Relatoría LACIGF 12

Título de la sesión: Sesión 10 – Ciberseguridad y Ciberdefensa: Realidad actual y cómo hacer a nuestras sociedades más resilientes hacia el futuro

Resumen de la sesión:

La sesión 10, moderada por **Ernesto Bojórquez (LACTLD, México)**, trató sobre la ciberseguridad y ciberdefensa. Ernesto propuso una breve reflexión sobre cómo el mundo se convirtió en un cibermundo y cómo la seguridad se convirtió en la ciberseguridad, después de lo cual leyó 3 preguntas, que fueron respondidas por los panelistas:

1. ¿Cuál es el mayor / avance / retroceso o dificultad de la ciberseguridad en América Latina?
2. ¿Qué esfuerzos se están haciendo en la región para desarrollar buenas prácticas de ciberseguridad?
3. ¿Qué tipo de cooperación se está llevando a cabo en la región o en sus países con respecto a la defensa cibernética?

La primera en responder fue **Maryleana Mendez (ASIET, Costa Rica**). Ella comenzó señalando que la seguridad cibernética es muy compleja, hay una escasez de especialistas en seguridad cibernética y que el costo del delito cibernético alcanza los $ 600 mil millones, También dijo que los ataques han crecido mucho y se han vuelto más sofisticados, señaló que la capa de usuario es la que necesita más inversión, porque la falta de educación digital del usuario permite varias fallas, siendo el eslabón más débil de esta cadena. Es necesario enseñarle al usuario a no convertirse en una víctima o una posible fuente de ataque.

Lía Solís (ISOC Bolivia, Bolivia) respondió la segunda pregunta, después de dar una breve explicación sobre ISOC y sus objetivos. Ella mostró el plan de acción para 2019, que se divide en 4 puntos, dos de los cuales estaban directamente relacionados con la sesión: mejorar la seguridad técnica y generar confianza a través de la creación de buenas prácticas y estándares para tablas de enrutamiento, y la creación y adopción de MANRS, un proyecto que apunta a acciones defensivas para reducir las amenazas a enrutamiento.

Carlos Guerrero (Hiperderecho, Perú) empezó su presentación citando John Perry Barlow, en la declaración de independencia del ciberespacio, en 1996 en la ciudad de Davos. Esta cita la utilizó para explicar cuál era la situación en ese momento de Internet y la posición de los gobiernos. Luego afirmó que hoy sería imposible decir que el Estado no debe regular lo que ocurre en Internet. Luego de este preámbulo, indicó que la ciberseguridad es una preocupación relativamente reciente en América Latina y el Caribe; no obstante, se han desarrollado proyectos interesantes, gracias al apoyo de entes como la OEA y BID. Luego, Carlos desarrolló la diferencia entre ciberdefensa y ciberseguridad, señalando que este último versa sobre la ciberseguridad de la seguridad de las personas y los posibles ataques que puedan sufrir, y por lo tanto es necesario determinar las prácticas seguras que pueda emplear o aprender, para poder manejarse mejor en entornos digitales. Él afirmó que actualmente, los gobiernos, el sector privado y la sociedad civil están manteniendo una discusión, sobre qué debe implicar la ciberseguridad y esto a su vez está generando un correlato, en la forma

cómo se implementan los planes de ciberseguridad, a través de la compra de tecnología y el desarrollo de capacidades.

Lorena Naranjo (DINARDAP, Ecuador) inició su presentación citando un índice de seguridad global para las Américas, donde existe 5 pilares de evaluación: el ámbito jurídico, técnico, organizativo, creación de capacidades y cooperación. Este índice permite ver cómo estamos en la región en temas de ciberseguridad. Según, lo que comentó Uruguay es el único país en toda la región que cumple con criterios adecuados de ciberseguridad. Ella mencionó la debilidad de formar parte del convenio de Budapest y la dificultad que eso representa para generar una buena cooperación. Recalcó que no hay personal capacitado en temas de ciberseguridad. Sin embargo, se presentan avances importantes, como por ejemplo el hecho que ya existan planes o estrategias de ciberseguridad en 10 países de la región. Por ejemplo, en Ecuador están trabajando en una estrategia de ciberseguridad llamada Ecuador Digital, que establece la conectividad, la seguridad y la dinámica económica como sus pilares fundamentales. Se trata de una visión integral, donde el ser humano es el centro de la ciberseguridad y donde se conjugan las distintas visiones. Esto es importante porque el concepto de seguridad ha mutado, ya no se habla sólo de seguridad estatal o territorial, sino de un concepto de seguridad de las personas, donde el eje central son los Derechos Humanos.

Outputs y otros links relevantes:
Sesión completa en: https://youtu.be/fIN3dDH7FzI

Por: Carlos David Carrasco Muro (Observatorio del Gasto Fiscal, Chile), Matheus Figueiredo Lima (UNICURITIBA, Brasil)

Revisado por: Verónica Arroyo (Access Now, Perú)

Coordinación y edición: Nathalia Sautchuk Patrício (NIC.br, Brasil) y Guilherme Alves (Youth Observatory, Brasil)