16^{0} FORO DE GOBERNANZA DE INTERNET DE AMÉRICA LATINA Y EL CARIBE - LACIGF

PANEL: COOPERACIÓN PARA LA SEGURIDAD EN LÍNEA

RELATORIA

TÍTULO DE LA SESIÓN: Ciberseguridad, ciberdelincuencia y seguridad en línea

Fecha y hora: Diciembre 5 de 2023 – 09:30 – 11:00

Organizan: Miguel Ignacio Estrada, LACNIC. Valeria Betancourt, APC.

Lugar: Universidad Externado de Colombia. Calle 12 No. 1-17 este, Auditorio 3 – Edificio i

Moderador: César Díaz, LACNIC.

Co-moderador en línea: Lia Hernández, IPANDETEC.

Panelistas:

- Michele Bordachar.Asesora jurídica y legislativa, Coordinación Nacional de Ciberseguridad, Chile.
- Dominique Paz. Unidad Fiscal de Cibercrimen, Argentina.
- Yunuhen Rangel, Luchadoras, México.
- Maite Altoaguirre, Telefónica.
- Graciela Martinez, CSIRT, LACNIC.
- Karen Cruz, Youth LACIGF.

Relator: Mónica Juliana Correa, Colnodo.

Puntos principales por panelista:

1. **Michele Bordachar. Coordinación Nacional de Ciberseguridad, Chile.**

- La colaboración hay que pensarla en varios niveles Público-Público, Estado-Estado, Público-Privado.
- Conocer las experiencias de otros países o sectores es clave para evitar ataques o para recuperarse más pronto de las vulnerabilidades y parchar estas amenazas.
- Es clave para los gobiernos no dejar los avances atrás y comenzar de cero.
- Avanzar en Latinoamérica en temas de reglas y reportes de vulnerabilidad, generar normas que obliguen al reporte.
- Reporte de ataques y reporte responsable de detección de vulnerabilidades.
- Es importante ver este tema como una política de Estado y no de gobierno.
- Son importantes las leyes, porque permiten a las autoridades actuar. Las víctimas de delitos digitales en muchas ocasiones no comprenden qué paso.
- Tomar medidas escuchando a quienes buscamos proteger. Generar mesas para conocer necesidades de las personas porque es difícil trabajar y legislar en temas de ciberseguridad si no se conocen todas las amenazas.
- Apoyo público privado para la generación de medidas de protección de niños, niñas y adolescentes.

2. **Dominique Paz. Unidad Fiscal de Cibercrimen, Argentina.**

- La ciberdelincuencia es derecho penal y es algo reactivo y para que aparezca ya debe haber ocurrido algo.
- Debe haber leyes que contengan tipos penales en esos temas, es importante generar reglas que regulen estos temas.
- Entender que hoy en día todos los delitos tienen un aspecto informático.
- Es importante la tipificación que ayude a la denuncia, avanzar en el derecho procesal con equipos multidisciplinarios.
- Uno de los mayores problemas es la detección y recolección de evidencias porque por lo general la información está alojada en el extranjero.
- Las normas estadounidenses permiten la colaboración y que se proporcione información de forma voluntaria.
- Preservar información es un tema clave, ya que la información digital es volátil.
- En el tema de registro de dominio no es tan fácil conseguir información. Existen redes en Latinoamérica con puntos de contacto para solicitar información. Acceder a esta información está mediado por las leyes de cada país.
- Las recomendaciones para la cooperación es que todos los países se adhieran a los convenios de cooperación internacionales para que en la región se pueda responder a las amenazas sin restricciones.
- Para mejorar en la cooperación de información, la preservación de la información, es un tema vital para la investigación de delitos, las empresas tienen la facultad de colaborar con las autoridades para permitir la obtención de evidencia digital.
- Comprender que la cadena de custodia digital es distinta a la física.
- Protocolo de obtención de evidencia digital y guía de cooperación internacional: https://www.mpf.gob.ar/ufeci
- Es importante contar con asistencia a los sistemas judiciales para que puedan avanzar las investigaciones, en la actualidad casi todos los delitos tienen componentes digitales.

3. **Yunuhen Rangel, Luchadoras, México.**

- La violencia se ha trasladado al espacio digital y son las mismas violencias que hemos tratado de resolver en el espacio físico.
- Tipología de violencias digitales de género para reconocerlas, posicionarlas y combatirlas.
- Las violencias de género además de permitidas son invisibilizadas.
- Es necesario hacer frente común a las dinámicas en línea que muestran además de violencia de género, problemáticas como el racismo, clasismo y el discurso de odio.
- Es importante ayudar a las personas con mecanismos de defensa en ciberseguridad que sean acordes a su realidad.
- Las redes y las cooperaciones son alternativas a las que las mujeres han podido acceder para buscar justicia ante la incapacidad por parte del estado para responder a todos los casos.
- Hacer activismo digital para crear contranarrativas poderosas que ayuden a cambiar el mundo, las redes de colaboración son potentes y ayudan a maximizar el trabajo.
- Apoyar a las mujeres en su análisis de riesgo propio.
- Es necesario humanizar los términos para que sean masivos.
- Más leyes no se traduce necesariamente en más justicia.

4. **Maite Altoaguirre, Telefónica.**

- En el entorno privado se es consciente de que la seguridad digital es un tema que trasciende y requiere de un trabajo responsable, organizado y tener en cuenta que la información es un valor inconmensurable.
- Todo está bajo las normas ISO.
- Seguridad del diseño, que todos los actores que participan en el proceso tengan el tema de la seguridad afianzado.
- Este es un trabajo mancomunado en el que deben trabajar varios sectores.

5. **Graciela Martinez, CSIRT, LACNIC.**

- La comunidad técnica ha contribuido en la prevención de delitos al generalizar el enlace para permitir compartir información.
- Hemos contribuido a construir vínculos entre los diferentes actores del ecosistema de internet y una base de conocimiento a la hora de actuar contra el cibercrimen.
- Hemos aportado en la generación de consciencia, aportamos una mirada sistémica y no tan reactiva, para tener planes de respuesta y monitoreo de amenazas para aportar a la estabilidad del internet de la región.
- Los centros de respuesta hacen que sean más efectivas las respuestas, manejamos un mensaje común y tenemos un procedimiento.
- No es solo decir voy a compartir información, sino el compartir la información de forma efectiva para contribuir a los planes de resistencia, ayudar a construir y consolidar la confianza.
- No se trata solo de conocer la técnicas, también es necesario conocer su evolución, hay que acompañar la evolución del ciberdelito para saber hacia dónde va.
- El Ransomware tuvo una evolución, ya no se ataca persona a persona, ahora se ataca a organizaciones buscando la información más sensible.
- Contribuir con la generación de capacidades y conocimientos para que la comunidad en la región esté preparada para responder a estos delitos.
- Cooperación internacional que no se centre en los datos involucrados en un ciberdelito, debemos colaborar en compartir conocimiento y experiencias y tratar de implementar infraestructura para compartir información, estadísticas y conocimientos para generar base de conocimientos en la región.

6. **Karen Cruz, Youth LACIGF.**

- La ciberseguridad no es solo un problema de archivos infectados, ni tampoco es solo un tema técnico, debemos preocuparnos por la vulneración de la información de los niños, el Ciberbullying y otros temas que afectan a niños, niñas y jóvenes.
- Es necesario promover la educación digital entre los niños para que sepan actuar cuando encuentren con delitos en línea.
- A muchos niños se les ha obligado a estar en los ambientes digitales, pero no se les ha educado sobre cómo habitar estos espacios.
- Es necesario educar y aprender junto a los niños en cuanto a los temas de violencia digital.
- Los niños se han convertido en un objetivo fácil y perseguido en temas de delitos digitales.

Público:

Es positivo saber que la cooperación internacional ha ayudado en el reporte de incidentes de seguridad cibernética y en los procesos de investigación ¿Cuáles serían los puntos de mejora en esa cooperación internacional?

Cuáles serían las sugerencias en temas de generación de regulación para el resguardo de información.

¿Cuáles son los riesgos al observar contenidos piratas?

Ciberseguridad y cibercrimen son dos términos y temas distintos.

En las medidas que se están desarrollando en temas de resguardo de datos e información cómo está planteando el tema de derechos humanos y derechos digitales.

Cómo plantear canales de ayuda para la colaboración en casos de ataques, por ejemplo, por parte de los Hackers éticos.

Puntos principales:

Los sistemas informáticos son por naturaleza inseguros, están compuestos de miles de millones de líneas de código, en algunos casos hecho por humanos, por lo que siempre va a existir la vulnerabilidad. La estrategia más efectiva para mitigarla es contar con la información necesaria, por esa razón los acuerdos de colaboración son un tema clave.

La colaboración debe estar pensada en todos los niveles entre los estados y los sectores públicos y privados, ya que conocer las experiencias de otros países o sectores ayuda a evitar ciberdelitos, a recuperarse más pronto y a resolver vulnerabilidades. Un ejemplo de esto, es el apoyo público privado que es clave a la hora de proteger a niños, niñas y adolescentes.

La cooperación internacional no debe centrarse en el intercambio de datos involucrados en ciberdelitos, es necesario compartir conocimientos, experiencias, estadísticas y protocolos y a la vez implementar la infraestructura necesaria para compartir esta información. Es necesario crear una base de conocimientos para aportar a la estabilidad de la región.

Es importante tomar medidas escuchando a quienes buscamos proteger. Conocer las necesidades de las personas es indispensable para trabajar en mecanismos de defensa acordes a la realidad y legislar en temas de ciberseguridad y ciberdelincuencia. Si bien más leyes no se traducen necesariamente en más justicia, las leyes son indispensables porque permiten a las autoridades actuar.

Es necesario humanizar los términos para que sean masivos, la ciberseguridad no es solo un problema de archivos infectados, ni tampoco es solo un tema técnico, por eso se debe contribuir con la generación de capacidades y conocimientos para que la comunidad en la región esté preparada para responder a los ciberdelitos, de igual forma es importante contar con asistencia a los sistemas judiciales para que puedan avanzar las investigaciones, ya que en la actualidad casi todos los delitos tienen componentes digitales.