Reporte de la
Reunión Técnica sobre ciberdelincuencia de la
Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC)

Virtual
2 & 4 de septiembre 2020

Antecedentes

La Reunión Técnica sobre ciberdelincuencia de la Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC) fue organizada por el Centro de Excelencia para Información Estadística de Gobierno, Seguridad Pública, Victimización y Justicia (CdE), proyecto conjunto de la Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) con el Instituto Nacional de Estadística y Geografía (INEGI) de México.

La UNODC, a través del CdE, apoya técnicamente al levantamiento de Encuestas de Victimización en la Región de América Latina y el Caribe desde 2013. Estos proyectos estadísticos son una fuente importante de información para el reporte de los Objetivos de Desarrollo Sostenible de la Agenda 2030 de las Naciones Unidas. La Iniciativa VICLAC promueve el uso de una metodología común a través de un cuestionario regional homologado (disponible 4 idiomas: español, inglés, francés y portugués) en línea con los estándares internacionales. Esta Iniciativa está liderada por la UNODC y el CdE, y cuenta con el apoyo del Banco Interamericano de Desarrollo (BID), la Organización de Estados Americanos (OEA) y el Programa de las Naciones Unidas para el Desarrollo (PNUD). En la construcción de este instrumento regional han contribuido los países miembros del Grupo de Trabajo: Argentina, Belice, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haití, México, Panamá, Perú y República Dominicana.

El nuevo módulo de ciberdelincuencia es un esfuerzo para medir fenómenos delictivos cada vez más relevantes y fue desarrollado en 2019 por solicitud de Santa Lucía, que incluyó dicha medición en su primera Encuesta Nacional de Victimización (SLNCVS) y fue presentado durante de la 7ª Reunión Técnica del Grupo de Trabajo de la Iniciativa VICLAC en octubre de 2019. Derivado de esta 7ª Reunión Técnica, se acordó discutir más a fondo el módulo propuesto en una reunión especializada sobre ciberdelincuencia en el primer semestre de 2020. Debido a la situación de contingencia global por COVID-19, la Reunión Técnica sobre Ciberdelincuencia, inicialmente planeada para abril 2020 en la ciudad de Santo Domingo, se pospuso a septiembre 2020 y se llevó a cabo virtualmente (para agenda, ver Anexo 1).

Una versión mejorada del Módulo (Versión 04 agosto 2020) ha sido producida y circulada durante la Reunión Técnica sobre ciberdelincuencia para recibir comentarios de parte de los y las participantes.

Objetivo de la reunión técnica:

Entender el panorama conceptual y normativo global, regional y nacional de la ciberdelincuencia con el objetivo de definir qué conductas mínimamente se tienen que medir a través de una encuesta en hogares. Esta discusión, entre expertos de las Oficinas Nacionales de Estadística y de las Autoridades del Sistema de Justicia Penal de los países miembros del Grupo de Trabajo de la Iniciativa VICLAC, así como expertos de otros países y Organismos Internacionales y regionales está orientada a aportar mejoras al Módulo sobre Ciberdelitos (Versión 04 Agosto 2020) de la mencionada Iniciativa. Los objetivos específicos fueron:

A. Presentar brevemente la Iniciativa VICLAC a los participantes.
B. Compartir el conocimiento de expertos en tema de ciberdelitos.
C. Presentar el marco jurídico internacional en la materia.
D. Presentar experiencias de medición de la ciberdelincuencia (México, Perú, Santa Lucía)
E. Discutir la propuesta de Módulo sobre Ciberdelitos (Versión 04 agosto 2020) con los participantes para llegar a un consenso.

En esta reunión técnica participaron un total de 35 personas de las Oficinas Nacionales de Estadística y del Sistema de Justicia Penal de Argentina, Colombia, México, Perú, República Dominicana y Santa Lucía; por parte de Naciones Unidas estuvieron presentes la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés), la Comisión Económica para América Latina y el Caribe (CEPAL) y el Programa de las Naciones Unidas para el Desarrollo (PNUD). También formaron parte del encuentro el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), así como dos expertos internacionales del Instituto de Investigación de Ciberdelincuencia y la Univeristat Abat Oliba CEU (para Lista de asistentes, ver Anexo 2).

A. Bienvenida y nociones generales de la reunión

- *Enrico Bisogno, Jefe de la Sección de Desarrollo y Difusión de Datos, UNODC HQ*
  El Sr. Bisogno dio la bienvenida a los participantes de la reunión y habló de las actividades de UNODC en apoyar a los Estados Miembros en su lucha contra los ciberdelitos.
- *Salomé Flores, Coordinadora del Centro de Excelencia, UNODC México*
  La Sra. Flores presentó la Iniciativa VICLAC y habló de los objetivos de la reunión y de las razones por las cuales es importante medir la ciberdelincuencia.

B. Entendiendo la ciberdelincuencia

- Sr. Marco Gercke, Director del Instituto de Investigación sobre Ciberdelincuencia, Alemania

El Sr. Gercke habló de la ciberdelincuencia como un delito que es parte integrante de la vida cotidiana de individuos y empresas y recalcó que se trata de un delito en constante mutación. Además, indicó que el ciberdelito no es nuevo, que lleva en nuestras vidas desde que el internet se inventó, pero que hasta ahora se le ha considerado como un tema crucial. Para mayor referencia a los retos relacionados a este delito y la respuesta legal, proporcionó la liga de un estudio elaborado en conjunto con la Unión Internacional de Telecomunicaciones: https://bit.ly/3382rah

- *Sr. José Ramón Agustina, Catedrático de Derecho Penal y Criminología de la Universitat Abat Oliba CEU, España:*

Desde una perspectiva académica, el Sr. Agustina indicó que hay seis diferentes enfoques para comprender el ciberdelito y enfrentar sus retos. Además habló de la cifra oculta, de las falacias relacionadas al cibercrimen y de la importancia de nombrar, medir y clasificar. Además, recalcó que ahora vivimos en una dicotomía, una realidad híbrida entre el espacio físico y el espacio virtual. Lo peligroso del ciberespacio es que no tiene fronteras y de que las personas no toman en serio su seguridad en el mundo del internet. Finalmente, destacó el gran reto del componente legal y la falta de coordinación entre países por motivo de que el ciberespacio no respeta frinteras. Para un mayor entendimiento, el experto proporcionó una liga donde es posible encontrar sus publicaciones en la materia: https://bit.ly/2R5gEPA

C. Contexto internacional

- Sra. Nayelly Loya, Coordinadora regional del Programa Global de Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) de Centroamérica y el Caribe (ROPAN)

La Sra. Loya habló del Programa Global de Ciberdelito, de su objetivo y alcance global y regional. Además, indicó que s aún no existe una definición acordada internacionalmente sobre el delito cibernético, además de que aún no se cuenta con una Convención de Naciones Unidas al respecto. y abordó la perspectiva internacional, explicando qué está pasando en el ciberespacio y qué se está haciendo para contrastar este fenómeno. De igual forma, habló sobre las actividades que se están llevando a cabo en la región para combatir este delito, sobre el Repositorio de Ciberdelito disponible al público, así como la oportunidad de tomar un curso online gratuito de 14 módulos disponibles en inglés y español (limitado a ciertos módulos). Cerró su presentación destacando la clasificación que UNODC identifica a través del Estudio Exhaustivo sobre el Delito Cibernético (UNODC, 2013).

D. Propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC

- Sra. Luisa Sánchez, Investigadora en Delincuencia y Justicia Penal del Centro de Excelencia, UNODC México

En esta sesión se presentó el contexto del Módulo dentro de la Iniciativa VICLAC y se habló de cómo UNODC clasifica el ciberdelito en su Clasificación Internacional de Delitos con Fines Estadísticos (ICCS). Se habló de la brecha de seguridad digital y de los ciberdelitos incluidos en la Iniciativa VICLAC (ciberacoso, software malicioso, hackeo de correo electrónico, hackeo de medios/redes sociales, ransomware) además de presentar la estructura del Módulo, especificando las preguntas incluidas para cada delito incluido.

E. Experiencia de países en la medición de la ciberdelincuencia

En esta sesión, los países con experiencia en la medición de la ciberdelincuencia presentaron su práctica a los demás participantes:

- Santa Lucía: Resultados de la Encuesta Nacional de Victimización de Santa Lucía (SLNCVS):
  - Sra. Linn Lelia Brown, Estadística, Oficina Central de Estadísticas (CSO)

- México: Módulo sobre Ciberacoso (MOCIBA):
  - Sr. Mario Santillana, Director de Encuestas Nacionales de Gobierno, Seguridad Pública y Justicia, Instituto Nacional de Estadística y Geografía (INEGI)

- Perú: Investigación de Delitos de Alta Tecnología:

- Sra. Cinthya Cárdenas Rondón, Capitana de la División de Investigación de Delitos de Alta Tecnología, Policía Nacional del Perú (PNP).

F. Discusión sobre la propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC

El CdE presentó las siguientes preguntas detonadoras sobre la conceptualización de los ciberdelitos incluidos en el cuestionario, la propuesta metodológica contenida en el cuestionario del módulo y los pasos a seguir para su levantamiento en el futuro. Estas preguntas son parte del *Formato para la SESIÓN 2: Discusión sobre la propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC* (Anexo 3). Fueron dirigidas a los y las participantes, con el objetivo de mejorar el Módulo sobre Ciberdelitos (versión 04 agosto 2020).

Este formato se envió a los participantes previo inicio de la reunión y aborda los siguientes temas:

- TEMA 1: Estructura y metodología del módulo
- TEMA 2: Tipos de ciberdelitos propuestos para medir
- TEMA 3: Inclusión de preguntas específicas de contexto sobre ciberdelincuencia

Debido a los comentarios recibidos en la primera jornada de discusiones, el orden en que se abordaron las preguntas detonadoras durante la sesión 2 sufrió una modificación.

1. **TEMA 3: 3.1. No todos los países tipifican los ciberdelitos / delitos cibernéticos / delitos apoyados por la tecnología. ¿Podría indicarnos qué tipos de ciberdelitos están tipificados en su país?**
   - Para cuestiones de tiempo, se retomaron los avances que otras organizaciones internacionales han generado sobre el tema de la ciberdelincuencia. Por ejemplo, los Reportes de Ciberseguridad en América Latina y el Caribe realizados por el BID y la OEA en 2016 (https://bit.ly/35ieEfl) y 2020 (https://bit.ly/2R81cTa) en los que se evalúan los riesgos que los países de la región enfrentan y las capacidades de los Estados y las sociedades para afrontarlos. Las experiencias de los países en materia de tipificación de ciberdelitos se recopilarán de los formatos que los participantes envíen al CdE, Secretario Técnico de la Iniciativa VICLAC.

2. **TEMA 2: 2.1 ¿Tiene alguna sugerencia o comentarios sobre los delitos ya incluidos en la propuesta del módulo?**

   Entre las cinco conductas que ya han sido piloteadas en el cuestionario de la Encuesta Nacional de Victimización de Santa Lucía (SLNCVS) se encuentran: el ciberacoso, el

software malicioso, el hackeo de correo electrónico, el hackeo de medios/redes sociales y el *ransomware*. Se recibieron comentarios respecto a algunos ciberdelitos en específico.

- Definición de ciberacoso: "*Alguien envió o publicó en línea y de manera visible para otros algún texto, imagen o video con la intención de avergonzarlo u ofenderlo personalmente, herir sus sentimientos o causar alguna otra angustia emocional. Excluya los mensajes amenazantes o agresivos en los que usted era el único destinatario*."
  Colombia (DANE) y UNODC ROPAN comentaron que, para que haya ciberacoso, y entonces un daño a la víctima, no es necesario que sea "visible para otros".
- Definición de hackeo (de correo electrónico y de medios/redes sociales): "*Alguien obtuvo acceso a su(s) cuenta(s) de correo electrónico en línea sin su permiso, y dio lugar a que sus contactos (por ejemplo, amigos/familiares) recibieran un correo electrónico de su parte que usted no había enviado.*" "*Alguien obtuvo acceso a su(s) cuenta(s) social(es) en línea sin su permiso, como Facebook, Twitter, Instagram, LinkedIn, etc. y provocó que se enviaran mensajes o publicaciones desde su(s) cuenta(s) de redes sociales que usted no envió*."
  Colombia (DANE) indicó que el hackeo puede incluir medios adicionales a los propuestos como los blogs y cuentas de redes sociales de carácter laboral. El CdE aclaró que es importante diferenciar entre cuentas personales y cuentas institucionales o corporativas porque la frontera entre ambos tipos de cuentas delimita conductas distintas (victimización a personas versus victimización a organizaciones). Este punto se vincula con una discusión sostenida la jornada anterior sobre las limitantes de una encuesta de victimización, que convencionalmente recolectan información sólo entre personas mayores de 18 años, para capturar el conjunto de las conductas delictivas realizadas a través de medios digitales. En aquella ocasión se observó que muchas veces niñas, niños y adolescentes son víctimas de la ciberdelincuencia y que se requieren mediciones que incluyan sus experiencias.

3. **TEMA 2: 2.2 ¿Considera fundamental incluir otros ciberdelitos? Se propusieron los siguientes:**
   - Suplantación de identidad: *"Creación de un perfil falso, pero con la identidad de otra persona a la que se pretende suplantar."*
     Robo de identidad: "Se produce cuando el que suplanta la identidad lo realiza por haber sustraído los datos de acceso a Internet y redes sociales de la persona.
     República Dominicana (Ministerio del Interior y Policía y ONE), Perú (INEI) y Colombia (DANE) se manifestaron a favor de incluir estos dos delitos en la nueva versión del Módulo. Para evitar malentendidos, Colombia y Perú sugieren revisar las dos definiciones para que sean mutuamente excluyentes y entendibles. PNUD recalcó que en estos dos delitos es crucial indagar la relación con el victimario, ya que, en los dos ciberdelitos, el impacto sobre las víctimas puede ser muy distinto.

- Noticias falsas: *"Son un tipo de bulo que consiste en un contenido pseudo-periodístico difundido a través de portales de noticias, prensa escrita, radio, televisión y redes sociales y cuyo objetivo es la desinformación. Se diseñan y emiten con la* ***intención deliberada de engañar, inducir a error, manipular decisiones personales, desprestigiar o enaltecer a una institución, entidad o persona u obtener ganancias económicas o rédito político.*** *Al presentar hechos falsos como si fueran reales, son consideradas una amenaza a la credibilidad de los medios serios y los periodistas profesionales, a la vez que un desafío para el público receptor."*

  BID recalcó que las noticias falsas afectan al conjunto de la población y su medición no sería precisa. Además, no hay relación directa entre victimario y víctima. PNUD reconoció la complejidad de este tema ya que es un reto distinguir si la víctima es el individuo o la persona en cuanto parte de un grupo organizado o de un país. CEPAL estuvo de acuerdo con que todos somos víctimas de las noticias falsas y agregó que también hay un problema para delimitar el concepto ya que, posiblemente, todas las noticias tienen un componente falso y un componente verdadero. Sugirió enfocarse en la intencionalidad de engañar con una noticia falsa.

  Colombia (DANE) recalcó que el tema no es un delito personal, pero podría indagarse por la ocurrencia o la percepción que tengan las personas sobre la ocurrencia de esto y su impacto. República Dominicana (ONE) también indicó que es un delito de muy difícil medición y delimitación.

  Considerando el interés en el tema, se propuso medirlo en otra sección del cuestionario VICLAC (por ejemplo, en el apartado B de Percepción, para la obtención de una medición de la percepción sobre este fenómeno o de medición de su impacto en quienes fueron expuestos a la información falsa).

  UNODC ROPAN recalcó la importancia de distinguir y ocupar los términos en inglés " "misinformation" - sin intención de engañar - y "disinformation" - como acto deliberado de desinformación.

- Grooming

  República Dominicana (Ministerio de Interior y Policía) manifestó interés en incluir este modus operandi. Se recalcó el reto de medirlo considerando que, de acuerdo a las recomendaciones internacionales, en una encuesta de victimización se entrevistan informantes de 18 años y más. Con este reto metodológico, se excluirían de la medición los informantes más vulnerables a este tipo de delito. En el caso de Colombia (DANE), se indicó que no existiría este problema, ya que su encuesta de victimización tiene como población objetivo, personas de 15 años y más.

- Phishing: República Dominicana (Ministerio de Interior y Policía) manifestó interés en incluir este acto. Colombia (DANE) se mostró de acuerdo en incluir phishing. Perú (INEI) sugirió una revisión de la definición de phishing, para evitar malentendidos. El CdE destacó que tanto el *grooming* y como el *phishing* son un tipo de *modus operandi*

para lograr un delito, a través del engaño. Por lo tanto, se puede incluir una pregunta que indague sobre cómo es que fue engañada la víctima para caer el cualquiera de los delitos que se miden en el módulo.

- Sextorsión: *"Una forma de chantaje en la que se utiliza información o imágenes sexuales para obtener favores sexuales de la víctima. Las redes sociales y los mensajes de texto son a menudo la fuente del material sexual y el medio amenazado de compartirlo con otros. Un ejemplo de este tipo de sextorsión es cuando las personas son extorsionadas con una imagen desnuda de sí mismas que compartieron en Internet a través del sexting."*
  República Dominicana (Ministerio de Interior y Policía) manifestó interés en incluir este delito.
- Comentarios adicionales:
  Colombia (DANE) y PNUD recordaron que es necesario no perder el horizonte sobre la longitud del Módulo, que se inserta en un cuestionario ya considerablemente largo. República Dominicana (ONE) recalcó que estas numerosas definiciones aumentan la complejidad y los retos para la capacitación y entrenamiento del personal que participa en el levantamiento de datos. Para resolver este problema de la longitud, República Dominicana (Ministerio de Interior y Policía) sugiere dividir los módulos en función de grupo etario para enfocar la medición de los principales grupos afectados por cada ciberdelito.

4. **TEMA 1: 1.1 ¿Considera que este módulo sobre ciberdelitos debería ser incluido como un *delito nuclear* o un *delito no-nuclear* dentro del cuestionario de la Iniciativa VICLAC? Y ¿por qué?**
   - A favor de que sea nuclear: UNODC ROPAN de acuerdo en que este Módulo sea nuclear al Interior de la Iniciativa VICLAC ya que los resultados podrían nutrir las discusiones que se iniciarán y que se mantendrán en la convención de Naciones Unidas sobre el mal uso de las Tecnologías de la Información y Comunicación (TIC). República Dominicana (Ministerio de Interior y Policía y ONE) recordaron que es importante tener datos para crear ley para persecución de ciberdelitos. Es importante tener una manera de favorecer una tipificación común, para facilitar cooperación internacional. OEA recalcó la importancia de visibilizar el tema y de comenzar a recolectar datos sobre los ciberdelitos.
   - A favor de que sea no-nuclear: Perú (INEI) manifestó su reserva en que este Módulo sea nuclear en la Iniciativa VICLAC ya que la legislación de cada país es variable. PNUD sugiere que, aunque idealmente este Módulo debería ser nuclear, su inclusión debería ser a discreción de los países para favorecer una mejor asignación de recursos de acuerdo con las prioridades de información internas. Colombia (DANE) recalcó que, considerando el listado de delitos ya considerados como nucleares en la Iniciativa

VICLAC y la carga adicional que pueda significar la inclusión del Módulo, sería importante mantenerlo como discrecional para cada país. Sin embargo, hay que reconocer la importancia y relevancia que ha tomado la ciberdelincuencia en los últimos años y más recientemente durante la pandemia de COVID-19. También propuso llegar a un acuerdo sobre que sea nuclear, pero que se pueda evaluar los ciberdelitos a incluir.

5. **TEMA 1: 1.2 ¿Tiene algún comentario, por ejemplo, sobre la estructura del módulo, la formulación de las preguntas o el lenguaje utilizado, entre otros?**
   - Colombia (DANE) presentó comentarios muy detallados respecto a la estructura del Módulo. Mencionó algunos de ellos (como, por ejemplo, la importancia de agregar el dispositivo tecnológico desde el cual ocurrió el delito, las preguntas abiertas incluidas en el módulo podrían representan un reto a la hora de sistematizar la información, la inclusión de una pregunta filtro inicial para verificar que el informante se haya conectado a internet por razones personales establecer lista de daños en caso de malware, sugirió que en el concepto de salud incluido en las preguntas debía mencionarse explícitamente que esta engloba tanto salud física como mental, entre otros). Estos comentarios se enviarán por correo al Secretario Técnico de la Iniciativa VICLAC, el CdE.
   - PNUD coincidió con los comentarios de Colombia (DANE) respecto a una posible victimización del informante por más de un ciberdelito. También se sugirió indagar por los dispositivos donde ocurrió la victimización en los últimos 12 meses. También se sugirió incluir una medición del impacto económico y también en la confianza en las autoridades a cargo de mitigar este impacto.
   - República Dominicana (Ministerio de Interior y Policía) preguntó acerca de asistencia técnica y capacitación en caso de que un país decida pilotear e implementar este Módulo.
   - UNODC ROPAN recalcó que hay que considerar la responsabilidad de las empresas privadas que trabajan en el ciberespacio, además de la responsabilidad de las autoridades, en perseguir estos ciberdelitos. Esto se tendría que reflejar en el Módulo.

6. **TEMA 3: 3.2 Ser víctima de un ciberdelito puede tener cierto impacto en los hábitos de la víctima y se considera fundamental medirlo. ¿Considera que la medición de los cambios de hábitos del informante debería incluirse? Si es así, ¿en qué sección del cuestionario?**
   - Colombia (DANE), República Dominicana (Ministerio de Interior y Policía) y PNUD manifestaron interés en medir los efectos de los ciberdelitos en la vida de las personas al interior del Módulo. Se recalcó que, en el caso de los ciberdelitos, podría haber afectaciones/consecuencias en la frecuentación de sitios internet, en el uso de los dispositivos, en el manejo de contraseñas, por ejemplo. Se propone incluir dicha medición antes de la de los efectos en la salud física y psicológica, para evitar posibles sesgos.

- OEA indicó que sería importante saber si a partir de casos de ciberacoso, *malware*, hackeo o *ransomware*, la persona cambió sus comportamientos. Esto se podría preguntar en la sección de Preguntas para TODOS los ciberdelitos o analizar si convendría formular la pregunta para alguna situación particular. Por ejemplo, para casos de ciberacoso, la persona podría haber decidido dejar de postear comentarios o foto, o dejar de utilizar redes sociales.

Acuerdos

La Sra. Flores, Coordinadora del Centro de Excelencia sintetizó los principales acuerdos producto de la discusión entre las personas que participaron en las dos jornadas de la reunión técnica:

- Definición de ciberacoso: La diferenciación entre ciberacoso visible e invisible para los demás no abona para la definición de ciberacoso, ambas tipologías de este crimen deben ser incluidas en el concepto.
- Definición de hackeo medios/redes sociales: se acordó incluir los blogs como medio social que pudiera sufrir un hackeo, aunque se mantiene la propuesta inicial de mantener diferenciados el hackeo de cuentas personales y de cuentas de redes sociales institucionales y/o corporativas.
- Definiciones de suplantación y robo de identidad: se sugirió mejorar estas definiciones para que sean más claras y mutuamente excluyentes.
- Noticias falsas: se acordó no incluirlo como delito, por su complejidad en medir la amplitud de su ocurrencia, pero se toma nota de la importancia del tema. Se generará una pregunta en el Apartado B de Percepción de la Iniciativa VICLAC, considerando la diferencia entre los conceptos de "misinformation" y "disinformation". Habrá un intento de utilizar una definición lo más neutra posible, aunque se reconoce el reto de separar el concepto de noticias falsas de su significado/asociación política. También se tratará de identificar áreas o sectores a las que están vinculadas estas noticias y de identificar los medios por los cuales se reciben estos tipos de noticias.
- Delito nuclear o no: La mayoría de los participantes señalaron que este Módulo podría ser no nuclear dentro de la Iniciativa VICLAC. Sin embargo, el CdE buscará promover la medición de la ciberdelincuencia con los países de la región de América Latina y el Caribe.
- Delitos a incluir: para favorecer una mejor asignación de recursos de los países de acuerdo con las prioridades de información internas, la decisión sobre el número y tipo de ciberdelitos a medir se dejará a discreción de los países.
- Estructura y metodología del Módulo: la Secretaría Técnica de la Iniciativa VICLAC, el CdE, implementará los comentarios muy puntuales recibidos durante las discusiones: en particular, se ajustarán los reactivos para tener un concepto amplio de las afectaciones en salud del ciberdelito (incluyendo la salud mental), y se tomará en cuenta que la denuncia

de estas conductas muchas veces se hace a las compañías que proveen de servicios tecnológicos y no a la autoridad.

- Evidente demanda de ampliar estos trabajos de medición de los ciberdelitos: de las dos jornadas de trabajo, surge la importancia de hacer un diseño particular para población que es víctima de la ciberdelincuencia pero que comúnmente no forma parte de la población objetivo de una encuesta de victimización a personas: niños y empresas. El CdE se comprometió a buscar potenciales organismos socios con experiencia de trabajo con estas poblaciones (por ejemplo, cámaras empresariales o el Fondo de las Naciones Unidas para la Infancia-UNICEF). Las sugerencias para que participen otras instituciones o potenciales aliados permanece abiertas a propuesta de las y los participantes de la reunión.

Seguimiento

- Los participantes se comprometieron a revisar la nueva propuesta de Módulo (Versión 04 agosto 2020) y enviar comentarios/observaciones (Anexo 3: Formato para la SESIÓN 2: Discusión sobre la propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC) con fecha límite 30 de septiembre 2020.
- El CdE tomará en cuenta los comentarios recibidos y los aplicará para generar una nueva versión del Módulo que esté lista a finales de octubre 2020.
- El CdE, como Secretario Técnico de la Iniciativa VICLAC, compartirá la nueva versión del Módulo sobre Ciberdelitos con los participantes a finales de octubre para su aprobación final. En caso de no recibir comentarios, se procederá por aprobación silenciosa.
- El CdE publicará la nueva versión del Módulo en su página web, en los cuatro idiomas de la Iniciativa VICLAC (inglés, español, francés y portugués).
- El CdE organizará la 8ª Reunión Técnica del Grupo de Trabajo de la Iniciativa VICLAC en noviembre de 2020. La reunión se llevará a cabo virtualmente. En esta reunión, además de aprobar el módulo oficialmente dentro del seno de la Iniciativa VICLAC, se sumarán otras propuestas en los campos relacionados con la enfermedad por COVID-19 y mediciones experimentales de incidencia delictiva.
- Los países que se postulen como voluntarios para pilotear el módulo sobre ciberdelitos podrán contactar al CdE al correo electrónico unodc-mexico.cde.estadistica@un.org.
- Los países que requieran asistencia técnica para implementar el Módulo sobre Ciberdelitos podrán contactar al CdE, haciendo una solicitud formal al correo electrónico: unodc-mexico.cde.estadistica@un.org.

Anexo 1

AGENDA

Reunión Técnica sobre ciberdelincuencia de la
Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC)
- 2 y 4 de septiembre de 2020 - Reunión virtual

SESIÓN 1: miércoles, 2 de septiembre de 2020

9:00 – 11:30 hrs MEX/PANAMA | 10:00 – 12:30 hrs NYC/CARACAS | 11:00 – 13:30 hrs BUENOS AIRES

08:15 – 09:00	**VoiceBoxer: https://portal-v3.voiceboxer.com/account/login (traducción simultánea disponible)**
09:00 – 09:30	**Bienvenida & nociones generales de la reunión** • Enrico Bisogno, Jefe de la Sección de Desarrollo y Difusión de Datos, UNODC HQ • Sra. Salomé Flores, Coordinadora del Centro de Excelencia, UNODC México • Antecedentes y objetivos • Dinámica de la reunión técnica • Presentación de las y los participantes
9:30 – 10:15	**Entendiendo la ciberdelincuencia** **Modera:** Enrico Bisogno, Sección de Desarrollo y Difusión de Datos, UNODC HQ • Instituto de Investigación sobre Ciberdelincuencia (15 min) – Sr. Marco Gercke, Director, Alemania ***Preguntas & respuestas (5 min)*** • Universitat Abat Oliba CEU (15 min) – Sr. José Ramón Agustina, Catedrático de Derecho penal y Criminología, España ***Preguntas & respuestas (5 min)***
10:15 – 10:25	**Receso**
10:25 – 10:45	**Contexto internacional** • Programa Global de Ciberdelito de UNODC (15 minutos) ○ Sra. Nayelly Loya Marín, Coordinadora del Programa Global de Ciberdelito, UNODC Panamá ***Preguntas & respuestas (5 min)***
10:45 – 11:00	**Propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC** **Presenta:** Sra. Luisa Sánchez, Centro de Excelencia, UNODC México (15 min) • Necesidades de información en Latinoamérica y el Caribe • Revisión de la estructura del módulo y como complementa la medición de otros delitos incluidos en VICLAC (fraude bancario, amenazas, extorsión) ***Preguntas & respuestas***
11:00 – 11:10	**Receso**
11:10 – 12:00	**Experiencia de países en la medición de la ciberdelincuencia** **Modera:** Sra. Salomé Flores, Centro de Excelencia, UNODC México

	• Santa Lucía: Resultados de la Encuesta Nacional de Victimización de Santa Lucía (SLNCVS) (15 min)
	  ○ Sra. Linn Lelia Brown, Estadística, Oficina Central de Estadísticas (CSO)
	• México: Módulo sobre Ciberacoso (MOCIBA) (15 min)
	  ○ Sr. Mario Santillana, Instituto Nacional de Estadística y Geografía (INEGI)
	• Perú: Investigación de Delitos de Alta Tecnología (15 min)
	  ○ Sra. Cinthya Cárdenas Rondón, Policía Nacional del Perú (PNP)
	Preguntas & respuestas (10 min)
	
	PREPARACIÓN PARA LA SESIÓN 2:
	• De acuerdo con las presentaciones de los/las expertos y las experiencias de los países, reflexionar y valorar la propuesta de módulo sobre ciberdelito (enviada por correo electrónico).
	• **Las reflexiones y comentarios serán discutidos en la sesión 2.**

SESIÓN 2: viernes, 4 de septiembre de 2020

9:00 – 11:30 hrs MEX/PANAMA | 10:00 – 12:30 hrs NYC/CARACAS | 11:00 – 13:30 hrs BUENOS AIRES

08:15 – 09:00	**VoiceBoxer: https://portal-v3.voiceboxer.com/account/login (traducción simultánea disponible)**

9:00 – 10:30	**Discusión sobre la propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC**
	Modera: Sra. Luisa Sánchez, Centro de Excelencia, UNODC México
	• Comentarios de los/las participantes sobre la propuesta de UNODC con relación a:
	  ○ Estructura y metodología del módulo
	  ○ Tipos de ciberdelitos propuestos para medir
	  ○ Inclusión de preguntas específicas de contexto sobre ciberdelincuencia

10:30 – 10:45	**Receso**
10:45 – 11:15	**Acuerdos de la Reunión Técnica** **Modera:** Sra. Salomé Flores, Centro de Excelencia, UNODC México • Temas que cubrirá el módulo • Países piloto para el módulo
11:15 – 11:30	**Cierre de la Reunión Técnica** • Próximos pasos de la Iniciativa VICLAC • Cierre de la Reunión

ⓘ Más información:

- ☞ *Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC)*
- ☞ Marco Conceptual Iniciativa VICLAC (español) (inglés)
- ☞ Minuta de la 7ª Reunión Técnica del Grupo de Trabajo de la Iniciativa VICLAC – 22 y 23 de octubre 2019, Ciudad de México (español) (inglés)
- ☞ VicLab talks (grabadas en español o inglés, subtítulos disponibles)

Anexo 2

Lista de asistentes

N°	País	Participante	E-mail	Institución	Cargo/posición
1	Argentina	Horacio Azzolin	HAzzolin@mpf.gov.ar	Ministerio Público Fiscal (Unidad Especializada en Ciberdelincuencia)	Fiscal de la Procuración General de la Nación
2	Colombia	Diana Carolina Peña	dcpenab@dane.gov.co	DANE	Coordinadora GIT Capital Social
3	Colombia	Horacio Coral Díaz	hcorald@dane.gov.co	DANE	Asesor
4	Colombia	Rodrigo Javier Acevedo Nieto	rodrigo.acevedo6500@correo.policia.gov.co	Policía Nacional de Colombia (Dirección de Investigación Criminal e Interpol - DIJIN)	Mayor en el Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL
5	México	Mario Santillana	alberto.santillana@inegi.org.mx	INEGI	Director General Adjunto de Modelos de Información Gubernamental y Encuestas Nacionales de Gobierno, Victimización Seguridad y Justicia
6	Perú	Aníbal Sánchez Aguilar	anibal.sanchez@inei.gob.pe	INEI	Subjefe de Estadística
7	Perú	Juan Trejo	Juan.Trejo@inei.gob.pe	INEI	
8	Perú	Cinthya Julissa Cárdenas Rondón	cjjcinthya@gmail.com	Policía Nacional del Perú (PNP)	Capitán en la División de Investigación de Delitos de Alta Tecnología de la Dirección de Investigación Criminal
9	Perú	Luis Alberto Loayza Ramírez	lloayzar@gmail.com	Policía Nacional del Perú (PNP)	Jefe de la División de Estadística de la dirección de Tecnologías de la Información y Comunicaciones (DIRTIC)
10	Perú	Marco Antonio Vilchez Asenjo	vilchezasenjo@gmail.com	Policía Nacional del Perú (PNP)	Jefe del Dpto de Análisis de la DIVEST DIRTIC
11	Perú	Roger Chipa Sierra	rogerchipa@gmail.com	Policía Nacional del Perú (PNP)	Jefe del Dpto de Procesamiento de la DIVEST
12	República Dominicana	Dangela Ramirez	dramirezg@mip.gob.do	Ministerio de Interior y Policía	Directora de asuntos internos
13	República Dominicana	Maridalia Rodríguez	maridalia.rodriguez@one.gob.do	ONE	Encargada del departamento de Articulación Sectorial del

					Sistema Estadístico Nacional
14	República Dominicana	Ivan Féliz Vargas	ifeliz@pgr.gob.do	Procuraduría General de la República	Procurador General de Corte de Apelación, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología
15	Santa Lucía	Linn Lelia Brown	linn.brown@govt.lc	Central Statistical Office (CSO)	Statistician (Demography)
16	(CDMX)	Salomé Flores	salome.flores@un.org	CdE	Oficial Nacional de Programas
17	(CDMX)	Luisa Sánchez	luisa.sanchez@un.org	CdE	Investigadora en Delincuencia y Justicia Penal
18	(CDMX)	Giada Greco	giada.greco@un.org	CdE	Técnico en Estadísticas Delictivas
19	(CDMX)	Javier Tun	javier.tunchim@un.org	CdE	Especialista en gestión del conocimiento
20	(CDMX)	Héctor Duarte	hector.duerte@un.org	CdE	Especialista de estadísticas delictivas
21	(CDMX)	Justo Rojas	rojasjusto@gmail.com	CdE	Asistente técnico en estadísticas delictivas
22	(CDMX)	Víctor Merchand	victor.merchand@un.org	UNODC	Specialist Information Technology Strategies
23	(Washington)	Ariel Nowersztern	ARIELN@IADB.ORG	BID	Especialista en Ciberseguridad
24	(Washington)	José Antonio Mejía	JoseAM@IADB.ORG	BID	Modernisation of the State Lead Specialist
25	(Chile)	Xavier Mancero	xavier.mancero@cepal.org	CEPAL	Senior statistician
26	(Chile)	Pablo VIllatoro	pablo.villatoro@cepal.org	CEPAL	Senior statistics assistan
27	(Washington)	Kerry-Ann Barrett	KABarrett@oas.org	OEA	Cybersecurity Policy Specialist
28	(Washington)	Karen Bozicovich	KBozicovich@oas.org	OEA	Chief of the Public Security Information and Knowledge Section
29	(Panamá)	Marcela Smutt	marcela.smutt@undp.org	UNDP	Chief Technical Specialist
30		Pablo Gordillo	juan.gordillo@undp.org	UNDP	Project Coordinator
31	(El Salvador)	Nayelly Loya Marín	bertha.loya@un.org	UNODC	Cybercrime Programme Coordinator
32	(España)	José Agustina	jagustinas@uao.es	Universitat Abat Oliba CEU	Catedrático de Derecho penal y Criminología

33	(Viena)	Enrico Bisogno	enrico.bisogno@un.org	UNODC HQ	Chief of Data Development Unit
34	(Viena)	Fatma Ismetova Usheva	fatma.usheva@un.org	UNODC HQ	Data Analyst
35	(Alemania, Colonia)	Marco Gercke	gercke@cybercrime.de	Cybercrime Research Institute (CRI)	Director

Anexo 3

Formato para la SESIÓN 2: Discusión sobre la propuesta de módulo sobre medición de ciberdelincuencia de la Iniciativa VICLAC (viernes, 4 de septiembre de 2020)

Nombre del / de la participante:

Institución / País:

Los temas para discutir durante la sesión serían los siguientes. Para cada tema, usted puede agregar cualquier otra pregunta que considere pertinente discutir en el Grupo de Trabajo:

TEMA 1: Estructura y metodología del módulo

1.1. ¿Considera que este módulo sobre ciberdelitos debería ser incluido como un *delito nuclear* o un *delito no-nuclear* dentro del cuestionario de la Iniciativa VICLAC? Si/No y ¿por qué? ***Delito nuclear:*** aquellos delitos que se consideran prioritarios a medir (y que, al adoptar la Iniciativa VICLAC, cada país lo tendrá que medir) ***Delito no-nuclear:*** aquellos delitos cuya inclusión es totalmente discrecional y dependen mucho de la realidad de los países y los recursos destinados a la realización de la encuesta
Inserte su respuesta aquí:

1.2. ¿Tiene algún comentario, por ejemplo, sobre la estructura del módulo, la formulación de las preguntas o el lenguaje utilizado, entre otros? Le agradecemos indicar el número de pregunta correspondiente en el módulo y su propuesta específica.
Inserte su respuesta aquí:

TEMA 2: Tipos de ciberdelitos propuestos para medir

2.1. ¿Tiene alguna sugerencia o comentarios sobre los delitos ya incluidos en la propuesta del módulo?

Inserte su respuesta aquí:

2.2. En el mundo de la ciberdelincuencia, existen otros ciberdelitos que se podrían incluir en el módulo como, por ejemplo: S*uplantación/Robo de identidad*, Fake news, *Grooming*, Sextorsión, entre otros.
¿Cuáles considera ustedes fundamentales incluir y por qué, considerando el contexto regional y de su país? En términos metodológicos, considere que este módulo será incluido en una encuesta a hogares, recomendado para personas de 18 años y más.

Suplantación de identidad: creación de un perfil falso, pero con la identidad de otra persona a la que se pretende suplantar.
Robo de identidad: se produce cuando el que suplanta la identidad lo realiza por haber sustraído los datos de acceso a Internet y redes sociales de la persona.
Noticias falsas: También conocidas como con el anglicismo *fake news*, son un tipo de bulo que consiste en un contenido pseudo-periodístico difundido a través de portales de noticias, prensa escrita, radio, televisión y redes sociales y cuyo objetivo es la desinformación. Las noticias digitales han recuperado y aumentado el uso de noticias falsas o periodismo amarillo. Se diseñan y emiten con la intención deliberada de engañar, inducir a error, manipular decisiones personales, desprestigiar o enaltecer a una institución, entidad o persona u obtener ganancias económicas o rédito político. Al presentar hechos falsos como si fueran reales, son consideradas una amenaza a la credibilidad de los medios serios y los periodistas profesionales, a la vez que un desafío para el público receptor.
Phishing: obtener información confidencial de forma fraudulenta en donde el estafador, conocido como phisher, *se vale de técnicas de ingeniería social,* haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales, a raíz de un malware.
Grooming: forma delictiva de acoso que implica a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual. Se trata de un proceso en el que se produce un vínculo de confianza entre la víctima y el acosador. Este intenta aislar poco a poco al/ a la menor, y lo consigue desprendiéndolo de su red de apoyo (familiares, profesores, amigos, etc.) y generando un ambiente de secretismo e intimidad. El abusador envía, a través de un medio tecnológico, material sexual al niño o niña. Además, se suele hacer pasar por menor y adapta el lenguaje a la edad de la víctima.
Sextorsión: Una forma de chantaje en la que se utiliza información o imágenes sexuales para obtener favores sexuales de la víctima. Las redes sociales y los mensajes de texto son a menudo la fuente del material sexual y el medio amenazado de compartirlo con otros. Un ejemplo de este tipo de sextorsión es cuando las personas son extorsionadas con una imagen desnuda de sí mismas que compartieron en Internet a través del *sexting*.

Inserte su respuesta aquí:

TEMA 3: Inclusión de preguntas específicas de contexto sobre ciberdelincuencia

3.1. No todos los países tipifican los ciberdelitos / delitos cibernéticos / delitos apoyados por la tecnología. ¿Podría indicarnos qué tipos de ciberdelitos están tipificados en su país?
En su caso, le agradecemos si nos puede indicar la ley correspondiente.

Inserte su respuesta aquí:

3.2. Ser víctima de un delito cibernético puede tener un gran impacto en los hábitos de la víctima y se considera esencial medirlo. ¿Cree que debería incluirse la medición de los cambios en los hábitos del informante? En caso afirmativo, ¿en qué parte del cuestionario LACSI?
Inserte su respuesta aquí:

3.3. ¿Tiene alguna otra sugerencia o comentario adicional al módulo?
Inserte su respuesta aquí:

Anexo 4

Preguntas a expertos y respuestas correspondientes

José Ramón Agustina, Catedrático de Derecho Penal y Criminología de la Universitat Abat Oliba CEU, España

1. **"¿No se debería también fortalecer las capacidades de las policías para el registro y la investigación del ciberdelito? Me parece importante el tema de la victimización por delitos cibernéticos, pero me parece importante también fortalecer el registro administrativo, así como la capacidad de responder e investigar. En ese sentido, ¿existen líneas especiales para denunciar este tipo de delitos en los países, atendidas por personal policial especializado? (Sra. Karen Bozicovich / OEA):**
   Sí, en efecto, se debería también fortalecer las capacidades de las policías para el registro y la investigación del ciberdelito. Pienso que sería muy importante fomentar la colaboración de los investigadores y expertos del mundo académico (especializados en estadística, criminología y ciberseguridad) con los cuerpos policiales. En mi país no es fácil, pues existe una elevada desconfianza por parte de la policía a dejar entrar a nadie de fuera. En ese contexto de colaboración, se deberían crear equipos de trabajo multidisciplinares para que los registros permitan extraer información para la inteligencia policial y, a su vez, para realizar investigaciones criminológicas bien coordinadas en los que se conozca a fondo los perfiles de ofensores y víctimas, la dinámica delictiva, la valoración de los daños, las medidas de reacción adoptadas, las vulnerabilidades de la víctima, etc. Como dije en mi ponencia, el concepto de ciberdelito es criminológico y abarca muy distintas modalidades o figuras jurídicas de delito. Por tanto, el registro debería permitir señalar si las TIC han jugado un papel esencial en la comisión del delito sea cual sea. Asimismo, por supuesto, se deberían formar policías y crear líneas especiales para denunciar este tipo de delitos. Ahora mismo, en los cuerpos policiales en mi país, hasta donde yo sé, solo existen unidades especializadas en policía judicial, pero ni en la atención inmediata a las víctimas, ni en la formación preventiva en escuelas se aprecia un esfuerzo de calidad para afrontar un problema tan importante. Sin duda, se trata de una cuestión de invertir muchos más recursos personales, económicos y materiales.

2. **"¿Qué experiencias interesantes conoce de educación cívica/socialización sobre el ciberdelito y qué hacer si uno/a es víctima?" (Sra. Karen Bozicovich / OEA):**
   En España tenemos el INCIBE y Is4k (tienen acceso online a materiales). Hay varios grupos de investigación importantes que están trabajando en el análisis criminológico del

ciberdelito, como CRIMINA, dirigido por el Dr. Fernando Miró. Pienso que hay que trabajar mucho más en el problema desde una perspectiva victimológica. A este respecto, les adjunto un artículo que publicamos en la Revista Española de Pedagogía: https://revistadepedagogia.org/lxxvii/no-273/retos-educativos-ante-los-riesgos-emergentes-en-el-ciberespacio-claves-para-una-adecuada-prevencion-de-la-cibervictimizacion-en-menores/101400073259/

3. **"Muchas gracias por la excelente presentación. Quisiera saber si: ¿hay alguna experiencia que pueda compartir sobre procesos de articulación e interacción interinstitucional (entes que por su marco legal participan en el diseño y ejecución de políticas públicas, sobre ciberseguridad) para la identificación de demandas, generación e intercambio de datos estadísticos relacionados al tema? (Sra. Maridalia Rordíguez, ONE, República Dominicana)**

   En cuanto a experiencias sobre procesos de colaboración interinstitucional en ciberseguridad la sensación generalizada es que, más allá de medidas efectistas, hay poca coordinación en el ámbito público. Los que invierten en ciberseguridad son sobre todo las empresas privadas que ven el problema y además se tienen que defender a sí mismas sin contar con el Estado, pues carece de medios. El enfoque es claramente el de la prevención y estamos todos muy poco concienciados a todos los niveles. Recientemente he participado en una jornada de formación para administraciones públicas, pues obviamente los ciberfraudes y los ciberataques a entes públicos son muy importantes. En breve publicaremos un libro con las experiencias.

Nayelly Loya, Coordinadora regional del Programa Global de Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) de Centroamérica y el Caribe (ROPAN)

1. **"Para la cuestión de la información y la educación, ¿están trabajando con periodistas y medios de comunicación (tradicionales y no-tradicionales)?" (Sra. Karen Bozicovich / OEA)**

   Sí. Ello con el propósito de educar a través de ellos, pero también para que ellos entiendan y aborden de mejor manera el fenómeno. Esto incluye talleres con medios tradicionales, así como podcast y en diversos formatos digitales.

2. **¿Tienen un assessment tool para evaluar/diagnosticar las capacidades de los sistemas de justicia penal para prevenir/investigar/procesar delitos cibernéticos? (Sra. Karen Bozicovich / OEA)**

   Sí. En conjunto con el Banco Mundial y otras agencias del sistema se desalló una herramienta que puede ser accesada aquí: http://www.combattingcybercrime.org/

3. **(Trad.) "¿Habrá un calendario de reuniones para ese grupo sobre el nuevo tratado? (Sra. Kerry-Ann Barret / OEA)**

   Los Estados miembros debían reunirse en Nueva York, en agosto, en una sesión organizativa del Comité Ad Hoc sobre el Cibercrimen. Debido a COVID19, la sesión ha sido pospuesta por la Asamblea General de las Naciones Unidas y actualmente se debe convocar en una fecha no decidida antes del 1 de marzo de 2021. Es en este período de sesiones de organización donde los Estados Miembros decidirán cómo, dónde y cuándo se celebrarán los períodos de sesiones sustantivos.