TETÃ REKUÁI
GOBIERNO NACIONAL

INFORME DE COMISIONAMIENTO INTERNACIONAL/NACIONAL

Nombre y Apellido:	Giuliana Galli Campos Cervera	Firma:
Dependencia:	Dirección de Asesoría Jurídica	CI Nº: 2.237.505
Tipo de Funcionario	Permanente_X____ Contratado_____ Comisionado_____ Particular _____	
Fecha de Comisionamiento:	DEL 04 AL 07 de diciembre de 2017	
Resolución N°	Senatics N° 174/2017	
Evento y/o Misión (nombre, lugar)	"Foro Hemisférico de Cooperación Internacional contra los Delitos Cibernéticos", llevado a cabo en la sede del Ministerio de Relaciones Exteriores de la República Dominicana, en la ciudad de Santo Domingo, los días 5, 6 y 7 de diciembre del año 2017. Fue organizado conjuntamente por el Consejo de Europa de la Unión Europea, la Organización de Estados Americanos (OEA) y el Departamento de Justicia de los Estados Unidos de Norteamérica.	
Temas tratados y/o actividades realizadas:	Este Foro convocó a funcionarios públicos de numerosos países de América Latina, América Central y el Caribe, involucrados en los procedimientos de investigación, obtención de evidencias y procesamiento de Delitos Cibernéticos, así como funcionarios relacionados a la elaboración y promulgación de legislación vinculada a esta problemática. El objetivo principal del mismo fue el compartir experiencias y casos de éxito en la región, en la investigación y persecución de delitos cibernéticos basandose en la cooperación internacional y los principios sustantivos y procesales establecidos en el Convenio de Budapest, identificando herramientas y su forma de utilización por parte de los países miembros, así como aquellos principales ajustes legislativos o de normativa que deben experimentar aquellos que aun no forman parte de esta Convención y desean hacerlo.	

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
PRESIDENCIA DE LA REPÚBLICA
SENATICS

Resultados:	La adhesión a este Convenio nos permitirá formar parte de los diálogos que se propician entre todos los miembros de esta convención, en los que se discuten guías y pautas de operativas a ser adoptadas para la correcta aplicación de la misma, siempre con el objetivo de lograr la obtención e implementación de las mejores prácticas y herramientas para un efectivo combate a la ciberdelincuencia. Por otra parte, atendiendo a la reciente aprobación de nuestro Plan Nacional de Ciberseguridad, será fundamental poder poner en marcha aquellos ejes y objetivos identificados, siempre a bajo la guía del Convenio de Budapest y todos sus protocolos adicionales, que marcan el camino hacia una efectiva política de ciberseguridad como preventiva del cibercrimen. Por ello, sería fundamental capacitar a todos los actores designados para la ejecución de este Plan, en el alcance y los términos del Convenio de Budapest. Por último, desde el punto de vista institucional, es necesario propiciar un trabajo más coordinado del CERT-Py con los demás actores locales que combaten esta problemática, de forma a complementar esfuerzos, compartir experiencia y capacitación y lograr una posición más fortalecida frente a demás actores que deben ser involucrados en el accionar conjunto: Departamento de Ciberdelitos de la Policía Nacional y Unidad Especializada del Ministerio Público para los Delitos Informáticos.
Compromisos asumidos:	Dar continuidad e impulso al Plan Nacional de Ciberseguridad. Analizar adehsión de SENATICs en representación del Gobierno de Paraguay al "Global Forum on Cyber Expertise o Foro Global para la Ciber Experiencia (GFCE)", que consiste en una organización integrada por países, organizaciones intergubernamentales y empresas privadas, como partes interesadas en el desarrollo de la capacidad cibernética.
Se anexa copia del Certificado u otros Documentos	**Si** ___ **No_X__**
V° B° del Responsable de la Dependencia:	**Firma** **Sello** **Aclaración** G. ALFREDO J. MOREIRA B. Director General de Políticas y Desarrollo de TICs SENATICs

MEMORANDUM A J N° 36/2017

A: **Ing. David Ocampos Negreiros,** Ministro

Cc: **Lic. Mario Benítez,** Director General de Administración y Finanzas

De: **Abg. Giuliana Galli,** Directora
Dirección de Asesoría Jurídica

Objeto: Presentar Informe sobre viaje realizado para participar del "Foro Hemisférico de Cooperación Internacional contra los Delitos Cibernéticos" y Rendición de Cuentas.-

Fecha: 15/12/2017

Tengo el agrado de dirigirme a Usted, con el objeto de informar sobre mi participación en el *"Foro Hemisférico de Cooperación Internacional contra los Delitos Cibernéticos"*, llevado a cabo en la sede del Ministerio de Relaciones Exteriores de la República Dominicana, en la ciudad de Santo Domingo, los días 5, 6 y 7 de diciembre del año 2017.-

Este Foro convocó a funcionarios públicos de numerosos países de América Latina, América Central y el Caribe, involucrados en los procedimientos de investigación, obtención de evidencias y procesamiento de Delitos Cibernéticos, así como funcionarios relacionados a la elaboración y promulgación de legislación vinculada a esta problemática. Fue organizado conjuntamente por el Consejo de Europa de la Unión Europea, la Organización de Estados Americanos (OEA) y el Departamento de Justicia de los Estados Unidos de Norteamérica.

El objetivo principal del mismo fue el compartir experiencias y casos de éxito en la región, en la investigación y persecución de delitos cibernéticos basandose en la cooperación internacional y los principios sustantivos y procesales establecidos en el Convenio de Budapest, identificando herramientas y su forma de utilización por parte de los países miembros, así como aquellos principales ajustes legislativos o de normativa que deben experimentar aquellos que aun no forman parte de esta Convención y desean hacerlo.

Algunos puntos y notas resaltantes tomadas de las intervenciones de cada uno de los expositores, se traen a colación:

- ❖ Sobre la elaboración de una Estrategia Nacional de Ciberseguridad:
- Contar con oficiales de seguridad de la información en las instituciones públicas, que puedan ser nexos para la conformación de una red integrada.
- Buscar implementar Sistemas de Gestión de Seguridad de la Información, con sus respectivas unidades en cada institución pública.
- Establecer un mecanismo de control central.
- Dotar de Presupuesto y personal suficiente para el CERT.

Abg. Giuliana Galli
Directora de Asesoría Jurídica
Secretaría Nacional de Tecnologías de la Información y Comunicación

- Elaborar la Estrategia Nacional sobre una plantilla compatible con las disposiciones del Convenio Budapest.

❖ Elementos principales del Convenio de Budapest:

- El Convenio otorga la base legal que algunos países necesitan para brindar información a otros en cooperación en la investigación de ciberdelitos.
- Tiene un alcance global: 56 países parte.
- Se compone de tres pilares: 1) Derecho Sustantivo, 2) Derecho Procesal y 3) Cooperación Internacional.
- Se han elaborado numerosas Notas Guías sobre las disposiciones del Convenio de Budapest, sobre aquellos aspectos que no estén expresamente en el Convenio (*Botnets, identity theft, DDos attacks, critical infraestructura, malware, subscriber information*).
- La Convención de Budapest no obliga a países a adoptar o imponer medidas de retención de datos de tráfico de forma general, sino solo dispone la necesidad de prever la posibilidad de solicitar la preservación de información concreta de un caso específico, a los proveedores de servicios. Esta posibilidad debe ser dispuesta por Ley.

❖ Evidencias en la Nube:

- Acceso transfronterizo de datos: numerosa jurisprudencia en tal sentido. Existen requerimientos para solicitar el acceso a datos transfronterizo.
- Los países pueden iniciar diálogos de cooperación mutua con grandes prestadores de servicios, de forma a agilizar o estandarizar solicitudes de acceso a información (MOUs).
- Artículos 16, 17 y 18 del Convenio.

❖ Derecho Procesal – Evidencias Electrónicas:

- Desafíos de TICs para proceso penal: regulación expresa vs. libertad probatoria. Al inicio se pensó utilizar medios de prueba convencionales y adaptarlos a lo digital. Principio de Libertad probatoria: "En materia penal, cualquier medio de prueba se puede utilizar para probar cualquier hecho relevante". A diferencia del derecho civil, en el que la prueba debe ser tasada, determinada. Sin embargo, la incorporación de pruebas no reguladas expresamente se ha visto dificultada y enfrentando grandes desafíos. Se insta a aplicar garantías de medios de prueba conocidos a medios no conocidos o nuevos.

❖ Set de medidas procesales básicas incluidas en la Convención de Budapest:

- Concepto de delitos informáticos: todos aquellos que necesitan evidencia digital para probarlos (informáticos, cometidos por medios digitales y comunes en los que se necesita evidencia digital).
- **Conservación de Datos Informáticos:** (vs. Retención de datos), éste último quita necesidad al segundo. No obstante, se optó por el primer mecanismo como regla –conservación de datos-. La segunda –retención de datos de tráfico- en la mayoría de países este tipo norma fue declarada inconstitucional. Hoy en día, está siendo dejada de lado. Se tiene una medida "cautelar" probatoria, que constituye la orden de conservación de datos, que implica ordenar conservación rápida de datos informáticos específicos, incluidos los de tráfico, cuando haya riesgo de pérdida o modificaciones: *"Obligar a esa persona a conservar y a proteger su integridad (máx. 90 días, prorrogables) para que las autoridades puedan obtener la reve-*

Abg. Giuliana Galli
Directora de Asesoría Jurídica
Secretaría Nacional de Tecnologías de la Información y Comunicación

lación. Obligación a mantener el secreto de la ejecución de la medida". Buena práctica: ordenar esta medida al inicio de investigación. No hay afectación a garantías, porque los datos no serán exhibidos ni divulgados, salvo que con orden judicial sean incluidos como medios de pruebas al proceso.

- **Orden de presentación:** Paso previo al allanamiento. Art. 18 de la Convención. No impone obligación de guardar la información a Proveedores de Servicios, se refiere a información existente. Paraguay lo tiene previsto. Prever qué tipo de datos (suscriptor/abonado, contenido, etc.). Prever accesos transfronterizos, datos que una empresa tenga legítimo acceso en su grupo (servidores fuera).
- **Registro y confiscación de datos almacenados:** Art. 19 de la Convención. Analogía de normas de registro y secuestro de elementos físicos. Secuestro del dispositivo y luego orden que habilite registro de datos en laboratorio por ejemplo.
- **Obtención en tiempo real de datos de tráfico:** Art. 20 de la Convención. Se utiliza por analogía intervención de teléfonos, pero puede ser excesiva.

❖ Nuevos problemas surgidos con posterioridad a la Convención:

- Anonimato/ encriptación / Deep Web / Alojamiento de información en la nube: Con mismas garantías de agente encubierto.
- Rastrillaje informático. Redes abiertas. Big Data, ingeniería social. Desafíos que aun por medio de redes abiertas, se obtengan datos privados que podrían no ser válidos.
- Técnicas de *"remote forense"*. Troyanos federales, malware utilizado por el Estado. Casos de encriptación, es útil pero peligroso ante garantías constitucionales, éstas deben ser más fuertes que incluso figura de allanamiento en domicilio. Regulación es fundamental para que la intromisión en garantías constitucionales pueda ser aceptada.

❖ Evidencia digital y cooperación internacional para su obtención:

- EEUU divide evidencia en 3 categorías: a) información del subscriptor; b) registros de transacciones; c) contenido del mensaje.
- Hay dos maneras para que fiscales extranjeros obtengan información: **a) Mecanismos de los prestadores** (Facebook formulario online): Utilizar cuenta de correo institucional. Tener en cuenta que si vas al proveedor de servicios, estos pueden notificar al suscriptor. También implica preservación de tal como se encuentra (no de otros estados, anterior, futuro); **b) Grupo 24x7:** Garantiza preservación. Requisitos de disponibilidad y conocimiento técnico básico. Conocimiento de leyes de preservación de su país. Inglés.
- Solo se utiliza preservación en casos penales no civiles. Dura 90 días y si necesitas tiempo adicional, se notifica antes del vencimiento de ese periodo para ampliación por otros 90. Eventualmente debe hacerse requisito formal pero ya se encuentra preservada la información.
- Fuentes informales: agregados de la Embajada de US, FBI. No obstante, uso limitado de la evidencia, no admisible pero de gran valor investigativo.

Abg. Giuliana Galli
Directora de Asesoría Jurídica
Secretaría Nacional de Tecnologías de la Información y Comunicación

Conclusiones para el contexto Paraguay

En el país actualmente se encuentra en proceso la adhesión formal al Convenio de Budapest (a la fecha en estudio por la Cámara de Diputados, con sanción favorable de la Cámara de Senadores).

La adhesión a este Convenio nos permitirá formar parte de los diálogos que se propician entre todos los miembros de esta convención, en los que se discuten guías y pautas de operativas a ser adoptadas para la correcta aplicación de la misma, siempre con el objetivo de lograr la obtención e implementación de las mejores prácticas y herramientas para un efectivo combate a la ciberdelincuencia.

Por otra parte, atendiendo a la reciente aprobación de nuestro Plan Nacional de Ciberseguridad, será fundamental poder poner en marcha aquellos ejes y objetivos identificados, siempre a bajo la guía del Convenio de Budapest y todos sus protocolos adicionales, que marcan el camino hacia una efectiva política de ciberseguridad como preventiva del cibercrimen. Por ello, sería fundamental capacitar a todos los actores designados para la ejecución de este Plan, en el alcance y los términos del Convenio de Budapest.

Por último, desde el punto de vista institucional, es necesario propiciar un trabajo más coordinado del CERT-Py con los demás actores locales que combaten esta problemática, de forma a complementar esfuerzos, compartir experiencia y capacitación y lograr una posición más fortalecida frente a demás actores que deben ser involucrados en el accionar conjunto: Departamento de Ciberdelitos de la Policía Nacional y Unidad Especializada del Ministerio Público para los Delitos Informáticos.

Adjunto Rendición de Cuenta de Viático institucional.

Atentamente.-

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN · PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY · SENATICs · Asunción

Abg. Giuliana Galli
Directora de Asesoría Jurídica
Secretaría Nacional de Tecnologías de la Información y Comunicación

RECIBIDO
Dir. Gral. de Adm. y Finanzas
SENATICS
Por: Lic. Noelia Rojas
Fecha: 19/12/2014 Hora:.....