El "Foro de Gobernanza de Internet" se presentó como un espacio crucial para el diálogo y la reflexión sobre el futuro digital. El moderador del evento fue Roberto de Sousa, quien coordina el equipo de respuesta de las Naciones Unidas para América Central, con sede en Panamá.

Apertura y Contexto General

De Sousa destacó que, desde hace más de una década, se ha abierto el camino para utilizar la tecnología en beneficio de la vida. Sin embargo, en la era digital actual, persisten desafíos significativos, como la confianza en el uso de los datos personales y el hecho de que millones de personas aún no tienen acceso básico a Internet.

En este contexto, el Pacto Digital de 2024 emerge como una hoja de ruta esencial. A través de este pacto, los estados se han comprometido a fomentar un uso seguro e inclusivo de la tecnología. Además, el foro se caracteriza por permitir que todas las partes interesadas participen en igualdad de condiciones, promoviendo un diálogo constructivo.

Un principio fundamental que se enfatizó fue la necesidad de poner a las personas en el centro de la transformación digital. La tecnología, se afirmó, debe ser una herramienta para construir sociedades más justas. Esto implica la urgencia de regular el uso nocivo de la tecnología para evitar que los algoritmos tomen decisiones que vayan en contra de la humanidad. Se subrayó que este no es un debate meramente técnico, sino un espacio para discutir las necesidades de nuestra sociedad. Una pregunta central que surgió fue: "¿Quién está realmente detrás de la pantalla?"

Panel de Expertos y la Identidad Digital

El panel estuvo conformado por **Vielsa Gómez, Omar Gudiño, Juan Carlos Paris y Lidia María Ng**, quienes abordaron diversos aspectos de la identidad digital.

Inicialmente, se reconoció que aún existe una brecha digital en el acceso a Internet. Sin embargo, Panamá cuenta con normativas para proteger al ciudadano, como la Ley de Protección de Datos. Aunque existen mecanismos como la firma electrónica, su uso no está generalizado y se limita principalmente a ámbitos comerciales y ciertos procesos específicos.

Una pregunta clave que se planteó fue: **"¿Qué entendemos por identidad digital confiable?"**

- **Vielsa Gómez** definió la identidad digital como aquello que nos dice quiénes somos y está intrínsecamente ligada a lo que compartimos. Hizo hincapié en la necesidad de tener precaución con lo que se comparte, recordando que todo lo que se hace en el ciberespacio permanece allí.

- **Omar Gudiño** se refirió a la identidad digital como la capacidad de identificar a un individuo. Al cuestionarse "¿Quiénes somos?", señaló que los mecanismos tradicionales, como la cédula, ya no son suficientes. Destacó que los mecanismos de Inteligencia Artificial (IA) son capaces de realizar esta identificación, pero advirtió que a medida que la tecnología avanza, también lo hacen los métodos que la hacen vulnerable.
- **Juan Carlos** Paris explicó cómo los mecanismos de autenticación han evolucionado para incluir la biometría, así como la capacidad de la tecnología para analizar las acciones del usuario y determinar quién está detrás de los dispositivos. Resaltó que las técnicas de autenticación siguen perfeccionándose y enfatizó la importancia de educar a los usuarios sobre el uso de la biometría para fomentar una mayor confianza en su adopción.
- **Lidia Ng** conceptualizó la identidad digital como "un yo en el mundo digital" y la forma en que nos identificamos en este entorno. Subrayó las intenciones gubernamentales de generar confianza en el uso de la tecnología en el ámbito digital, especialmente en relación con trámites y procesos.

Desafíos y Propuestas en Ciberseguridad

En cuanto a los desafíos y la implementación de la ciberseguridad en Panamá, los panelistas ofrecieron diversas perspectivas:

- **Vielsa Gómez** identificó la falta de conocimiento sobre la seguridad de la información como un obstáculo principal. Propuso implementar la concienciación en las escuelas a largo plazo, así como promover la salud digital y la sensibilización en los hogares, haciendo hincapié en los casos de hackeo en redes sociales.
- **Omar Gudiño** se refirió a la inseguridad en las redes sociales, donde "nunca se está seguro de con quién se habla". Mencionó que las redes que ofrecen seguridad suelen cobrar por ello, y que la seguridad debería ser una característica predeterminada en las aplicaciones. Afirmó que solo las grandes empresas brindan una seguridad robusta, mientras que el resto de los usuarios están expuestos a información falsa. Criticó que la identificación en redes sociales "sigue siendo un chiste" y abogó por la implementación de autenticación biométrica en todas las aplicaciones, mejorando los mecanismos de autenticación y fomentando una mayor culturización. Consideró crucial la implementación de la seguridad informática en los centros educativos, ya que los jóvenes pueden llevar el mensaje a casa.
- **Juan Carlos Paris** señaló que muchas leyes han llegado tardíamente y que el mayor reto en Panamá es la educación. Enfatizó que cada ciudadano tiene un derecho absoluto sobre sus datos, lamentando la baja protección que a menudo se recibe. Hizo hincapié en cómo los datos sensibles siguen siendo utilizados de mala manera para discriminar, y destacó la importancia de la Ley 81 (Derechos de nuestros datos), invitando a la ciudadanía a conocerla para tener mayor confianza en el uso de su información.

- **Lidia Ng** resaltó la necesidad de concientizar a los padres sobre el uso de equipos tecnológicos para evitar que sean víctimas de robos de identidad. Percibe la urgencia de implementar la educación cibernética y que se necesita reforzar las leyes para brindar confianza a los usuarios de las oficinas gubernamentales.

La educación en ciberseguridad y un estudio más profundo de la Ley 81 surgieron como temas prioritarios.

Firma Electrónica, IA y Autenticación

El panel también abordó la firma electrónica y el papel de la IA en la identificación:

- **Lidia Ng** planteó las condiciones necesarias para el uso de la firma electrónica en Panamá: un marco jurídico que coordine a todas las instituciones para su uso intercomunicativo. Destacó la importancia de la transparencia, explicando dónde se encuentran los datos de los usuarios y por qué se utilizan, para fomentar una mayor confianza y el uso generalizado de la identidad digital.
- **Omar Gudiño** se refirió al uso de la IA en la identificación y autenticación digital, afirmando que la biometría correctamente implementada es "sumamente robusta". Esto puede ayudar a reducir los márgenes de error, pero advirtió sobre el mal uso, que puede llevar a malas consecuencias. Subrayó que las probabilidades y estadísticas son claves en la biometría, y que la investigación es crucial para determinar qué otros métodos se utilizarían si la tecnología falla. Instó a utilizar la biometría con las herramientas adecuadas.
- **Juan Carlos Paris** destacó el rol pionero de la banca en la autenticación digital, donde los usuarios constantemente intentan vulnerar sus fondos. Resaltó que los mecanismos de seguridad bancarios son a menudo adoptados por los gobiernos. La necesidad de sistemas robustos en la autenticación digital es fundamental. Finalmente, abogó por una firma digital centralizada en un solo ente, cuyo uso sea simple pero seguro para que su adopción sea más global.
- **Vielsa Gómez** se centró en la ciudadanía digital y el rol de los programas educativos desde edades tempranas. Considera esencial enseñar el uso de la identidad digital y entrenar a los niños para su protección desde una edad temprana, dando el ejemplo de un código para recoger a los niños. La meta es que la concienciación no sea solo una capacitación, sino que se transforme en un hábito. Aludió a la existencia de la desinformación (infodemia) y la necesidad de tener cuidado con el uso de aplicaciones de IA, ya que no toda la información es real. Mencionó el "error de capa 8", refiriéndose a las habilidades blandas.

Una pregunta clave dirigida al panel fue: **"¿Cómo se garantiza una mayor confianza en la ciberseguridad en el contexto de la Ley 81?"**

La respuesta sugirió que un castigo penal puede ser una mejor garantía. Se mencionó la importancia de la firma digital y la necesidad de traducir el contenido publicado por la AIG (Autoridad Nacional para la Innovación Gubernamental) al respecto.

Se resaltó la disponibilidad de numerosas herramientas gratuitas para implementar la ciberseguridad y la necesidad de tener cuidado al proporcionar dispositivos electrónicos a menores. Finalmente, se destacó que la ciberseguridad es un "negocio muy bueno".

Como conclusiones clave, se enfatizó la necesidad de capacitación a todos los niveles en "seguridad digital" y "anonimato". Además, se propuso la implementación de una verificación clara y accesible para el ciudadano, la educación en ciberseguridad desde edades tempranas, la ética en plataformas que contienen nuestros datos, y la imposición de un castigo penal para la difusión indebida de datos personales.

Infraestructura Digital, Juventud y Ciudadanía

Expositores

- Alejandro Carbonell
- Juan Pablo Cardozo
- Leila Robles
- Nicole Lasso
- Yaiza Gonzales

Este foro tuvo como eje central la infraestructura digital para la juventud y la ciudadanía. Se abordaron las brechas existentes en materia de conectividad y equidad digital, la importancia de la educación crítica sobre Inteligencia Artificial y privacidad, y el rol protagónico de los jóvenes y las instituciones universitarias en la gobernanza de Internet. Esta conversación se consideró fundamental para avanzar hacia una Internet verdaderamente inclusiva y accesible para todos los sectores de la sociedad.

Al hablar de infraestructura, se hizo referencia a los recursos, la solvencia y los espacios necesarios para que algo funcione. Se reconoció que la brecha digital en Panamá sigue siendo considerable, lo que subraya la necesidad de estructuras robustas. En la Universidad del Istmo, por ejemplo, el proceso de cambio se realiza a través de la virtualidad, aunque en las comarcas, donde existen más debilidades, solo el 3% de la comunidad estudiantil tiene acceso a dispositivos digitales como Tablet y celulares. Esto contrasta con el 70% de disposición de dispositivos en áreas urbanas como la Ciudad de Panamá. Cerrar esta brecha es una responsabilidad de las universidades, y si bien la tecnología ha avanzado, es crucial que los docentes estén capacitados para la formación virtual y que los estudiantes también aprendan a formarse de esta manera.

Se mencionó la existencia de dos "Panamá": el Panamá urbano con acceso a Wi-Fi y el Panamá del interior, que a menudo carece de acceso a Internet e incluso de infraestructura vial. Se propusieron proyectos conjuntos con el gobierno y emprendedores, como el arreglo de computadoras, y se destacó la importancia de la innovación para impulsar el cambio social, especialmente en el Panamá menos conectado.

Yaiza Gonzales enfatizó la desigualdad en el acceso, señalando que no todos los jóvenes nacen con las mismas condiciones ni tienen los mismos recursos, como dispositivos adecuados o planes de servicio asequibles. Mencionó su experiencia en una gira donde observó cómo las redes comunitarias y los proyectos de turismo rural transformaron vidas al brindar conectividad. Subrayó que la participación en la gobernanza digital va más allá

de tener conexión, incluyendo el acceso a dispositivos adecuados, la accesibilidad y los costos de los servicios. El éxito de un programa de becas que recibió más de 200 postulaciones de jóvenes para participar en el foro de gobernanza demostró el gran interés y la necesidad de estos espacios, lo que ha llevado a la segunda edición del Foro de Gobernanza Juvenil.

Se abordó la importancia de las universidades en este contexto, las cuales "sí o sí tienen que dar apertura a este tipo de espacios para conectar y para prestar sus instalaciones y sus estudiantes". También se hizo una invitación a las empresas para que aprovechen la conexión con las universidades para testear proyectos piloto, fomentando una colaboración más activa. La Universidad del Istmo, por ejemplo, transformó su modelo educativo durante la pandemia para ser líderes en educación virtual, enfocándose en desarrollar competencias como el pensamiento crítico digital, creatividad, innovación y transformación digital. Estas habilidades, según el ponente, son lo que permitirá a los estudiantes ser mejores que la IA. El desafío es transformar un sistema tradicional y adaptarse a las leyes exigentes, buscando un enfoque por competencias más que por logros.

Finalmente, se reflexionó sobre el futuro, señalando la falta de compartición de información y datos reales en Panamá, lo que dificulta la implementación de buenas prácticas y la colaboración. Se destacó un cambio cultural donde la sociedad civil, especialmente los jóvenes, se une para generar grandes impactos y proponer cambios, ya que a menudo no tienen estructuras que defender o proteger. Se identificaron tres puntos clave para un futuro más realista: la mentalidad actual, la colaboración entre gremios, y la valentía para generar cambios trascendentales.

Inteligencia Artificial y Gobernanza Ética

Este foro se centró en los usos prácticos, éticos y los riesgos de la Inteligencia Artificial.
Los expositores incluyeron

- Ing. María Elena García,
- Magister Merio Peña,
- Lic. Morales Franklin,
- Dr. Philippe Aniorte
- Lic. Alex Marroquin.

La pregunta central fue

Si es necesario regular la Inteligencia Artificial.

Se planteó que la cuestión no es si se debe regular, sino cuándo y cómo, y con qué conocimiento. Actualmente, Panamá está diseñando una Estrategia Nacional de Inteligencia Artificial. Antes de la regulación, el país debe entender qué busca y qué objetivos debe cumplir un marco regulatorio, siempre en beneficio de la competitividad nacional y de los ciudadanos. No se trata solo de crear leyes, sino de considerar estándares, metodologías (auditoría, educación) y el rol de la sociedad civil y el gobierno.

El momento óptimo para regular es un tema en aprendizaje para muchos países. Es crucial tener claridad sobre los puntos a regular, con la participación de todos los sectores: academia, empresa privada, sociedad civil y gobierno. La SENACYT está evaluando esta estrategia, buscando un enfoque multisectorial para definir dónde Panamá debe empezar a regular, con principios como la transparencia y garantizando una IA para todos los panameños. Se mencionó que ya se han presentado tres proyectos de ley de regulación en la Asamblea Nacional, pero se reconoció que era arriesgado sin una dirección clara.

La Estrategia Nacional de Inteligencia Artificial de Panamá, disponible en línea, ha sido el resultado de un proceso multisectorial. Se está trabajando con la Universidad de Georgetown y se encuentra en la fase de diagnóstico, recopilando información a través de mesas intersectoriales y una encuesta disponible hasta el 31 de julio para entender las oportunidades, desafíos y el estado actual de la IA en el país.

Los pilares de la estrategia incluyen:

- **IA para el desarrollo económico:** Enfocarse en el impacto de la IA en sectores críticos como logística, finanzas y agricultura para potenciar la capacidad nacional.
- **IA para los ciudadanos:** Asegurar que la IA sea un tema nacional, cubriendo brechas de formación y capacidades, e investigación, y mapeando iniciativas.
- **Gobierno y Gobernanza:** Trabajar con entidades gubernamentales para avanzar hacia la regulación y normativas de la IA.

En colaboración con la UNESCO, se está lanzando un estudio de preparación tecnológica, y con la Unión Internacional de Telecomunicaciones (UIT), se están regulando para construir capacidades antes de promulgar leyes. La SENACYT está identificando actores clave para formar una red de aprendizaje sobre cómo otros países están regulando la IA y los desafíos que han enfrentado.

Se espera tener la estrategia lista este año y se está recomendando a la presidencia la creación de una comisión de tecnologías políticas emergentes con una subcomisión de Inteligencia Artificial. Esto busca tener un esquema unificado para abordar no solo la IA, sino también otras tecnologías emergentes como la biología sintética y la ciberseguridad, y cómo Panamá se insertará en ellas.

Desde el público,

Se preguntó por la inclusión de la administración de justicia, específicamente el Ministerio Público, la Procuraduría de la Nación, la Fiscalía General Electoral y la Fiscalía de Cuentas, en las iniciativas de la SENACYT.

En respuesta, se indicó que se ha estado colaborando con la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), que planteó desafíos en estas áreas, y que la estrategia definitivamente las abordará. La SENACYT se ve como un articulador, no como el único definidor, y está en un proceso de identificación de todos los actores y de escuchar las áreas de preocupación, siendo un proceso abierto y flexible que busca la guía de instituciones como las mencionadas para integrarlas en la estrategia de IA.