sus funciones individualizar la actividad relativa al cibercrimen.

4.3. PRECISIONES METODOLÓGICAS

En algunas casillas se presenta el conteo de un proceso como “1A”, esto debido a que hay un proceso con un potencial concurso real o ideal.

En algunas casillas se presenta el conteo de un proceso con un dígito suelto (1), sin el paréntesis del artículo correspondiente en el código penal, esto sucede porque la autoridad no ha especificado el tipo penal y solamente el bien jurídicovulnerado.

Es frecuente evidenciar en las tablas correspondiente a los delitos informáticos que hayan procesos que versan sobre ambos delitos informáticos de manera concurrente.

4.4. AUSENCIA DE DATOS

No por el hecho de no verse registrado en las tablas, infiere que no existan procesos, sino que esto ocurre debido a: a) la no provisión de información, b) a la inexistencia de sistemas para recabar información, c) a la falta de voluntad del funcionario por entender que no es parte de sus funciones o d) por inhibición al acceso a la información.

4.5. PROTECCIÓN DE DATOS PERSONALES

En los casos en los que sí se ha provisto de información, se puede evidenciar que no existen ni la más mínima noción para con el respeto a la protección de datos personales, habiendo previsto de conversaciones y contenido multimedia sensible.

En el informe de la Fiscalía General del Estado, la autoridad recurrida precisa que en los datos provistos no se contemplan delitos de acción privada, es decir: delitos contra el honor (Arts. 282-290). Esta salvedad no es menos importante, porque, por la política penal adoptada por el Estado Boliviano, se entiende que dichos ilícitos no constriñen el orden público con tal gravedad que amerite la intervención del Estado, y deberán proseguirse por instancia de parte, sin embargo cabe señalar que uno de los fenómenos mas destacables en la era digital es la vulneración masiva y concurrente del honor como bien jurídicamente tutelado, alcanzando; por tal particularidad; un daño calificado que a su vez trasciende eventualmente al menoscabo de otras

garantías y derecho fundamentales, confrontando el postulado tradicional de considerar que dicho disvalor comprenda un daño (lesión) insignificante al orden público (sociedad).

4.6. ACCESO A LA INFORMACIÓN

Así, de la respuesta de la Fiscalía General del Estado signada por el secretario general se puede inferir una disociación entre el flujo comunicacional: ciudadano- Estado, sin poder establecer con certeza cómo y qué información es la que la administración pública gestiona y comparte, conforme a la política estatal de estándares abiertos, plasmada por un plan específico contenido en el Decreto Supremo N° 3251 de 9 de noviembre de 2015.

Por lo que debe concebirse el acceso a la información como un baluarte progresivo, desde la libertad de información consagrada como corolario de la libertad de expresión en otros instrumentos internacionales importantes, como el Pacto Internacional de Derechos Civiles y Políticos (1966) y la Convención Americana sobre los Derechos Humanos (1969).

4.7. POLÍTICAS CRIMINALES

Como Estado, se requieren establecer políticas criminales, progresivas que respondan a los lineamientos que establece en dicha materia el derecho internacional público, a partir del Convenio de ciberdelincuencia, y a su vez, con la tipología instaurada en la abrogada ley N° 1005 de 15 de diciembre de 2017 en la sección IV relativa a delitos informáticos, desde los principios de lesividad calificada y extraterritorialidad.

Como se señala en la parte inicial del presente diagnóstico, la administración de justicia se delata arraigada en la capacidad de realizar una prosecución óptima cuando se trata de ilícitos relacionados con el internet.

Quienes hoy por hoy administran la justicia boliviana, aun no hay tomado plena conciencia de todos los daños directos, colaterales y transversales que ocasiona la ciberdelincuencia.

