GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para
la Innovación Gubernamental

DOCUMENTO DE POSICIÓN

Resilencia de las Infraestructuras Criticas, protección de menores de edad en Internet y Seguridad Cibernetica

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:

Fecha	Cambios	Autores	Versión
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 resilencia de infraestructuras criticas	Juan Carlos Espinosa – Ministerio de Relaciones Exteriores	0.3

CONTENIDO

Autoridad Nacional para la Innovación Gubernamental
Vía Ricardo Arango y Calle 61 Obarrio, Bella Vista Edificio Sucre, Arias & Reyes – Nivel 300
Tel: +507 282-0328 Fax: +507 517-9500

1. INTRODUCCIÓN

Con el crecimiento sin precedentes de Internet en todo el mundo, las dimensiones internacionales del delito cibernético, y las amenzas que el mismo representa a las infraestructuras criticas del páis, 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 consona con las mismas.

Con el fin de determinar la posición del país al respecto de esta problemática, se ha desarrollado 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. Resilencia de las infraestructuras criticas 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.
- El panorama del **riesgo cibernético** evoluciona a un ritmo acelerado: las estrategias defensivas nos llevan siempre a librar la última batalla, y existen numerosas "interrogantes".
- Se ha incrementado el riesgo cibernético en todos los ámbitos y sus modus operandi evolucionan constatemente, 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.

Autoridad Nacional para la Innovación Gubernamental
Vía Ricardo Arango y Calle 61 Obarrio, Bella Vista Edificio Sucre, Arias & Reyes – Nivel 300
Tel: +507 282-0328 Fax: +507 517-9500

- La **libre circulación de información** contribuye al fortalecimiemnto 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, el objetivo consiste en restablecer 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 sigue siendo inaccesible para la mayoría de los habitantes del planeta, y para disminuir esta diferencia entre los ciudadanos Panamá a puesto a la dispoción de más del 85% de la población acceso a internet gratuito, a través de puntos de acceso WiFi, con controles de contendio y de seguridad para mantener la integridad del bien público compartido por miles de cuidadanos.

El acesso a Internet debe estar orientado a la universalidad y a los principios de los derechos humanos y a 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, discapacitados, entre otros, contra cualquier tipo de abuso y violación de sus derechos humanos.

Considerando la visión del Gobierno Nacional de impulsar la agenda digital, el Plan estratégico para el desarrollo de la Banda Ancha en la Republica de Panamá, y la Estrategia Nacional para la

Autoridad Nacional para la Innovación Gubernamental
Vía Ricardo Arango y Calle 61 Obarrio, Bella Vista Edificio Sucre, Arias & Reyes – Nivel 300
Tel: +507 282-0328 Fax: +507 517-9500

Seguridad Cibernetica y Protección de Infraestructura Critica, los retos de protección al ciudadano y especialmente a los menores, que se generan de la disponibilidad de información y conectividad que las TICs proveen; se hace necesario apoyar todas las iniciativas destinadas a enforzar la legislación existente y hacer los ajustes necesarios a la misma para lograr la persecución del delito cibernético, que actualmente se protege bajo el anonimato que Internet provee.

Esto es especialmente cierto cuando dichos delitos involucren a menores de edad, donde se hace necesario tratar los temas asociados con solicitación, 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 disposciones legales.

2.3. Politica de delito cibernético y estrategia nacional de seguridad cibernetica

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**; 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, Trafico ilegal de Drogas, Blanqueo de Capitales, Propiedad Intelectual, proteccion 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 del Estado Panameño para la protección de su ciberespacio y la colaboración con otras instituciones nacionales e internacionales para alcanzar este mismo fin a nivel mundial.

La Estrategia Nacional cuenta con los siguientes pilares:

- Promover el desarrollo de conectividad y telecomunicación nacional desde el ciudadano hasta el sector privado y el sector gubernamental..

Autoridad Nacional para la Innovación Gubernamental
Vía Ricardo Arango y Calle 61 Obarrio, Bella Vista Edificio Sucre, Arias & Reyes – Nivel 300
Tel: +507 282-0328 Fax: +507 517-9500

- **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

La Dirección de Organismos sugiere respetuosamente que se tome en cuenta el Plan de Acción de Túnez, del 2005, sobre la Sociedad de la Información y de la Declaración de Principios de Ginebra y el Plan de Acción del año 2003, asi como las resoluciones relevantes del Consejo de Seguridad de las Naciones Unidas.

La posición de la Republica de Panama en torno al ciberterrorismo **ha sido apoyar todas las iniciativas regionales e internacionales en el combate el ciberterrorismo y cibercrimen y el cumplimiento de las Resoluciones de la ONU y de la OEA, o sea conforme a las normas del Derecho Internacional**

Autoridad Nacional para la Innovación Gubernamental
Vía Ricardo Arango y Calle 61 Obarrio, Bella Vista Edificio Sucre, Arias & Reyes – Nivel 300
Tel: +507 282-0328 Fax: +507 517-9500