Relatoría Panamá, 20 de julio de 2023.
Foro de Gobernanza de Internet – Panamá 2023

Fecha del evento: 20 de julio de 2023.
Lugar: hotel Riu Panama Plaza.
Transmisión: YouTube Live.
Hora: 09:30am – 10:30am
Organizado por: AIG, NIC-Panamá y CAPATEC.
Moderador: Ing. Eli Faskha (Soluciones Seguras).

Panelistas:
Mgter. Leandro Espinoza (Universidad Tecnológica de Panamá - Academia),
Ing. Annya Martínez Foster (Cisco - Empresa Privada),
Ing. Juan Ramón Anria (AIG - Gobierno),
Mgter. Johanna Andreina Parra Acevedo (En representación de Sonda y Palo Alto Networks - Empresa Privada) e
Ing. Ericka Valdés (Wosec Panamá- Sociedad Civil).

Panel II – Ciberseguridad en el contexto de la Gobernanza de Internet.

Esta sesión inicia con el saludo por el moderador del panel, Ing. Eli Faskha quien dio un agradecimiento por la asistencia y motivó a la participación durante las sesiones del foro de Gobernanza de Internet.

Posteriormente Eli Faskha da paso al panel con la interrogante, ¿Cuál es el papel de la ciberseguridad dentro del marco de la Gobernanza de Internet?

El Mgtr. Leandro Espinoza inicia su intervención señalando que nadie puede regular el Internet y que su evolución depende de un consenso primario sobre cuestiones técnicas y códigos para su funcionamiento.

Pregunta del moderador para los panelistas ¿cuáles son las principales tendencias y desafíos en materia de ciberseguridad que están afectando la gobernanza de Internet en la actualidad?

Seguidamente toma la palabra la Ing. Annya Martínez, indicando que debido a que el uso del Internet se ha vuelto más importante por el consumo de aplicaciones y servicios que hoy día se encuentran de manera distribuida, permitiendo una mejor flexibilidad y disponibilidad, expandiendo la capacidad de usuarios brindándoles un servicio mucho más ágil; lo que a su vez deriva en retos en cuanto al control del uso de esos recursos pues habría que evaluar comportamiento normal de los mismos. También señala que la automatización del estudio del comportamiento de los usuarios puede ayudar a la visibilidad y cambia el esquema de un ambiente reactivo a ir a un paso más adelante para prever cualquier situación que se pudiera dar y actuar antes de la eventualidad.

Eli Faskha continúa con la interrogante ¿Qué iniciativas y estrategias ha implementado el Gobierno para abordar los desafíos de ciberseguridad en el contexto de la gobernanza de Internet? dirigida al Ing. Juan Ramón Anria.

El Ing. Juan Ramón Anria expresa que el Gobierno está trabajando en aspectos de Gobernanza de Internet desde el 2021 en la actualización de la Estrategia Nacional de Ciberseguridad, y hace énfasis en que Gobernanza y Gobierno no son sinónimos, y que no es papel del Gobierno ni fiscalizar ni controlar el Internet sino promover el trabajo conjunto de las múltiples partes interesadas.

La estrategia tiene la visión de que Panamá se convierta en una nación que opera con un ciberespacio abierto, libre, seguro y resiliente que salvaguarda los derechos y libertades fundamentales del pueblo, confiando en el trabajo colaborativo y continuo, promoviendo una conciencia universal que la ciberseguridad es responsabilidad de todos.

El moderador pregunta a los panelistas ¿Cómo pueden los ciudadanos participar activamente en el proceso de Gobernanza de Internet para asegurar que sus intereses sean tomados en cuenta? La Ing. Ericka Vega, interviene indicando que la participación de cada uno en el foro es parte de la contribución como ciudadanos, que nuestra voz es importante y debe hacerse presente incluso en temas de legislación pues aparte de que es parte de nuestros derechos, una Internet abierta; también es nuestro deber participar en todos los aspectos de ciberseguridad.

Eli Faskha menciona que las empresas privadas juegan un papel fundamental en la infraestructura y servicios de internet y cuestiona a la Mgtr. Johanna Parra sobre ¿cómo la empresa privada aborda los desafíos de la ciberseguridad para proteger a los activos y usuarios?

La panelista empezó indicando que el principal desafío de los activos digitales y usuarios es la seguridad ante las amenazas, por lo cual las empresas se enfocan en 4 aspectos fundamentales: implementar soluciones consolidadas, la automatización y orquestación de los incidentes de ciberseguridad dando paso a departamentos de seguridad robustos, capacitación y formación de los usuarios como eje primordial de la protección tanto de ellos como de sus activos digitales, y la creación de procesos y procedimientos a eventualidades de seguridad cibernética con respuestas rápidas y eficaces.

El moderador procede a consultar ¿cuál es el papel de la investigación y la educación en ciberseguridad para fortalecer la resiliencia y protección de los sistemas y usuarios en el entorno digital? Interviene el Mgtr. Leandro Espinoza indicando que, como parte de las iniciativas en base a esta temática, es importante que el sector Academia mantenga su oferta académica actualizada. Posteriormente, el moderador puntualiza que hay iniciativas como INDICATIC, lo que permite visualizar la importante de todos estos proyectos de tipo educativo a favor del fortalecimiento tanto de los usuarios como de los sistemas, con un alto impacto en materia de resiliencia.

Consulta del moderador al Ing. Juan Ramón Anria, ¿Cómo se están coordinando a nivel nacional e internacional para enfrentar amenazas cibernéticas que trascienden fronteras?

El Ing. Anria plantea que actualmente Panamá no cuenta con una ley de cibercrimen con lo cual se limitan las funciones del fiscal de ciberdelito, sin embargo, a nivel internacional, el panorama es complicado ya que muchos países no cuentan ni con leyes ni con estrategias de ciberseguridad, lo que hace que el trabajo en modo colaborativo sea su única alternativa. Cada vez que ocurre algún suceso es a través de los CERT (Computer Emergency Response Team) que se han podido solventar muchos de estos casos. La red de CSIRTS de las Américas y a través de acuerdos internacionales públicos y privados, permite la integración e intercambio de información de amenazas o vectores de ataques, sin revelar información sobre la víctima del ataque, solo el tipo de ataque. También indica que es primordial el entrenamiento de fiscales, peritos, jueces, magistrados y demás, para que puedan entender el flagelo del cibercrimen y todos los términos subyacentes y procesar eventos cibernéticos.

Eli Faskha apoya esta información, indicando que a través del Threat Map para visualizar todo lo que está pasando en tiempo real a nivel mundial:

El moderador dirige la pregunta ¿Por qué hacemos todo esto? ¿Una mejor ciberseguridad afecta el crecimiento económico, es una ventaja o desventaja?

Interviene la Ing. Annya Martínez, señalando que la seguridad no es algo opcional, sino que debe ser algo intrínseco en las organizaciones y usuarios en general. En su opinión, la ciberseguridad puede impactar de manera positiva la economía de los países.

Como país podemos aprender lecciones tomando en cuenta los eventos de ciberseguridad ocurridos en otros países, lo que puede ser de gran ayuda para actuar antes que algo suceda en el nuestro. Todo esto apoya el crecimiento económico dentro de las organizaciones y al final en el país.

La siguiente pregunta del moderador fue ¿cuáles son las principales preocupaciones en torno a la ciberseguridad y su impacto en la privacidad y los derechos humanos?

La Mgtr. Johanna Parra interviene indicando que, al consumir contenido en línea en cuestión de segundos, también es un grave riesgo para la seguridad de los ciudadanos. Por ejemplo, a través del malware, ingeniería social y demás, los ciberdelincuentes pueden tener acceso a nuestra información privada y bancaria, desde el anonimato total.

Opina que los usuarios debemos conocer a qué nos estamos enfrentando para hacernos responsables de nuestras propias acciones y así crear prácticas seguras que nos permitan

tener soluciones para prevenir amenazas que nos ocasiones un daño y vulneren nuestros derechos humanos.

Luego, Eli Faskha pregunta ¿Cómo se logra el equilibrio entre la seguridad en línea y los principios de apertura, inclusión y libre expresión?

Interviene la Ing. Ericka Valdés, indicando que el equilibrio es importante llegando a una sinergia multipartita, donde cada uno debe aportar esfuerzos, ya que la mayoría de los ataques inicia a través de los individuos por ende debemos estar alertas.

Plantea que través de estos principios, se puede lograr que haya más oportunidades para comunidades remotas. Puntualiza que debemos recordar que el Internet nació de protocolos no seguros, que a través de la evolución de la tecnología y la práctica ha sido necesario ir evaluando, han tenido que nacer las capas de seguridad para fortalecer nuestra experiencia como usuarios. Menciona que todo comienza con nosotros, el Internet es de doble filo, hay que utilizar el hilo adecuado.

Para finalizar, pasamos a la sesión de preguntas del público, donde consultaron algunas recomendaciones a la sociedad para introducirse de manera adecuada al ecosistema digital, para posteriormente, el cierre del panel por parte del moderador.