



## DOCUMENTO DE POSICIÓN PAÍS

# Resiliencia de las Infraestructuras Críticas, protección de menores de edad en Internet y Seguridad Cibernética

Tipo de Documento: Otros

Fecha de Publicación: 31 de diciembre de 2012

Clasificación: Acceso Público

## CONTROL DE VERSIÓN

DOCUMENTO NO.: AIG-035  
PREPARADO POR: Raúl Millán  
APROBADO POR: Eduardo Jaén  
FECHA DE INICIO: 27 de diciembre de 2012.  
ESTADO DEL DOCUMENTO: Borrador  
HISTORIA DE CAMBIOS:

<b>Fecha</b>	<b>Cambios</b>	<b>Autores</b>	<b>Versión</b>
2012/12/31	Documento inicial	Raúl Millán - AIG	0.1
2013/1/4	Protección de menores	Pablo Ruizdiaz - AIG	0.2
2013/1/9	Protección de menores y resiliencia de infraestructuras críticas	Juan Carlos Espinosa – MINREX	0.3
2013/1/15	Correcciones de formato y adiciones	Eduardo Jaén - AIG	0.4
2013/1/17	Cambios sugeridos	Leoncio Hernández - MINREX	0.5
2013/1/22	Revisión ortografía y gramática	Silvia Batista / Raúl Millán - AIG	0.6

## **CONTENIDO**

<b>1. INTRODUCCIÓN .....</b>	<b>4</b>
<b>2. TEMAS .....</b>	<b>4</b>
<b>2.1. RESILIENCIA DE LAS INFRAESTRUCTURAS CRITICAS DEL PAÍS .....</b>	<b>4</b>
<b>2.2. PROTECCIÓN DE LOS CIUDADANOS EN LA RED, ESPECIALMENTE LOS MENORES DE EDAD .....</b>	<b>5</b>
<b>2.3. POLÍTICA DE DELITO CIBERNÉTICO Y ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA ...</b>	<b>6</b>
<b>3. CONCLUSIONES.....</b>	<b>7</b>

## 1. INTRODUCCIÓN

---

Con el crecimiento sin precedentes de Internet en todo el mundo, las dimensiones internacionales del delito cibernético, y las amenazas que el mismo representa a las infraestructuras críticas del país, a los menores conectados a la red, a la libertad de expresión y a la seguridad en el ciberespacio en general; es necesario que el país adopte una posición cónsona con las mismas.

Los avances tecnológicos como es el uso de Internet, han facilitado la globalización del delito cibernético, que constituye una amenaza a la infraestructura crítica del país, de manera especial a los menores conectados a la red, a la libertad expresión y la seguridad en el ciberespacio de los ciudadanos, por lo que es necesario establecer mecanismos adecuados para combatirlo

Con el fin de determinar la posición de la República de Panamá al respecto de esta problemática, se ha preparado el presente “documento de posición”, donde se da a conocer las acciones adoptadas por el país en cada uno de los temas relacionados.

## 2. TEMAS

---

### 2.1. Resiliencia de las infraestructuras críticas del país

Se asumen las siguientes políticas y posiciones con respecto a este tema:

- La dependencia cada vez mayor de la conectividad para el funcionamiento normal de la sociedad hace que la protección de la conectividad sea una cuestión crítica para todos; al tratarse de un recurso compartido como lo son el aire limpio o el agua, el reto se define como un reto de **interdependencia**.
- Ninguna organización puede resolver esta cuestión por sí sola, y debe adoptarse un enfoque multilateral de **colaboración**; incluso los competidores de un mismo sector deben convertirse en asociados en un intento por garantizar un entorno estable y de confianza.
- Se ha incrementado el riesgo cibernético en todos los ámbitos y sus modus operandi evolucionan constantemente, lo que nos obliga a implementar estrategias con nuevas tecnologías y metodologías para enfrentar el ciberdelito.

- Las soluciones que se centran en aspectos específicos pronto quedarán obsoletas; es necesario un enfoque basado en **principios**; ideas fundamentales que rijan sobre futuras soluciones.
- La **libre circulación de información** debe seguir impulsando el valor económico; una economía aislada es una economía congelada.
- La **libre circulación de información** contribuye al fortalecimiento del desarrollo económico, social y cultural de la nación.
- El objetivo es la **resiliencia**, no la intensificación del aislamiento; sabiendo que se van a producir fallos, se deben procurar mecanismos para el pronto restablecimiento de las operaciones habituales y garantizar la protección de los activos y de la reputación.
- La principal vulnerabilidad de numerosas organizaciones es de carácter humano: **concienciación, liderazgo y ejecución**.
- La función de los líderes consiste en **fijar la estructura y marcar la pauta**; el perfil de riesgo de una organización puede mejorar sustancialmente mediante la aplicación de prácticas sencillas.

Así, el objetivo de esta iniciativa consiste en alcanzar un compromiso con respecto a un conjunto común de principios compartidos en materia de liderazgo: cambiar la mentalidad para dejar de limitarse a asegurar las fronteras e incluir también la **atención a la interdependencia y a la resiliencia**.

## 2.2. Protección de los ciudadanos en la red, especialmente los menores de edad

Internet es cada vez más accesible para la mayoría de los habitantes del planeta. En Panamá, el Gobierno Nacional ha puesto a la disposición de más del 85% de la población acceso a internet gratuito, a través de puntos de acceso WiFi, con controles de contenido y de seguridad para mantener la integridad del bien público compartido por miles de ciudadanos.

En Panamá consideramos que el acceso a Internet es parte de los derechos ciudadanos y por lo tanto, compartimos la tesis que debe ser parte de los derechos humanos y de las libertades fundamentales debidamente reconocidas por el derecho internacional y nacional.

El libre acceso a las redes de internet y el intercambio de conocimiento humano deben fundamentarse en base a los principios de acceso universal a la información sin discriminación, tomando las medidas necesarias para proteger a los grupos vulnerables en la

sociedad, en especial a los menores, contra cualquier tipo de abuso y violación de sus derechos humanos.

Considerando la visión del Gobierno Nacional de impulsar una Agenda Digital Estratégica, el Plan estratégico para el desarrollo de la Banda Ancha en la República de Panamá, y la Estrategia Nacional para la Seguridad Cibernética y Protección de Infraestructura Crítica, los retos que generan la disponibilidad de información y conectividad en la protección al ciudadano y especialmente a los menores, hace obligante apoyar todas las iniciativas destinadas a reforzar la legislación existente y cuando fuera necesario, hacerle los ajustes requeridos, para lograr la persecución del delito cibernético que actualmente se protege bajo el anonimato que la Internet provee.

Esto es especialmente cierto cuando dichos delitos involucren a menores de edad, donde se hace necesario tratar los temas asociados con sollicitación, pornografía infantil, bullying, grooming y otros.

Es la posición del Estado Panameño, la **protección de los menores en la red** (Internet), a través de todos los medios técnicos y legales que estén a su alcance.

El Internet es un instrumento para promover la paz, la estabilidad, la cohesión social, la buena gobernanza y el estado de derecho, por lo tanto, el gobierno, el sector privado y la sociedad civil deben trabajar armónicamente para que este instrumento sea accesible a toda la población panameña y utilizarla adecuadamente conforme a las disposiciones legales.

### **2.3. Política de delito cibernético y estrategia nacional de seguridad cibernética**

Creemos firmemente que para poder obtener un desarrollo regional sostenible de las nuevas maneras de hacer negocio (comercio electrónico) y comunicarse con los ciudadanos (gobierno electrónico), es imperativo que se actué sobre el plano de **cooperación regional y multilateral**; con el fin de armonizar las legislaciones existentes y en desarrollo, destinadas a combatir al delito a través de Internet en todas sus modalidades, tales como, Terrorismo, Crimen Organizado, Tráfico ilegal de Drogas, Blanqueo de Capitales, Propiedad Intelectual, protección al menor, entre otros.

La **Estrategia Nacional de Seguridad Cibernética** es un instrumento que refleja un acuerdo de Estado y sirve como guía para la ejecución de políticas públicas en Seguridad Cibernética y Protección de Infraestructuras Críticas, y refleja el compromiso máximo de la República de

6

Panamá para la protección de su ciberespacio y la colaboración con otras instituciones nacionales e internacionales con el propósito de alcanzar este mismo fin a nivel mundial.

La Estrategia Nacional cuenta con los siguientes pilares:

- Promover el desarrollo de **conectividad y telecomunicaciones** a nivel nacional.
- **Proteger la privacidad y los derechos fundamentales** de los ciudadanos en el ciberespacio
- **Prevenir y detener las conductas delictivas en el ciberespacio** o el uso de éste para cualquier tipo de delitos o actos ilícitos.
- **Fortalecer** la seguridad cibernética de las infraestructuras críticas nacionales.
- Fomentar el **desarrollo de un tejido empresarial nacional** fuerte en seguridad cibernética, como referencia para la región.
- Desarrollar una **cultura de seguridad cibernética** a través de la formación, innovación y la adopción de estándares.
- **Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes** de los organismos públicos.

### 3. CONCLUSIONES

---

Afrontar los retos derivados de vivir en un mundo hiperconectado requiere de una política nacional clara, que, protegiendo la libre circulación de información, evite que las nuevas tecnologías y en especial el Internet, sea utilizada para actividades ilícitas y contra la reputación de los ciudadanos.

Especial mención merece la necesidad de impulsar la resiliencia de las infraestructuras críticas, la protección de ciudadanos y menores de edad en la red y fortalecer la seguridad cibernética de las organizaciones públicas y privadas del país. Creemos que la mejor manera de enfrentar las tareas resultantes, es a través de la colaboración multilateral, de la capacitación de usuarios y de la adopción de mejores prácticas.

En las acciones a seguir, el país debe tomar en cuenta el Plan de Acción de Túnez, del 2005, sobre la Sociedad de la Información y la Declaración de Principios de Ginebra, así como las resoluciones relevantes del Consejo de Seguridad de las Naciones Unidas.

La posición de la República de Panamá es **apoyar todas las iniciativas regionales e internacionales en el combate del ciberterrorismo y cibercrimen**, en cumplimiento de las Resoluciones de la ONU y de la OEA sobre la materia.

7

Panamá cree y defiende una Internet libre, solo regulada en aspectos que tienen que ver con su uso inadecuado o para fines ilícitos.