DECÁLOGO METODOLÓGICO PARA EL ESTUDIO DEL CIBERCRIMEN

Mtro. Rolando Granados Muñoz
Universidad de Guanajuato
r.granadosmunoz@ugto.mx
México
Orcid ID

Recepción 09 de marzo de 2020 / Aceptación 31 de mayo de 2020
Información, Tecnología y Empresa

Resumen

El desarrollo que ha tenido la tecnología en la actualidad ha provocado un impacto considerable en la criminalidad transformando la conducta a un fenómeno que se denomina cibercrimen. Es importante elaborar estrategias que tengan fundamentos sólidos para tener certeza de la seguridad de la información que se maneja en las TIC (Tecnologías de la información y la Comunicación). Es un estudio de tipo documental, de corte exploratorio-descriptivo y de diseño transversal, el objetivo es integrar un decálogo de líneas estratégicas para el estudio de la cibercriminalidad. Para ello fue utilizada la síntesis de distintas fuentes de información. Como resultado se obtuvo un decálogo con 10 puntos para la prevención y estudio del cibercrimen basados en las estrategias de conocer, preparar, indagar y aplicar. Los puntos del decálogo comprenden redefinir el concepto de cibercrimen, analizar el fenómeno cuantitativa y cualitativamente, aumentar las investigaciones sobre el tema, practicar la capacitación, especialización y profesionalización (CEP), distribuir redes de información sobre la problemática, delimitar espacios de interacción social, considerar víctimas y victimarios con actitudes distintas, orientar acciones a la política criminológica, aplicar teorías de prevención y evaluar las estrategias de prevención. Se concluye que, para afrontar el cibercrimen, se debe optar por herramientas, metodologías, estrategias, políticas y demás elementos que dependerán del cómo se va estableciendo el delito.

Palabras clave: Cibercrimen; protección de datos; seguridad de los datos.

A METHODOLOGICAL DECALOGUE FOR STUDYING CYBERCRIME

DÉCALOGUE MÉTHODOLOGIQUE POUR L'ÉTUDE DE LA CYBERCRIMINALITÉ

Abstract

The development that technology has experienced today has caused a considerable impact on crime, transforming behavior into a phenomenon called cybercrime. It is essential to develop solidly based strategies to be confident in information security handled in ICT. This is a documentary study, which is exploratory-descriptive, and transversal in design. Its objective is to integrate a Decalogue of strategic lines for the study of cybercrime. As a result, a 10-point Decalogue was obtained to prevent and study cybercrime based on the strategies of knowing, preparing, investigating, and applying. The aspects of the Decalogue include redefining the concept of cybercrime, analyzing the phenomenon quantitatively

Résumé

Le développement que la technologie a eu aujourd'hui a eu un impact considérable sur la criminalité, transformant le comportement en un phénomène appelé cybercriminalité. Il est important de développer des stratégies qui reposent sur des bases solides pour être certain de la sécurité des informations traitées dans les TIC (Technologies de l'Information et de la Communication). Il s'agit d'une étude de type documentaire, de conception exploratoire-descriptive et transversale, l'objectif est d'intégrer un décalogue de lignes stratégiques pour l'étude de la cybercriminalité. Pour cela, la synthèse de différentes sources d'informations a été utilisée. En conséquence, un décalogue de 10 points a été obtenu pour la prévention et

and qualitatively, increasing research on the subject, practicing training, specialization, and professionalization (PTSP), distributing information networks on the problem, defining spaces for social interaction, considering victims and perpetrators with different attitudes, orienting actions to criminological policies, applying prevention theories, and evaluating prevention strategies. It is concluded that to deal with cybercrime, one must opt for tools, methodologies, strategies, policies, and other elements that will depend on how the crime is established.

Keywords: Cybercrime, data protection, data security.

l'étude de la cybercriminalité sur la base des stratégies de connaissance, de préparation, d'enquête et d'application. Les points du décalogue incluent la redéfinition du concept de cybercriminalité, l'analyse du phénomène quantitativement et qualitativement, l'intensification des recherches sur le sujet, la pratique de la formation, de la spécialisation et de la professionnalisation (CEP), la diffusion des réseaux d'information sur la problématique, la délimitation des espaces d'interaction sociale, considérer les victimes et les auteurs avec des attitudes différentes, orienter les actions vers la politique criminologique, appliquer les théories de prévention et évaluer les stratégies de prévention. Il est conclu que, pour faire face à la cybercriminalité, il faut choisir des outils, des méthodologies, des stratégies, des politiques et d'autres éléments qui dépendront de la manière dont le crime est établi.

Mots clés: cybercriminalité; Protection de données; sécurité des données.

Introducción

El auge tecnológico que han tenido los dispositivos electrónicos ha impactado en la vida de los seres humanos, ello es comprensible por los beneficios que suelen significarle; aunque en ciertas ocasiones pasan desapercibidos los riesgos o peligros que conlleva su uso, ambos procesos han crecido circunstancialmente y de modo paulatino convirtiéndose la tecnología en una necesidad social (Azaola, 2010). Según reflejan algunas estadísticas, la cantidad de usuarios de Internet en México crece considerablemente, para el año 2018 en México, la cantidad de internautas registrada fue de 82.7 millones, en edades desde los 6 años en adelante, usando el teléfono celular para conectarse en su mayoría para acceder a redes sociales (Asociación de Internet MX, 2019). Esto supone la interacción humana en una era digital, es decir, una época caracterizada por el desarrollo del humano en un ambiente globalizado en el que se puede acceder a diferentes espacios del mundo, donde el protagonismo lo adquiere la información, porque esta misma genera conocimiento y este último significa poder, siendo ahora los datos automatizados y estando contenidos en los dispositivos electrónicos (Alcántara, 2008; García, 2012; Martínez, 2009; Vázquez, 2012), en esta analogía quien accede a los datos personales contenidos en las TIC, tiene el conocimiento y el poder de los usuarios.

En sentido de estos cambios en el manejo de la información y el control en el uso de las tecnologías, una de las realidades es que no se sabe lidiar con esta evolución tan apresurada, ocasionando dificultades al tratar conductas, la dependencia humana hacia la tecnología se ha desarrollado a tal grado que se ha convertido en la morada de la delincuencia, ha venido sofisticando el crimen. Este movimiento se ha constituido lo que ahora se le define como cibercrimen. A esta modalidad del crimen se le puede considerar una forma novedosa de conducta antisocial que mantiene interrogantes constantes a causa de las deficientes capacidades de respuesta de estudio. Respecto al debate que surge al definir esta conducta, son varias las maneras de referirse al mismo fenómeno de cibercrimen, no obstante, este término implica una descripción genérica y por no gozar de una definición única no es de importancia, siempre y cuando no se aplique desde el área jurídica (Instituto Nacional de Estadística Informática, 2001; Unión Internacional de Telecomunicaciones, 2014).

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

En algunos casos se niega la existencia de dichos términos como el ciberespacio, porque en México legalmente no aplican, quedan sin sentido para las leyes (Flores, 2012; Montoya, 2015). Sin embargo, al entender el cibercrimen no desde la perspectiva jurídica, se indica que a mayor introducción de bienes o intereses (información) al espacio virtual, aunado a una interacción constante en este ambiente virtual y sin una protección capaz de reducir vulnerabilidades, en estas condiciones crece la probabilidad de ser víctima de algún cibercrimen (Miró, 2013).

Considerando esta base teórica que se enfoca a las teorías de la oportunidad criminal, específicamente a la teoría de las actividades rutinarias (Agustina y Reales, 2013; Miró, 2011), las tecnologías pueden usarse como medio para cometer el delito o son objetivo para poder perpetrarlo (Nava, 2007; Téllez, 2008). Bajo la configuración desde una nueva plataforma a la que se le denomina ciberespacio, donde las distancias, los tiempos, víctimas y victimarios presentan características diferentes a las del espacio físico (Miró, 2012), es como se puede llegar a la comprensión de la cibercriminalidad y pensar en una eficaz seguridad informática o seguridad de la información personal y, por ende, de las propias personas.

Para entender esta seguridad informática, su definición hace referencia a:

> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Gómez, 2011, p. 38).

Por su parte, Roa (2013) la divide en seguridad informática lógica que vendría a ser las aplicaciones que contiene un equipo, ejecutables, para proteger la información digital de las amenazas como los virus, troyanos, malware, pérdida de datos y ataques a las aplicaciones de servidores; en lo que la seguridad informática física, siguiendo al mismo autor, concierne todo lo relacionado a los equipos informáticos como son las computadoras, servidores especializados y equipamiento de la red los cuales son amenazados por desastres naturales, robos o fallos de

suministro. Estas descripciones coinciden en que el objetivo en el cibercrimen es la información, aunque las intenciones sean económicas, políticas o sociales, los datos son los que mueven este tipo de conducta, además, el factor que permite su desarrollo es el humano, el más sensible y el cual puede vulnerarse con más facilidad.

Hay quién estudia la cibercriminalidad desde sus aspectos técnicos (Cano, 2009; Lira, 2014), aplicando la criminalística para auxiliar casos de materia forense cuando se encuentran vinculados dispositivos informáticos, lo que se denomina informática forense. Desde otro campo de estudio la ciencia que se encarga de la parte conductual del cibercrimen es la criminología informática o virtual, la cual como rama de la criminología general busca generar conocimientos especializados en esta área específica del crimen, pretendiendo prevenir y combatir estas conductas realizadas por medios electrónicos (Hikal, 2013). En este tópico entra en análisis uno de los retos para hacer frente al cibercrimen, es decir la prevención, vinculada a la labor de la política criminológica, una disciplina que atiende la violencia entre sujetos y la violencia estructural mediante estrategias para frenar el crimen (Martínez, 2007), estas estrategias deben atender las necesidades que el problema vaya generando, aun cuando evolucione a prisa como lo es el cibercrimen, retomando la idea de que el conocimiento es poder y que la prevención es conocer anticipadamente si una conducta antisocial pueda desarrollarse, esas necesidades deben conocerse a partir del estudio de estas conductas realizadas a través de medios informáticos.

Materiales y Método

El estudio que se presenta es de tipo documental, de corte exploratorio-descriptivo y de diseño transversal, el objetivo es integrar un decálogo de líneas estratégicas para el estudio de la cibercriminalidad. Para ello fue utilizada la síntesis de distintas fuentes de información.

Criterios de inclusión y exclusión

En la selección de información fueron incluidos textos en formato físico y electrónico, tanto de bibliotecas como de bases de datos en Internet, pudiendo ser libros, tesis, artículos de investigación y estudios sobre tecnologías. Se incluyeron trabajos a partir del año 2000,

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

documentos de años anteriores fueron excluidos.

Selección de estrategias

Para poder establecer los puntos del decálogo se adoptaron cuatro estrategias con el fin de generar líneas de investigación para guiar los procedimientos, estas fueron: Conocer, que contempla aumentar la generación de conocimiento teniendo de referente el cibercrimen como conducta. Preparar, el enfoque va dirigido al tomar consciencia de los riesgos y peligros, es decir, trabajar con los usuarios. Indagar, tener a consideración el fenómeno desde diferentes perspectivas lo que implica ser la base para generar teoría. Aplicar, desarrollando conocimiento especializado para la resolución práctica del problema.

Instrumentos

La organización de los datos se hizo a través de tablas de contenido con los apartados de fecha y resumen en el cual se describían los hallazgos más relevantes acerca de las formas en que se ha venido estudiando el cibercrimen y los problemas al momento de estudiarlo. En el caso del manejo de estrategias lo que se hizo fue un cuadro sinóptico en el que se organizan las estrategias con las síntesis obtenidas.

Procedimiento

Se hicieron las respectivas búsquedas para acceder a los documentos, una vez que se consiguieron las fuentes de información se procedió a realizar la síntesis de los documentos usando Word en respectivas tablas. Al hacer las relecturas de los resúmenes o síntesis se fijaron estrategias y al mismo tiempo se iban apuntando hallazgos y problemas de estudio del cibercrimen.

Teniendo las cuatro estrategias a seguir y el alcance de cada una de ellas, posteriormente se hizo un listado de los 10 puntos relevantes para el estudio del cibercrimen según los datos encontrados en la teoría. Esta lista de puntos fue de utilidad para describirlos, en algunas ocasiones se hizo uso de esquemas para su mejor comprensión.

Resultados

La mayor parte de los trabajos encontrados fueron libros en formato físico y en menor medida de manera electrónica, fueron obtenidos una cantidad mínima de tesis, artículos de investigación y estudios de tecnologías, con un rango de los años 2001 al 2019. Se logró establecer las cuatro estrategias y diez puntos importantes que conforman el decálogo. Estos últimos se describen a continuación.

1. Redefinir el concepto de cibercrimen

Los paradigmas del estudio científico giran en torno a la relación tecnológica con problemáticas de antaño como la trata de personas, lavado de dinero, tráfico de drogas, delitos económicos entre otras. Para entender lo que es el cibercrimen y su prevención, la cuestión es asimilar que son delitos que tienen auge pragmático y novedoso, sin embargo, hay que atender la maniobra mediante el surgimiento de las TIC.

Así que, si se logra discernir este supuesto se encontrará no sólo ante una fenomenología nueva, sino una delincuencia que no se aparta de los abordajes convencionales de prevención a los ya conocidos en la criminalidad que desde tiempos anteriores corroe el tejido social, se encuentra en colusión con las TIC. La Figura 1 muestra la relación entre los delitos que tienen un tipo penal que, junto a las nuevas tendencias tecnológicas se produce el cibercrimen pasando por un factor humano en los procesos de comunicación (conducta).

Se indica que toda relevancia toma fuerza en cuanto al comportamiento del ser humano, cuando su conducta está focalizada en adiestrarse a los recursos que existen en el medio para complementar o aumentar su capacidad de lesión criminal, en este caso a las personas, de modo que permitan sofisticar las formas de cometer el delito, persiguiendo un beneficio mayor y una menor exposición al alcance del derecho.

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

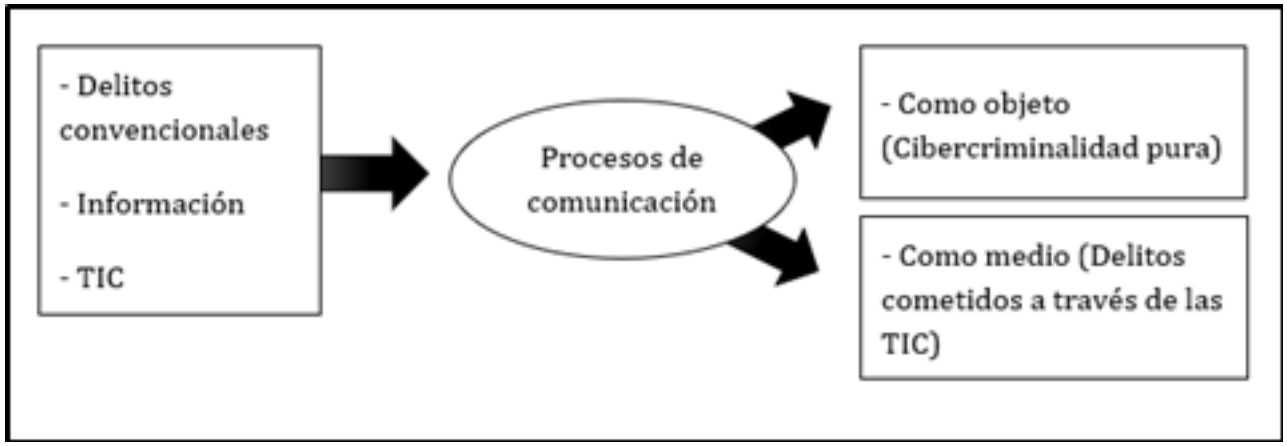

Figura 1. Relación de los delitos convencionales con las Tecnologías de la Información.
Fuente: Modificado de Granados y García (2016). Clasificación realiza por Téllez (2008)

2. Analizar el fenómeno cuantitativamente y cualitativamente.

El conocimiento es poder, la información puede generar ese conocimiento y, por consecuente, el apoderamiento de las situaciones que den acceso al cibercrimen. Resulta una obligación obtener y administrar adecuadamente la materia prima para emitir criterios certeros hacia la formulación de acciones, de tal manera que eso precisamente influirá en los enfoques preventivos. La consideración es que las personas no son números únicamente, no basta con saber cuántos usuarios se conectan a Internet, se requiere establecer qué es lo que realizan cuando navegan entre otras cosas.

Al centrar los estudios cualitativos y cuantitativos surgirán los reflejos de las variaciones conductuales, se puede indicar el estatus de la criminalidad de forma panorámica y las características lesivas. En este punto las tendencias y orientaciones canalizan al saber cómo y porqué se comparta así el cibercrimen.

3. Aumentar las investigaciones sobre el tema.

Una situación notable con relación al cibercrimen es el remanente de un supuesto conocimiento sobre este tipo de delincuencia. Se hace alusión a la impotencia jurídica, a

menudo ignorando que en el tema confluyen aspectos variados que tarde o temprano dejan de ser omitidos por ciencias como la informática, cibernética, electrónica, sociología, psicología, criminalística, antropología y muchas otras áreas más.

En el ámbito criminológico los estudios en coadyuvancia con la estadística y en general de otras ciencias, deben complementar informes que tendrán como fin la anticipación y por secuencialidad, la conversión de las víctimas potenciales en receptores de la política criminológica. Al respecto se hace mención del contexto de estudio de cuatro ciencias:

- Criminología. Estudio de las tendencias del comportamiento antisocial.
- Informática. Descripción instrumental que se utilizó para llevar a cabo la conducta.
- Estadística. Análisis de los datos obtenidos que tengan auge criminógeno.
- Prevención. Enfocar estrategias con base al perfil criminológico, informático y estadístico.

Las premisas preventivas pueden ser alcanzadas por la propia ciudadanía. Los estudios técnicos requieren de personal docto para su desarrollo, la prevención es llevaba a cabo por las propias personas.

4. Practicar la capacitación, especialización y profesionalización (CEP).

Teniendo conocimiento del cibercrimen y lo que se tiene al alcance para hacerle frente, se puede generar la capacidad para una respuesta concisa, a expensas de un proceso de transformación a personas encargadas de la seguridad en las distintas áreas que se relacionen con la informática y prácticamente con las TIC, la preparación vendría a ser por inmersión dirigida a todos, puesto que los efectos de éstas se consideran globales.

La renuencia por asimilar metodologías de políticas de seguridad en las instituciones es frecuente, aunque el Estado no lo haga es deber de los usuarios poner en marcha acciones de seguridad, tres de las acciones para implementar medidas de seguridad son:

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

- Capacitar. Brindando constantemente actualizaciones de seguridad, usando elementos necesarios para el manejo adecuado y uso tecnológico de la información, no sólo proporcionándolo, sino realmente ofrecer y recibir una cultura preventiva.

- Especializar. Generando oportunidades de aprovechamiento académico continuo a quienes dediquen labores de atención a estos ilícitos. También se elevará la promoción de dicha cultura preventiva.

- Profesionalizar. Promoviendo sistemas de educación en el aspecto forense acorde a la investigación, tratamiento penal y tecnológico del cibercrimen.

- En dicho orden de ideas estas medidas contribuyen de manera colateral a la construcción de la política criminológica que se emita. El tan sólo hecho de mostrar dominio de conocimiento a cualquier nivel, se espera ayude a aumentar la conciencia de los usuarios.

5. Distribuir redes de información sobre la problemática.

Al proveer las herramientas necesarias y el contar con personas hábiles en dar solución a las manifestaciones del cibercrimen, por consiguiente, se ocupa tener destinatarios o usuarios aptos para la comprensión del fenómeno, estos receptores ciudadanos, tendrán no sólo la capacidad de enterarse sino de racionalizar el contenido. Por inercia devendrá de una circulación como la presentada en la Figura 2.

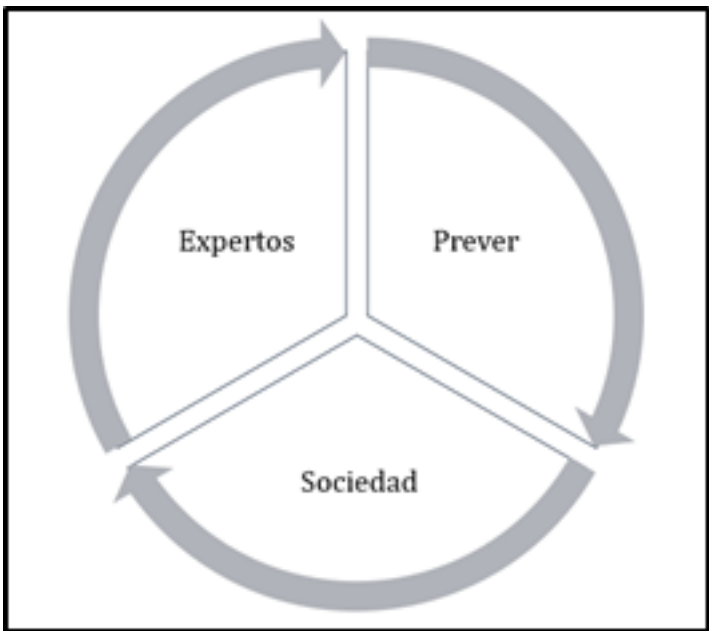

Figura 2. Proceso de producción estratégica de conocimiento.

La difusión puede generarse de distintas maneras, con mayor eficacia que la antes mostrada, pero dentro de los propósitos generales es que la información llegue a la población no solamente emulando condiciones de saber, sino que tenga fundamento técnico, en dicho precepto, qué mejor idealismo que venir de quienes por experticia tendrán las nociones correctas y más actuales.

6. Delimitar espacios de interacción social.

Establecida la distribución social de los datos, se tienen que considerar momentos o lugares (tangible e intangiblemente) de interacción por parte de los usuarios, estos dos espacios totalmente distintos: el espacio físico y el ciberespacio. Comúnmente la clasificación obedece al uso de tecnologías al utilizarse como medio o instrumento o bien, dicho de otra manera, que sean el objetivo o fin. Aunque no es en estricto sentido la idea central de este punto, es importante aclarar la forma inminentemente distinta la interacción presencial a la que se da en el ciberespacio (ver Figura 3).

Se considera que, partiendo en la siguiente nivelación se categorice al triángulo como ciberespacio ante un proceso bidireccional. Por tanto, un usuario más aislado del ciberespacio,

más lejano al cibercrimen se encuentra. No obstante, el tan sólo ingresar lo convierte en objetivo específico para poder ser vulnerado.

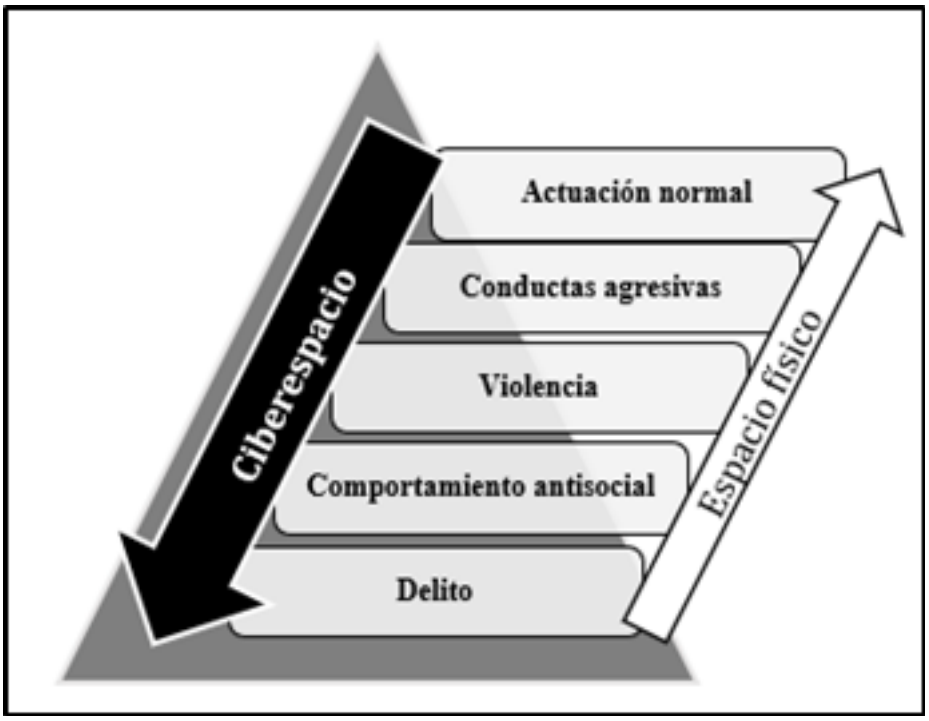

Figura 3. Explicación de interacción en ciberespacio y espacio físico. Fuente: Extraída de Granados & García (2016).

7. Considerar víctimas y victimarios con actitudes distintas.

En los espacios de interacción existe garantía de riesgos y no de seguridad, habrá de estar presente la existencia de individuos en un sistema con nuevos riesgos, peligros y oportunidades para maniobrar y emprender distintas formas de delito. Si las TIC como es el caso de Internet ponen en riesgo la convivencia humana y tienen un impacto directo en la criminodinámica de la delincuencia, esto supone el surgimiento de nuevos objetos del crimen, es decir, tendencias latentes a victimar (Agustina, 2014). Para entonces se habla de una criminología y una victimología.

a. Criminología del cibercrimen. Se adaptan las TIC, los conocimientos técnicos y el

incentivo victimal para ejecutar la conducta. Los objetivos que merodea el cibercriminal dependen de la víctima.

b. Victimología del cibercrimen. Se denota ingenuidad, desconocimiento, mal uso de las TIC y el ciberespacio. El éxito del cibercriminal corresponde a la víctima.

Las características para comprender los comportamientos de ambos sujetos a groso modo tratan de la aparición sustancial de un activo y la completa actuación del pasivo, pues sobre la cibervíctima recae su protección. Retomando ideas anteriores, para entender se ocuparía abundar en el estudio criminológico, victimológico, tecnológico, con acentuación, como se ha venido indicando en la prevención. Si se logra identificar el rol víctima-victimario se puede interpretar el vínculo estratégico con la política criminológica.

8. Orientar acciones a la política criminológica

La opción es retomar una vertiente de la Criminología con toques ciudadanos y desde la perspectiva victimal. Es recurrente inclinar acciones de atención desde el soporte de la política criminal. Aunque pareciera que significan lo mismo no es así, ambas buscan la prevención, sin embargo, los medios de los que se dispone para conseguirla son diferentes y difieren unos de los otros, el procedimiento puede ser muy variado y puede llevar a una enorme diferencia de calidad en los resultados. Las diferencias se orientan a los siguientes planteamientos (Martínez, 2007):

Política Criminológica. Es el concepto evolucionado de la Pólítica Criminal, busca ir a la raíz, el análisis, anticipación al crimen; se práctica entre gobernados; contempla el ejercicio del Derecho Penal como fin último. Formulación de estrategias que abreaccionen a la causalidad, su entendimiento y su conocimiento desde la génesis, el producto pueden ser programas para minimizar los impactos en la sociedad, fovorecendo la relación entre los mismos ciudadanos.

Política Criminal. Busca soluciones para reducir la criminalidad con base y sustento represivo; se da entre Estado-gobernados; se vale del Derecho Penal como mecanismo de control. La creación de leyes sin precedentes, sin tomar a consideración las partes medulares,

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

las tendencias y los factores de la cibercriminalidad. Trata de crear legislación, quedando simplemente a la deriva por no tener cedimentados los objetivos.

Es imperante buscar soluciones desde la Política Criminológica, cuando más tiempo pasa, las TIC funcionan en sentido de codependencia al ser humano, lo que hace evidente una situación jurídica que jamás podrá ir a la par de la tecnología, ante tal posición, qué otra alternativa que comparecer con la prevención.

9. Aplicar teorías de prevención

Como ya se hizo mención la actuación de la víctima culmina el acto y el espacio de interacción social es diferente, en este aspecto, al prever el cibercrimen, debe extinguirse la oportunidad de delito, la opción a seguir es el fortalecimiento de conducta de las personas concebidas como objetivos o probables cibervíctimas.

Para su mejor entendimiento, como se ha venido haciendo antes, la Figura 4 muestra algunas teorías con un amplio potencial de explicar el cibercrimen (Agustina y Reales, 2013; Miró, 2011; Hikal y Estrada, 2012).

Esta postulación se realiza desde la prevención situacional. Se asume que la delincuencia es consecuencia de factores ambientales, habituales y conductuales que generan oportunidades para que ésta ocurra. La última en mención es la de mayor auge para abordar el cibercrimen, pretendiendo minimizar los daños, identificar los riesgos y observar la dinámica ambiental.

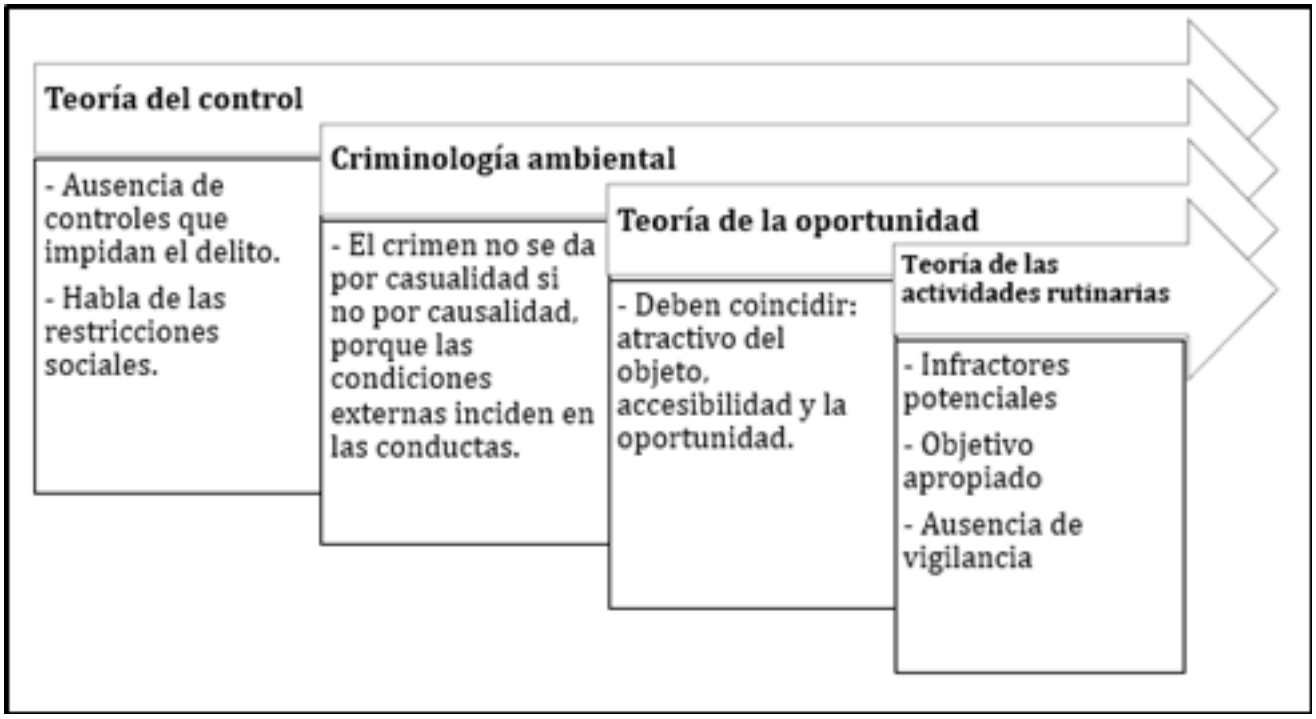

Figura 4. Teorías que están orientadas a la explicación del cibercrimen

Las características esenciales de la prevención situacional consisten en:

- Reducir la oportunidad criminal
- Elevar el nivel de los riesgos de detección del cibercriminal
- La reducción de beneficios del crimen

Este tipo de prevención tiene fallos en el desplazamiento de la criminalidad, es decir, con los ataques que fluyen en el ciberespacio, alguno que se logre evitar, será redireccionado a cualquiera de los tantos millones de usuarios.

10. Evaluar las estrategias de prevención

La evaluación o diagnóstico consiste en verificar el producto de la aplicación metodológica empleada al materializar las estrategias, significa valorar la incidencia de los planteamientos marcados y dar cuenta al pronóstico de las tendencias del cibercrimen. Habrá opciones para

medir los impactos, siendo necesario generar sub-estrategias.

Algunas sub-estratégicas a tener presentes al evaluar la política pueden comprender:

- Ser coherente en el cómo y qué es lo que se requiere evaluar, es un todo que a menudo se confunde, lo que se operacionaliza son las teorías.
- Es preponderante la opinión de las personas, ellas participan activamente en la evaluación.
- Tener presente la inversión y los recursos con los que se cuenta.
- No abandonar la propuesta de más objetivos y su dosificación, así mismo utilizar una comparativa para evidenciar su cumplimento.
- Definir los criterios sobre los cuales se evaluará, dentro de este aspecto se adjuntarán las ciencias que participaron en las gestiones.
- Armar balances sociales que sinteticen la política criminológica con enfoque a la cibercriminalidad y que den paso a la retroalimentación.

La amplitud del cibercrimen es muy variada que únicamente en la Tabla 1 se presentan los posibles alcances y características básicas complementarias de prevención, mostrando los tipos y el plazo que tardan en concretarse.

Tabla 1 Características básicas complementarias de prevención

Tipo	Plazo	Descripción (ejemplificación)
Primario	Largo	El fomento de ética informática e inculcar valorares en el uso de TIC en los niveles educativos y de las personas en general.
Secundario	Corto-mediano	Empresas, instituciones o corporaciones con posibilidad de sufrir un incidente de cibercriminalidad. Lo correcto sería estandarizar y gestionar políticas de seguridad informática.
Terciario	Corto-mediano	Desarrollo de la criminología con las demás ciencias para que una vez que se logren designar tipos penales, se hará el diagnóstico del cibercriminal desde la perspectiva de reinserción.

Conclusiones

El principal objetivo de este trabajo documental fue integrar un decálogo de líneas estratégicas para el estudio de la cibercriminalidad, mismo que por la esencia de su diseño transversal y su naturaleza exploratoria y descriptiva las discusiones no se pueden extender en demasía porque es un terreno poco explorado, siendo esa una de las principales áreas de oportunidad para retomar en futuras investigaciones, ya que la mayor parte de la literatura encontrada le corresponde a los libros y no especialmente a fuentes de información especializada o avanzada.

Si bien es cierto que el poder de los datos genera dominio por motivo del conocimiento (Alcántara, 2008; García, 2012; Martínez, 2009; Vázquez, 2012), precisamente la primera estrategia se enfoca en conocer, es decir ir más allá de lo que pueda decir la teoría, se trata de buscar un trasfondo en el fenómeno del cibercrimen que no se puede lograr únicamente filosofando.

La estrategia de preparar se fundamenta a partir de las pretensiones acerca de la seguridad de la información (Gómez, 2011; Roa, 2013); se requiere no solamente hacer consciente a los usuarios de los peligros a los que se encuentran expuestos, sino que implica trabajar con las personas que son el medio para hacer llegar dichos conocimientos.

Por su parte algunos de los estudios (Agustina y Reales, 2013; Miró, 2011) dejan demostrado más que el descubrir la función de la tecnología sobre las personas o cómo estás se comportan, demuestra cómo es que modelos de estudio ya existentes pueden ser adaptados a estas necesidades, algo que se refiere en la estrategia de indagar.

A propósito de la estrategia basada en aplicar, lo que se hace es seguir de manera firme el supuesto de que se requiere la especialización (Hikal, 2013) para poder llegar a la comprensión de la problemática. De ahí que se haga bastante hincapié en la prevención, que se relaciona enteramente con el intervenir en el cibercrimen.

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142

Como ya se ha establecido con anterioridad (Granados y García, 2016), una de las características principales sobre el cibercrimen es que su evolución es constante por la misma naturaleza que le forja la tecnología; no obstante, tener parámetros definidos que tiendan a identificar sus causas y sus consecuencias apoyan para hacerle frente.

Los temas de cibercriminalidad en la actualidad pueden ser difusos y con tratamiento tenue, la situación con la que se puede encontrar es la obtención de información que no tenga criterios de explicación eficientes. En México significa una proyección muy poco favorecedora para las prácticas preventivas, pues se niega rotundamente el acceso a sistemas verídicos del funcionamiento cibercriminal. Una de las máximas premisas por aplicar será el que lejos de apegarse a los convenios internacionales de cibercriminalidad, la postura que debe adquirir consistirá en el afrontamiento del cibercrimen con visión propia, las herramientas, metodologías, estrategias, políticas, y demás elementos, dependen del cómo se va estableciendo el delito, de ahí el hincapié en el conocimiento del fenómeno.

La idea es generar un sentido crítico para no decaer en buscar técnicas magníficas de manera desesperada o pretender desarrollar nuevos métodos que sean la panacea, el reto es adecuar los medios con los que se cuenta a las necesidades del cibercrimen en distintos ámbitos; ya que lo necesario es entender la adhesión de las TIC en las conductas para cometer delitos y no seguir inertes tomando como justificación que hacen falta leyes. Si se logra cambiar esta mentalidad, se podrá acceder al fructífero campo de la prevención.

Referencias Bibliográficas

Agustina, J. R. (2014). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. Cuadernos de Política Criminal, (114), 143-178.

Agustina, J. R., y Reales, F. (2013). En la mente de un asaltante de viviendas: Estudio cualitativo de una muestra de autores de robo en casa habitada. Revista Española de Investigación Criminológica, (11), 1-30.

Alcántara, J. (2008). La sociedad del control, privacidad, propiedad intelectual y el futuro de la libertad. España: El Cobre Ediciones.

Asociación de Internet Mx. (2019). 15° Estudio sobre los hábitos de los usuarios de Internet en México 2018. Recuperado de https://www.asociaciondeinternet.mx/es/estudios

Azaola, L. (2010). Delitos informáticos y derecho penal. México: Ubijus Editorial.

Cano, J. (2009). Computación forense: Descubriendo los rastros informáticos. México: Alfaomega Grupo Editor.

Flores I. (2012). Criminalidad informática, aspectos sustantivos y procesales. México: Tirant lo Blanch.

García J. (2012). Crecimiento urbano, tecnologías de la información y comunicación (TIC) y criminalidad. México: Universidad Autónoma de Baja California y Jorale Editores.

Granados, R., y García, S. (2016). El delito cibernético y su evolución criminológica y tecnológica en el Estado de Guanajuato. Tesis en opción al grado de licenciado en Criminología (Universidad Humani Mundial, Guanajuato).

Gómez, Á. (2011). Enciclopedia de la seguridad informática (2ª ed.). México: Alfa omega Grupo Editor.

Hikal, W. (2013). La especialización de la criminología: de lo general a lo específico, ¿hacia una

neocriminología? Teoría de las criminologías específicas. Derecho y Cambio Social, 1-23.

Hikal, W. S., y Estrada, I. (2012). Criminología ambiental: los delitos ambientales. Los derechos de la naturaleza. (pp. 177-191). México: Editora Laguna.

Instituto Nacional de Estadística Informática. (2001). Delitos informáticos. Lima.

Lira, Ó. (2014). Cibercriminalidad: Fundamentos de la investigación en México. México: Instituto Nacional de Ciencias Penales.

Martínez, A. (2009). La libertad de expresión en la nueva sociedad de la información, perspectivas y conflictos entre derechos. Ecuador.

Martínez, E. (2007). Política criminológica. México: Porrúa.

Miró, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología, (13), 1-55.

Miró, F. (2012). El cibercrimen: Fenomenología y Criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.

Miró, F. (2013). La victimización por cibercriminalidad social: Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. Revista Española de Investigación Criminológica, (11), 1-35.

Montoya, J. (2015). Delitos federales cometidos a través de medios informáticos. México: Editorial Flores.

Nava, A. (2007). Delitos informáticos (2ª ed.). México: Porrúa.

Roa, J. (2013). Seguridad informática. España: Mc Graw-Hill.

Téllez, J. (2008). Derecho informático (4ª ed.). México: McGraw-Hill.

Unión Internacional de Telecomunicaciones. (2014). Ciberseguridad, comprensión del ciberdelito: Fenómenos, dificultades y respuesta jurídica. Recuperado de http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Vázquez, C. (2012). Combate a la delincuencia cibernética. México: Editorial Universidad de Xalapa.

Volumen 05 - N° 03, Julio - Diciembre 2020
Depósito Legal N° DC2017000305/ISSN: 2542-3142