UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

CENTRO DE EXCELENCIA UNODC-INEGI
para Información Estadística de Gobierno, Seguridad Pública, Victimización y Justicia

UNODC Research

2 Nota informativa de la ICCS

Midiendo la ciberdelincuencia a través de la óptica de la ICCS

Julio 2023

Midiendo la ciberdelincuencia a través de la óptica de la ICCS

¿Qué es la Clasificación Internacional de Delitos con Fines Estadísticos (ICCS)?

La ICCS es una clasificación estadística, un conjunto de categorías discretas, exhaustivas y mutuamente excluyentes que pueden asignarse a una o más variables utilizadas en la recopilación y presentación de datos sobre actividades delictivas. Se trata de un marco global de conceptos y definiciones de delito acordados internacionalmente que mejoran la recopilación, organización, análisis y difusión de datos estadísticos sobre delincuencia, incluidas las características de los actos delictivos, las víctimas, los autores, la motivación y otros datos esenciales.

La ICCS es, por lo tanto, una herramienta estadística para comprender el alcance y los factores que impulsan la delincuencia. Su unidad primaria de clasificación es el acto o suceso que constituye un delito, y la descripción del acto delictivo se basa en conductas mutuamente excluyentes y no en disposiciones legales. Desde 2015, ha contribuido a mejorar la coherencia y la comparabilidad internacional de las estadísticas sobre delincuencia y a aumentar la capacidad para su análisis, tanto a escala nacional como internacional.[1]

¿Por qué es relevante medir la ciberdelincuencia a través de la ICCS?

La sociedad ha cambiado radicalmente desde la adopción y evolución de las Tecnologías de la Información y la Comunicación (TIC), que han revolucionado la forma en que las personas se conectan. A medida que la sociedad adoptaba las TIC, la gama de delitos que podían perpetrarse utilizándolas se volvía cada vez más cambiante, tanto en términos de cambio tecnológico como de interacción social con las nuevas tecnologías. Desde su concepción, la ICCS ha reconocido la relevancia de producir datos sobre la ciberdelincuencia y el uso de las TIC en actividades delictivas. Sin embargo, esta necesidad se ha hecho más imperativa a raíz de la pandemia COVID-19. Durante la pandemia, se produjo un aumento del phishing, fraudes de tarjetas de crédito, sitios web pirateados que pedían donaciones falsas y ciberataques, incluidos los organizados por grupos delictivos organizados.[2]

¿Cuáles son las ventajas de medir la ciberdelincuencia y las TIC utilizadas con fines delictivos?

Gracias a la aplicación de la ICCS, las estadísticas sobre delincuencia adquieren mayor relevancia para una serie de cuestiones relacionadas con la ciberdelincuencia y las TIC, por ejemplo:

- Legislación sobre ciber-delincuencia: con la adopción de la ICCS cuyo enfoque está basado en las conductas, las estadísticas nacionales sobre un número de ciberdelitos o delitos cometidos utilizando las TIC se pueden producir de forma estandarizada y completa. Estas estadísticas sobre ciber-delincuencia pueden servir de base para introducir cambios

[1] La ICCS fue aprobada por la Comisión de Esta-dística de las Naciones Unidas, en su 46ª sesión de marzo de 2015, y por la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), en su 24ª sesión de mayo de 2015, como norma estadística internacional para la recopilación de datos. Las dos Comisiones también han confirmado a la UNODC como custodio de la ICCS. Para más información, visite: https://www.unodc.org/unodc/en/data-and-analysis/statistics/iccs.html

[2] El impacto de COVID-19 en la delincuencia organizada, Research Brief (Oficina de las Naciones Unidas contra la Droga y el Delito, 2020).

legislativos en materia de investigación y tipificación penal.

- Protección de las víctimas: al hacer visibles los ciberdelitos mediante estadísticas, se puede instaurar una cultura de ciberseguridad y un sistema de sensibilización para que los particulares, las empresas y las organizaciones se protejan.
- Justicia para las víctimas: al hacer visibles los ciberdelitos, las víctimas también pueden buscar justicia en un sistema que sancione estos delitos.
- Estadísticas sobre ciberdelincuencia: Estas pueden utilizarse para conocer mejor y describir con mayor precisión la ciberdelincuencia, tomar decisiones basadas en evidencia y alentar al personal de investigación a formarse y cualificarse para hacer frente a los ciberdelitos que afectan a una población.
- Promover la colaboración entre los Estados miembros a través de alianzas estratégicas para el intercambio de datos, análisis e investigación, considerando la naturaleza transnacional de la ciberdelincuencia y la interdependencia de los sistemas y dispositivos digitales conectados a Internet dentro y fuera de los países.
- Comprender mejor qué mecanismos deben establecerse para conocer los efectos de la ciberdelincuencia, adoptando o mejorando herramientas de recopilación de datos adaptadas a esta realidad.

¿Cómo se miden la ciberdelincuencia y otras TIC utilizadas con fines delictivos a través de la ICCS?

El análisis de la ciberdelincuencia y otras TIC utilizadas con fines delictivos es un elemento transversal en el marco de la ICCS. El uso de las TIC es identificado por la ICCS como un factor que puede facilitar diversos tipos de conductas delictivas. La clasificación está diseñada para registrar sistemáticamente la dimensión cibernética de los delitos, lo que facilita la medición de los delitos *ciber-dependientes*[3] y los delitos *ciber-facilitados*.[4] Aunque en la actualidad estos términos no se incluyen explícitamente en la ICCS, la clasificación puede utilizarse para distinguir entre las dos formas de ciberdelincuencia.

La ICCS establece definiciones de algunos delitos específicamente *ciber-dependientes* dentro de la categoría de nivel 2 "Actos contra sistemas informáticos" (0903). Esta incluye, entre otros, la piratería informática, los ataques de denegación de servicio, la eliminación de archivos de sistemas informáticos sin autorización, los daños a sistemas informáticos, la creación, difusión y colocación de malware o ransomware, y ataques a infraestructuras nacionales críticas.

Los delitos *ciber-facilitados*, por su parte, no tienen códigos ICCS específicos, ya que son delitos tradicionales que se cometen utilizando un ordenador. Para ayudar a identificar estos delitos como ciberdelitos, la ICCS también ofrece la variable de acto relacionado con la ciberdelincuencia (Cy). Debe aplicarse cuando el uso de datos de computadora o sistemas informáticos haya

[3] Los delitos *ciber-dependientes* son delitos que tienen como objetivo un ordenador o un sistema informático per se. Estos delitos sólo pueden cometerse a través de una infraestructura TIC y a menudo se tipifican como acceso no autorizado, interceptación, interferencia o uso indebido de datos informáticos o equipos/sistemas de información. Véase la nota 128 (página 98) de la ICCS para las definiciones de datos informáticos, sistema informático/de información y programa informático/de información.

[4] Un delito *ciber-facilitado* es un delito en el que se utiliza un ordenador o Internet para cometerlo. Es un delito que puede ocurrir en el mundo físico pero que también puede verse facilitado por las TIC.

sido una parte clave del modus operandi del delito.

Nótese que la variable de acto relacionado con la ciberdelincuencia también debe utilizarse para los delitos *ciber-dependientes*. Sin embargo, dado que estos delitos tienen códigos ICCS específicos, pueden identificarse como ciberdelitos sin utilizar la variable. Los delitos *ciber-facilitados*, por otro lado, no pueden ser reconocidos en las estadísticas como ciberdelitos sin la variable de acto relacionado con la ciberdelincuencia

¿Cómo funciona la variable de acto relacionado con la ciberdelincuencia?

Ciertas características de los hechos delictivos o de su modus operandi pueden registrarse mediante la aplicación de la ICCS utilizando una de las variables incluidas en las desagregaciones de los hechos. Estas variables deben utilizarse a nivel de registro individual y sirven para asignar información específica a cada hecho delictivo registrado.

La variable de acto relacionado con la ciberdelincuencia está considerada en las desagregaciones de los hechos. La variable puede utilizarse junto con otras variables de desagregación incluidas en la ICCS para crear una imagen más completa del delito. Esto incluye el sexo y la edad de la víctima y el autor, detalles sobre la relación víctima-autor, y la fecha y hora del delito, entre otros.[5]

Como ya se ha señalado, los delitos pueden categorizarse utilizando la variable de *ciber-facilitado* si el uso de datos o sistemas informáticos es parte clave en el modus operandi del delito. Se consideran delitos que pueden cometerse en el mundo físico pero que se facilitan en el mundo virtual y pueden incluir el fraude en línea, la compra de drogas en línea, el ciberacoso, el ciber-hostigamiento, las amenazas, la violación de los derechos de autor, el blanqueo de dinero, la usurpación o suplantación de identidad, el chantaje, la difamación, la sextorsión, los delitos de pornografía (incluidos el porno de venganza y la captación de menores con fines sexuales), la producción y distribución de pornografía infantil, entre otros.

Con este enfoque, es posible registrar y contabilizar los delitos ciber-relacionados de manera exhaustiva. Aparte de los delitos contra los propios sistemas informáticos, el uso de las TIC para cometer delitos no siempre es explícito. La variable de acto relacionado con la ciberdelincuencia proporciona información más completa para identificar todos los delitos perpetrados utilizando un facilitador cibernético o virtual.

La variable de acto relacionado con la ciberdelincuencia no debe aplicarse cuando el uso de las TIC no sea clave en el modus operandi del delito. Por ejemplo, se recomienda utilizar la variable de acto relacionado con la ciberdelincuencia para un acto de acoso cometido a través de mensajes de texto o una cuenta de redes sociales. El uso de las TIC es una parte clave del delito, por lo que se registrará como un acto de ciberacoso. Por otro lado, si un homicidio fue cometido por un autor que localizó a la víctima utilizando la señal de su celular, no deberá utilizarse la variable de acto relacionado con la ciber-delincuencia. En este caso, el uso de las TIC no es una parte clave del delito, es un aspecto incidental del homicidio que proporciona evidencias electrónicas que pueden utilizarse, por ejemplo, para determinar la intencionalidad y distinguir entre homicidio intencional y no intencional.

[5] Para más detalles, vea las tablas II-V de la ICCS.

¿Qué se está haciendo para seguir mejorando la medición de la ciberdelincuencia a través de la ICCS?

Los Estados miembros están negociando una nueva convención sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos, que está prevista para presentarse en el 78º periodo de sesiones de la Asamblea General de las Naciones Unidas. Esto se lleva a cabo a través de los trabajos del *Comité Ad Hoc encargado de preparar una convención internacional integral contra la utilización de las tecnologías de la información y la comunicación con fines delictivos*.[6]

Una vez concluidas las negociaciones de la convención, UNODC y las organizaciones pertinentes podrían entablar discusiones para elaborar un marco estadístico que permita medir el ciberdelito.[7]

La ICCS se está aplicando actualmente en un número cada vez mayor de países con vistas a mejorar los datos sobre delincuencia y justicia penal. UNODC sigue de cerca esta implementación, que también es útil para recopilar retroalimentación y sugerencias sobre las posibles inconsistencias y brechas que puedan surgir a nivel de país para que puedan ser abordadas en futuras versiones de la ICCS.

UNODC agradece las propuestas sobre la incorporación de delitos relacionados con la ciberdelincuencia al marco de la ICCS o el ajuste de las variables de desagregación, como la ampliación del espectro de la variable de acto relacionado con la ciberdelincuencia para crear más especificidad. Por ejemplo, la variable podría distinguir entre delitos *ciber-dependientes* y *ciber-facilitados*.

Para más información y cualquier consulta relacionada con la ICCS, póngase en contacto con UNODC: iccs@unodc.org o consulte el sitio web: https://www.unodc.org/unodc/en/data-and-analysis/statistics/iccs.html

[6] Para más información, visite: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[7] Estas discusiones podrían seguir la misma lógica que las de la construcción del "Marco estadístico integral para medir el homicidio de mujeres y niñas por razones de género (femicidio/feminicidio)", aprobado por la Comisión de Estadística de las Naciones Unidas en 2022. El marco fue elaborado por UNODC conjuntamente con la Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres (ONU Mujeres), en plena consonancia con la ICCS. Para más información, visite: https://www.cdeunodc.inegi.org.mx/index.php/statistical-framework/