VERSIÓN DIGITAL

SEGURIDAD
SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

GN
GUARDIA NACIONAL

GUARDIA NACIONAL Y POLICÍA CIENTÍFICA
ESTUDIOS SOBRE CIBERSEGURIDAD, CRIMINALÍSTICA, INNOVACIÓN Y POLÍTICA CRIMINAL

Prólogo
Comisario General, Luis Rodríguez Bucio
Comandante de la Guardia Nacional

Alejandro Carlos Espinosa
Coordinador

VERSIÓN DIGITAL

GUARDIA NACIONAL Y POLICÍA CIENTÍFICA

ESTUDIOS SOBRE CIBERSEGURIDAD, CRIMINALÍSTICA, INNOVACIóN Y POLÍTICA CRIMINAL

Alejandro Carlos Espinosa
Coordinador

La presente obra ha sido aprobada para su publicación.
Coordinador de la obra: Alejandro Carlos Espinosa
Cuidado de la edición: Alma Brisa Gómez Guerrero
Formación Tipográfica: Cristihan Arturo Salazar Gales
Portada: Vocería de la Guardia Nacional.
Guardia Nacional y Policía Científica. Estudios sobre ciberseguridad, criminalística, innovación y política criminal.

Primera Edición: Junio de 2022.
D. R. Guardia Nacional
Boulevard Adolfo Ruiz Cortines # 3648, Col. Jardines del Pedregal, 01900, Alcaldía Álvaro Obregón, Ciudad de México.

Guardia Nacional
Certificado del Registro Público de Derechos de Autor con número: 03-2022-022513464200-1
ISBN: 978-607-99677-2-7
Sello editorial: (978-607-99677)

Impreso y hecho en México.

Lic. Rosa Icela Rodríguez Velázquez
Titular de la Secretaría de Seguridad y Protección Ciudadana

Comisario General GN
Luis Rodríguez Bucio
Comandante de la Guardia Nacional

Comisario General GN
Inocente Prado López
Jefe General de Coordinación Policial

Lic. Evangelina Hernández Duarte
Coordinadora de Administración y Finanzas

Comisario Jefe GN
Arturo Medina Mayoral
Titular de la Unidad de órganos Especializados por Competencia

Comisario Jefe GN
Miguel Ángel Huerta Ceballos
Titular de la Unidad para la Protección de los Derechos Humanos, Disciplina y Desarrollo Profesional

Comisario Jefe GN
David Enrique Velarde Sigüenza
Titular de la Unidad de Asuntos Internos

Comisario GN
Manuel Javier Francisco
Titular de la Unidad de Asuntos Jurídicos y Transparencia

Lic. Norma Leticia Castillo Lara
Titular del órgano Interno de Control

Inspector General GN
Jorge Jesús Borrego Álvarez
Director General Científica

Dr. Luis Antonio Balcazar Bustos
Director General de Desarrollo Profesional

Dr. Alejandro Carlos Espinosa
Director de Investigación Académica

Índice

Prólogo ---------- 9
Comandante de la Guardia Nacional
Comisario General GN, Dr. Luis Rodríguez Bucio

Introducción ---------- 12
Titular de la Unidad de órganos Especializad os por Competencia de la Guardia Nacional
Comisario Jefe GN, Mtro. Arturo Medina Mayoral

Capítulo I. Estudios de Criminalística

Identificación humana en México ---------- 14
Suboficial GN, Deyanira Bucio Vázquez
Suboficial GN, Rubí Yesenia Espinosa Villa
Lic. Alejandro Samuel Lovera
Inspector GN, Roberto Caballero Velasco Lic.
Elena Sofía Abarca Ávila
Suboficial GN, Hess Roberto Gutiérrez Aguiar

CENADEM: En combate de los delitos que atentan contra la integridad de niños, niñas y adolescentes en el ciberespacio ---------- 33
Inspectora GN, Mtra. Olivia Mendoza Cruz
Primer Subinspector GN, Lic. Elohim Hernández Morales

La Policía Científica de México como agente investigador de la tortura ---------- 41
Inspectora GN, Adriana López Torres Oficial GN,
Beatriz Cuautle Hornilla
Suboficial GN, Jesús Florentino García

La importancia y obtención de la evidencia ---------- 57
Primer Subinspector GN, Lic. Víctor Agustín Jiménez Juárez

Capítulo II. Estudios de Ciberseguridad

La Ciberseguridad: Estrategia para el crecimiento de México ---------- 79
Mtro. Radamés Hernández Alemán

El impacto de la tecnología en las operaciones policiales ---------- 93
Mtro. Luis Fabián Olivo Ramírez

Criptomonedas y Blockchain ----------103
Dr. Lancelot García Leyva

Capítulo III. Estudios de Innovación

Innovando soluciones para la Seguridad Pública ---------- 124
Mtro. Oscar Manuel Rojas Padilla
Mtro. Norberto Ciprés Lugo

El perfil científico policial ---------- 136
Comisario GN, Mtro. Severino Cartagena Hernández
Subinspectora GN. Dra. Rosa María Richards Uribe
Subinspector GN, Dr. Héctor Barrón González
Suboficial GN, Lic. Yolanda Ramírez Morales

Vigilancia y prospectiva tecnológica ---------- 155
Dr. Juan Carlos Rivera Dueñas
Mtra. Beatriz Olivia Sánchez Flamenco

Visión prospectiva de la investigación científica en la Guardia Nacional ---------- 167
Mtro. Oliver González Barrales

Capítulo IV. Política Criminal y Ciberseguridad

Política criminal en la ciberseguridad: retos y perspectivas ---------- 187
Dr. Alejandro Carlos Espinosa

Tendencias, retos y desafíos de la ciberseguridad y los ciberdelitos en la cuarta revolución industrial ---------- 200
Mtro. Jacobo Bello Joya

Entrevistas

Grupos de trabajo de la INTERPOL para la unidad de cibercrimen de las Américas ----------218
Mariano Manfredi. Interpol

Dinámica y transversalidad del ciberdelito ---------- 232
Adrián Eduardo Acosta. Interpol

Prólogo

El mundo actual se transforma a una velocidad sin precedentes. Junto con los grandes cambios en beneficio de la sociedad, aparecen nuevos retos en materia de seguridad pública.

La conexión tecnológica cotidiana, que la mayoría de la población tiene a través de redes sociales, permite que la información se conozca en tan solo segundos después de haber ocurrido, sin importar distancias ni condiciones; lo cual también incluye a los posibles hechos delictivos. De esta manera, la sociedad de la información representa, a la vez, un reto y una oportunidad, en muchos campos, en los que se incluye a la seguridad.

La delincuencia avanza con formas de operación cada vez más sofisticadas, haciendo uso de la transformación y vanguardia tecnológica. En este sentido, las investigaciones en seguridad deben considerar el perfeccionamiento de sus estrategias, con la finalidad de combatir con contrainteligencia y prevención.

Para el caso mexicano, la responsabilidad de coadyuvancia en la investigación, persecución, prevención y disuasión de los delitos federales incumbe a la Guardia Nacional, de ahí la diversificación, especialización y desarrollo de la investigación científico-social en el tema.

"Guardia Nacional y Policía Científica. Estudios sobre Ciberseguridad, Criminalística, Innovación y Política Criminal" retoma algunas de las innovaciones en materia de investigación criminal, que son resultado del trabajo de la Dirección General Científica, como parte de la Unidad de órganos Especializados por Competencia de la Guardia Nacional.

Respecto al contenido de la obra, el capítulo primero trata sobre los estudios de criminalística, donde se abordan aspectos sensibles y complejos de la investigación criminal, por ejemplo, un análisis y propuesta sobre la identificación humana que, dicho sea de paso, resulta un aspecto prioritario de las políticas públicas en materia de seguridad.

Asimismo, se detallan los avances científicos y técnicos que involucran aspectos previos al análisis de pruebas, como es el caso de la búsqueda de personas.

En este mismo apartado se desarrollan los siguientes tres temas:

- El combate de los delitos que atentan contra la integridad de las niñas, niños, y adolescentes en el ciberespacio; problemática que aumenta gradualmente y pone en riesgo a esa población vulnerable.

- La tortura, uno de los grandes flagelos que azota aún a las sociedades en América Latina, donde la Policía Científica de México es un agente investigador y ha realizado importantes aportes para la identificación de casos.
- Por último, se estudia la importancia y obtención de la evidencia, recordando que los casos se acreditan con pruebas.

En el capítulo segundo, relativo a estudios de ciberseguridad, se desarrolla la idea del ex Secretario General de las Naciones Unidas, Kofi Annan: "no hay seguridad sin desarrollo y no hay desarrollo sin seguridad".

También se aborda el impacto de la tecnología en las operaciones policiales, tema donde se amalgaman dos aspectos de gran trascendencia para la función policial: el quehacer operacional y las tecnologías de la información y la comunicación, ambos necesarios en la investigación y persecución de los delitos.

Se cierra este capítulo con un análisis vinculado con las nuevas relaciones comerciales y de negocios lícitos e ilícitos, a través de criptomonedas y blockchain.

Lo que respecta al tercer capítulo, relativo a estudios de innovación, se presenta el artículo "Innovando soluciones para la seguridad", en donde se detalla que los productos tecnológicos desarrollados en la Dirección General Científica, se hacen pensando en la seguridad del pueblo y con el compromiso de brindar a México justicia y paz.

Por otra parte, se presenta un tema de vanguardia: el perfil científico policial, donde se expone que el policía es un profesional de la seguridad pública que utiliza el método científico; de ahí que el modelo de la policía científica haya evolucionado a lo largo del tiempo con el conocimiento, la práctica policial, y la profesionalización, consolidando recursos humanos, la vinculación con la comunidad científica y la certificación de competencias laborales.

De igual manera, en este apartado se desarrolla el tema de vigilancia y prospectiva tecnológica, donde es necesario destacar el desarrollo tecnológico como un fenómeno social que se manifiesta, no solo con el surgimiento de productos innovadores orientados a la solución de problemas y necesidades, sino que también propicia la creación de nuevos procesos, paradigmas vanguardistas y campos de estudio emergentes a través del monitoreo, análisis interno de requerimientos tecnológicos en el mercado, academias y unidades administrativas tecnológicas; lo que permite lograr el fortalecimiento de infraestructura científico tecnológica y posicionar a la Guardia Nacional en el liderazgo científico e innovador.

Lo anterior da cuenta de cómo en la Guardia Nacional se afinan los procesos tecnológicos especializados, operativos de servicio y mantenimiento de la infraestructura tecnológica y comunicación que permiten una planeación metódica y prospectiva en función de las nuevas tecnologías.

La obra desarrolla estudios sobre política criminal y ciberseguridad en México, por ser una exigencia que invita al desarrollo de capacidades institucionales, del fortalecimiento y en algunos casos creación de ciberinvestigaciones profesionales.

El que en el libro se traten las tendencias, retos y desafíos de la ciberseguridad y los ciberdelitos en esta llamada cuarta revolución industrial, es primordial para entender las nuevas figuras delictivas y el modus operandi de los criminales, elementos fundamentales para poder atender los antagonismos actuales de la seguridad pública.

El libro cierra resaltando uno de los principios en los que se basa la Guardia Nacional: la seguridad se combate con inteligencia, no con violencia. La capacitación de cada uno de los integrantes es uno de los pilares por los que atraviesa el cambio de paradigma en el combate a la delincuencia.

Este compendio contribuye con ese desarrollo académico, al integrar un apartado impulsado por el área de Investigación Académica de la Dirección General de Desarrollo Profesional, respecto a la formación y capacitación policial en el cibercrimen.

Por lo anteriormente expuesto, tengo la entera confianza de que esta investigación será el inicio de posteriores trabajos sobre la seguridad pública en el ámbito de la ciberseguridad.

Comisario General GN, Dr. Luis Rodríguez Bucio
Comandante de la Guardia Nacional.

Introducción

Comisario Jefe GN, Mtro. Arturo Medina Mayoral.[1]

En su obra "La aventura de la diadema de berilo", Sir Arthur Conan Doyle le hace decir a Sherlock Holmes: "Una vez descartado lo imposible, lo que queda, por improbable que parezca, debe ser la verdad". Siglo y medio después de que surgiera el detective más famoso de la literatura universal, la investigación criminal ha avanzado a pasos agigantados al grado de poder distinguir con certeza: lo imposible, lo improbable y la verdad.

Desde los primeros logros que realizó a finales del siglo XIX, el policía parisino Alfonso Bertillon en la individualización antropológica que inició el famoso método de las fotografías de identificación de los procesados que perdura hasta nuestra días y los notables avances del británico Francis Galton y el policía argentino Juan Vucetich, en la identificación del patrón común en las huellas dactilares y la elaboración de su sistema de clasificación (que también ha llegado hasta nuestros días) hasta el logro trascendental en el ámbito forense que representó el descubrimiento de las huellas genéticas que hizo en 1985 el francés Alec Jeffreys, quién pudo identificar la huella digital del ADN, única e irrepetible en cada ser humano, lo que produjo que un pequeño y casi invisible elemento piloso o una insignificante gota de sangre en una escena del crimen, fuera suficiente para la condena de una persona sustentada en una prueba científica.

En los últimos años, la investigación científica del delito ha mostrado espectaculares avances tales como la identificación humana por tecnologías biométricas; los análisis por activación neutrónica en el campo de las pinturas, para revelar falsificaciones, o para identificar rastros de elementos metálicos por disparo de arma de fuego; la técnica de emisiones electromagnéticas para determinar la cantidad de arsénico contenida en el cabello como prueba de envenenamiento; los radares para la exploración geológica, en la búsqueda de cuerpos humanos enterrados en fosas clandestinas; entre otros muchos ejemplos del desarrollo que han logrado el uso de la técnica y la ciencia en la investigación de hechos criminales.

La existencia del trabajo que realiza la Dirección General Científica de la Guardia Nacional y las investigaciones contenidas en el libro "Guardia Nacional y Policía Científica. Estudios sobre ciberseguridad, criminalística, innovación y política criminal", son una muestra de cómo el inmortal personaje de Sherlock Holmes traspasa las páginas de los libros para encarnarse en cada uno de los guardias nacionales que realizan la investigación científica del delito, con la misma acuciosidad, aguda observación y esmero en el análisis del detalle al igual que el famoso detective inglés. Confirmando con ello la veracidad de la definición de la criminalística como la ciencia del pequeño detalle.

1 Titular de la Unidad de órganos Especializados por Competencias de la Guardia Nacional.

Cada uno de los artículos de investigación de la obra que el lector tiene en sus manos, demuestran que la Guardia Nacional, como la institución cuya misión constitucional se centra en salvaguardar la vida, libertades, integridad y el patrimonio de las personas; así como contribuir a la generación y preservación del orden público y la paz social hace como una institución con una gran fortaleza: la convicción de la participación determinante de la ciencia y la tecnología en la prevención, investigación y persecución de los delitos, para el cumplimiento de los altos fines que la Constitución Política de los Estados Unidos Mexicanos le mandata.

La Guardia Nacional cumple con su misión constitucional, apoyada en el compromiso de hombres y mujeres que todos los días contribuyen con sus saberes especializados y su esfuerzo con estricto apego a las atribuciones que tiene asignadas la Dirección General Científica, en la Ley de la Guardia Nacional y su Reglamento: utilizar los conocimientos, herramientas científicas y técnicas en la prevención, investigación y persecución de los delitos.

La importante función que realiza la Dirección General Científica es multidisciplinaria y se expresa en la formación profesional de alta especialización de los autores de la presente obra, en la que se advierte la participación de especialistas provenientes de diversos campos del conocimiento que comprenden desde la antropología, ciencias forenses, tecnologías de la información y comunicación, ciberseguridad, política criminal hasta los derechos humanos.

Una de las grandes aportaciones de la obra es la presencia de un diálogo multidisciplinario que lleva al análisis de la investigación científica del delito desde diferentes ópticas, técnicas, metodologías y procesos científicos.

Anthony Burgess decía: *Si la ley requiere del testimonio del perito, como mujeres y hombres de ciencia, su tarea no es reivindicar a la víctima, salvar a un inocente o destruir a un culpable. Al perito solamente le corresponde dar su testimonio hasta el límite de su saber y de su patrimonio científico y no ser juez ni justiciero.*

Para la Unidad de órganos Especializados por Competencia ha sido una experiencia extraordinaria integrar la labor especializada de la Guardia Nacional tanto de las operaciones tácticas como de las científicas para dar cumplimiento a los objetivos y metas institucionales en estricto apego a los derechos humanos. Esta obra describe también la labor de la Dirección General Científica, que queda expresada como testimonio de éxito en cada uno de los capítulos de ésta.

Que la Guardia Nacional impulse la investigación científica representa un claro ejemplo de la trascendencia de su aplicación en el ámbito de investigación policial, erigiéndose como un referente en la materia en la región y una institución abierta al conocimiento, al intercambio de experiencias y mejores prácticas a nivel internacional.

CAPÍTULO I
ESTUDIOS DE CRIMINALISTICA

IDENTIFICACIÓN HUMANA EN MÉXICO

Identificar a una persona significa sosegar el alma de un padre o de una madre que busca incansablemente y con gran tristeza en el rostro a su familiar... Es, quizá, acallar el alma de aquél que ya no está. Es cerrar el círculo, es poder decir: por fin te encontré. (ESAA)

Lic. Elena Sofía Abarca Ávila[1] **y otros**[2]

Sumario: I. Introducción. II. Criminalística de campo. III. Arqueología Forense. IV. Antropología Forense. V. Odontología Forense. VI. Genética Forense.

I. Introducción

Sobre identificación humana existen definiciones científicas y académicas, pero en todos los casos subyace un nombre, una personalidad, una historia. Cada uno de los más de 70 mil desaparecidos en México al 2020 (Secretaría de Gobernación, 2020) tienen nombre y una familia que los busca incesantemente. Definir identificación humana es un "por fin te encontré, por fin descansaré y hoy sé dónde estás".

---

[1] Antropóloga Física, egresada de la Escuela Nacional de Antropología e Historia. Participó en la búsqueda de fosas clandestinas, apoyó en la recuperación de restos óseos de origen humano, así como, en el área de laboratorio para determinar el perfil biológico de restos humanos.

[2] **Suboficial GN, Deyanira Bucio Vázquez**. Antropóloga Física, egresada de la Escuela Nacional de Antropología e Historia. Participó en la búsqueda de fosas clandestinas, apoyó en la recuperación de restos óseos de origen humano, y en el laboratorio para determinar perfil biológico de restos humanos.

Suboficial GN, Rubí Yesenia Espinosa Villa: Lic. en Arqueología por la Universidad Veracruzana, asesor de métodos y técnicas de reconocimiento de superficies en investigación y conservación en el proyecto Yohualichan, en el municipio de Cuetzalan del Progreso, Puebla. Arqueóloga encargada de supervisar obras públicas en San Martín Teotihuacán.

Lic. Samuel Alejandro Pérez Lovera: Odontólogo forense graduado del Instituto politécnico Nacional. Ha colabora en comisiones multidisiplinarias para la búsqueda e identificación de restos óseos de origen humano. Participó en "Protocolo Nacional de Odontología Forense para Personas Fallecidas No Identificadas".

Inspector GN, Roberto Caballero Velasco: Lic. en Turismo egresado del Instituto Politécnico Nacional, pionero en la creación de la Policía Cibernética participando en operativos contra la pornografía infantil y pedofilia. Se especializó en el procesamiento del lugar de intervención y participó en búsqueda de fosas clandestinas.

Suboficial GN, Hess Roberto Gutiérrez Aguilar: Maestro en Criminalística y en Sistema Adversarial e Inteligencia y Contrainteligencia contra el Terrorismo Global. Dedicado a llevar a cabo investigación forense y policial.

Para lograr la identificación de esas personas, especialistas, científicos y técnicos de la Dirección General Científica de la Guardia Nacional y otras autoridades trabajan arduamente removiendo tierra, basura, cenizas, analizando huesos, dientes, restos humanos quemados o en estado de descomposición, con el único objetivo de dar respuestas a esas personas sobre el paradero de sus seres queridos.

En el ámbito científico ¿Qué es identificación humana? Es la acción de reconocer a una persona como la misma, a través de sus características particulares y, fuera de toda duda establecer su identidad.

Identificar es reconocer si es la misma persona que se supone o se busca. Es el empleo de un sistema o conjunto de conocimientos científicos, procedimientos técnicos y operaciones prácticas en áreas especializadas para constatar su existencia, conocerla, reconocerla con seguridad y vincularla de modo inequívoco a sus actos, conducta y comportamiento.

El proceso de Identificación Humana es una etapa crucial. Es un trabajo que demanda la correcta acción de las instituciones involucradas (Guardia Nacional, Comisión Nacional de Búsqueda, Fiscalía General de la República, Servicios Periciales de cada entidad federativa del país, Derechos Humanos y Cruz Roja Mexicana) para llevar a cabo de forma correcta y sistemática la búsqueda, ubicación, recuperación y análisis forenses de las personas fallecidas no identificadas, a fin de obtener y ofrecer información que dé certeza y seguridad a aquéllos que buscan con tenacidad a un hijo, una hija, un padre, un esposo, un hermano...

Con esa claridad, es necesaria la aplicación seria y profesional de un conjunto de conocimientos científicos y procedimientos técnicos para llevar a cabo la identificación humana, con respeto irrestricto a sus derechos humanos.

La Guardia Nacional, a través de su Dirección General Científica, cuenta con áreas y laboratorios especializados, así como expertos forenses para emprender la búsqueda, localización, levantamiento, individualización de restos humanos, de arcadas dentales y muestras genéticas de los mismos para llegar a esa identificación humana.

El trabajo es multidisciplinario y se cuenta con la colaboración conjunta de áreas especializadas en Criminalística de Campo, Arqueología, Antropología, Odontología y Genética Forenses. Cada especialidad tiene una tarea fundamental. Esa labor de conjunto participa en el armado de un gran rompecabezas que culmina con la identificación de una persona.

II. Criminalística de campo

La Criminalística de Campo forma parte de un esfuerzo conjunto con esas áreas, su intervención será siempre el inicio de cada investigación, que conducirá a la localización e identificación de personas.

De acuerdo con el Sistema Penal Acusatorio, los elementos de la Guardia Nacional están capacitados en la función de primer respondiente, es decir, son aquella autoridad de seguridad pública que puede llegar primero al lugar donde presuntamente se ha cometido un delito. En caso de necesidad o urgencia, tienen la facultad, los conocimientos y las habilidades para procesar los indicios, identificarlos, señalarlos, fijarlos, embalarlos, describirlos y registrarlos en una cadena de custodia para conservar su integridad hasta llegar al juicio oral.

La criminalística de campo cobra relevancia, pues cada día se le concede mayor valor a las evidencias físicas en los procesos judiciales, lo que, sumado al avance en el análisis de pruebas de los laboratorios de criminalística, aumenta la responsabilidad de los investigadores de campo, en atención a que en el lugar de intervención deberá hacerse una minuciosa investigación, recolección y transporte de los indicios.

De este modo la importancia de la criminalística como función inherente de la Guardia Nacional radica en la especialización y en la aplicación de conocimientos amplios y específicos dentro de las ciencias forenses, donde la planeación, organización y coordinación de las tareas en un lugar de intervención corresponde a todos los que conforman el ámbito de la seguridad.

El valor de la prueba durante las investigaciones contribuye a establecer los lineamientos rectores a nivel judicial sobre los medios probatorios que se necesitan para formalizar una teoría del caso convincente, sustentable y eficaz. Sobre esa base, la Dirección General Científica de la Guardia Nacional puede ejecutar intervenciones técnicas y científicas de índole forense en el territorio nacional. Durante un evento presuntamente delictivo fija la relación entre el delito y las pruebas, establece el carácter científico y vincula la criminalística con otras ciencias y disciplinas, hasta conformar un todo de conocimiento concurrente en el esclarecimiento de un delito y la identificación de una víctima.

El integrante de la Guardia Nacional dentro de sus políticas de investigación considerará todo aquello que proporcione elementos materiales probatorios que hagan posible reconocer los indicios de importancia para la resolución del caso, lo cual le permitirá iniciar la búsqueda encaminada al

descubrimiento de indicios, rastros o vestigios. En este contexto aplicará el razonamiento deductivo que se deriva de la criminalística, sin olvidar que el primer contacto con el evento es cardinal para las fases de control de detención y vinculación a proceso.

En la práctica cuando se presenta un hecho, el guardia nacional dará protección al lugar, identificará oportunamente el perímetro donde se localiza la mayor parte de los indicios, implementará técnicas de fijación inmediatas para la conservación de los mismos, en la inteligencia de brindar la máxima priorización y protección de esos elementos probatorios, llevará a cabo acciones de identificación de accesos y vinculación de espacios relacionados con el lugar de investigación, asegurará y trasladará esos indicios con todas las consideraciones de seguridad.

Desde el año 2016, el criminalista de campo está facultado para las intervenciones en la búsqueda y localización de personas desaparecidas, mediante técnicas de prospección en el lugar de la investigación, a fin de recuperar restos óseos encontrados en fosas clandestinas a lo largo de todo el país, que lleven a una individualización, es decir, a la identificación humana.

La actuación especializada de la Guardia Nacional ha logrado el acercamiento social con familiares y colectivos que buscan a víctimas desaparecidas. En este sentido, su impacto social, ha sido significativo, lo anterior marca la percepción social de la función constitucionalmente encomendada.

Las acciones que emprende el primer respondiente que tiene noticia y contacto con algún hecho presumiblemente constitutivo de un delito, son básicas en el procedimiento penal, de esta manera su adecuada aplicación contribuirá a una mejor administración de la justicia en el marco del Sistema Penal Acusatorio, en el que se respeten las leyes, se combata la impunidad y se acabe con la absolución de delincuentes debido a la presentación inapropiada de los casos ante tribunales, la cual puede ser por error en la investigación o por falta de pruebas.

III. Arqueología forense

Desde el ámbito de la Arqueología Forense, la identificación humana comienza en campo con el proceso de exhumación y recuperación de restos humanos, es *in situ* donde el trabajo se nutre con la multidisciplina.

El proceso de búsqueda desde la Arqueología Forense requiere de dirigir una documentación puntual y la recuperación precisa de los datos durante el proceso de excavación, la cual debe ser minuciosa, a efecto de que permita interpretar el contexto.

Los métodos y técnicas que auxilian a ese proceso es el uso de la retícula, la cual se emplea para referenciar algún objeto o elemento a través de ejes cartesianos, los cuales pueden ser restos humanos, fragmentos y segmentos óseos que son registrados.

Ser meticuloso durante la exhumación es muy importante, ahí se procede al exhaustivo análisis del contexto, en el cual se observan características, patrones, indicios asociados, relación entre los restos humanos, características de los cadáveres tales como tatuajes, signos de violencia, al igual que prótesis dentales o corporales, prendas y artículos personales, datos que pueden ser confrontados con aquéllos *ante mortem* obtenidos de los cuestionarios respondidos por los familiares de las personas desaparecidas o extraviadas. De igual manera, la criba es esencial porque de ella se obtienen elementos óseos no visibles, los cuales son recuperados para un futuro análisis por especialistas.

Un adecuado trabajo arqueológico en la excavación resulta determinante para enriquecer y aportar datos para un siguiente proceso como el análisis osteológico. El informe o dictamen que ofrezca contribuirá a la interpretación de los contextos forenses a partir de la implementación de técnicas y métodos en apoyo de las autoridades especializadas en la impartición de justicia.

En campo se aplican dos métodos principales: la prospección y la excavación, la primera es el recorrido de superficie, es el trabajo previo a la excavación y se auxilia de la cartografía.

Con el apoyo de un instrumento de geolocalización (GPS), cartas topográficas, fotografías aéreas y brújulas se geoposicionan los cuerpos o sus vestigios. Se colocan en transeptos aleatorios o puntos que determine el arqueólogo; se observa el suelo para ubicar fosas clandestinas, indicios, restos humanos y anomalías en superficie como manchas en la tierra, depresiones,

elevaciones, entre otras variables, mismas que son marcadas con banderines y estacas para posteriormente delimitar el terreno a excavar o discriminar en esa área.

Luego de observar e identificar la dispersión del material en superficie, éste será recogido por las unidades de recolección (UR) y se determinará en dónde perforar para futuras excavaciones.

En tiempos recientes, este trabajo se complementa con los levantamientos planimétricos con el auxilio de drones, lo que ofrece obertura y precisión en el resultado.

La excavación es la etapa metódica del trabajo, por lo que debe ser escrupulosa para asegurar su contribución a una buena investigación pericial. Así, el arqueólogo determinará en dónde ubicar la unidad de excavación, pozo de sondeo, cala, pozo por barreno, trinchera o retícula, además observará las circunstancias y el hallazgo como anomalías, restos óseos e indicios, para interpretar el contexto.

El material óseo de origen humano y los indicios hallados en contexto, serán controlados y recuperados mediante capas estratigráficas de origen antrópico. Es decir, a través de la observación del suelo, subsuelo y estratos geológicos se determinará si existe o no alguna alteración o que haya sido modificada por la actividad humana contemporánea para ser recolectada.

Igualmente cuando estos sean visibles *in situ* serán recolectados y fotografiados, se les asignará una nomenclatura de identificación, y en caso de observar anomalías, se dibujará y registrará para un mejor análisis del contexto y se llenará el Registro de Cadena de Custodia (RCC). Dicho proceso continúa con la entrega-recepción de los indicios y/o los RCC, y concluye al emitir un informe pericial o dictamen.

IV. Antropología forense

La Antropología Forense es la rama de la Antropología Física que se encarga de la identificación de restos humanos, más o menos esqueletizados para determinar edad, sexo, estatura, filiación racial, además de rasgos particulares al momento de la muerte.

Esta disciplina nace de la necesidad de identificar restos humanos involucrados en muertes violentas que han perdido los rasgos necesarios para su reconocimiento y se apoya en la arqueología, somatología, odontología, medicina, genética forense y criminalística.

El antropólogo forense en su formación debe tener conocimientos en materia de derechos humanos y procesos legales, así como del *modus operandi* de las organizaciones criminales y en su sistema de desaparición.

Procesos en Antropología Forense

Las actividades del antropólogo forense, se dividen en dos escenarios: campo y laboratorio.

A) Trabajo de campo

El trabajo en campo incluye la prospección, que es la búsqueda de irregularidades en el suelo y flora que nos indiquen la existencia de fosas clandestinas. Cuando se inhuma un cadáver en la tierra, se perturba el suelo y se remueve la flora, pasado un tiempo, el proceso de putrefacción del cadáver hace que la tierra colapse y cree pequeñas ondulaciones en el suelo. Los nutrientes del cuerpo en descomposición favorecen al crecimiento de nueva vegetación. Aquí entra la pericia del especialista para reconocer las pequeñas diferencias que se muestran en el lugar a investigar.

También la flora, la acidez de la tierra y la humedad descomponen el cuerpo. La fauna del lugar es todavía más destructiva y puede mover los restos humanos a kilómetros de distancia de donde fueron depositados.

Con la certeza del hallazgo de una fosa clandestina, la exhumación se tiene que hacer con el mismo cuidado y pericia que la búsqueda. Cada capa de tierra que cubre los restos humanos proporciona importantes detalles que ayudan a darle identidad y justicia.

Cuando el trabajo en campo se termina, los restos humanos son recuperados y se trasladan a un laboratorio para su análisis. Durante esta etapa, el trato del cuerpo hallado debe ser respetuoso y digno, sin importar si éste fue la víctima o el victimario.

B) Trabajo de laboratorio

En el laboratorio se materializará la cuarteta básica de identificación, en la que se observan los cambios en el hueso durante toda la vida, cómo se afecta por diversos factores tanto endógenos (desórdenes, metabólicos endócrinos, infecciosos) como exógenos (fracturas, marcas de estrés ocupacional, estrés

nutricional y factores culturales). Aunado a esto, están las características típicas como las filogenéticas, sexuales y de crecimiento corporal. El recuento de todos estos cambios que se dan en vida, contribuyen a obtener una identificación.

La información que proporcionen los familiares de la persona desaparecida, como la media filiación del individuo (peso, estatura, color de pelo, etcétera), además de su historia clínica (tratamientos odontológicos, intervenciones quirúrgicas, traumas antiguos y hábitos personales) serán confrontados con los obtenidos de los análisis a los restos no identificados.

Actualmente, la Antropología Forense en México se enfrenta a grandes retos. La desaparición forzada ha traspasado los crímenes de estado. Ahora, los victimarios son la delincuencia organizada, civiles y feminicidas.

Al corte de la presente investigación, la Secretaría de Gobernación documentó que en el país suman 73 mil personas desaparecidas, 3 mil 978 fosas clandestinas, de las cuales se han exhumado mil 682 cuerpos. Las cifras hablan de una especialización de la violencia y en el trato de la muerte. Sobran los lugares para esconder cuerpos y las formas para borrar los rasgos que den un nombres.

El miedo de las familias a denunciar, la carga de trabajo para las autoridades, la escasez de especialistas suman tiempo vital para encontrar a una persona, mismo que también cuenta cuando una persona fallecida se encuentra en una fosa clandestina o depositada en basureros y parajes deshabitados.

Si hablamos de destrucción y desaparición, el ser humano se ha especializado en ello. En México hay lamentables ejemplos de este tipo de destrucción como la cremación de cuerpos que los reducen casi a cenizas, la disolución de cuerpos en ácido y la desmembración de cuerpos.

Los huesos cuentan una historia y es trabajo del antropólogo escribirla, es un compromiso moral dar voz a las personas que ya no pueden exigir justicia; es permitir cerrar un duelo a las familias que buscan a sus seres queridos; es un reencuentro entre vivos y muertos, un regreso a casa. Gracias a la ciencia, a las respuestas que nos ofrece y a la finalidad de toda disciplina científica se logra ayudar a la gente y prestar cooperación a una sociedad.

Sánchez. Encinas, "Registro histórico en México de 73 mil 201 personas desaparecidas", Periódico La Jornada online, México, 13 de julio de 2020, cfr.

https://www.jornada.com.mx/ultimas/politica/2020/07/13/registro-historico-en-mexico-de-73-mil218personasdesaparecidas4640.html#:~:text=En%20M%C3%A9xico%20se%20tiene%20un,Felipe%20Calder%C3%B3n)%20y%20hasta%20la

V. Odontología forense

La Odontología Forense es otra de las disciplinas de este gran entramado que contribuye a la identificación de personas. El experto en la materia debe tener la capacidad de reconocer, encontrar, obtener, recabar, analizar, comparar y almacenar aquellas características odontológicas individualizantes de una persona, después deberá plasmarlas en un dictamen y entregarlo a la autoridad requirente para su mejor disposición.

Es una especialidad ejercida por un perito que coadyuva en la impartición de justicia, por medio de un requerimiento, con el aporte de sus conocimientos (opiniones, análisis, hallazgos y conclusiones bien fundamentadas) vertidos en un dictamen dirigido a la autoridad (Ministerio Público o Juez), quien las tomará en cuenta para poder emitir una resolución motivada y fundamentada de manera científica.

De acuerdo al requerimiento de la autoridad y al perfil del perito, los casos en los cuales puede tener vista son:

- **Valoración de lesiones:** análisis y valoración de posibles secuelas posteriores a una lesión, como un golpe en la mandíbula y fractura dental derivada.

- **Controversia por *mal praxis*:** estudio y análisis de una posible negligencia cometida por el odontólogo, así como el pronóstico derivado de la misma.

- **Mordedura humana vs. mordedura animal:** establecimiento o descarte del origen de una lesión en una persona, es decir de origen humano o animal de acuerdo a sus características.
- **Obtención de características odontológicas individualizantes**: las características odontológicas de una persona son únicas y no hay dos exactamente iguales; éstas se registran y se archivan para una confronta.

- **Identificación por medio de comparación de mordida**: comparación entre dos mordidas, ambas de origen humano; determinar entre dos o más personas quién infringió una lesión por mordedura a la otra.

- **Identificación de restos óseos de origen humano**: de acuerdo a las características observadas, diferenciar entre restos óseos de origen humano contra aquellos de origen animal.

- **Estimación de la edad dental**: hay diversas técnicas para la estimación de la edad, de acuerdo a las características dentales de una persona (radiográfico, nivel de maduración y erupción, transparencia radicular, etcétera), así se determinará si el individuo es mayor o menor de edad .

- **Necroscopia Oral**: procedimiento quirúrgico llevado a cabo por un profesional, mismo que requiere del abordaje, descubrimiento, observación, registro y análisis de las características odontológicas individualizantes de una persona para el establecimiento de la identidad. Este procedimiento es requerido en casos como: identificación de personas víctimas de accidentes masivos (accidentes aéreos, incendios, explosiones, deslaves, etcétera); personas donde las características externas no aportan datos claros reconocibles debido a un proceso de putrefacción o de conservación; aquellas de identidad desconocida y personas no identificadas.

La labor del odontólogo forense es compleja, por lo que debe ser capaz de reconocer esas características únicas y peculiares de una persona, aquéllas que le hacen diferente a las demás, y contribuir a la identificación.

Debe actuar de manera honrada, eficaz, legal, profesional, objetiva y sin dejar de lado que las acciones desarrolladas en el ejercicio de su profesión estarán apegadas estrictamente al respeto de los derechos humanos; propiciará siempre y por encima de todo, el trato digno a la persona motivo de estudio forense, así como a los familiares o víctimas indirectas del hecho que se investiga.

Sin embargo ¿cuáles son los datos de interés que obtiene el odontólogo forense de una persona? Primero verificará el estado del indicio e identificará varias características, antes del análisis odontológico forense:

- Estado (conservación, putrefacción, esqueletización).
- Complejidad del caso (completo, segmentado, desarticulado, con exposición térmica).

- Indicadores dentales de grupo etario (tipo de dentición, presencia del tercer molar, dentadura completa o incompleta).
- Estado de salud (lesiones, estado/presencia/ausencia de tejido).
- Estado y presencia de estructuras óseas craneales y poscraneales más significativas.

Una vez ubicado el grupo etario, se seleccionará la técnica de estimación dental más idonea para obtener un resultado con menor sesgo, al final se deben identificar dos rubros: las características odontológicas individualizantes y la estimación de la edad dental de una persona motivo del estudio forense.

Para alcanzar el objetivo anterior, el odontólogo utiliza la siguiente metodología, que se describe de manera secuencial:

1. Recepción de indicio con el respectivo formato de RCC y revisión de coincidencia con el formato de RCC.
2. Apertura del embalaje.
3. Limpieza del indicio.
4. Análisis de características odontológicas.
   - Registro de características odontológicas en la ficha dental.
   - Registro de hallazgos de interés odontológico.
   - Registro de características odontológicas individualizantes.
5. Análisis de tejidos duros.
   - Registro de características.
6. Selección de la técnica para la estimación de edad dental.
   - Selección de muestra.
   - Toma de muestra.
   - Registro de características.
   - Colocado de muestra en su sitio original.
7. Embalaje y rotulado del indicio.
   - Entrega de indicio con el respectivo formato de RCC y revisión de coincidencia con el formato de RCC.
8. Consideraciones.
9. Conclusiones.

La selección de la técnica para la estimación de edad dental es posterior a la fase de limpieza y también dependerá del tipo y estado de los elementos óseos, dentales y de interés odontológico recibidos.

La estimación de la edad resulta un elemento importante para la identificación de una persona cuya identidad desconocemos, o bien de personas bajo interés judicial, por ejemplo el caso de los menores transgresores

de la Ley; esto en virtud de que el crecimiento y desarrollo son eventos constantes y progresivos y el estudio de los dientes es necesario para el cálculo de la edad, pues su desarrollo paulatino comienza desde la vida intrauterina y perduran incluso posterior a la muerte, sin embargo su periodo de mayor actividad se prolonga hasta la segunda década de la vida.

Los métodos de estimación dental cubren un rango muy amplio de edades, en virtud de que el desarrollo de los primeros ejemplares dentales en un embrión humano empieza en el segundo mes tras la concepción, mientras que el último diente permanente (tercer molar) termina su desarrollo aproximadamente entre los 21 a 25 años.

Cuando se completa la conformación de la corona dental se inicia la formación de las raíces, luego los órganos dentarios migran hacia la cavidad oral hasta adoptar su posición final en la arcada dentaria, esto se conoce como erupción dental, el último órgano dental en erupcionar es el tercer molar, por ello, la valoración del estado de maduración del tercer molar es un método importante dentro de la odontología forense, tanto para su aplicación en adolescentes como en jóvenes adultos. Debido al hecho de que todos los dientes permanentes se han terminado de formar, los terceros molares representan el único diente todavía en desarrollo.

Por su parte, la autopsia oral quirúrgica es una técnica que extrae los maxilares para facilitar el estudio bucodental en cadáveres que deben ser identificados, permite la descripción detallada de cada una de las estructuras del sistema estomatognático (Moya, V., Roldán. B., 1994). Debe ser completa, metódica y documentada (Téllez, N. 2002).

Para poder efectuar la autopsia oral quirúrgica es necesario que el cuerpo reúna una serie de características tales como rigidez cadavérica, fenómenos de putrefacción, carbonización y momificación (Lozano, O., Andrade, 2006; Moya, V., Roldán. B., 1994).

La autorización legal para efectuar la autopsia oral, puede quedar implícita en la práctica de la autopsia médico legal, siendo importante revisar el código relativo en la entidad federativa en la que se efectúe, ya que se llevarán a cabo una serie de cortes que alterarán las características del cadáver. En las técnicas utilizadas es fundamental contar con el equipo necesario. (Lozano, O., Andrade, 2006).

Como actuación previa es necesario practicar fotografías de frente y de perfil del cadáver, dado que tras la práctica de la autopsia pueden producirse modificaciones desfigurativas (Vargas, E. 2014).

Para el examen clínico odontológico en cadáveres frescos con rasgos faciales intactos únicamente se debe manipular la mandíbula tratando de relajarla mediante la apertura y cierre hasta lograr un espacio suficiente para el examen adecuado.

En el caso de cadáveres calcinados donde no haya rasgos faciales que conservar y cuando se requiera la toma de rayos X dentales no disponibles en el sitio de la necropsia, o en caso de que se requiera la intervención de un experto en odontología forense, se lleva a cabo la resección de maxilares para remitirlos a interconsulta mediante su RCC.

Diente Rosado

La característica del "diente rosado" fue descrito por primera vez en 1829 por un científico inglés de nombre Thomas Bell, quien observó una pigmentación rosa en los dientes de cadáveres cuya causa de muerte había sido asfixia por sumersión o ahorcadura (Labajo González, Sánchez, & amp; Cienfuegos- Jovellanos, 2006).

Dicha pigmentación se ha asociado a cambios de coloración en la dentina por un aumento en la presión intravascular a nivel facial lo que genera hemorragias a nivel pulpar sin afección del esmalte (Pessoa Soriano, Vitor-Diniz de Carvalho, & Bernardo Dos Santos, 2009).

El fenómeno *post mortem* de diente rosado consiste en una coloración rosa que principalmente se observa a nivel de los incisivos, caninos y premolares. (Gowda, Sivapathasundharam, & Chatterji, 2015) y se debe a una liberación de la hemoglobina soluble alrededor de la pulpa dentaria a partir del proceso de autolisis.

Los dientes son considerados las estructuras más resistentes del cuerpo humano, pudiendo soportar temperaturas de hasta 1600°C sin una pérdida importante de su micro-estructura (Moreno et al., 2009), permaneciendo casi intactos tiempo después de que los tejidos blandos y esqueléticos han sido destruidos por la incineración.

Otra característica a considerar, es que los dientes se encuentran articulados en el hueso alveolar del maxilar y de la mandíbula, tejidos óseos que, unidos a los tejidos blandos, mucosos, epiteliales y musculares que los rodean,

les proporcionan una mayor protección en caso de exposición a altas temperaturas (Myers et al., 1999; Fereira et al., 2008).

El análisis de los dientes sometidos a altas temperaturas constituye un aspecto fundamental en el campo de las ciencias forenses. Una gran variedad de acontecimientos se producen en los que el fuego actúa como protagonista: accidentes aéreos, de tráfico, terremotos, atentados con bombas o cremaciones ilícitas.

Además, el fuego puede ser empleado para destruir pruebas forenses en casos criminales, a menudo tratando de evitar la identificación y recuperación de la víctima (Savio et al., 2006). En estos casos, los dientes de los cadáveres carbonizados pueden aportar valiosa información sobre la identificación del individuo, pero también de las circunstancias que rodean al fuego, la temperatura alcanzada en el lugar de los hechos, la fragilidad para la recuperación de la muestra, la degradación del ADN, etc. (Pol et al., 2015).

VI. Genética Forense

La Dirección General Científica de la Guardia Nacional cuenta con un laboratorio de genética forense, cuyos recintos certificados, equipamiento y personal especializado laboran con la finalidad de analizar todo tipo de indicio cuyo material biológico de origen humano permita alcanzar la identificación de una persona.

La genética forense siempre será el último recurso para identificar a las personas cuando no es posible que el estado de los restos humanos localizados, proporcione información útil en materia de odontología o antropología forense, y cuando éstas no tienen los indicios en condiciones para llegar a esa identificación, pues sólo es un "trozo" de tejido, y quizá quemado, entonces el área de genética forense procede al análisis en el laboratorio, en el que se obtendrá un perfil genético, siempre y cuando la muestra no esté en muy malas condiciones de conservación.

Después se ingresa ese perfil a una base de datos para determinar si hay o no concordancia con alguna de las muestras biológicas de referencia proporcionadas por algún familiar y así, de esta forma, encontrar relaciones de parentesco, para lograr una identificación humana.

Es importante mencionar que el trabajo empeñado a lograr una identificación humana, recorre un largo camino en dónde se unen los

conocimientos de especialistas en criminalística, antropología, arqueología y odontología forense, utilizando herramientas científicas que permitan llegar a un resultado confiable.

La genética forense se basa en el estudio de la transmisión de los caracteres hereditarios y el análisis del polimorfismo o variabilidad genética humana aplicada a los problemas judiciales.

Esta disciplina estudia los elementos orgánicos derivados del cuerpo de una persona viva o no (piel, sangre, saliva, semen, cabello) a través de los cuales se puede lograr establecer su perfil genético, ya sea para empatarlo, excluirlo o encontrar parentesco con alguna otra, también para establecer o descartar su presencia en un lugar de investigación forense.

Esta labor de analizar las diferencias a nivel molecular entre seres humanos, a través del método científico, generalmente se acompaña de la solicitud de una autoridad judicial.

Las muestras o indicios que estudia el laboratorio de genética forense tienen que ver con el delito que se perpetró, un homicidio o una agresión sexual. En ese supuesto se toman muestras de fluidos biológicos como manchas de sangre, saliva o semen, que se encuentren en algún pañuelo desechable o ropa interior.

En este laboratorio todo es identificación: si hay fluidos humanos, hay células, hay núcleos, hay AND qué identificar. De ahí la necesidad de contar con un perito, un observador experto para que al llegar al lugar donde se llevó a cabo un delito, éste pueda levantar una huella dactilar, un cabello, un fluido o un objeto que pueda conectar a la gente.

Actualmente, la Guardia Nacional trabaja con delitos del orden federal como la desaparición forzada y secuestro. Su prioridad es la búsqueda en vida de las personas, sin embargo, la mayoría de las veces no es así.

Debido a que se han encontrado gran cantidad de fosas clandestinas en el país y los cuerpos ya se encuentran en avanzado estado de putrefacción, y ya no hay huellas dactilares, la piel cumplió con su proceso de descomposición y quizá el tatuaje que tuvo la persona ya no existe, es entonces que se procesan otros indicios.

La delincuencia organizada se ha especializado y eso obliga a la participación del laboratorio de genética forense, en razón de que los indicios que se encuentran muchas veces no pueden ser procesados por el antropólogo o el odontólogo para la identificación. En muchas ocasiones los cuerpos que se encuentran están destazados o "cocinados", entonces los restos con los que se cuenta pueden ser un tejido quemado, que no esté calcinado, un torso de donde el analista forense debe utilizar el cartílago, fragmentos de costilla, pero

si no cuenta con ese material, ocupará un fémur, un cúbito, o bien cualquier otro hueso.

Si cuenta con la cabeza, utilizará los terceros molares que tienen la cantidad necesaria de material biológico para procesar en el laboratorio y obtener un buen perfil genético.

El laboratorio de genética forense de la Guardia Nacional, desde el 2012 es el primer laboratorio acreditado por la Entidad Mexicana de Acreditación A.C. gracias a su alta calidad de gestión, el cual inicia con la elaboración de un expediente, en el cual se hace la trazabilidad del indicio, se fija, y se llena el formato donde se establece cómo será procesado, hasta llegar a una opinión técnica científica final.

El perfil genético obtenido se ingresará a la base de datos genética con la que cuenta la institución y de esta manera se verificará si existe alguna coincidencia o concordancia, si es así podemos decir que se ha identificado a una persona. La preservación de los materiales así obtenidos representa quizá el mayor compromiso de la labor forense con el método científico.

Fuentes de Consulta

Barba, Luis (1990) Radiografía de un sitio arqueológico, IIA. UNAM, México.

Rodríguez Cuenta José Vicente (2011) La identificación humana en Colombia: avances y perspectivas. Bogotá: Universidad Nacional de Colombia.

Domingo, Ines. Burke, Heather, Smith, Claire. Manual de campo del arqueólogo. Ariel Prehistoria

Duday, Henry (2000) Antropología biológica y de campo, tafonomía y arqueología de la muerte en: "El cuerpo Humano y su tratamiento mortuorio", Coord. Varios, INAH, Centro Francés de estudios Mexicanos y Centroamericanos.Págs. 91-126.

Lara Barajas, Israel David (2009) Fundamentos de Antropología Forense: técnicas de prospección, exhumación y análisis de restos óseos en casos forenses.

EPAF (2002) Ficha antemortem. Cuestionario elaborado por el equipo Peruano de Antropología Forense para investigación forense. Lima, Perú.

Fernández, Víctor (1990) Teoría y método de la Arqueología. Colección Historia Universal, Editorial Síntesis, Madrid, España.

Harris, E. (1991) Principios de estratigrafía arqueológica. Barcelona, Crítica.

Ley Federal sobre Monumentos y zonas arqueológicas, artísticas e históricas. 1972.

Talavera, Arturo, et. al. (1999) Los peritajes de arqueología y antropología forense en México: "Un nuevo campo de trabajo en las Ciencias Sociales" En Diario de Campo. (Boletín interno de los investigadores de antropología) N. 17. Coordinación Nacional de Antropología. CNA. INAH. México.

Tim D. White, Michael T. Black and Pieter A. Folkens (2011) , Human Osteology, Book 3rd Edition.

Varios (2014) Técnicas de Prospección y excavación para la búsqueda de restos óseos humanos. Guía Práctica. PGR. Ciudad de México.

Arqueología Forense INAH.
https://www.revistas.inah.gob.mx/index.php/arqueologia/issue/view/826/83
Consultada 15 de diciembre de 2019.

Caterina Morbiato (2017). Prácticas resistentes en el México de la desaparición forzada. Programa de posgrado en estudios Latinoamericanos. UNAM. México.

Ordaz Díaz Arturo (2020). México tiene más de 73,000 personas desaparecidas, actualiza, SEGOB. Forbes México, Julio 13, 2020.

Rodríguez Cuenca, José Vicente (1994). Introducción a la Antropología Forense. Análisis e identificación de restos óseos humanos. Departamento de Antropología. Universidad Nacional de Colombia. Santa Fe de Bogotá.

PhD Sanabria-Medina, César. "Odontología Forense: identificación humana y alteraciones del sistema estomatognático en el contexto forense". Bogotá, Colombia; Universidad Antonio Nariño. (2018).

Correa Ramírez, Alberto Isaac, "Odontología Forense". México, Ciudad de México:

Editorial Flores (2018).

Kasper K, Austin D, Kvanli AH, Rios TR, Senn DR. "Reliability of third molar development for age estimation in a texas hispanic population: a comparison study". J Forensic.

Lamendin, H., Baccino, E., Humbert, J. F., Tavernier, J. C., Nossintchouk, R. M., and Zerilli, A., "A simple technique for age estimation in adult corpses: the two criteria dental method," Journal of Forensic Sciences, JFSCA, Vol. 37, No. 5, Sept. 1992, pp. 1373-1379.

Rodríguez Cuenca, José Vicente. "Dientes y diversidad humana avances de la Antropología Dental". Universidad Nacional de Colombia

Solari AC, Abramovitch K. "The Accuracy and precision of third molar development as an indicator of chronological age in hispanics". J Forensic.

Vega Dulanto, María del Carmen. "Estimación de edad en subadultos: estudio dental y métrico en poblaciones andinas peruanas". Tesis para optar el grado académico de Magíster en: Antropología Forense y Bioarqueología.

Heit, Oscar (2011) Autopsias bucales en odontología legal: Revisión de técnicas de incisiones. Revista de la Asociación de Médicos Forenses de la República Argentina. Año 34; No. 59 Pag 13-16.

Hernández Carla, López Uriel, Olmedo Alejandra, y Díaz Lidia (2017) Autopsia oral quirúrgica (método Keiser-Nielsen). Revista Electrónica de investigación del CICS UST IPN, Numero 6, Año 3, Volumen 1, diciembre.

Moya V, Roldán B, Sánchez JA. Odontología legal y forense. Barcelona: Elsevier España; 1994.

Labajo, M. E., Sánchez, J. A. & Cienfuegos, B. B. (2006). Postmortem pink-teeth: un curioso fenómeno. Revista de la Escuela de Medicina Legal, 35-46.

Pessoa, E., Vitor-Diniz, M. & Bernardo, F. (2009) The post-mortem pink teeth phenomenon: A case report. Med. Oral Patol. Oral Cir Bucal, 337-339.

Gowda, C., Sivapathasundharam, B. y Chatterji, A. (2015) Histological appearance of Postmortem pink teeth report of two cases. Journal of Forensic Dental Sciences, 7, 2, 168-170.

Engel G. (1977) The need for a new medical model: a challenge for biomedicine. Science; 196:129-36.

CENADEM: EN COMBATE DE LOS DELITOS QUE ATENTAN CONTRA LA INTEGRIDAD DE NIÑOS, NIÑAS Y ADOLESCENTES EN EL CIBERESPACIO

Inspectora GN, Mtra. Olivia Mendoza Cruz[1]
Primer Subinspector GN, Lic. Elohim Hernández Morales[2]

Sumario: I. Introducción. II. Delitos contra menores(pornografía infantil). III. Operación Nacional Ciberguardián. IV. Trata de personas: niñas, niños y adolescentes desaparecidos. V. Alerta AMBER México.

I. Introducción

Para proteger a la infancia en México, la Guardia Nacional cuenta con el Centro Nacional de Delitos Electrónicos contra Menores (CENADEM), a cargo de la Dirección General Científica. Este centro tiene sus orígenes en la Policía Cibernética y Delitos contra Menores de la extinta Policía Federal, sin embargo su misión no ha sufrido grandes modificaciones con el paso del tiempo, al ser responsable de prevenir, atender e investigar desde el aspecto tecnológico, los delitos de trata de personas, pornografía infantil y temas relacionados con niñas, niños y adolescentes desaparecidos, así como conductas antisociales en agravio de la ciudadanía, que para su comisión utilicen medios electrónicos, tecnológicos y/o cibernéticos, sigue siendo primordial.

La era tecnológica a nivel global, trajo consigo una diversidad de oportunidades y desventajas aunadas a situaciones de riesgo que derivan de usuarios maliciosos, que han encontrado en la red pública de internet, un terreno fértil para delinquir. Las niñas, niños y adolescentes son los más vulnerables ante estos usuarios y fácilmente son víctimas de delitos tales como pornografía infantil, explotación sexual infantil, trata de personas, y algunas conductas antisociales como son el *grooming, el sexting y el cyberbullying*.

El cumplimiento de esta misión de protección a la infancia será posible, mediante la colaboración activa y comprometida de servidores públicos que cuenten con las capacidades y conocimientos necesarios, que les permitan identificar y prevenir las conductas antisociales y los delitos antes mencionados, en beneficio del interés superior de la niñez.

Con 18 años de experiencia en actividades de prevención del delito electrónico contra menores, ha participado en diversos foros, pláticas y conferencias a nivel nacional sobre medidas preventivas, seguridad en Internet y prevención de explotación sexual comercial infantil.

Con licenciatura en Sistemas Computacionales, se ha desempeñado como investigador de delitos cibernéticos como de pornografía infantil y de conductas antisociales en agravio de niñas, niños y adolescentes.

El objetivo del CENADEM, es colaborar con las autoridades de los tres órdenes de gobierno, actores sociales, instituciones académicas y sociedad en general, en la prevención e investigación de los delitos o conductas antisociales que se cometen a través de medios electrónicos, cibernéticos o tecnológicos, en agravio de niñas, niños y adolescentes, así como la trata de personas, mediante la atención a mandamientos ministeriales y judiciales y la colaboración con organismos nacionales e internacionales, en preponderancia al interés superior de la infancia, principalmente en el bienestar y seguridad de su libre desarrollo psico -sexual y de su personalidad.

Por lo que respecta al Centro de Delitos Electrónicos contra Menores, sus atribuciones se encuentran plasmadas en el artículo 36 del Reglamento de la Ley de la Guardia Nacional,[1] para dar cumplimiento a las mismas, cuenta con un estado de fuerza que oscila entre los 35 a 40 integrantes, entre hombres y mujeres comprometidos con nuestra nación.

Las mujeres y los hombres que integran el CENADEM, tienen de 1 a 18 años de experiencia en ciberinvestigaciones de delitos contra menores, trata de personas, así como en la búsqueda y localización de niñas, niños y adolescentes desaparecidos; la escolaridad mínima es de nivel superior y al menos un certificado de competencia laboral en un estándar de competencias del personal que cuenta con más de 3 años de experiencia, existiendo incluso nivel de posgrado como especialidades, diplomados y maestrías.

El CENADEM, recibe diversas solicitudes de colaboración en la investigación de delitos, prevención de delitos electrónicos contra menores y prevención de conductas antisociales, capacitación a funcionarios públicos, búsqueda de niñas, niños y adolescentes desaparecidos o extraviados; el CENADEM cuenta con el acceso al banco de datos NCMEC,[4] lo que permite la identificación de usuarios, quienes mediante el empleo de servicios, como: almacenamiento en la nube (*Dropbox, Drive, Google Drive, plus.google.com/photos*), mensajería instantánea (*Facebook, Twitter, Whatsapp, Skype, Yahoo Groups, Instagram*), envío de correos electrónicos (*Microsoft, Yahoo, Gmail*) y páginas web, foros o *blogs,* realizaron la transmisión, producción, almacenamiento, intercambio y distribución de material de abuso sexual y/o pornografía infantil, en diversos Estados de la República Mexicana, investigar los delitos de trata de personas,

[1] http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf

[4] Centro Nacional de Niños Desaparecidos y Explotados de los Estados Unidos de Norteamérica.

niñas, niños y adolescentes desaparecidos, todos estos relacionados con indicios en la red pública de internet o dispositivos electrónicos.

II. Delitos contra Menores (pornografía infantil)

Esta área es la encargada de investigar todos los delitos en agravio de niñas, niños y adolescentes, que tienen al menos una línea de investigación en la red pública de internet o dispositivos electrónicos.

En este sentido, se ha detectado que **Facebook** es la red social más utilizada; sin embargo, esta red social ha dado a conocer que al menos **80 millones** de perfiles registrados son falsos, lo que significa que pudiera haber una gran cantidad de agresores sexuales en la red pública de internet.

En México al menos uno de cada siete menores de edad ha recibido solicitudes sexuales, generalmente por adultos que se hacen pasar por amigos de su misma edad en las redes sociales.

La pornografía infantil a nivel mundial, genera 34 mil millones de dólares anuales y México ocupa el primer lugar en distribución de pornografía infantil (de acuerdo al Departamento de Seguridad Nacional de los Estados Unidos de América). El 60% del material pornográfico consumido en el mundo se encuentra en nuestro país.

La pornografía infantil es el tercer delito que genera mayores ganancias en el mundo, sólo por debajo del narcotráfico y la trata de personas.

Por lo que respecta a la atención de los requerimientos ministeriales, se lleva a cabo la búsqueda en la red pública de Internet, que consiste en la investigación de los datos que se desprendan del requerimiento, realizando consultas en bases de datos a las que la Guardia Nacional tiene acceso, consultas de antecedentes, y se realizan solicitudes de información a proveedores de servicios de internet, telecomunicaciones y telefónicas, mediante los mecanismos legales vigentes.

Derivado de la colaboración con organismos internacionales y con base en las incidencias notificadas por los prestadores de servicio y contenidos en internet al Centro Nacional de Niños Desaparecidos y Explotados (NCMEC), de usuarios reportados que tienen su origen de conexión en México y están

relacionados con la transmisión, almacenamiento y producción de contenido de pornografía infantil, de agosto del año 2011 al 31 de diciembre de 2020, se han recibido 1,513,593 reportes, lo que refleja un daño al tejido social en el sector más vulnerable "LA NIÑEZ MEXICANA".

En el marco de la Operación Nacional Ciberguardián, se presentaron 109 denuncias, de las cuales 7 fueron remitidas a la Fiscalía Especial para los Delitos de Violencia Contra las Mujeres y Trata de Personas (FEVIMTRA) de la Fiscalía General de la República, con la identificación de probables responsables en los estados de Ciudad de México, Baja California, Sonora, Sinaloa; 1 remitida a la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (SEIDO)-Unidad Especializada en Investigación de Tráfico de Menores, Personas y órganos (UEITMPO) de la Fiscalía General de la República, con la ubicación de un probable responsable en Baja California; y 101 fueron remitidas a las Fiscalías Especializadas en Delitos Sexuales y/o trata de personas, en los estados de: Aguascalientes, Baja California, Baja California Sur, Campeche, Chiapas, Chihuahua, Ciudad de México, Coahuila, Colima, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Oaxaca, Puebla, Querétaro, Quintana Roo, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán y Zacatecas. Lo anterior, con la detención de probables responsables.

En el contexto de la "Operación Nacional Ciberguardián", se implementó el "**Operativo Salvación**", que tiene por objeto rescatar de forma simultánea víctimas menores de edad del delito de Pornografía Infantil, y poner a los probables responsables o agresores sexuales en manos de la justicia.

Por lo que respecta al mismo periodo, se han presentado 8 denuncias derivadas de los reportes ciudadanos a las Fiscalías Especializadas en Delitos Sexuales y/o trata de personas en: Ciudad de México, Estado de México, Nuevo León, Puebla y Tamaulipas.

Caso de éxito

En el marco de las facultades conferidas en la Ley de la Guardia Nacional, el 26 de febrero de 2021, la Dirección General Científica en colaboración con la Fiscalía General de Justicia del Estado de Nuevo León, logró la detención de Rubén Vignolle "N" y María Isabel "N", de 57 y 37 años de edad respectivamente, por el delito de trata de personas en su modalidad de pornografía infantil, así como el rescate de dos víctimas menores de edad.

La investigación inició derivado de la colaboración Internacional de la Dirección General Científica con el Centro Nacional de Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés), quien remitió 9 reportes sobre incidencias en trasmisión y producción de material de abuso sexual infantil; por lo que se presentó la denuncia de hechos, por el delito de pornografía infantil ante la Fiscalía General de Justicia del Estado de Nuevo León; así mismo, se aportó la evidencia digital y se realizó el análisis y la investigación cibernética, logrando identificar y ubicar a los probables responsables y a las víctimas menores de edad, lo que permitió al Ministerio Público solicitar ante el Juez de Control las órdenes de aprehensión y diligencia de cateo a un domicilio para asegurar los dispositivos electrónicos relacionados con el delito.

Trata de personas: niñas, niños y adolescentes desaparecidos

Esta área es la encargada de investigar el delito de trata de personas que tengan una línea de investigación en la red pública de internet o algún dispositivo electrónico, cibernético o tecnológico.

De acuerdo a un estudio del Departamento de Estado de los Estados Unidos de América, México es un país de origen, tránsito y destino de hombres, mujeres y menores sometidos al tráfico sexual y al trabajo forzoso. Los grupos considerados más vulnerables a la trata de personas en México incluyen mujeres, menores de edad, indígenas, personas con discapacidad mental y física, migrantes y personas lésbico, gay, bisexual, transexual, transgénero, travesti e intersexual (LGBTTTI)1.

La trata de personas a nivel mundial es el segundo negocio ilícito más rentable con 36 MMD en ganancias anuales, ya que genera ingresos de 13,000 dólares en promedio por cada víctima.

Por lo que respecta a México, las fronteras Norte y Sur son las que registran mayor incidencia de trata de personas, sin embargo, los siguientes estados cuentan con más solicitudes de investigación en el CENADEM: Baja California, Chihuahua, Tamaulipas, Jalisco, San Luis Potosí, Quintana Roo, Chiapas, Tlaxcala, Ciudad de México y Estado de México.

Una de las modalidades más utilizadas por las células delictivas dedicadas a la trata de personas es la de "explotación sexual", cuya forma de operar es a través de sitios web donde se promocionan servicios de "scorts", formando las denominadas "Agencias" principalmente de mujeres extranjeras en estado de vulnerabilidad, las cuales son traídas al país con ofertas de trabajo como

1. Trafficking In Persons Report 2018. U. S. Department of State

modelos o edecanes y/o enamoradas, para luego ofertarlas a través de dich os sitios.

Caso de éxito

Se inició una técnica de intervención de comunicaciones privadas de una línea telefónica propiedad de Natty Paola N. N., con la cual se tuvo de conocimiento que se dedicaba a realizar actividades ilícitas relacionadas al delito de trata de personas en su modalidad de explotación sexual; con apoyo de Gabriela Karina N. N., quien le ayudaba a reclutar, organizar y amenazar a las víctimas de explotación sexual de nacionalidad principalmente colombiana y venezolana.

Una vez que las víctimas se encontraban en territorio nacional se les quitaba el pasaporte y se les tomaban fotografías de exhibicionismo sexual por el fotógrafo de nombre Víctor N.N., quien les cobraba con relaciones sexuales.

De la intervención de comunicaciones se desprende que las víctimas tenían que realizar servicios sexuales hasta que pagarán una deuda de 60,000 pesos por gastos de transporte, hospedaje, alimentación y vestido, a Natty Paola y Gabriela Karina, de la investigación se contabilizaron 60 víctimas que trajeron para ser explotadas sexualmente de esos países.

El 21 de marzo de 2018, personal del CENADEM denunció los hechos posiblemente constitutivos de delito, poniendo a disposición los audios ante la Fiscalía Especial para los Delitos de Violencia contra las Mujeres y Trata de Personas (FEVIMTRA); posteriormente, se rindieron informes policiales a la Autoridad Ministerial, derivados de las investigaciones de gabinete (Científica) y de campo (Investigación).

Después de un año de investigación de gabinete, campo y el análisis de la información obtenida, se logró contar con todos los elementos necesarios para que el juez otorgara la orden de cateo, es así que, el 23 enero de 2019, se realizó la detención de Natty Paola, Gabriela Karina y Víctor, así como la liberación de víctimas del delito de trata de personas en su modalidad de explotación sexual.

VI. Alerta AMBER México

Por lo que respecta a la búsqueda y localización de niñas, niños y adolescentes desaparecidos o extraviados, el Centro de Delitos Electrónicos

contra Menores, además de atender los requerimientos de colaboración de las diversas autoridades competentes, participa desde mayo de 2012, en el Programa Nacional Alerta AMBER México, el cual es un mecanismo nacional de coordinación y cooperación sistemática entre los tres órdenes de gobierno, medios de comunicación, organizaciones de la sociedad civil y otros que pudieran estar involucrados desde el ámbito de sus respectivas competencias, para la búsqueda y pronta recuperación de niñas, niños y adolescentes que se encuentren en riesgo inminente de sufrir daño grave a su integridad por motivo de ausencia, extravío, privación ilegal de la libertad, no localización o cualquier circunstancia donde se presuma la comisión de algún ilícito, ocurrido en territorio nacional.

La Dirección General Científica de la Guardia Nacional, como coadyuvante en el "Programa Nacional Alerta AMBER México" y responsable de la diseminación nacional de Alertas y Pre - Alertas a instancias de seguridad pública, en una primera fase efectuará la difusión a través de las Coordinaciones Regionales y Estatales de la Guardia Nacional, para que se integren en las labores de búsqueda de niñas, niños y adolescentes desaparecidos, en sus diferentes unidades operativas.

Caso de éxito

El 18 de diciembre de 2018, la Oficina Federal de Investigación ***(Federal Bureau of Investigation, FBI)***, a través del agregado en México, informo sobre la privación ilegal de dos menores de edad de nacionalidad estadounidense, cometida por dos varones adultos de la misma nacionalidad mismos que al parecer se adentraron en territorio Mexicano y posiblemente se encontraban en el Estado de México.

Se activó la alerta AMBER a nivel nacional por los dos menores de edad dándole puntual seguimiento, se llevó a cabo la coordinación con el personal de la entonces División de Investigación a fin de establecer las acciones en campo, a su vez se contactó al personal del Instituto Nacional de Migración (INAMI), ante la posible detención y deportación de los presuntos implicados, una vez ubicados.

Se verificaron 4 domicilios en la Ciudad de México, ubicaciones proporcionadas por el agregado del FBI en México, en donde posiblemente estuvieron los presuntos responsables y las víctimas menores de edad, uno de estos lugares era un hotel ubicado en la zona centro de la Ciudad de México,

donde se entrevistó al gerente, quién señaló haber observado a personas con las características descritas de los objetivos, con vestimentas de alguna religión ortodoxa; asimismo, el encargado de un negocio aledaño corroboró la presencia de esas personas, con la colaboración del gerente del hotel se obtuvieron algunas imágenes de las cámaras de video vigilancia del interior del lugar, donde se aprecian dos varones adultos con las características previamente descritas.

Derivado de la investigación, se confirmó que uno de los objetivos, realizó una compra de dos equipos de telefonía celular en una sucursal de la empresa Coppel, en Nezahualcóyotl, Estado de México.

Se obtuvieron los números telefónicos que se asignaron a los equipos presuntamente adquiridos por el objetivo, así como el número telefónico que proporcionó el objetivo, para que se le enviaran los códigos de desbloqueo de los números anteriores, gracias a lo cual se les pudo realizar la georreferenciación y ubicarlos en tiempo real.

Fue así que el 27 de diciembre de 2018, se logró la recuperación de las víctimas de 12 y 14 años de edad, así como la detención de los secuestradores, todos de nacionalidad estadounidense.

LA POLICÍA CIENTÍFICA DE MÉXICO COMO AGENTE INVESTIGADOR DE LA TORTURA

Inspectora GN, Adriana López Torres[1]
Oficial GN, Beatriz Cuautle Hornilla[2]

Sumario: I. Introducción. II. Marco Jurídico. III. La tortura como fenómeno psicológico y social. IV. Metodología de investigación de la tortura con perspectiva de Derechos. V. Conclusiones.

I. Introducción

El objetivo del presente artículo, es dar a conocer la metodología científica que ha permitido aplicar el Protocolo de Estambul en la investigación de la tortura de conformidad a las atribuciones legales y en cumplimiento a los principios rectores de la Dirección General Científica de la Guardia Nacional para dar paso a una documentación eficaz de denuncias de tortura; ésto a razón de que bajo el mandato del Ministerio Público se fortalece el combate al delito de tortura.

Se entiende a la tortura como todo acto por el cual se infrinja intencionadamente a una persona, dolores o sufrimientos graves, ya sean físicos o mentales, con el fin de obtener de ella o de un tercero, información o una confesión, de castigarla por un acto que haya cometido, o se sospeche que ha cometido, o de intimidar o coaccionar a esa persona o a otras, o por cualquier razón basada en cualquier tipo de discriminación, cuando dichos dolores o sufrimientos sean infligidos por un funcionario público u otra persona en el ejercicio de funciones públicas, a instigación suya, o con su consentimiento o aquiescencia del Estado. No se considerarán torturas los dolores o sufrimientos que sean consecuencia únicamente de sanciones legítimas, o que sean inherentes o incidentales a éstas.[3]

---

[1] Mtra. en Ciencias Farmacéuticas y licenciatura en Químico Farmacéutico Biólogo, por la Universidad Autónoma Metropolitana. Publicó el artículo "Perfiles de liberación de Indometacina desde acuosomas utilizando el método de diálisis" en la revista Mexicana de las Ciencias Farmacéuticas, así como la reciente colaboración con el capítulo "La ciudadanía Base de la política criminal", en el libro "Derecho Operacional".

[2] Lic. en Psicología, Maestra en Psicología Criminal y Forense y Doctora en Derechos Humanos. Es experta en la aplicación del Protocolo de Estambul. Publico del artículo "Consideraciones técnicas para detectar falsos negativos en la valoración psicológica del Protocolo de Estambul" en la revista Psicología sin fronteras; es coautora del libro "Tortura y protocolos de Estambul: Perspectiva, alternativas y contextos", por la editorial Académica Española.

[3] Artículo 1 de la Convención contra la tortura y otros tratos o penas crueles inhumanos o degradantes, adoptada y abierta a la firma, ratificación y adhesión por la Asamblea General en su resolución 39/46, de 10 de diciembre de 1984, retomado de la página de las Naciones Unidas para los Derechos Humanos de la Oficina del Alto Comisionado de las Naciones Unidas, https://www.ohchr.org/SP/ProfessionalInterest /Pages/CAT.aspx

Así, igualmente referimos el Protocolo de Estambul, como el manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes, publicado por la Oficina del Alto Comisionado para los Derechos Humanos de las Naciones Unidas.

La Policía Científica es el área de la Guardia Nacional bajo la nomenclatura de la Dirección General Científica que fue creada con la finalidad de utilizar los conocimientos, herramientas tecno-científicas en la investigación para prevenir los delitos, así como coordinar, supervisar y operar el funcionamiento de los servicios científicos; es la encargada de generar metodología científica y tecnológica para la prevención e investigación del delito, a través del desarrollo de herramientas técnico-científicas con la participación del personal experto en criminalística, investigación cibernética y seguridad en sistemas de información y de servicios científico-tecnológicos hasta el año 2019, estas funciones contribuyeron a los objetivos de la entonces Policía Federal.[4]

La Dirección General Científica, antes División Científica, comenzó sus labores en el año 2010, derivado de la reestructuración de la Policía Federal Preventiva; posteriormente formó parte de la Policía Federal, misma que se publicó en el Diario Oficial de la Federación el 17 de mayo de ese mismo año.[5] En el año 2012, se inauguró el edificio de la División Científica, arrancando actividades y a su vez el devenir histórico de las Policías Científicas en México, pues el aporte que brindan las ciencias a la investigación policial y forense, generaron un fenómeno de réplica en las actividades de la Federación, mismos que iniciaron en la conformación de sus propias policías científicas con tecnología en la investigación científica y forense de los delitos en México.

De manera retrospectiva, la historia de las policías en México se sitúa años antes de este marco contextual, pues inicia de 1870 a 1930 con la consolidación y fin del modelo de la Gendarmería Municipal de la Ciudad de México. Con base en esta fuerza, se fundó el sistema policial mexicano compuesto, al igual que otros en el mundo, de un aparato burocrático en comisarías,[6] marco histórico de referencia desde el Porfiriato que permite conocer los cambios en el sistema policial de México, hasta llegar a la construcción de la Policía Científica.

---

4 Retomado de https://www.gob.mx/policiafederal/estructuras/division_cientifica

5 DOF: 17/05/2010, Reglamento de la Ley de la Policía Federal Capítulo Segundo, De la estructura orgánica. Artículo 5°.

6 Pulido Esteva D. (), Gendarmes, inspectores y comisario, historia del sistema policial en la Ciudad de México, 1870-1930, Open edition Journals, pp. 37-58. Retomando de https://journals.openedition.org/erhistoria/2696

Tras ocho años de experiencia y trayectoria, la ahora Dirección General Científica de la Guardia Nacional continúa sentando las bases de su actuación al servicio de la investigación policial y se solidifica como auxiliar fundamental dentro de la actuación de los operadores de Justicia en la investigación de los delitos del fuero común y federal.

II. Marco Jurídico

El marco normativo que faculta a la Dirección General Científica sobre la cientificidad en su actuar bajo el principio de profesionalismo,[7] la enmarca como ente meramente científico que requiere de este mismo, como base para investigar los probables hechos referidos como tortura.

A través de estos antecedentes, es posible señalar que la Policía Científica en México se reformula como el ente especializado de las policías en México, respecto de la atención a víctimas del delito en el camino al acceso expedito de la justicia en el marco de implementación de metodología científica/académica en sus diversas áreas de conocimiento para la adecuada investigación de los delitos.

Históricamente, las policías han estado enfocadas a la investigación de delito en sus diversas formas de manifestación, una de ellas es el delito de la tortura, mismo que lacera la dignidad humana y los derechos al acceso a la justicia de una persona, y es en este sentido que la Dirección General Científica de la Guardia Nacional como ente policíaco, brinda aportes significativos a la investigación de la tortura mediante la aplicación del Protocolo de Estambul.

A partir del 23 de septiembre de 2003, el Estado Mexicano firma el pacto para la implementación del Protocolo de Estambul, ratificándolo el 30 de marzo del 2005, con la finalidad de prevenir, pero sobre todo la de erradicar la tortura en el país mediante su investigación bajo la documentación eficaz de denuncias de tortura, malos tratos, crueles, inhumanos o degradantes, contando únicamente en ese entonces con la otrora Procuraduría General de la República (PGR), ahora Fiscalía General de la República (FGR), a través de su Coordinación de Servicios Periciales, con personal capacitado en el tema, proponiendo en el año 2005, la homologación de la aplicación del citado protocolo, de manera colegiada y "frecuente", en las denuncias de tortura.

7 Consiste en mantener una actitud personal positiva hacia la función policial por parte de quienes se desempeñan dentro de ésta, y que los lleva a buscar una constante superación

Del año 2005 al 2014, en México imperó una institución en la aplicación del Protocolo de Estambul, atrayendo casi por completo las denuncias de tortura para su investigación con base en su protocolo homologado, evidenciando de esta manera sesgos importantes en la investigación de dicho delito al ser "juez y parte", ello sustentado en la Ley General para Prevenir, Investigar, y Sancionar la Tortura y Otros Tratos Crueles Inhumanos o Degradantes, artículo 6 fracción III[8] respecto de la debida diligencia y artículo 36[9] párrafo segundo de la elección de los peritos por parte de los denunciantes, aunado a estos se tienen datos del informe del relator sobre la tortura en México que menciona al respecto:

> 47. El Relator fue informado de que sólo una de cada veinte presuntas víctimas de tortura que presentan quejas ante la CNDH son sometidas a un examen forense oficial por la PGR. Se lamenta constatar que en la mayoría de los casos no se aplica el dictamen especializado para supuestos de posible tortura y que existen al menos 1,600 peticiones pendientes de tramitación y tan solo 185 exámenes han sido practicados en 2014. El examen se realiza meses o años después de los actos de tortura, **de forma deficiente o bien de manera tal que el perito termina concluyendo que no hay huellas de tortura**. Esta demora adicionalmente afecta al proceso judicial del encausado, que en ocasiones opta por desistir del examen forense con el fin de acelerar su proceso ante los tribunales.

8 Debida diligencia: Que se traduce en que toda prevención, investigación, proceso penal y reparación que se inicie por los delitos o violaciones a derechos fundamentales previstos en esta Ley, se deberá garantizar su desarrollo de manera autónoma, independiente, inmediata, imparcial, eficaz; y deberán ser realizadas con oportunidad, exhaustividad, respeto de derechos humanos y máximo nivel de profesionalismo. LGPISTOTCID

9 Las Víctimas tendrán derecho a ser examinadas por médicos especializados y/o psicólogos de su elección.

10 Naciones Unidas (2017), Informe de seguimiento del Relatos Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes-México párrafo 47, 34° sesiones tema 3 de la agenda A/hrc/34/54/Add4, retomado de https://www.hchr.org.mx/index.php?option=com_k2&view=item&id=936:informe -de-seguimientodel-relator-especial-sobre-la-tortura-y-otros-tratos-o-penas-crueles-inhumanos-o-degradantesmexico&Itemid=281

Posteriormente, dentro de este mismo informe se hace hincapié en la importancia de la independencia y autonomía de los peritajes, por lo que en estricto sentido esto visualiza los sesgos en las investigaciones de la tortura que se refirió, al principio por no existir una independencia dentro de las investigaciones de dicho delito, y en estricto sentido lógico es acorde a la realidad de la falta de capacitación de peritos instituciones y particulares, pues hasta el año 2010, no se tiene registro a nivel académico de capacitaciones para la aplicación del Protocolo de Estambul.

Referéndum histórico de la investigación de la tortura en México, en el año 2014 con datos aportados por Amnistía Internacional existieron dos mil cuatrocientas denuncias de tortura, el doble que en el año 2013, siendo estos datos poco fiables pues hasta ese momento no se tenía un registro estadístico de las denuncias, de los casos atendidos y mucho menos el número de víctimas.

Añadiendo a su vez que en México existen leyes contra la tortura, pero casi nadie les presta atención, y los torturadores quedan impunes, se requiere que la iniciativa de ley gubernamental más reciente sobre la tortura sea eficaz. Datos que permitieron saber que dentro del marco de la investigación de la tortura se requerían de nuevas estrategias de conformidad a lo ya establecido en el marco jurídico del país.

Es en este orden histórico, ante el desolador panorama de organismos internacionales como lo es Amnistía Internacional, desde el año 2015, la antes conocida Policía Federal, con su nuevo modelo policial operable a través de sus Divisiones, como es la Científica, comenzó la tarea de coadyuvar en la investigación de la tortura, malos tratos, crueles e inhumanos y degradantes con la aplicación del Protocolo de Estambul, tarea que hasta ese año era asignada únicamente a instituciones como: fiscalías y peritos adscritos a las mismas; el presente texto tiene por objeto, en sentido estricto dar una breve reseña de la construcción del modelo que permitió aplicar dicho Protocolo a la Policía Federal para colocarla como la única policía a nivel Latinoamérica con las facultades y capacitación para poder llevar a cabo esta tarea, un camino que sin duda generó precedentes y una fortaleza interna entre sus atribuciones y la academia forense.

---

11 Pagina oficial de amnistía Internacional, Datos retomados el 06 de septiembre del 2020 de https://www.amnesty.org/es/latest/campaigns/2015/10/stop -torture-mexico/

12 Página oficial de amnistía Internacional, Datos retomados el 06 de septiembre del 2020 de https://www.amnesty.org/es/latest/campaigns/2015/10/stop -torture-mexico/

Como hecho consecuente de los alcances de operadores jurídicos del sistema de justicia y de la propia investigación de la tortura en México, es que en el año 2017, se publicó la Ley General para Prevenir y Sancionar la Tortura, que sistematiza la investigación de la tortura y que permite generar objetivos claros en la actuación de los operadores de justicia en el tema, acompañándose de los Protocolos de la Suprema Corte de Justicia de la Nación de la investigación de la tortura, del acompañamiento jurídico y protección a las víctimas de tortura, sin duda brinda aportes significativos en materia de Derechos Humanos.

Por último, es importante señalar que:

> *..." En 1997, el Comité Contra la Tortura (CCT) señaló que la ineficacia de las iniciativas para poner término a las prácticas de tortura, a juicio del Comité es causada, entre otros factores, **por la impunidad en que permanecen los torturadores**, y por la persistencia de las autoridades encargadas de impartir justicia en admitir como medios probatorios en los juicios, las confesiones y declaraciones obtenidas mediante ella, no obstante, las expresas disposiciones legales que declaran su admisibilidad*[13]*... "(Sic)*

Exigiendo este marco, que las actuaciones del Estado para una investigación, sanción y erradicación eficaz de la tortura sean en apego a derecho, por tanto, la Guardia Nacional como ente coadyuvante de la investigación de delitos retoma este asunto de importancia para reflejarlo en su abordaje a la erradicación e investigación de la tortura desde su hacer y sus atribuciones que el marco jurídico le ha conferido.

En primera instancia es conducente conocer a la tortura como fenómeno histórico y social de carácter psicológico para una debida comprensión para su estudio científico.

III. La Tortura como Fenómeno Psicológico y Social

El fenómeno de la tortura debe comprenderse desde una mirada ecológica, es decir, a nivel sociedad, comunidad, familiar e individual siendo este último perteneciente al ámbito psicológico mismo, en este apartado se formularán algunos tópicos.

13 SCJN. (2014) Protocolo de actuación para quienes imparten justicia en asuntos que involucren hechos constitutivos de Tortura y Malos Tratos. Suprema Corte de Justicia de la Nación. Impreso en México.

Como parte de una profundización concreta del fenómeno psicológico de la tortura a nivel psicoanálisis se habla de una perversión referida por Rivadeneira y citada por Bezanilla JM (2016) que todo acto de perversión y en especial la tortura, se constituyen como la realización de fantasías humanas a partir de un retorno de lo reprimido, especialmente aquellas pulsiones sádicas que hablan de una re-negación de la castración que conllevan el gozo con la destrucción y transgresión de la Ley y el otro.

Ello aporta a que la tortura pueda interpretarse desde el punto de vista como una de las violencias más frecuentes en el ser humano pero al mismo tiempo aberrantes, que visualizan la vulnerabilidad del ser humano ante el Estado que degradan al individuo como parte de una colectividad desolada por el dolor y sufrimiento que recibe, entonces la tortura convierte al sujeto a un objeto que recibe violencia con una finalidad.

Algunos investigadores del tema de tortura como Pérez Sales P. mencionan que "el síndrome más frecuente asociado a las situaciones de maltrato y tortura es la depresión grave o crónica, que resulta con frecuencia en conductas de inhibición y en un pobre relato. Respecto del denominado Trastorno de Estrés Postraumático constituye, con todo, el diagnóstico más popular y es bien conocido por abogados y jueces"; en relación con lo anterior, el Protocolo de Estambul los específica en el listado que se presenta más adelante como indicios psicológicos de la tortura.

Por lo que, se describen a las secuelas psicológicas, que refiere el Protocolo de Estambul en el Capítulo IV INDICIOS PSICOLóGICOS DE LA TORTURA, B. Secuelas psicológicas de la tortura. 2. Reacciones psicológicas más frecuentes con el probable resultado que tendrá la tortura como impacto Psicológico reflejado en:

a) Re experimentación del tema
b) Evitación y embotamiento emocional
c) Hiperexitación
d) Síntomas de depresión
e) Disminución de la autoestima y el sentido del futuro
f) Disociación, despersonalización y comportamiento atípico
g) Quejas Somáticas

---

14 Bezanilla J. M y Miranda, A. (2015) NOTAS para una valoración Psicológica de la Tortura, Editorial PEI, México.

15 Pérez Sales P. (S/F) Peritación Psicológica y Psiquiátrica de maltrato y tortura en solicitantes de asilo, uso de protocolo de Estambul. España Pp 267, retomado de: http://www.pauperez.cat/wpcontent/uploads/2017/11/pau -perez-sales-peritacion-psicologica-y-psiquiatrica-de-maltrato-y-torturaen-solicitantes-de-asilo.pdf

16 OACNUDDHH, (2004) Manual para la investigación y documentación eficaces de la tortura y otros tratos crueles, inhumanos o degradantes. Protocolo de Estambul, 1 Revisión, Naciones Unidas, Nueva York-Pp 88.

h) Disfunciones sexuales
i) Psicosis
j) Consumo excesivo de sustancias psicotrópicas
k) Daño neuropsicológico

Otros autores, como Madariaga abordan a las secuelas de la tortura como un estrés postraumático como entidad nosológica; no obstante, es importante aclarar que no hay estudios profundos que determinen que, por lo menos en México las principales secuelas sean éstas. En estricto sentido esto obedece a que no son las únicas consecuencias, pero sí, las más frecuentes detectadas (como sintomatología individual), por lo menos al momento de la publicación del protocolo.

Posteriormente, en ese mismo apartado se hace mención de las sintomatologías citadas con anterioridad y estas deben de estar agrupadas y bajo criterios de tiempo e intensidad para poder establecer la existencia de trastornos depresivos, trastorno de estrés post traumático, transformación duradera de la personalidad, consumo excesivo de sustancias psicotrópicas y lo que menciona como otros diagnósticos como: el trastorno por ansiedad generalizada, trastorno de pánico, de estrés agudo, de aspecto somático, bipolar, causado por una dolencia general, así como fobias.

Éstas, como consecuencias de índole clínica dentro del ámbito psicológico, pero no las únicas, pues al realizar una revisión de literatura en dicha materia (en atención a que el Protocolo de Estambul hace hincapié que las directrices que proporciona no deben ser concebidas como prescripción fija, por lo que se debe de considerar en atención al objetivo de cada evaluación y de los recursos con los que se cuenten) se habla de un trauma transgeneracional, biopsicosocial y hasta cultural derivados de la tortura.

Como lo cita Enrique Echeburrúa (Echeburúa, Corral y Amor, 2004) al hablar de la importancia de diferenciar el daño psicosocial del daño clínico, en razón de que es muy importante para la historia de la Psicología, pues nos referimos al daño clínico como aquel impacto psicológico que le representa a las víctimas un evento traumático. En resumen, el cómo los mecanismos de defensa de cada persona se activen ante eventos traumáticos como lo es la tortura, van a depender de las propias características de la psicodinámia del sujeto teniendo como opción mantenerse equilibrado bajo un esquema de resiliencia, o bien, quebrantarse en su integridad total para hacer lo que pretende el torturador.

---

17 Echeburúa, E., Corral P. y Amor P.J. (2004) La evaluación de daño psicológico en víctimas de delitos violentos. Psicopatología Clínica y Legal. Volumen 04, retomado de http://masterforense.com/pdf/2004/2004art19.pdf.PP28

Ésto aunado a los datos aportados por las investigaciones epidemiológicas de Benjamín Vicente y sus colegas de la Universidad de Concepción, originadas en muestras representativas, revelan que las tasas de prevalencia de los trastornos psiquiátricos en la población mayor a 15 años, oscila de un 32% a un 42%, de 6 meses desciende a un 70 %. Argumento que da mayor soporte a lo citado respecto de las consecuencias clínicas, que si bien en la mayoría de los casos está presente, éste no va a ser una constante.

También se debe de considerar que a largo plazo las **consecuencias más que clínicas de la tortura tendrán un impacto a nivel comunidad** (como individuo, parte de la sociedad) como individuo desestructurado psíquicamente que no será funcional, con una familia ya de por sí desestructurada como en la mayoría de los casos que se tiene registro y se han atendido, por el tiempo que pasan en prisión y profundos daños a nivel de salud mental comunitaria por los estragos que la tortura tiene y de quien ejerce.

En resumen, la desconfianza a los cuerpos policíacos por dichos actos van a pasar de generación en generación por lo que de no atenderlos tendremos como consecuencia el debilitamiento del Estado y el deterioro de la sociedad en su conjunto.

De este modo, desde el punto de vista del enfoque clínico y enfatizando el psicosocial, se busca no causar (nuevo) daño, y se responda tanto a las dinámicas individuales y comunitarias, en el mismo nivel de importancia. Se propone integrar acciones que van de lo emocional y lo relacional bajo una comprensión desde el contexto y reconocimiento del daño provocado por el conflicto, como se procura en las sentencias internacionales, a modo de reparación integral de daño; es así como se debe valorar psicológicamente a la tortura y los malos tratos desde una perspectiva clínica, en razón de la fecha de los hechos pero acompañada del enfoque psicosocial y transgeneracional para entender al fenómeno de la tortura en México desde su total amplitud.

Ahora bien, respecto del perfil de quien comete la tortura, se ha comentado en diversos foros que abordan la investigación de la tortura acerca de una patologización del individuo que lo comete, es decir, que puede tratarse de una persona que atraviesa por una psicopatía.[20] No obstante, se puede decir que no es así, pues la tortura puede ser ejecutada por cualquier persona.

---

18 Madariaga, C. (2002), Trauma Psicosocial, Trastornos de Estrés postraumático y Tortura. Santiago de Chile: Editorial Cintras, Serie Monografías, pp 3

19 Anacona, 2014, pp 14 citado por Virseda-Heras JA., Villanueva López Juan Miranda Salazar Ma. A. y Cols (2018) perspectiva psicosocial de los Derechos Humanos, publicado y editado por la Universidad Autónoma del Estado de México. México. pp 99.

Razones por las cuales cualquier servidor público está en posibilidad de ejecutar actos como la tortura sin tener que atravesar por un trastorno mental de tipo psicótico y en relación a que estos actos no generan remordimientos de consciencia como lo han expresado las víctimas de la tortura, realmente no hay estudios profundos a nivel cognitivo con perpetradores de la tortura que permitan afirmar esto, pero si se puede sostener con los puntos establecidos en el párrafo anterior.

Es hasta el año 2015, 3 años después de haber comenzado su operación que la extinta División Científica comienza a estudiar el fenómeno de la tortura desde el ámbito de la medicina legal. Posteriormente, en ese año se comienza a colaborar en el área de psicología en la aplicación de dicho protocolo, con tres casos y la participación de dos psicólogas, sin mayor referencia que las directrices del Protocolo de Estambul. Para el año 2016, se recibe un mayor número de solicitudes en el tema, obligando a la entonces División Científica a sumar personal capacitado en el tema ante la demanda de las autoridades para coadyuvar en la documentación de denuncias de tortura, así como de su investigación en atención a las directrices que establece el protocolo, citadas a continuación:

a) ¿Hay una concordancia entre los signos psicológicos y la denuncia de tortura?
b) ¿Se puede decir que los signos psicológicos observados constituyen reacciones esperables o típicas frente a un estrés extremo dentro del contexto cultural y social del individuo?
c) Considerando la evolución fluctuante con el tiempo de los trastornos mentales relacionados con traumas, ¿Cuál sería el marco temporal en relación con los hechos de tortura? ¿En qué punto del proceso de recuperación se encuentra el sujeto?
d) ¿Cuáles son los factores de estrés coexistentes que afectan al sujeto (por ejemplo, una persecución, migración forzada, exilio, pérdida de la familia o pérdida de la función social)? ¿Qué repercusiones tienen estos factores sobre el sujeto?
e) ¿Qué condiciones físicas contribuyen al cuadro clínico? Merecen especial atención los traumatismos craneales sufridos durante la tortura o la detención.
f) ¿Hace pensar el cuadro clínico que la denuncia de tortura es falsa?

20 Trastorno de personalidad caracterizado por falta de afecto, sentimientos, remordimientos, así como empatía y seducción, para terceros basados en manipulación y utilización.21 Asamblea General de las Naciones Unidas, (2017), Informe del Relator Especial sobre la Tortura y otros tratos o penas crueles inhumanos o degradantes, A/HRC/34/54 Add.4 en México.
21 Asamblea General de las Naciones Unidas, (2017), Informe del Relator Especial sobre la Tortura y otros tratos o penas crueles inhumanos o degradantes, A/HRC/34/54 Add.4 en México.

Bajo una metodología científica que ha permitido la implementación de buenas prácticas en psicología forense, basadas en el protocolo de actuación de la materia, jurisprudenciales, en aproximaciones fenomenológicas, dejando de lado los sesgos ideológicos, reflejando así un documento resultado de la aplicación del Protocolo de Estambul meramente ético-científico sin sesgos.

Basados en el pensamiento crítico, las y los expertos que participan en la aplicación del citado protocolo son considerados especialistas en su materia, puesto que cuentan con una capacitación idónea, misma que por sus características, contribuye con información médico-psicológica que permite a los operadores de justicia llegar a conclusiones certeras, basados en la metodología científica en los casos de tortura que se investigan.

Es importante recalcar que la temporalidad de las denuncias de tortura en México, subsisten en períodos que van de los 5 y hasta los 15 años, esto en consideración a que, si bien existieron o existen aún indicios de lesiones físicas visibles, éstas se han desvanecido casi por completo o en su caso ya son inexistentes; ante esto la importancia de que en el ámbito de la psicología permita documentar con la metodología referida las probables secuelas profundas que dejaron estos hechos de tortura así como documentar las afectaciones de tipo psicosocial.

En síntesis, la importancia que retoma el área de psicología en la investigación de la tortura cobra relevancia desde la historicidad de la tortura en el sistema anterior de justicia (por los procesos administrativos y de desahogo que conllevan), además de que la mayoría de las denuncias que se atienden se dan en ese ámbito o por llamarlo así en ese sistema.

Ahora bien en el área médica, el dictamen emitido por el área de Medicina Legal, se fundamenta en la consistencia encontrada en todas las fuentes de información solicitada (declaraciones tanto ministeriales, como iniciales y preparatorias, ampliación de declaración, puestas a disposición, dictámenes previos de Protocolo de Estambul u otros como los de mecánica de lesiones, exámenes de integridad física, notas médicas anteriores y actuales). Lo anterior con el propósito de corroborar el estado de salud, interconsultas de alguna especialidad, relato de hechos de la víctima, hallazgos físicos obtenidos de la exploración física, literatura médica, solo en caso de considerarlo conveniente el perito médico solicitará exámenes de gabinete.

Párrafo 287. Para formular una opinión clínica a fin de informar sobre signos psicológicos de tortura, deben formularse las siguientes preguntas importantes, del Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes

Este procedimiento permite documentar de manera eficaz denuncias de tortura, respecto de la medicina legal como lo son: las señales físicas de la tortura referidas en el Capítulo V, basadas en aspectos como la evaluación de las formas específicas de tortura, como son: traumatismos por objetos contundentes, golpes en los pies, suspensión, torturas de posición, tortura por choques eléctricos, tortura dental, asfixia, tortura sexual, incluida la violación.

Historial médico: integra la semiología que consiste en el estudio de signos y síntomas que llevan a establecer lo que la persona padece, su aplicación reside en el examen físico.

El examen físico:

1. La piel
2. La cara que comprende los ojos, oídos, nariz, mandíbula, orafaringe y el cuello, la cavidad bucal y los dientes.
3. El tórax y el abdomen.
4. El sistema musculo esquelético.
5. El sistema genitourinario.
6. Sistemas nerviosos central y periférico.

También se toman en cuenta las directrices del Protocolo de Estambul contenidas en un apartado de anexos que incluyen: los principios relativos a la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes, pruebas de diagnóstico y dibujos anatómicos para documentar la tortura y los malos tratos.

Como último tópico, las adversidades que se presentaron en el desahogo de cada uno de los casos que se atendieron como parte de la antigua División que permitieron implementar un mecanismo que procurara el respeto a los Derechos Humanos de las víctimas de tortura, entre los que destacan: entregar a las autoridades planes y cronogramas de trabajo que permitieran establecer a través de acuerdos, fechas de ingreso para los centros de internamiento, así como el material a utilizar, que garanticen una documentación efectiva de las denuncias de tortura atendiendo a las directrices de la Ley General para Prevenir, Investigar, y Sancionar la Tortura y Otros Tratos Crueles Inhumanos o Degradantes.

También se implementó el uso de bitácoras de trabajo como medio de protección del personal de la División y del propio evaluado, donde la función principal de esta bitácora era señalar los días que se aplicó el protocolo de Estambul, la hora y las condiciones por escrito, que permitió garantizar buenas prácticas y la no revictimización del denunciante.

IV. Metodología de Investigación de la Tortura con Perspectiva de Derechos

Se ha establecido que la tortura jurídicamente es una Violación Grave a los Derechos Humanos, como violación en específico a la Dignidad Humana que a nivel individual tiene impactos en la estabilidad psíquica de un sujeto y en segunda instancia a nivel físico (dependiendo de la intensidad en la que se ejerció) dejando secuelas irreparables basadas en un modelo ecológico[24] de análisis.

Tanto en materia de medicina como en psicología es menester seguir las directrices que marca el Protocolo de Estambul para una efectiva documentación de la Tortura y que éstas a su vez se vean reflejadas en el marco del método científico.

Porque justamente este último sirvió de base para las áreas de Psicología y Medicina de la División Científica, a efectos de emplearse en el dictamen resultante de la aplicación de dicho protocolo, específicamente con la Perspectiva de Derechos Humanos que ha permitido en diversos ámbitos de la ciencias sociales y forenses, la documentación efectiva de las Violaciones Graves a los Derechos Humanos.

Esta perspectiva de Derechos Humanos ha hecho aportes desde hace menos de una década a la investigación de las Violaciones Graves a los Derechos Humanos, por lo que se retoma como parte fundamental en el desahogo de las peticiones del Protocolo de Estambul en la Guardia Nacional, en razón de la cientificidad que merece el actuar de la Dirección General Científica, la cual consiste básicamente en tres directrices, la primera en la aplicación de protocolos, la segunda en una metodología científica y la tercera en un metanálisis.

1. El uso de protocolos: tiene que ver con el marco constitucional y las obligaciones del Estado en la investigación de violaciones graves a los derechos humanos en específico de la tortura, considerando de esta manera que la investigación de la tortura no sólo debe basarse en el manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes, sino retomar protocolos como el protocolo de actuación para quienes imparten justicia en asuntos que involucren hechos constitutivos de tortura y malos tratos de la Suprema Corte De Justicia de la Nación publicado en el año 2014, que de manera clara citan las actuaciones de los Juzgadores y Juzgadoras, Ministerios públicos y de los peritos como entes investigadores en el tema, así como los lineamientos en la investigación para el trato a la víctimas de tortura y reparación integral del daño.

2. Metodología Científica: la implementación de una metodología científica mediante el empleo e integración de mecanismos de análisis[23] y técnicas basadas en el análisis nomotético e ideográfico, los cuales consisten en comparar los hallazgos médicos y psicológicos con un conocimiento previamente establecido, que se puede agrupar en categorías privilegiando así el dato empírico, en segunda instancia se retoma al análisis ideográfico donde se pretende entender al individuo globalmente mediante el conocimiento intensivo e individual, en consideración a que cada caso es diferente y merece una atención individual basada en su propio contexto desde los ámbitos de la medicina forense como de la propia psicología forense.

3. Meta-análisis: este último está basado en retomar el punto anterior, desde diversos niveles de análisis, como lo son: 1) nivel técnico logístico (cómo se recoge la información) basado en literatura, y protocolos de actuación que derivan de buenas prácticas en ámbitos de medicina y psicología Forense; 2) nivel logico metodológico (cómo se interpreta la información) que deriva en el diseño de la evaluación o bien la propia estructura del dictamen; 3) nivel crítico meta analítico (cómo se auto cuestionan los resultados) este último, deriva de la integración de los dos primeros niveles que evitan la opinión con sesgos personales o ideológicos por parte del experto evaluador, respecto del fenómeno en este caso de la tortura, mirándola como resultado de una relación desigual de poder.

En resumen, estos tres aspectos que conforman la perspectiva de derechos humanos que atinadamente retoma la Guardia Nacional bajo la Dirección General Científica, sumada a las directrices del Protocolo de Estambul, han permitido una documentación eficaz de las denuncias de tortura, evitando basar los resultados en opiniones personales sesgadas por juicios ideológicos.

A nivel nacional la Guardia Nacional es la única institución que ha retomado e implementado este modelo para la investigación de la tortura y se pretende que por lo menos en ámbitos de estudios de comportamiento humano se implemente esta perspectiva de buenas prácticas, teniendo como resultado el mismo fenómeno de replica que tuvo en su momento la creación de la Policía Científica a nivel federación en México. En ese sentido se espera que el presente estudio sea una herramienta de difusión que permita a las demás instituciones replicar este conocimiento.

23. Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes. Protocolo de Estambul. Serie de capacitación profesional N° 8/Revi. capítulo V, secciones A, B, C Y D.

24. El modelo ecológico para comprender la violencia consiste en cuatro áreas; nivel sociedad, comunidad, familiar e individual. Olivares Ferreto E., Inchaustegui Romero T., (2011) Modelo ecológico para una vida libre de violencia Comisión Nacional Para Prevenir y Erradicar la Violencia contra las Mujeres, México.
Coronado Mares A., Cervantes Domínguez S. E. (20189), Niveles de análisis en la psicología forense, revista Forense, Número 1, México.

V. Conclusiones

Desde cualquier ámbito el fenómeno de la tortura es un acto deleznable, y como violación grave a los Derechos Humanos merece una atención integral por parte del Estado (prevenir, investigar y sancionar), entonces es así, que la Dirección General Científica de la Guardia Nacional en el marco de sus atribuciones, coadyuva en la investigación mediante la aplicación de dicho protocolo, superando el devenir histórico que le ha permitido convertirse en la única institución policial a nivel Latinoamérica que investiga la tortura mediante la aplicación directa del Protocolo de Estambul, logrando especialización en sus elementos no por la cantidad de casos que se atendieron, sino, por la cientificidad que aportaron los dictámenes emitidos y las metodologías empleadas.

En específico, uno de los hallazgos importantes al aplicar dicho protocolo en materia de Psicología fue que desde un entendimiento psicosocial, se valoró el trauma resultante de la tortura y no desde una perspectiva meramente clínica con la finalidad de evitar la revictimización de las personas evaluadas; es decir, se tomó en consideración los años que habrían transcurrido desde la denuncia de tortura hasta la fecha en que se entrevistó al denunciante de tortura, lo que permitió profundizar a conocer el fenómeno de la tortura en México, marcando pautas así para la investigación de la tortura desde una perspectiva de Derechos Humanos (uso de protocolos de actuación y metodología científica).

La perspectiva citada, ha permitido investigar los fenómenos de violaciones graves a los Derechos Humanos como se ha citado anteriormente, y en este caso el de la tortura, bajo estrictas categorías de análisis que permitirán evitar sesgos en las investigaciones periciales coadyuvando con las y los juzgadores a visualizar a la tortura e impartir justicia de conformidad con el marco jurídico aplicable, sumado ello a que las y los expertos que participan en la aplicación del citado protocolo, son considerados especialistas en su materia cada uno, puesto que cuentan con una capacitación idónea en la misma.

Es de conocimiento público que a finales del 2020 figura la publicación de la versión actualizada del Protocolo de Estambul, lo que sin duda será un aporte significativo a la documentación de las denuncias de tortura, y quizás sea positivo pensar en un proceso de "actualización" del protocolo cada cierto periodo de tiempo, permitiendo delimitar cada vez más los sesgos que obstaculicen visualizar los actos de tortura en contextos regionales de cada país, como México que es un país multicultural que dentro de su marco jurídico visualiza a grupos vulnerables específicos y el trato que se debe tener con cada uno de estos.

Así mismo, es importante resaltar que se deben de aplicar los conocimientos adquiridos, como en este caso lo es la perspectiva de Derechos Humanos y que ello siga garantizando una eficaz documentación de denuncias de tortura mediante la aplicación del Protocolo de Estambul, aportando cientificidad a la investigación más que un desahogo de mandamientos.

De entre los aportes más significativos de la Guardia Nacional a través de su Dirección General Científica, destaca la investigación de la tortura con la aplicación del Protocolo de Estambul, más sobre todo se resalta porque dentro de esta aportación la implementación de la perspectiva de Derechos Humanos en el desahogo de los dictámenes colegiados.

En atención al conjunto de argumentos presentados, se puede establecer que el retomar esta perspectiva, de manera eficaz y científica ha permitido generar acciones en pro de la erradicación de esta violación grave a los Derechos Humanos, retomando el lema de la Guardia Nacional, Justicia. Este aporta elementos para que las víctimas verdaderamente estén en posibilidad de accesar a la justicia.

LA IMPORTANCIA Y OBTENCIóN DE LA E VIDENCIA DIGITAL

Primer Subinspector GN, Lic. Víctor Agustín Jiménez Juárez[1]

Sumario: I. Introducción. II. La Prueba digital. III. El proceso de obtención de la prueba digital. IV. La responsabilidad del perito. V. consideraciones y metodología aplicada para el procesamiento y obtención de pruebas digitales. VI. El lugar de los hechos. VII. La importancia de la obtención de la prueba digital durante la diligencia de cateo.

I. Introducción

A partir de que la tecnología es parte del día a día, se ha hecho indispensable disponer de ella para todas las acciones que denominamos "comunes" y que realizamos con solo tener un teléfono celular a la mano, desde revisar las noticias por la mañana, realizar pagos de servicios en línea, compras, entre otras prácticas cotidianas.

El avance tecnológico ha sido tal que actualmente, los aparatos electrodomésticos cuentan con una conexión a internet, por lo que ahora estos dispositivos almacenan datos confidenciales que la mayoría de las personas aporta de manera automática, sin considerar que individuos malintencionados con conocimientos cibernéticos, pueden cometer delitos utilizando los medios electrónicos que usamos a diario y a través de la red, suplantar la identidad y tener acceso a sus cuentas bancarias obteniendo beneficios económicos de manera ilegal, incitar a jóvenes y adultos a realizar actos indebidos como fotografías o videos íntimos y ocupar estos archivos para extorsionar a los usuarios y exigirles un pago.

Lo cierto es que siempre quedan rastros digitales, los cuales se pueden buscar y preservar mediante técnicas especializadas y procesos forenses que personal capacitado y entrenado en investigación y forensia digital, rastrea aplicando los protocolos para que no puedan ser manipulados o alterados con el objetivo de ser presentados como un indicio, para que sean evaluados por las autoridades competentes y convertirse en evidencia que vincule al presunto responsable con el delito cometido ante las autoridades competentes, atendiendo en todo momento al debido proceso.

[1] Licenciado en Ciencias de la Informática, egresado del Instituto Politécnico Nacional. Con 17 años de servicio en seguridad pública enfocados a la investigación de delitos electrónicos.

Aquí se plasma la importancia de las evidencias digitales en los procesos legales y brinda una guía que puede ser utilizada por los expertos encargados de investigar los delitos cibernéticos (en general aplica para cualquier delito donde se haya utilizado un dispositivo electrónico como herramienta u objetivo para su comisión) en distintas situaciones, tales como el lugar de los hechos durante un cateo.

II. L a prueba digital

Si bien es cierto que en los Códigos Penal Federal y el Nacional de Procedimientos Penales no se hace ninguna distinción especial para los indicios electrónicos y para las pruebas digitales, si lo hace de manera general al referirse a ese universo de evidencias como "prueba", la clave para no chocar con el formalismo jurídico es un conjunto de habilidades con las que deberán contar aquellos operadores del Sistema de Justicia Penal que en algún momento tengan conocimiento o contacto con material electrónico y digital.

Hoy en día la mayor cantidad de información existente está en formato digital, y aunque no todos los intercambios de información se realizan por medio de la red, esto no impide que esta información pueda ser puesta en las manos de la fiscalía o del juez.

Es de señalar que el experto en la materia tiene la responsabilidad de obtener pruebas digitales siempre apegado a la legalidad, con respeto a los derechos de las personas y métodos que garanticen la mismidad y la integridad de la información presentada ante la autoridad que la requiera.

Aunado a lo anterior, al ser los indicios digitales la materia prima de los peritos, misma que se encuentra en medios electrónicos que los expertos identifican, fijan, recolectan y analizan en la búsqueda de la verdad, es menester señalar que poseen las siguientes características:

A) Volátil. La evidencia desaparece con el tiempo, ya sea como resultado de la actividad normal del sistema o como resultado de los actos de los usuarios.

En cada paso está la posibilidad de destruir la información, por lo que todas las medidas de identificación, recolección, obtención, etc., que tomen, deben ser bien aplicadas desde el primer contacto o se puede perder mucha información valiosa para la investigación.

Es importante que no se busque información en áreas que normalmente no tienen razón alguna para ser consultadas (como archivos personales) a menos que se haya notificado al usuario (por ejemplo, a través de un banner de inicio de sesión) que toda la información almacenada en el equipo es objeto de

embargo o si se tienen razones suficientes para creer que un incidente de seguridad está ocurriendo o ha ocurrido.1

B) Confidencial. Cada persona es dueña de la información que se encuentre almacenada en sus dispositivos y de igual manera es responsable de ésta, y toda vez que se presume que la mayoría de los dispositivos almacenan información, también podrían almacenar de manera total o parcial algún tipo de comunicaciones, por lo que estos se encuentran protegidos por la ley.

En este sentido, dado que las comunicaciones están protegidas por la ley estas no pueden ser intervenidas sin una orden judicial o por aportación de la parte afectada, los fiscales tienen la responsabilidad de realizar estas peticiones de forma similar a una orden de cateo.

Es necesario resaltar las excepciones, verbigracia, el Principio del Interés Superior de las Niñas, Niños y Adolescentes, en dicho caso los jueces están facultados para emitir una autorización de intervención de comunicaciones privadas, siempre que la vida o seguridad de un menor se encuentra comprometida.

C) Duplicable. Es el caso que cualquier usuario con los conocimientos básicos en informática podría crear una copia de un archivo o clonar alguna unidad de almacenamiento masivo, esto tiene dos aristas, una es que la misma persona podría tener un sin número de copias de un archivo o de dispositivos completos. La otra posibilidad es que exista un archivo que viole las normas (ejemplo pornografía infantil) y éste se esté diseminando en la red, por lo que estaríamos frente a una multiplicidad de infractores.

D) Es alterable y modificable. Un archivo digital puede ser promovido como una prueba, ya sea documental o de comisión de una conducta. El uso de la tecnología digital se puede apoyar en el sistema de prueba libre, ampliamente difundido en los procesos civiles y penales iberoamericanos, y es una excelente opción de procedencia y conducencia; por ejemplo, en una imagen digital, se debe tomar en cuenta su pertinencia.

Los problemas de validez de la imagen digital en razón de su supuesta facilidad de manipulación, no son suficientes para que se presuma que todas las fotografías digitales no puedan tener validez en juicio. El que alegue la falsedad de una fotografía digital deberá probarlo o solicitar se investigue su autenticidad, a efecto de que sea factible probar una identidad o un acto.

[1] http://informaticaforenseunadcd.blogspot.mx/p/recoleccion-de-evidencia-digital.html

Estas características advierten sobre la exigente labor que se requiere por parte de los peritos en el desarrollo de las actividades relacionadas a la recolección y análisis de información sin ser alterada, contenida en los dispositivos de almacenamiento electrónico.

En ese orden de ideas y considerando la fragilidad de los insumos, es de destacar que los archivos digitales pueden ser alterados o modificados con relativa facilidad, cambiando fechas de creación, el propietario del archivo, ruta de almacenamiento, entre otros aspectos. Tales datos se conocen como metadatos (consiste en toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad) [1] y es una parte del archivo en donde se almacenan características y propiedades específicas de un archivo.

Una de las formas en las que se puede verificar la autenticidad de un archivo es la firma HASH, y es que todo archivo digital tiene características únicas, es decir, puede ser individualizado o diferenciado de cualquier otro. El método más común es el algoritmo matemático llamado MD5, el cual es capaz de generar una vez aplicado a un archivo digital una especie de firma digital única, lo que hace que ésta sea tan precisa como la huella dactilar humana.

III. El proceso de obtención de la prueba digital

Sirve para auxiliar a las autoridades competentes en la identificación y aseguramiento de dispositivos electrónicos que pudieran estar relacionados con la comisión de un hecho que se investiga, está supeditado a la solicitud que el Ministerio Público realice al Juez; consecuentemente, también de lo que este último autorice en los considerandos y resolutivos de la orden de cateo, es decir, si el fiscal realizó una solicitud de cateo y si ésta se emitió con o sin autorización de intervención de comunicaciones (en el entendido de que esta medida cautelar se haya promovido con el objeto de localizar dispositivos electrónicos o evidencias digitales).

Asimismo, se deberá observar que las actividades que realizará el perito, autorizadas por el juez, sean compatibles con la especialidad que se sustenta; en este caso, usando como ejemplo un cateo donde se localizarán, identificará, analizarán y levantarán dispositivos electrónicos.

En la Guía Nacional de Cadena de Custodia publicada el 28 de octubre de 2015, existen etapas y actividades que resultan muy específicas al momento de intervenir en una diligencia de cateo, estas etapas son:

[1] Metadatoshttps://www.opengeekservice.cl/sitio/es/blog/67-%C2%BFqu%C3%A9-son-y-paraqu%C3%A9-sirven-los-metadatos.html

1. Procesamiento

Es la etapa en la cual, el Policía con Capacidades para Procesar y, en su caso, el perito, detecta, preserva y conserva los indicios o elementos materiales probatorios; ésta inicia con la localización, descubrimiento o aportación y concluye con la entrega a la autoridad responsable de su traslado.

Durante el procesamiento se llevará a cabo la identificación, documentación, recolección y embalaje de los indicios o elementos materiales probatorios, a cargo de los Peritos y Policías con Capacidades para Procesar; según sea el caso, éstos podrán llevar a cabo las siguientes actividades elementales:

a. La observación, identificación y documentación de los indicios o elementos materiales probatorios, será mediante la observación ordenada, minuciosa, exhaustiva, completa y metódica, realizada a través de la aplicación de técnicas de búsqueda. Para la identificación, se asignará un número, letra o combinación de ambos, el cual será único y sucesivo.

   Asimismo, se deberá llenar la documentación correspondiente, antes, durante y después de aplicar las técnicas en cada etapa del procesamiento, a través del uso de diversos métodos y técnicas, tales como el fotográfico, el croquis general y a detalle, el escrito, entre otros.

   Con el propósito de individualizar la información relacionada con las características de los indicios o elementos materiales probatorios, en el lugar de la intervención, se deberá llenar el formato de Registro de Cadena de Custodia.

b. La recolección, embalaje, sellado y etiquetado de los indicios o elementos materiales probatorios, se realizará de forma manual o instrumental, de acuerdo con su tipo, con el propósito de garantizar su integridad, autenticidad e identidad.

   Posteriormente, se embalarán en contenedores o recipientes nuevos, de forma individual, salvo aquellos casos en que se pueda agrupar por tipo o naturaleza, finalizando con el sellado, etiquetado y firma del responsable del procesamiento.

   Todos los indicios, evidencias, objetos, instrumentos o productos del hecho delictivo, que tengan relación con el hecho que se investiga, entrarán en el Registro de Cadena de Custodia.

   La recolección, embalaje, sellado y etiquetado, a que se refiere este apartado, se realizará en los bienes, objetos o instrumentos producto del hecho delictivo, de conformidad con la naturaleza de los mismos.

Para su constancia, se elaborará un acta de inventario de bienes, después de que sean examinados, fotografiados o video grabados, siguiendo las reglas del Código Nacional de Procedimientos Penales, respecto al aseguramiento.

c. El inventario y recomendaciones para el traslado de los indicios o elementos materiales probatorios, se realiza por el Perito o la Policía con Capacidades para Procesar, previo al traslado, con el propósito de contabilizar y asegurar que los indicios o elementos materiales probatorios, estén documentados en el formato de Registro de Cadena de Custodia y en el Formato de Entrega-Recepción de Indicios o elementos materiales probatorios.

De ser el caso que el Perito o la Policía con Capacidades para Procesar, se encuentren imposibilitados para realizar el traslado, éstos emitirán las recomendaciones para el manejo y traslado de los indicios o elementos materiales probatorios, al Personal Facultado para el Traslado (PFT), con el fin de garantizar la integridad de éstos.

En las recomendaciones que se emitan al PFT, al menos, se deberán establecer las condiciones para el manejo de los indicios o elementos materiales probatorios, destino, condiciones ambientales y el tipo de transporte que corresponde emplear.

Una vez llevadas a cabo estas actividades elementales, los Peritos o la Policía con Capacidades para Procesar y el PFT, deberán llevar a cabo las siguientes acciones de verificación y control de la Cadena de Custodia:

a) Verificar que el embalaje de los indicios o elementos materiales probatorios, se encuentre debidamente sellado, etiquetado y firmado.
b) Cotejar la información de la etiqueta del embalaje, con la información del registro en el acta correspondiente, para que los datos asentados correspondan entre sí.
c) Revisar que se cuente con la documentación de los indicios o elementos materiales probatorios (escrita, fotográfica y croquis simple y a detalle).
d) Llenar el Registro de Cadena de Custodia por indicio, salvo aquellos casos en que sea estrictamente necesario agrupar por tipo o naturaleza, el cual, lo acompañará en todo momento, debiendo contener los siguientes datos:

- Identificación.
- Documentación.
- Recolección y traslado.
- Servidores públicos que intervinieron en el procesamiento.
- Tipo de traslado.
- Continuidad y trazabilidad.

e) Cuando un indicio o elemento material probatorio, se pierda, altere, destruya o contamine, el interviniente anotará dicha circunstancia en el apartado de observaciones del Registro de Cadena de Custodia, e informará de manera inmediata al Ministerio Público.

2. Traslado

Esta etapa es materializada por el Perito o la Policía con Capacidades para Procesar, en caso de que éstos se encuentren imposibilitados para realizar el traslado, podrán encomendarlo al PFT. Quien lleve a cabo el traslado, tiene como encomienda, transportar los indicios o elementos materiales probatorios, debidamente embalados, sellados, etiquetados, firmados y con el Registro de Cadena de Custodia del lugar de intervención hacia los servicios periciales, a la bodega de indicios, a las Instituciones que cuenten con áreas forenses, o a algún otro lugar con condiciones de preservación o conservación, en cumplimiento a las recomendaciones de los especialistas, previo conocimiento del Ministerio Público[4].

Durante esta etapa, quien realice el traslado documentará sus acciones, para tal efecto empleará los formatos de entrega-recepción de los indicios o elementos materiales probatorios y el Registro de Cadena de Custodia.

Cuando por causas de fuerza mayor, no puedan trasladarse los indicios o elementos materiales probatorios a la brevedad, hacia los servicios periciales, a la bodega de indicios, a las Instituciones que cuenten con áreas forenses, o a algún otro lugar con condiciones de preservación o conservación, éstos deberán ser canalizados a almacenes temporales para su almacenamiento transitorio, informando de ello al Ministerio Público.

Tan pronto cesen las causas que ocasionaron el impedimento y, se reúnan las condiciones logísticas necesarias, se realizará el traslado al lugar destinado, según corresponda, conforme a la naturaleza de la investigación

Quien realice el traslado (Perito, Policía con Capacidades para Procesar o PFT), deberá llevar a cabo las siguientes acciones, para la verificación y control de la Cadena de Custodia durante el traslado:

[4] Guía Nacional de Cadena de Custodia, Versión 1.0, p.p. 20 -23

f) Verificar que el embalaje de los indicios o elementos materiales probatorios, se encuentre debidamente, sellado, etiquetado y firmado;
g) Cotejar la información de la etiqueta del embalaje, con la información del registro en el acta correspondiente, para que los datos asentados correspondan entre sí;
h) Registrar los ingresos y salidas de la bodega temporal, en su caso;
i) Requisitar las actividades relacionadas con la continuidad y trazabilidad de los indicios o elementos materiales probatorios, en el formato de Registro de Cadena de Custodia, y
j) Cuando un indicio o elemento material probatorio se pierda, altere, destruya o contamine, anotará dicha circunstancia en el apartado de observaciones del Registro de Cadena de Custodia, e informará de manera inmediata al Ministerio Público[5].

3. Análisis

Es la etapa en la que se realizan los estudios a los indicios o elementos materiales probatorios, con el fin de determinar sus características relevantes para la investigación.

Cuando el análisis se lleve a cabo en los laboratorios de servicios periciales o instituciones con áreas para el análisis forense, el perito o especialista deberá iniciar con la recepción y registro de los indicios o elementos materiales probatorios, continuará con el estudio correspondiente y con la emisión del dictamen, informe o requerimiento y finalizará con la entrega de éstos para el traslado a la bodega de indicios, o a algún otro lugar con condiciones de preservación o conservación.

Si al finalizar el análisis, se advierte remanente o se haya consumido la muestra, el perito o especialista deberá realizar la anotación correspondiente en el rubro de observaciones de continuidad y trazabilidad, del registro de Cadena de Custodia.

Cuando los estudios se realizan en campo, el perito o la Policía con Capacidades para Procesar, iniciarán con la recolección de datos de los indicios o elementos materiales probatorios, continuarán con los estudios que se aplican a éstos y terminarán con la emisión del dictamen, informe o requerimiento y, en su caso, con la devolución del bien, con autorización de la autoridad competente.

En esta etapa, el personal que realiza el análisis deberá utilizar el equipo de protección personal.

[5] Guía Nacional de Cadena de Custodia, Versión 1.0, p.p. 23 y 24

Cuando el personal de Servicios Periciales o instituciones con áreas para el análisis forense, reciba los indicios o elementos materiales probatorios, se realizarán las siguientes actividades elementales:

a) Análisis o estudio. Se llevará a cabo de conformidad con la solicitud efectuada por el Ministerio Público, de acuerdo a sus atribuciones y facultades.

Cuando se realice un peritaje sobre objetos que se consuman al ser analizados, no se permitirá que se verifique el primer análisis, sino sobre la cantidad estrictamente necesaria para ello, a no ser que su existencia sea escasa, y los peritos no puedan emitir su opinión sin consumirla por completo.

Éste último supuesto o cualquier otro semejante que impida que con posterioridad se practique un peritaje independiente, deberá ser notificado por el Ministerio Público al Defensor del imputado, si éste ya se hubiere designado o al defensor público, para que, si lo estima necesario, los peritos de ambas partes, y de manera conjunta practiquen el examen, o bien, para que el perito de la defensa acuda a presenciar la realización del peritaje.

Los indicios o elementos materiales probatorios, sólo permanecerán en custodia temporal en servicios periciales o en las instituciones con áreas para el análisis forense, el tiempo estrictamente necesario para su análisis y, posteriormente, se procederá a su traslado a la bodega de indicios o a cualquier otro lugar con condiciones de conservación o preservación, con autorización del Ministerio Público.

b) Elaboración del informe, requerimiento o dictamen. Concluido el análisis, deberá remitirse a la autoridad solicitante.
c) Entrega de los indicios o su remanente. Deberán entregarse, debidamente embalados, sellados y etiquetados, hasta que se concluyan los estudios solicitados, con el registro de Cadena de Custodia correspondiente, a la autoridad responsable de su traslado, o en su caso, remitirlos a la bodega de indicios o a algún otro lugar con condiciones de preservación o conservación.

Toda persona que tenga contacto con el indicio o elemento material probatorio, debe dejar constancia de su actividad o propósito, en el apartado de "continuidad y trazabilidad" del registro de Cadena de Custodia correspondiente.

Durante esta etapa, el personal responsable del análisis deberá considerar como acciones de verificación y control de la Cadena de Custodia, las siguientes:

a. Verificar que los registros de Cadena de Custodia acompañen a los indicios o elementos materiales probatorios, y documentar cualquier cambio o alteración en el embalaje o en su contenido, e informar al Ministerio Público.
b. Verificar que el embalaje de los indicios o elementos materiales probatorios, se encuentre debidamente, sellado, etiquetado y firmado.
c. Al romper el embalaje, cerciorarse de que el contenido se encuentre íntegro, y cotejar que el contenido de la etiqueta, es el mismo del registro de Cadena de Custodia.
d. Cerciorarse de que se hayan observado las consideraciones de conservación o preservación requeridas por los especialistas que lo procesaron, en su caso;
e. Cotejar la información de la etiqueta del embalaje, con la información del registro en el acta correspondiente, para que los datos asentados correspondan entre sí;
f. Tratándose de peritajes irreproducibles, se estará a lo dispuesto por el artículo 274 del Código Nacional de Procedimientos Penales.
g. Requisitar las actividades relacionadas con la continuidad y trazabilidad de los indicios o elementos materiales probatorios, en el registro de Cadena de Custodia.
h. Cuando un indicio o elemento material probatorio se pierda, altere, destruya o contamine, anotará dicha circunstancia en el apartado de observaciones del registro de Cadena de Custodia, e informará de manera inmediata al Ministerio Público.

El personal responsable del análisis, empleará los formatos de registro de Cadena de Custodia, entrega-recepción de los indicios o elementos materiales probatorios, para documentar su actuación.[6]

4. Almacenamiento en la Bodega de Indicios

En esta etapa no ahondaremos en virtud de que esta actividad es propia del personal de las fiscalías que se encuentra adscrito a estas áreas de resguardo o también llamadas Bodegas de Indicios.

5. Presentación de los indicios o elementos materiales probatorios a juicio

Esta etapa tiene como propósito, llevar a cabo la presentación de indicios o elementos materiales probatorios ante el órgano jurisdiccional, como prueba

material a solicitud de las partes, e inicia con la salida de éstos de la bodega de indicios o del lugar donde se encuentren resguardados, con el propósito de ser incorporados en juicio, para posteriormente, ser reingresados a la bodega y finalmente se realice su determinación judicial.

En la presentación de los indicios o elementos materiales probatorios ante el órgano jurisdiccional, participa quien haya realizado el traslado (Perito, Policía con Capacidades para Procesar o Persona Facultada para Traslado).

Para la presentación de los indicios o elementos materiales probatorios, se deberá realizar lo siguiente:

a) El Ministerio Público instruirá al perito, Policía con Capacidades para Procesar o PFT, realizar el traslado de los indicios o elementos materiales probatorios al órgano jurisdiccional; posteriormente, el responsable del traslado, los depositará y resguardará en el lugar correspondiente, quien requisitará el rubro de continuidad y trazabilidad del registro de Cadena de Custodia.
b) Para la presentación de los indicios o elementos materiales probatorios en audiencia, cualquiera de las partes, de ser el caso, podrán solicitar al Juez, la interrupción de la Cadena de Custodia. Una vez exhibido, por solicitud de la parte correspondiente, el indicio o elemento material probatorio, regresa a la bodega de indicios o a algún otro lugar, para su resguardo, hasta su destino final y por ende la conclusión de la Cadena de Custodia.

En esta etapa se llevarán a cabo las siguientes acciones para la verificación y control de la Cadena de Custodia.

a. Verificar que los registros de Cadena de Custodia, acompañen a los indicios o elementos materiales probatorios, y documentar cualquier cambio o alteración en el embalaje, o en su contenido e informar al Ministerio Público;
b. Verificar que el embalaje de los indicios o elementos materiales probatorios, se encuentre debidamente, sellado, etiquetado y firmado;
c. El Ministerio Público, deberá cerciorarse de que se hayan observado las consideraciones para el traslado requeridas por los especialistas que lo procesaron, en su caso.
d. El Ministerio Público y el responsable del traslado, deberán cotejar la información de la etiqueta del embalaje, con la información del registro

en el acta correspondiente para que los datos asentados correspondan entre sí.

e. El responsable del traslado, deberá requisitar las actividades relacionadas con la continuidad y trazabilidad de los indicios o elementos materiales probatorios, en el registro de Cadena de Custodia.

f. Cuando un indicio o elemento material probatorio se pierda, altere o destruya, el responsable del traslado anotará dicha circunstancia en el apartado de observaciones del registro de Cadena de Custodia y deberá informarlo de manera inmediata al Ministerio Público.

g. El responsable del traslado deberá registrar la conclusión de la Cadena de Custodia, en el apartado de observaciones del rubro de continuidad y trazabilidad del registro de Cadena de Custodia, anexando el acuerdo o constancia correspondiente, por parte de la autoridad competente.

En esta etapa se emplearán los formatos de entrega-recepción de los indicios o elementos materiales probatorios y registro de Cadena de Custodia.

La disposición final de los indicios o elementos materiales probatorios, la determinará la autoridad competente, y podrá comprender alguno de siguientes supuestos: decomiso, devolución, destrucción, abandono, extinción de dominio o cualquier otro que determine la ley.

Para la instrumentación de cualquiera de los supuestos señalados en el párrafo anterior, se deberá atender la normatividad aplicable.[7]

El perito que acuda a la diligencia de Cateo podría participar en las etapas, con excepción del almacenamiento en la Bodega de Indicios ya que las bodegas pertenecen y son administradas por personal de las fiscalías que las posean. El objetivo principal es apoyar a las autoridades competentes en el correcto manejo y procesamiento de los dispositivos electrónicos para posteriormente realizar la extracción y análisis de información contenida en estos.

IV. **La responsabilidad del perito**

Un perito tiene dos responsabilidades: ante la sociedad, en razón de que como servidor público es parte importante y fundamental en el motor que mueve el sistema legal en el país, su habilidad, conocimientos y técnicas serán en todo momento las herramientas para auxiliar a establecer la verdad sobre un hecho o la relación que tiene una persona sobre este, no está por demás mencionar que en sus conocimientos está el camino hacia la verdad de un hecho.

Por otro lado, y no menos importante esta la responsabilidad legal que conlleva su investidura atento a que si realiza un buen trabajo nadie le dará una palmada, pero en caso contrario un mal manejo de indicios o evidencias, un procedimiento mal aplicado o unos resultados mal expresados, dejaran a la persona equivocada en el lugar equivocado, es decir, un inocente en reclusión o un culpable libre, esto sin mencionar las responsabilidades legales que esto implica *per se*.

V. Consideraciones y metodología aplicada para el procesamiento y obtención de pruebas digitales

El procesamiento de indicios electrónicos en una diligencia de cateo que se explica en el proceso mediante el cual se realiza un correcto procesamiento de indicios electrónicos y de las pruebas digitales, tomando todas las medidas necesarias para garantizar la integridad y mismidad[8] de éstos.

Cabe insistir en que la evidencia digital es muy frágil y puede perderse o modificarse con facilidad, aún por la simple inacción de quien tiene a su cargo el cateo o aseguramiento de los bienes, lo que implica la utilización de medidas especiales para su conservación en estado original, y con posterioridad esta pueda ser aportada como prueba válida en cualquier proceso penal.

Si la obtención de la evidencia digital en un proceso penal no es adecuada al cumplimiento de las garantías del debido proceso o afectan cualquier otro derecho constitucional, no podrían ser usadas en juicio en contra del sujeto activo, lo que aumentaría notablemente la impunidad que existe en materia de delitos informáticos o cometidos por medios informáticos, e incluso en delitos comunes donde la evidencia digital contenida en elementos electrónicos pudiere apoyar la investigación o el sentido condenatorio de la resolución judicial.

VI. El lugar de los hechos

Dado que el lugar de los hechos se define como "el espacio físico en donde se ha desarrollado un hecho probablemente delictivo, también denominado escena del crimen, escena del hecho, escenario del delito, siendo más recomendable citarlo como lugar de los hechos"[9]. Como primera medida, lo que se debe tener en cuenta es no alterar o perder ninguna de las evidencias en el lugar de los hechos, en atención a que sin importar que sean digitales o físicas, poder relacionar las mismas entre sí o, en su caso, poder hacerlo con el probable responsable.

---

7 Guía Nacional de Cadena de Custodia, Versión 1.0, p.p 28 y 39

8 Mismidad: Condición de ser uno mismo. REA. https://dle.rae.es/mismidad.

Es por ello que siempre se deben tomar las precauciones habituales de cualquier escena de crimen como, por ejemplo: procesamiento de los dispositivos electrónicos en el lugar de los hechos.

A. Observación: Inspeccionar el lugar de la intervención con la finalidad de identificar indicios electrónicos y ópticos que pudieran estar relacionados con el presunto hecho delictivo que se investiga. Una vez que se encuentra garantizada la seguridad del área, el paso a seguir es la observación y toma de fotografías generales del lugar.

B. Identificación: Fase en la cual se asigna un número, letra o una combinación de ambos, a los indicios electrónicos y ópticos, en el momento de su localización. Fije fotográficamente en primer plano, a detalle y en gran acercamiento para tener registro del estado y posición de los equipos, de sus puertos (conectores de cables, lectoras de cd, y cualquier otro punto de contacto del equipo con el exterior) y de igual manera de la pantalla en el estado en que se encuentre, con las debidas identificaciones, ya sea de marca, o cualquier otra que pueda dar certeza sobre el equipo, de ser posible es ideal poder tomar

C. Documentación: El registro fidedigno de la condición que guardan los indicios electrónicos y ópticos que se localizan en el lugar de los hechos o el hallazgo, señala la obligación de incluir la fijación fotográfica, planimétrica o video grabación, donde se especifiquen las características particulares de cada uno de los dispositivos electrónicos u ópticos, documentación que se debe entregar como anexos, esto debido a que no está incluido dentro de las acciones descritas en su dictamen.

El perito criminalista deberá realizar estas etapas con apoyo del perito en fotografía, de lo contrario si el perito está realizando el apoyo como perito en informática experto en forense digital puede realizar el plano del domicilio, este plano no requiere forzosamente estar a escala, sin embargo, si deberá estar lo más próximo a la realidad estructural del domicilio cateado.

a. Levante un croquis del domicilio, en especial de las habitaciones donde se encuentren los dispositivos electrónicos, realizando una descripción detallada de la ubicación de estos, y utilizando como referencia el norte geográfico.
b. Establezca la existencia de cámaras de video o de fotografía instaladas en el lugar de los hechos, para alcanzar plena certeza de la posibilidad de la obtención de pruebas adicionales de la relación usuario-equipo.

[9] Criminalística. Preservación y conservación del lugar de los hechos; Mtro. O. A. Román Contreras; México; año 2010

c. Pida a la autoridad que otorgue la intervención debida a los peritos en Dactiloscopia para que se pueda determinar la existencia de huellas dactilares sobre el equipo o bien, en su caso sobre los periféricos o soportes de cualquier índole que existan en el lugar de los hechos.

d. Una vez terminado el proceso de levantamiento de huellas dactilares, puede continuar la tarea del perito en informática.

A lo largo del proceso tiene prioridad el respeto a las normas vigentes y a los derechos humanos, para que de esta manera pueda otorgarse plena garantía de un correcto aseguramiento de la evidencia y de la imparcialidad de la misma, tanto como su integridad posterior.

Durante la duración de la diligencia es altamente recomendable tomar nota de las actividades realizadas desde la hora de llegada hasta la conclusión de la medida; así como tomar fotografía del estado de los equipos y sus componentes (centrales y periféricos) según ya se ha detallado en los pasos de aseguramiento del lugar de los hechos. D. Recolección:

Etapa donde se realiza el levantamiento del indicio electrónico u óptico, utilizando técnicas que garanticen su integridad; se deben tomar en cuenta las siguientes consideraciones: uso de pulsera y guantes antiestáticos, así como la descarga de energía estática del cuerpo humano a tierra.

Una vez que se hayan tomado las precauciones pertinentes se deberá identificar y levantar individualmente todos los medios de soporte (CD, tarjetas, memorias USB o cualquier otro según los listados anteriores) que se encuentren separados del equipo.

Verificar si los equipos se encuentran apagados o encendidos, si están apagados no se deben encender por ningún motivo, mientras que si están encendidos no se deben a pagar hasta contar con la fijación fotográfica.

Inmediatamente tomar fotografía detallada de la imagen de la pantalla, si se tratase de un protector de pantalla o el monitor estuviese en reposo, mueva lentamente el ratón hasta que aparezca la imagen del programa en proceso al momento anterior al inicio del ahorro de energía del equipo (únicamente se aconseja mover el ratón o la barra espaciadora dado que estos movimientos no suelen activar ningún proceso).

Asimismo, fotografiar inmediatamente la imagen de la pantalla que conexiones inalámbricas que pudieran ser fuente de acceso que pudieran modificar los contenidos.

Asentar inmediatamente en las actas de cateo la hora en que fueron realizadas las tres operaciones, es decir, la primera fotografía, el movimiento del ratón y la segunda fotografía de la pantalla. De igual manera se deben identificar las aplicaciones que se están ejecutando en segundo plano.

Si se encuentra encendido, se le debe primero aislar de intrusiones externas, para lo cual es necesario verificar la existencia de puertos de red o al encontrarse un cable de red o conexión inalámbrica, que en muchos equipos es interna por lo que no tendríamos acceso inmediato a la misma, se debe aislar de manera inmediata el equipo, precintando de manera inmediata las conexiones que se retiren a efecto de identificar todas las conexiones. Si se observa en el lugar de los hechos más de un equipo, es necesario identificar de manera clara cada uno de ellos con los identificadores correctos. Las fotografías deben ser claras y visible el número que se asigna a cada equipo y sus periféricos.

Es indispensable no desmontar o desconectar más de un equipo de manera simultánea, siempre bajo los procedimientos indicados en los puntos posteriores para evitar confundir las piezas o cables de cada uno de ellos.

Tampoco desconectar o retirar ningún periférico del equipo (CD, memoria USB, cables, tarjetas de memoria de cualquier tipo), sin la autorización previa de la autoridad competente, sólo fotografiar su posición y estado; una vez que obtenga la autorización podrá continuar, identificando cada uno por separado.

Una vez que se ha detectado que el equipo esta encendido, con la autorización necesaria de la autoridad, ya que para manipular el equipo se requiere de la orden expresa del juez de control, se procede a la extracción original de datos de la memoria de acceso aleatorio o volátil (RAM) mediante un volcado de memoria del equipo por parte de un especialista, para evitar la pérdida de la información volátil o la modificación de datos o registros de entrada al equipo.

¿Qué se puede obtener de la memoria RAM? Contraseñas, Archivos de imagen, texto, URL, procesos en ejecución y conexiones de Red.

A este respecto hay que mencionar que extraer la RAM durante una diligencia no es un procedimiento común, por lo que se podría caer en la situación de abuso de atribuciones y otras faltas.

Cateo. La extracción de información contenida en aparatos electrónicos considerados instrumentos u objetos del delito, incluso con el auxilio de peritos, autorizada en la orden relativa, excede el objeto y límite legales de dicha diligencia y vulnera el derecho a la inviolabilidad de las comunicaciones privadas.

Si se trata de unidades de lectura de tarjetas, o de CD, precintar los accesos a la misma, es decir, las ranuras por donde se insertan las unidades de lectura.

Recuerde que de ser posible el imputado deberá firmar y estampar sus huellas digitales en el embalaje, de esta manera asienta y acepta la propiedad de los indicios levantados.

E. Sellado y Etiquetado

El embalaje es sellado con cinta de seguridad con la leyenda evidencia (o el medio de sellado que le hayan asignado), la cual lleva nombre, fecha y firma del personal que realizó el embalaje.

Conviene señalar que la etiqueta que habrá de adherirse al embalaje para identificarlo y que además puede ser escrita o impresa, no existe como formato o anexo en la Guía Nacional de Cadena de Custodia, en el Protocolo Nacional de Primer Respondiente ni en el Protocolo de Policía con Capacidades para Procesar el lugar de la Intervención, sin embargo, si la mencionan de manera genérica, se aconseja utilizar el anexo 5 del acuerdo A/009/15, que bien puede servir para este fin.

F. Llenado del Registro de Cadena de Custodia

El Registro de Cadena de Custodia es un documento en el que se enuncian los indicios o elementos materiales probatorios y las personas que intervienen, desde su localización, descubrimiento o aportación en el lugar de intervención, hasta que la autoridad ordene su conclusión.

Finalizadas las etapas anteriores, los dispositivos electrónicos u ópticos se entregarán con su respectivo formato de cadena de custodia a la autoridad competente, utilizan el formato correspondiente de acuerdo con su actividad realizada como perito especializado o policía con capacidades para procesar el lugar de la intervención. Los equipos no pueden ser retirados cuando se trata de un servidor que no puede ser removido por el servicio que brinda, por su excesivo tamaño o por el mandamiento Ministerial el aseguramiento debe hacerse en el mismo lugar de los hechos.

1. Al abrir la carcasa, fotografiar la posición y estado de los medios a extraer.
2. Realizar fotografías de gran acercamiento (macro) de cada medio y de sus números de serie, asentando los mismos en el acta respectiva, de manera referenciada a las fotografías de aproximación y la general.
3. Una vez realizado lo anterior, se pueden retirar los medios de almacenamiento, que serán los que se deben asegurar.
4. Para lo anterior, al remover los cables de conexión del medio, se precinta cada uno de ellos con identificación de la posición que ocupaban en el equipo y haciendo lo mismo con los puntos de conexión del equipo.

5. Terminada esa tarea, igualmente precintar debidamente todos los tornillos del medio extraído.
6. Posteriormente se embala el medio en caja o bolsa utilizando la técnica arriba citada, dejando constancia de todo lo actuado y su orden en el acta respectiva.

Una vez desconectados e identificados todos los cables del equipo, se procede a su apertura por medio de la remoción de su carcaza.

Concluidas las operaciones anteriores se deben colocar nuevamente las carcasas y etiquetarlas así como sus tornillos de extracción para preservar el resto del equipo por si se presentara la necesidad de pruebas posteriores.

Si los equipos a procesar fueran portátiles (notebook o laptop)

Levante individualmente.

a. Si se encuentra encendido, capture la memoria RAM.
b. En caso de existir en alguna de ellas, cable de red o conexión inalámbrica, (que en estos equipos es interna) por lo que no tendríamos acceso inmediato a la misma, se debe aislar de manera inmediata el equipo, preferentemente con la asistencia del perito en informática presente y o si es usted tome sus precauciones, etiquete de manera inmediata las conexiones que se retiren.
c. Fije la pantalla utilizando el procedimiento antes explicado.
d. Posteriormente retire el cable de alimentación si es que se encuentra conectado y etiquételo.
e. Subsecuentemente retire la batería para realizar lo que se conoce como apagado duro.
f. Fije fotográficamente el equipo, su número de serie y el estado de la pantalla.
g. Ya una vez apagado etiquete y embale el dispositivo.
h. Agréguelo al registro de cadena de custodia.

Si el dispositivo es una TABLET:

a. Si se encuentra prendida no apagar por ningún motivo.
b. Si se encuentra apagada no prender por ningún motivo.
c. Fotografiar el estado del aparato y de ser posible lo que se muestra en la pantalla.

d. Fotografiar y registrar la marca, el modelo y el número de serie si es que estos son visibles.
e. Etiquetar todas las entradas y salidas de datos y energía.
f. Etiquetar los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
g. Localizar y etiquetar el cargador eléctrico.
h. Colocar en una bolsa de Faraday, (especial para aislar de emisiones electromagnéticas), si no tiene una disponible, embale utilizando la misma técnica para una laptop.
i. Recolecte, embale, selle y etiquete.

Si se trata de teléfonos celulares:

a. Si se encuentra prendido no apagar por ningún motivo.
b. Si se encuentra apagado no prender por ningún motivo.
c. Fotografiar el estado del equipo y la pantalla.
d. Fotografiar y registrar la marca, el modelo y el número de serie si es que estos son visibles.
e. Etiquetar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria externas.
f. Localizar y etiquetar el cargador eléctrico.
g. Colocar en una bolsa de Faraday, (especial para aislar de emisiones electromagnéticas), si no tiene una disponible, embale utilizando la misma técnica para una laptop.
j. Recolecte, embale, selle y etiquete.

Si cuenta con autorización de intervención de comunicaciones privadas y es el perito en informática experto en forense digital y cuenta con dicha autorización a fin de obtener la información que requiera en ese momento la autoridad para realizar una detención, etc., extraiga y analice la información en presencia de los demás peritos auxiliares y de la autoridad competente, personas desaparecidas o de pornografía infantil; en algunos de los casos, estas autorizaciones dependen puramente de la habilidad del agente investigador para plasmar en la solicitud de intervención.

VII. La importancia de la obtención de la prueba digital durante la diligencia de cateo

La importancia de una evidencia bien adquirida.

En los casos contrarios donde existen temas orientados a practicar intervenciones de comunicaciones, el juzgador autoriza estas intervenciones basado en las presunciones de delitos derivados de delincuencia organizada, personas desaparecidas o de pornografía infantil; en algunos de los casos estas autorizaciones dependen puramente de la habilidad del agente investigador para plasmar en la solicitud de intervención.

Obtención y presentación.

Ejemplo de extracción de información de un disco duro y el dictamen para presentación.

Es de resaltar que todo el equipo y software utilizado tiene que estar certificado y validado para las funciones que va a realizar, de lo contrario las pruebas obtenidas no podrán ser utilizadas en un proceso penal.

Fuentes de consulta

- http://www.cytrap.eu/files/ComMetrics/2009/image/12/2009-11-22-1969
- December-Arpanet-map.gif
- https://www.w3.org/History/19921103 -hypertext/hypertext/WWW/ TheProject.html
- http://4.bp.blogspot.com/ - giTCuNBN9Cc/VqpcjQSw5xI/AAAAAAAAmbI/w1H -
- 1WBhp00/s1600/virus -the-creeper.jpg
- https://upload.wikimedia.org/wikipedia/commons/ thumb/b/b4/Disquetes_i nstalacion_MSDOS_50.jpg/1200px-Disquetes_instalacion_MSDOS_50.jpg
- http://vxheaven.org/lib/img/atg00/fig1.gif
- https://cdn.line.do/uploads/57726d3203163f2c2b98bfd0_1467323100716.gif
- http://sophosiberia.es/wp -content/uploads/2013/03/c arta-nigeriana.gif
- http://www.monografias.com/trabajos12/virudos/Image1725.gif

http://securityresponse.symantec.com/es/mx/norton/cybercrime/definitio n.j sp

https://geekland.eu/acceder -a-la-deep-web/

https://es.wikipedia.org/wiki/Internet_profunda

https://q ph.ec.quoracdn.net/main-qimge23d780dc3f1f937a4f5b68ec483c855

http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html

http://www.itu.int/ITU -D/projects/ITU_EC_ACP/hipcar/events/2010/wg1/docs_wk1/Marco_Gercke_Regional_and_International_Trends_in_Informat io n_Society_Issues_HIPCAR_WG-1_workshop01_20100308.pdf http://www.itu.int/ITU

http://www.itu.int/ITU -D/projects/ITU_EC_ACP/hipcar/events/2010/wg1 / docs_wk1/Marco_Gercke_Regional_and_International_Trends_in_Informat io n Society_Issues_HIPCAR_WG-1_workshop01_20100308.pdf https://mx.norton.com/cybercrime -definition

http://www.ctf-fce.ca/en/Pages/Issues/Cyberbullying.aspx; Cyberbullying: Ontario College of Teachers' Perspective.pdf pág. 12

https://www.securityartwork.es/wp -content/uploads/2016/01/img1300x239.jpg

http://quod.lib.umich.edu/cgi/t/text/text idx?c=jep;view=text;rgn=main;idno=3336451.0007.104

http://www.monografias.com/trabajos92/breve -esena-delitosinformaticos/breve-resena-delitos-informaticos.shtml

http://www.paralibros.com/passim/p20 -tec/pg2050ci.htm

http://informaticaforenseunadcd.blogspot.mx/p/recoleccion -de-evidenciadigital.html

http://www.tuexperto.com/wp-content/uploads/2012/07/ipod-2.jpg

https: //api.sonymobile.com/files/sw2 -gallery-02-1240x840560d9729747d3d75c503f0bc644456c7.jpg

https://www.sams.com.mx/imagenes/productos/imagen -mediana/Camara-Fotografica-Canon--T6-mas-Accesori-185575M.jpg

http://static2.inventosabsurdos.com/wpcontent/uploads/NavajaMemoriaUS B.jpg

- http://www.informaticahoy.com.ar/aprenderinformatica/imagenes/Significa
- -clase-tarjetasmemoria-SD_clip_image004.jpg
- https://tecnologiasmexico.com/corporativo/wpcontent/uploads/2015/12/sma rtphone-collection.jpg
- https://doxz7msmg7sxx.cloudfront.net/media/catalog/product/cache/21/image/992x558/9df78eab33525d08d6e5fb8d27136e95/1/_/1_15588.jpg
- http://www.deskshare.com/images/OverviewPages/dap/DiscWritingFeature.jpg
- http://www.darklab.rutgers.edu/MERCURY/t15/pe2850dell/td03 - Hds14_500px.jpg
- Jorge Esteban Cassou Ruiz (2009) Delitos informáticos en México.
- Margarita Nahuatt Javier (2014), "Diferencia entre datos de prueba, medios de prueba y prueba: en el nuevo sistema penal acusatorio" Revista de la judicatura federal.
- Estudio "una perspectiva internacional sobre la lucha contra el delito cibernético". Lecture notes in computer science: 379-384. Doi: 10.1007 / 3-54044853-5_34
- Correa, c. - Batto, h. - Czar de Zalduendo, s. & Nazar Espeche, f. (1987). Cap. El derecho ante el desafío de la informática. En "derecho informático"(p. 295). Buenos aires: Depalma.
- "Plan de acción de Londres - red de control de seguridad cibernética internacional".
- «Arpanet». Diccionario español de ingeniería (1.0 edición). Real academia de ingeniería de España. 2014. Consultado el 1 de octubre de 2015.
- UNODC/Ccpcj/eg.4/2013/2, 23 de enero de 2013, estudio exhaustivo del problema del delito cibernético y las respuestas de los estados miembros, la comunidad internacional y el sector privado ante ese fenómeno pág. 5.
- Código Penal Federal, 18 julio de 2016.
- Guía Nacional de Cadena de Custodia.
- Código Nacional de Procedimientos Penales (2014)
- Eduardo J. Couture (1997) Vocabulario jurídico,
- Michele Taruffo (1997), La Prueba de los Hechos,
- Salvador Clemente Beltrán Santana (2016), Evidencia Digital e Informática Forense.

CAPÍTULO II

ESTUDIOS DE CIBERSEGURIDAD

LA CIBERSEGURIDAD: ESTRATEGIA PARA EL CRECIMIENTO DE MÉXICO

Mtro. Radamés Hernández Alemán[1]

Sumario: I. Contexto general. II. Contexto económico de México. III. Efectos de la pandemia COVID-19 en el ámbito tecnológico. IV. Términos y conceptos relacionados a la ciberseguridad. V. Capacidades de la Guardia Nacional en materia de ciberseguridad. VI. Prospectiva.

I. Contexto general

La evolución de las tecnologías de la información y comunicación a nivel global ha implicado a su vez una permanente necesidad de protección y seguridad en un entorno digital donde los incidentes cibernéticos son cada vez más frecuentes, complejos y de mayor magnitud, con un alto impacto en la economía y la sociedad. La generación de conocimiento y el desarrollo de nuevos modelos de negocio confirman que el ciberespacio es un recurso importante para potenciar el desarrollo económico, cultural, político y democrático de las naciones.

El ciberespacio[2], de acuerdo con la Real Academia Española, es por definición un ámbito virtual creado por medios informáticos, a través de Internet, hoy conviven más de 4 mil millones de personas (51% de la población mundial) según datos de la Unión Internacional de Telecomunicaciones[3] (UIT) y un número estimado de 38.5 mil millones de dispositivos interconectados se prevén para 2025[4], lo que convierte al ciberespacio en un asunto complejo para proteger tanto para el ámbito de Estado como para la empresa y las personas.

Cuando existen conflictos entre Estados/Naciones o incluso personas o grupos, en un entorno tradicional usualmente hay fronteras y límites, en el ciberespacio no están determinados; los que realizan un ciber ataque no necesitan trasladarse hasta el punto de afectación, lo que genera que el ciberespacio sea un entorno único, sin barreras geográficas, que permite el anonimato y la clandestinidad. A nivel mundial, diversos reportes de la industria

[1] Actualmente es el Director del Centro de respuesta a incidentes cibernéticos(CERT-MX). Estudió una Ingeniería en comunicación y electrónica, egresado del Instituto Politécnico Nacional y cuenta con una maestría en Estrategia de las tecnologías de la información por el Fondo de tecnología de la Información y la Universidad de Texas, así como 20 años de en áreas relacionadas con informática y tecnología de la información

[2] https://dle.rae.es/ciberespacio.

[3] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[4] Statista es uno de los proveedores de datos de mercado e información sobre consumidores. https://es.statista.com/estadisticas/517654/prevision-de-la-evolucion-de-los-dispositivos-conectadospara-el-internet-de-las-cosas-en-el-mundo/.

indican que se han incrementado y diversificado las modalidades de ataques cibernéticos, afectando a personas e instituciones públicas y privadas, incluyendo ataques cibernéticos supuestamente vinculados con la denominada "ciberguerra"[5] entre distintos Estados/Naciones. El ciberespacio se ha convertido en el entorno operativo cada vez más resguardado a nivel de Estado, al igual que el aire, el mar y la tierra para la defensa de la soberanía.

Por otra parte, el uso de las tecnologías y la incorporación del internet al mundo real han sido, sin duda, un factor de desarrollo político, social y económico de nuestro país, hacia la construcción de una sociedad más informada, conformada por individuos y organizaciones, públicas y privadas, que día con día, migran sus actividades cotidianas al ciberespacio. Inherentemente, este cambio de paradigma conlleva también riesgos diversos asociados al uso de las tecnologías y el incremento en la comisión de delitos, provocando una reflexión sobre este nuevo frente de batalla ¿qué implicaciones tiene y cuáles son sus posibles repercusiones?

Es importante mencionar que cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia tiene de los sistemas de información y comunicaciones, por lo que, los efectos de alguna intrusión, manipulación, sabotaje o interrupción de sistemas, flujos de información e incluso de la operación de las redes que usan de soporte, podría afectar el funcionamiento de los mismos y a millones de personas que los usan de manera cotidiana.

En 2020, la empresa Solarwinds[10] fue víctima de un ataque cibernético[11] del tipo "Supply Chain" o "Cadena de suministros", los ciberdelincuentes crearon un código malicioso de tipo troyano para el producto de Software Orion, simulando un paquete de actualización del programa que incluyó la firma y el sello oficial de la compañía, esto generó confianza en la actualización y miles de clientes descargaron el código malicioso creyendo que se había descargado una actualización más.

5. La ciberguerra es un término que incluye ataques, explotación y defensa de las Redes de los Estados/Naciones en el ciberespacio. Seguridad Nacional y Ciberdefensa, Oscar Pastor Acosta, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros, 2009, Madrid, España.
6. Verizon. Reporte Anual 2020 sobre Brechas de Seguridad, https://enterprise.verizon.com/resources/reports/dbir/.
7. Verizon Communications Inc. se formó el 30 de junio de 2000 y es uno de los principales proveedores mundiales de productos y servicios de tecnología, comunicaciones, información y entretenimiento. https://www.verizon.com/about/our -company.
8. La actividad de "hacking" tiene dos conceptos de acuerdo con la Real Academia Española, el primero refiere a los conocidos piratas informáticos que utilizan la tecnología para tener reconocimiento social, exhibir las vulnerabilidades de organizaciones e incluso obtener beneficios económicos, entre otros; el segundo refiere a aquellas personas con grandes habilidades en el manejo de computadoras que investigan un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. https://dle.rae.es/j%C3%A1qu er#TUznqw
9. Malware. Se llama programa malicioso, programa maligno, programa malintencionado, en inglés malware (acortamiento de malicious software), badware o código maligno, a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada. https://es.wikipedia.org/wiki/Malware

Para entender la importancia del evento, Solarwinds es un corporativo que juega un papel clave en la estructura del sector tecnológico a nivel global, dado que está dedicada a proveer programas de tipo empresarial a una muy amplia cartera de clientes en el Gobierno de Estados Unidos, y otras importantes compañías como Microsoft, Ford, Mastercard, Nestlé, la Universidad de Harvard y hasta 425 de las 500 compañías de Fortune 500. La "puerta trasera" se creó en marzo de 2020 y no fue detectada hasta diciembre, aún se desconoce el origen del ataque y se mantiene la investigación.

En México, eventos como el cifrado de información a instituciones federales como PEMEX (2019), la Secretaría de Economía y la Comisión Nacional de Seguros y Fianzas (2020) en el cual se exigía el rescate por la liberación de la misma, son ejemplos de afectaciones donde la ciberdelincuencia logra incidir en las operaciones de un país motivando que se implementen estrategias y acciones para evitar que estos incidentes en el ciberespacio impidan y dificulten el desarrollo económico, político y social.

Por otra parte, la constante incorporación de tecnologías emergente s como la nanotecnología, "blockchain"[12], los drones, la inteligencia artificial, entre otras, a los aspectos de la vida cotidiana implican a su vez que nuevas modalidades de amenazas en el ciberespacio obliguen a mejorar los aspectos de la seguridad y la protección que principalmente requiere personal especializado, herramientas de detección oportuna y diversos procesos que siempre estarán a prueba ante la también constante evolución de los atacantes.

Esto ha motivado que en las últimas décadas, hayan surgido diversos conceptos de seguridad vinculados al ámbito tecnológico en virtud del incremento de los riesgos a nivel global como son la diversificación de actores (y activos que son potenciales objetivos), la necesidad de proteger a las organizaciones públicas (tanto civiles como militares), las organizaciones privadas e incluso la ciudadanía.

I. Contexto económico de México

Ante el sistema internacional, México se ha convertido en un actor con un peso estratégico, al posicionarse como la segunda economía más grande de América Latina y la 15ª a nivel mundial, con un Producto Interno Bruto (PIB) de 1.2 mil millones de dólares. México ocupa el lugar 54 en el índice global de competitividad posicionado en el segundo a nivel Latinoamérica, con acceso a mercados que representan alrededor del 65 por ciento del PIB mundial como Canadá, Estados Unidos, Europa, entre otros, con más de mil 500 millones de consumidores.

10 Sitio web oficial en español de Solarwinds https://www.solarwinds.com/es/.
11 Medio digital El Confidencial, 2020. https://www.elconfidencial.com/tecnologia/2020-12-22/hackeosolarwinds-ataque-eeuu-microsoft-cisco_2881071/

Su posición geográfica en el occidente, posiciona a nuestro país como una potencia emergente, con capacidades para asumir mayores y más significativas responsabilidades a nivel regional y global.

La economía es un pilar de crecimiento para los diversos sectores sociales, así como es imperante establecer las condiciones de seguridad en todo el territorio, mediante estrategias y objetivos integrales con visión nacional y futurista, se logrará contribuir en el crecimiento de México.

En el análisis realizado por Banco Santander (marzo 2021) con datos del Banco Mundial, los sectores que más aportan al Producto Interno Bruto son el de servicios (60%), industria (30%) y agricultura (3%); el documento señala que los sectores de alta tecnología, información y desarrollo de software están "experimentando un verdadero auge", impulsado por la calidad de la fuerza laboral, los clúster y los bajos costos operativos que favorecen la creación de centros de llamadas. Además, la industria de TI fue una de las más afectadas por la pandemia, debido sobre todo a una caída abrupta de la inversión. Por tanto, la industria y la tecnología representan un vital factor de desarrollo económico considerando además que el sector servicios proporciona el 61% del mercado laboral dentro del cual se encuentra el tecnológico especializado.

Por tal motivo, al impulsar a la ciberseguridad en las instituciones públicas y privadas no sólo se pueden alcanzar los objetivos y metas de cada organización, de manera implícita se contribuye en otros factores como el crecimiento económico, el empleo y su profesionalización, nuevos modelos de negocio basados en tecnología, más oportunidades para la inversión, entre otros más. Establecer una estrategia que involucre a múltiples interesados en participar a nivel institucional con la Guardia Nacional es algo imprescindible para mantener y dar rumbo a nuestro país.

---

12 Blockchain. La cadena de bloques, más conocida por el término en inglés blockchain, es un registro único, consensuado y distribuido en varios nodos de una red, tecnología que ha impulsado las criptomonedas en virtud de que cada bloque tiene un lugar específico e inamovible dentro de la cadena, ya que cada bloque contiene información del hash del bloque anterior. La cadena completa se guarda en cada nodo de la red que conforma la blockchain, por lo que se almacena una copia exacta de la cadena en todos los participantes de la red, esto permite tener "libros contables" bastante seguros ya que un atacante tendría que eliminar todos los bloques en virtud de que bastaría uno sólo para tener el registro de toda la cadena.

13 Datos del Banco Mundial. 2019. Sitio web https://datos.bancomundial.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false.

No obstante lo anterior, las expectativas globales han dado un giro en torno a las economías, el Banco de México publicó en febrero de 2021, la "Encuesta *sobre las Expectativas de los Especialistas en Economía del Sector Privado*", donde el pronóstico de los analistas que participaron de la encuesta es desalentador para México en el corto y largo plazo, al advertir un decrecimiento paulatino durante los siguientes tres años (2021 a 2023) con una expectativa a diez años de un 2% en promedio, sin dejar de mencionar que entre las causas destacan los efectos a nivel mundial de la pandemia de COVID-19.

II. Efectos de la pandemia COVID-19 en el ámbito tecnológico

Al inicio de 2020, la economía global ha tenido cambios sustantivos como resultado de la pandemia COVID-19, ya que el problema sanitario se transformó en una "nueva realidad" inesperada en todo el mundo. En respuesta, los países han venido adoptando diversas medidas para su contención y mitigación, que a su vez ha repercutido en la actividad económica modificando los precios de materias primas, afectando los mercados financieros, reduciendo la demanda de bienes y servicios, lo que trajo consigo una mayor incertidumbre sobre los efectos que tendría a nivel global.

La pandemia de COVID-19 trajo consigo diversas consecuencias en el ciberespacio a nivel global y México no fue la excepción, además de las compras de pánico, saqueos a tiendas comerciales, desabasto de productos de limpieza e higiene personal cierre temporal o definitivo de empresas, y sobre todo permanecer en casa a fin de evitar la propagación del virus.

---

14 Artículo: Mexico: Política y Economía, Banco Santander, 2021.
https://santandertrade.com/es/portal/analizar-mercados/mexico/politica-y-economia#:~:text=La%20economía%20de%20México%20está%20activa%20del%20país%20en%2020

15 Refiere a Clúster empresarial, que es la concentración geográfica de proveedores especializados, compañías interconectadas, socios de industrias, proveedores de servicios e instituciones relacionadas que operan en un campo específico y al que están vinculadas de diferente forma.

16 Banco de México, 2021. En la encuesta participaron 36 analistas nacionales y extranjeros, se realizó en el mes de enero: Action Economics; Banco Actinver; Bank of America Merrill Lynch, Banorte Grupo Financiero; Barclays; BBVA; BNP Paribas; Bursamétrica Management S.A. de C.V.; BX+; Capital Economics; Centro de Estudios Económicos del Sector Privado, A. C.; CIBanco; Citibanamex; Consejería Bursátil; Consultores Internacionales; Evercore ISI México; Finamex, Casa de Bolsa; Harbor Inteligence; HSBC; IHS Markit; Invex Grupo Financiero; Itaú Asset Management; Itaú Unibanco; JP Morgan; Luis Foncerrada Pascal; Monex, Grupo Financiero; Morgan Stanley; Multiva, Casa de Bolsa; Natixis; Prognosis, Economía, Finanzas e Inversiones, S.C.; Raúl A. Feliz & Asociados; Santander, Grupo Financiero; Scotiabank, Grupo Financiero; UBS; Valmex; y Vector, Casa de Bolsa.
https://www.banxico.org.mx/publicaciones-y-prensa/encuestas-sobre-las-expectativas-de-losespecialis/%7B6139703D-D4C7-F0BF-9669-69AFA5E804D9%7D.pdf

En virtud de lo anterior, y de manera natural se incrementó el tráfico de datos desde el hogar, siendo el uso de internet la alternativa para continuar con las actividades educativas, profesionales, económicas e incluso de entretenimiento; esto también ha propiciado que la ciberdelincuencia recurra a los medios tecnológicos para la comisión de delitos a través de internet.

En 2020, la Dirección General Científica atendió más de 21 mil reportes ciudadanos relacionados con afectaciones en el uso de la tecnología, cifra que presentó un incremento de 42% respecto del año 2019, de los cuales destacan las modalidades de fraude (31%), amenazas y acoso (26%), robo de identidad (7%) y extorsión (6%).

En el periodo de enero a abril de 2020, de acuerdo con los registros de la Dirección General Científica de la Guardia Nacional, el número de reportes ciudadanos, sitios fraudulentos, reportes de transmisión de pornografía infantil y convocatorias a saqueos usando las redes sociales presentaron tendencias a la alza.

Por otra parte, respecto a la actividad criminal que afecta a datos y sistemas de información en los diversos sectores económicos del país presentaron un escenario complejo, con más de 180 mil incidentes cibernéticos en el periodo comprendido de diciembre de 2018 a marzo de 2021, donde la infección por código malicioso (malware) encabeza la lista con 84%, los sitios web apócrifos de tipo "phishing"[18] 7%, vulnerabilidades de infraestructura 4% y los ataques de fuerza bruta el 3%.

Los sectores más afectados por infección de código malicioso es el sector privado con 55%, seguido por el académico con 33% y el gubernamental con 12%; los sitios web apócrifos, sin embargo, afectaron más al sector gubernamental con 60%, sector privado con 37% y el financiero con 3%.

El uso de códigos maliciosos por delincuentes no es de extrañar, a través de internet es posible obtener un beneficio sin necesidad de acercarse a las víctimas, mantener el anonimato y el número de potenciales víctimas representa un ventaja ante los métodos tradicionales, lo cual en el contexto de la pandemia COVID-19 ha resultado además una necesidad al tener que permanecer más tiempo en la vivienda.

La información hoy en día es un activo esencial para cualquier individuo u organización, en atención a que la información genera conocimiento y a través del conocimiento se logran mejores condiciones al tomar decisiones con un amplio contexto de las causas y consecuencias.

17 El robo de identidad no se encuentra actualmente en la legislación mexicana, no obstante que algunas conductas asociadas como la suplantación de identidad y el uso ilegal de credenciales de acceso sin autorización podrían ejemplificar la referencia del término (Nota del Autor)

III. Términos y conceptos relacionados a la Ciberseguridad

Para entender con más claridad los diversos conceptos asociados a la protección de la información en el ciberespacio, es importante conocer los principales términos más utilizados y sus principales diferencias, si bien existen muchos autores que aún han mantenido sus posturas respecto a las mismas, definiremos para efectos de este capítulo uno de los ampliamente aceptados.

La Real Academia Española (RAE) define el término seguro como "libre y exento de riesgo" y también como "seguridad, certeza, confianza". La cual nos permite reflexionar respecto a que la seguridad es una condición ideal, en la realidad no es posible tener certeza de que se puedan evitar todos los peligros.

Por ende, la seguridad en cualquier tipo de ámbito de aplicación tendrá como objetivo reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes.

Por otra parte, la RAE define a la información como "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada", estos conocimientos se encuentran en distintas formas, aunque está asociado al aspecto digital (archivos en medios electrónicos u ópticos), también se incluye la forma física (escrita o impresa en papel), así como de manera tácita, las ideas o el conocimiento de las personas. En este sentido, los activos de información pueden encontrarse en distintas formas.

Además, la información puede ser almacenada, procesada o transmitida de diferentes maneras: en formato electrónico, de manera verbal o a través de mensajes escritos o impresos, por lo que también es posible encontrarla en diferentes estados.

Por lo tanto, la seguridad de la información (sin importar su forma o estado en que se encuentre) refiere a las medidas de protección adecuadas de acuerdo con su importancia y criticidad.

---

18 El "phishing" es un método que los ciber delincuentes utilizan para engañar y conseguir que se revele información personal, como contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros. Obtienen esta información mediante el envío de correos electrónicos fraudulentos o dirigiendo a la persona a un sitio web falso. Referencia Fundación UNAM, https://www.fundacionunam.org.mx/unam-al-dia/sabes-como-funciona-el-phishing/

19 Un ataque de fuerza bruta es un intento de descifrar una contraseña o nombre de usuario, de buscar una página web oculta o de descubrir la clave utilizada para cifrar un mensaje, que consiste en aplicar el método de prueba y error con la esperanza de dar con la combinación correcta finalmente. Referencia 20 https://dle.rae.es/seguro?m=form

Seguramente uno de los aspectos de la protección de la información en el ciberespacio está directamente vinculado a la seguridad informática, que está definida de manera general como "cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan 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).

Una visión distinta de la seguridad informática es la que plantea el experto en la materia de la firma "*Fire Eye*" Richard Bejtlich que la define como el "***proceso consistente en mantener un nivel aceptable de riesgo percibido***".

Así mismo, la **seguridad informática** aplica para el entorno digital, se limita a la protección de los sistemas y equipos que permiten el procesamiento, almacenamiento y transmisión de la información, que involucra los métodos, procesos o técnicas para la protección de las redes e infraestructura tecnológica.

Partiendo de ésta última definición, los objetivos de la seguridad informática serán los de buscar mantener los niveles aceptables de riesgo para:

- La Confidencialidad, que implica cuidar que:
  - Que nadie más lo vea,
  - Que la información sea revelada exclusivamente a usuarios autorizados, y
  - **Autenticación** (validar quién es).
- La Integridad, verificar:
  - Que nadie más lo modifique o elimine,
  - Que la información sea modificada sólo por personal autorizado,
  - Exactitud de la información, y
  - **Autorización** (determinar qué puede hacer).
- La Disponibilidad, asegurar:
  - Que siempre esté ahí,
  - Que la información sea utilizable cuando y como lo requieran los usuarios autorizados,
  - Asegurar el No repudio (qué nadie pueda decir que NO fue), y
  - **Auditoría** (qué ocurrió).

---

21 Seguridad Informática Básico. Álvaro Gómez Vieites, 2010, Madrid, España. https://www.ecoeediciones.com/wp-content/uploads/2015/08/seguridad-informatica-basico.pdf

22 Fire Eye, Empresa global que desarrolla una serie de productos de seguridad informática e inteligencia de amenazas cibernéticas, sitio web oficial https://www.fireeye.com/.

23 Blog de Richard Bejtlich, https://taosecurity.blogspot.com/.

Por otra parte, la Ciberseguridad es la "seguridad en el ciberespacio" de acuerdo con el estándar internacional ISO/IEC 27032:2012, el cual ofrece un conjunto de buenas prácticas en materia de Seguridad de la Información, brinda herramientas para implementar la gestión en cualquier tipo de organización, propone procesos para la protección de las operaciones y las actividades en línea, los programas recomendados, manejo de datos, servicios, capacitar al personal que va estar a cargo del manejo de estas herramientas.

Para la Unión Internacional de Telecomunicaciones de la Organización de las Naciones Unidas, la ciberseguridad es "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" (Resolución 181 Recomendación UIT–T X.1205).

Los activos de la organización son los dispositivos informáticos conectados, los usuarios, los servicios, aplicaciones, sistemas de comunicaciones, comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberespacio.

La ciberseguridad permite que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberespacio. Las propiedades de seguridad incluyen al menos las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio, y la confidencialidad.

IV. Capacidades de la Guardia Nacional en materia de Ciberseguridad

La Guardia Nacional, se consolida como una institución primordial en la estructura del Sistema de Seguridad del Gobierno de México, particularmente en el plano de la seguridad pública, contribuyendo en la consolidación de la democracia, la gobernabilidad y la seguridad del país.

Una de las principales metas en el campo de acción de la Guardia Nacional, es reducir la incidencia de los delitos con mayor impacto en la población. Dentro de este ámbito destaca el despliegue de capacidades y acciones policiales que lleva a cabo la Dirección General Científica para detectar y atender oportunamente los delitos cibernéticos.

---

24 Sitio oficial del estándar internacional ISO/IEC 27032:2012. https://www.iso.org/standard/44375.html.
25 Referencia de la Unión Internacional de Telecomunicaciones (UIT), Guadalajara Mexico, 2010. https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf

La ciberseguridad se ha convertido en un ámbito estratégico y de impulso a la economía nacional, que a su vez tiene impacto en la seguridad pública; en el Programa Sectorial de Seguridad y Protección Ciudadana 20202024, se encuentra definido el Objetivo prioritario 4, que busca:

> *"Fortalecer las capacidades tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno el intercambio seguro de la información en la generación de inteligencia, prevención y persecución del delito".*

En este sentido, la Dirección General Científica de la Guardia Nacional, tiene atribuciones y unidades especializadas en la atención de delitos cibernéticos y la gestión de incidentes cibernéticos, integrada por elementos con estudios de nivel licenciatura y posgrado, quienes cuentan con entrenamiento y certificaciones internacionales.

La Guardia Nacional se ha planteado una Estrategia de Ciberseguridad para el desarrollo de acciones planificadas, sistemáticas y coordinadas que se definen en tres ejes principales:

1. **Impulsar la prevención de los delitos** que se cometen a través de las tecnologías de la información y comunicación a fin de concientizar a la ciudadanía y los principales sectores económicos como el financiero y empresarial, a través de la cual:

   Se concientiza sobre los hábitos para una navegación segura y responsable, el cuidado de la información en el contexto personal, familiar y laboral, se promueven la cultura de prevención y denuncia de delitos cibernéticos mediante la impartición de pláticas y conferencias dirigidas a los diferentes sectores de la población.

   Una de las actividades con mayor audiencia es la Semana Nacional de la Ciberseguridad de la Guardia Nacional, evento al que asisten y participan expertos nacionales e internacionales del sector público, privado, financiero, académico, empresarial, industrial y organizaciones de la sociedad civil, a fin de actualizar y discutir sobre los temas globales y locales de la ciberseguridad, su impacto y avances en torno al ámbito de México y su desarrollo.

---

26 Programa Sectorial de Seguridad y Protección Ciudadana 2020 2024, Diario Oficial de la Federación, 2020 https://www.dof.gob.mx/nota_detalle.php?codigo=5596028&fecha=02/07/2020

- Se generan contenidos informativos que son difundidos en redes sociales oficiales y el sitio web de la Guardia Nacional, los cuales presentan las diversas modalidades de afectación a diversos sectores sociales incluyendo las niñas, niños y adolescentes, así como recomendaciones para identificarlas, buenas prácticas en materia de seguridad informática indispensables para una mejor experiencia en el uso de las tecnologías de la información y comunicación incluyendo internet.
- Se operan diversos medios de contacto ciudadano para recibir orientación técnica y legal como el sitio web de la Guardia Cibernética de la Dirección General Científica para la consulta de información temática y el reporte de incidentes.

2. Apoyar el **fortalecimiento de las capacidades ante los riesgos y amenazas a la ciberseguridad** esencial con una visión nacional.

En virtud de la complejidad que presenta México en relación a sus múltiples instituciones, geografía, recursos naturales y fronteras, entre otros, los esfuerzos de la ciberseguridad requieren de acciones que permitan:

- Fortalecer las capacidades de respuesta y coordinación institucional ante incidentes cibernéticos de impacto, para lo cual la Guardia Nacional opera el Centro de Respuesta a Incidentes Cibernéticos (CERTMX), que realiza el monitoreo en la red pública de internet las 24 horas al día, los 7 días a la semana, para la identificación de amenazas en el ciberespacio, así como para la prevención de ataques contra la infraestructura informática estratégica en el país; el CERT-MX se coordina con 574 equipos de respuesta de tipo gubernamental, privados, industriales y académicos de 97 países, siendo el CERT-MX el único punto de contacto a nivel nacional e internacional.

- Identificar los niveles de ciberseguridad actuales en las organizaciones, ya sean públicas o privadas, si brindan servicios estratégicos se convierten en esenciales para el crecimiento económico y por ende, deben contar con capacidades para el manejo adecuado de incidentes cibernéticos, a través de mejores prácticas o estándares internacionales.

- Implementar estándares en materia de ciberseguridad, en particular sistemas de gestión de seguridad de la información para la gestión de riesgos, vigilancia y mejora continua de los activos de información en servicios estratégicos del país.

- La Guardia Nacional desarrolla e implementa el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos a fin de brindar

servicios en auxilio a las instituciones públicas y privadas que cuenten con activos de información esenciales a fin de coordinar los esfuerzos a nivel nacional ante las amenazas que pongan en riesgo la ciberseguridad desde el punto de vista estratégico para el país en términos del cumplimiento de los objetivos de crecimiento económico.

Así mismo, la Estrategia de Ciberseguridad de la Guardia Nacional considera la colaboración en materia de comercio internacional al sumar esfuerzos con las entidades de gobierno de los Estados Unidos de América y Canadá en el marco del Tratado denominado como T-MEC, a fin de establecer los mecanismos de cooperación que permitan dar cumplimiento al capítulo de Ciberseguridad definido en el documento trilateral. En este mismo sentido, a través de la Dirección General Científica se participa en los foros globales de comercio electrónico que coordina la Organización Mundial del Comercio (OMC) a fin de alinear los objetivos globales con los regionales.

En coordinación con las instancias de seguridad nacional se realizan ejercicios de crisis cibernética a fin de incrementar las habilidades de los equipos de respuesta en instituciones federales, estatales y privadas que cuentan con activos esenciales de información, a fin de contener las amenazas que afectan servicios estratégicos en el país.

La Guardia Nacional a través de la Dirección General Científica participa de manera activa en el Comité Especializado en Seguridad de la Información del Consejo de Seguridad Nacional, para el desarrollo de acciones relativas a la seguridad de la información en las instancias federales y en el análisis y mejora continua de la legislación nacional en materia de ciberseguridad.

Finalmente, al despliegue de capacidades humanas y técnicas, se agrega el fortalecimiento de la coordinación y colaboración interinstitucional desde la Federación y hacia las Entidades Federativas, a través de la creación e implementación de un Modelo Homologado de Policía Cibernética para las entidades federativas que fue aprobado por unanimidad en el Pleno del Consejo Nacional de Seguridad Pública en diciembre de 2016, foro que ha permitido homologar criterios entre las Entidades Federativas y la Federación en los procedimientos y canales de atención ciudadana, la investigación de datos en la red pública de internet, el manejo de la evidencia digital, la generación de estadísticas locales y nacionales a través del Formato Homologado de Incidentes Cibernéticos, campañas de prevención del delito orientadas a los riesgos contra niñas, niños y adolescentes, así como del fraude cibernético, entre otras acciones que se generan a través del Comité de Ciberseguridad de la Conferencia Nacional de Secretarios de Seguridad Pública que preside la Guardia Nacional a través de la Dirección General Científica.

27 Guardia Nacional, 2021 El sitio web se puede acceder en https://www.gob.mx/gncertmx.

V. Prospectiva

Es un hecho que las tecnologías de la información incrementarán su presencia en cada vez más y mayores contextos de nuestra vida cotidiana, con el paso del tiempo veremos nuevas tecnologías e inversiones sobre éstas que incidirán en la forma en que vivimos haciendola parte de nuestra cultura. Es tiempo de empezar a preparar un mejor futuro basado en la socialización de la ciberseguridad como lo hacemos con los asuntos de seguridad tradicionales.

De esta manera, considero que a través de las distintas propuestas de la Estrategia de Ciberseguridad de la Guardia Nacional, se realizará una atención integral a los problemas de la ciberseguridad que tienen impacto en la economía nacional, sectores específicos como el de servicios relacionados al sector de las tecnologías de la información y comunicación, las instituciones financieras, el turismo, energético, entre otros, a partir de los cuales se logran establecer las cadenas de suministro y las cadenas de valor en todo el país, permitiendo además la creación de empresas, nuevos modelos de negocio y el crecimiento del empleo.

La ciberseguridad es también una responsabilidad de todos, a través de la conciencia social sobre los riesgos en el ciberespacio y el uso seguro de las tecnologías de la información y comunicación, es posible que los cuidados e higiene digitales generen resiliencia en la comunidad y a su vez, en los procesos económicos, se pretende que esta conciencia se haga más generalizada al incluir los aspectos de la ciberseguridad en la educación formal de los más jóvenes, por lo que, la Guardia Nacional a través de la Dirección General Científica mantendrá sus esfuerzos de las campañas y jornadas dirigidas a la prevención de los delitos cibernéticos en colaboración con aliados estratégicos de diversos sectores, así como la organización de la Semana Nacional de la Ciberseguridad cada año, a través de los cuales se logre tener un mayor alcance a la población y los distintos sectores económicos en el país.

Así mismo, el segundo eje estratégico es la reducción de los riesgos del ciberespacio mediante una diversidad de políticas, metodologías y herramientas, la formación de más profesionales desde la educación superior para su incorporación a los sectores económicos del país, que sean la fuerza laboral técnico especializada que brinda certeza a la protección de activos esenciales. Por otra parte, la Guardia Nacional a través del CERT-MX de la Dirección General Científica brindando el auxilio a las instituciones públicas y privadas, ofreciendo servicios técnicos y apoyando a las autoridades competentes en las investigaciones de ataques cibernéticos que afectan la economía nacional, siendo el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos un instrumento de colaboración para fortalecer las capacidades de protección basado en la confianza a través del trabajo coordinado de su comunidad.

EL IMPACTO DE LA TECNOLOGÍA EN LAS OPERACIONES POLICIALES

Mtro. Luis Fabián Olivo Ramírez[1]

"Los humanos nos distinguimos de otras especies por
nuestra singular capacidad para hacer milagros.
Llamamos a estos milagros tecnología".
Peter Thiel, co-fundador de Paypal

Sumario: I. Introducción. II. Tecnología y Función Policial. III. Innovación o disrupción. IV. Dispositivo táctico para la operación policial (DTOP): Caso de éxito. V. Reflexiones finales.

I. Introducción

La última década ha traído una diversidad de cambios a nivel tecnológico que han impactado en la manera en que se desarrollan las actividades de la sociedad actual, generando por una parte la dependencia a las tecnologías y por otra, el descubrimiento de una infinidad de oportunidades que configuran nuevas formas de hacer las cosas.

El ritmo del cambio tecnológico y sobre todo de su aplicación en la vida cotidiana permite visualizar una incipiente simbiosis entre el ser humano y la tecnología, acercándonos cada vez más a manifestar las visiones de los relatos de ciencia ficción que alimentaron la concepción de un futuro: un futuro gobernado por la tecnología.

Una de las frases atribuibles a Albert Einstein (1879-1955) acerca del futuro es: "no pienso nunca en el futuro porque llega muy pronto", y aunque pareciera algo simple esta frase no lo es, tal como las aportaciones a la física teórica que realizó Einstein, encierran gran sabiduría y pueden discutirse desde muchos enfoques, como por ejemplo desde el pensamiento filosófico, sin embargo, las tecnologías, las innovaciones en procesos, servicios y productos, y en general todos los esfuerzos que se realizan en la Dirección General Científica tienen como objetivo crear el futuro, lograr la mejora y efectividad de la Guardia Nacional, y contribuir al anhelo de vivir en una sociedad de justicia y paz.

[1] Se ha desempeñado como experto en tecnologías de seguridad. Paralelamente en función de oficial de policía de carrera durante más de 10 años, ocupó diversos cargos operativos y de mando en la División Científica de la Policía Federal y en la Guardia Nacional de México, participando activamente en la implementación exitosa de tecnologías para la obtención, procesamiento, análisis y generación de productos de inteligencia en apoyo a casos de investigación de secuestro y delincuencia organizada.

En este sentido, tratar el impacto de las tecnologías en las operaciones policiales, es aproximarnos a sí hemos llegado o aún nos falta para alcanzar al futuro que se imaginó, desde aquel primer ingeniero de la Dirección General Científica de la Guardia Nacional que propuso un prototipo o concibió las primeras ideas para solucionar una problemática, pues desde este primer instante ya estábamos ¡creando el futuro! Invito al lector a reflexionar sobre ello y al final del capítulo retomaré este planteamiento para juntos evaluar o determinar el impacto, o los resultados de la aplicación de las tecnologías en la función policial.

II. Tecnología y Función Policial

En los últimos 120 años, la función policial ha tenido una participación cada vez más importante para la sociedad, no solo para prevenir e investigar conductas delictivas, sino también para proteger la propiedad privada y representar un medio por el cual el Estado puede garantizar los derechos humanos, lo que contribuye el establecimiento de los sistemas económicos y democráticos actuales.

Durante este periodo la función policial ha recurrido al desarrollo e implementación de tecnologías para mejorar su eficacia,[1] desde la identificación de una persona por medio de huellas dactilares, la aplicación del radio de dos vías y la integración en vehículos especializados o carros radio patrullas (CRPs), hasta la utilización actual de sistemas de información geográfica para registro delictivo y aeronaves pilotadas a distancia o drones.

Sin embargo los avances tecnológicos que alguna agencia de seguridad pública llega a implementar no necesariamente introducen una mejora real en la operación policial o llegan a eliminar el factor humano asociado a la operación, puesto que incluso las condiciones y problemáticas particulares de una región podrían ser suficientes para que una tecnología no tenga el desempeño estimado, de esta manera resultan de importancia los procesos que permitan identificar, desarrollar e integrar la tecnología de una manera eficiente y orientada a las necesidades reales de cada institución de seguridad.

III. Innovación o Disrupción

El impacto que tienen las tecnologías en una institución policial está directamente relacionado con dos factores:

- El nivel de cambio que produce, y
- Su alineación con los objetivos institucionales

[1] SEASKATE, INC. pp 7-8. Véase en línea: https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf

De tal manera que, una tecnología podrá tener impacto positivo si su nivel de cambio dentro de una institución policial es mayor y este cambio incide directamente con la efectividad de las actividades realizadas, incluso más allá de la eficiencia obtenida con el uso de una tecnología, que no es algo por minimizar pero tampoco el consuelo para validar su impacto.

De este modo, se considera que el desarrollo de nuevas tecnologías o de las soluciones tecnológicas que se realizan en la Dirección General Científica de la Guardia Nacional, más allá del grado de especialidad o de la alta especialidad que cada una conlleva, tiene que ver con la manera en que su implementación produce un cambio en la Guardia Nacional y este cambio hace más eficiente el cumplimiento de las atribuciones de la Institución.

Como se observa en la gráfica, resulta de importancia identificar dos conceptos derivados y vinculados fuertemente: a) innovación y b) disrupción, siendo la innovación un requisito preliminar para lograr la disrupción, es decir una tecnología innovadora puede llegar a convertirse en una tecnología disruptiva, o en aquella tecnología que cambia las reglas del juego[3], que marca un antes y un después, que redefine una función y en la mayoría de los casos cambia el curso de la historia.

La disrupción se alcanza cuando una organización realiza un progreso vertical o intensivo, es decir pasar del 0 al 1[4], en cambio la mayoría de las organizaciones solo realizan un progreso horizontal o extensivo, es decir pasan de 1 a n; en el primer caso estamos ante nueva tecnología y para el segundo ante la globalización.

Sin embargo, independientemente de la metodología de desarrollo implementada, los recursos, estudios, análisis o pruebas llevadas a cabo, durante el proceso de creación de tecnologías, el éxito para que esta tecnología pasé de innovadora a disruptiva, tiene que ver con la manera en que se usa, se adopta, resuelve un problema y se benefician de ella sus usuarios (o clientes), es decir, el modo "en que perciben un beneficio", por lo que se vuelve valiosa y cambia la manera en que se realiza una actividad.

En este proceso, y hablando de entornos comerciales resulta de importancia el rol de las estrategias de marketing y el proceso de evangelización[5] para la adopción de una tecnología convertida en un producto, sobra decir a manera de ejemplo el éxito que han tenido compañías como

[3] Borghino, Mario, pp. 16-27
[4] Thiel, Peter y Masters, Blake. pp. 7-14
[5] Como lo define Guy Kawasaki en términos de la tecnología, "proclamar la buena nueva...dar a conocer los beneficios que se derivan de utilizar un producto... cuando la gente cree en tu producto, te ayudará a alcanzar el éxito a través de un proselitismo creíble, continuado y económicamente rentable"

Apple creando verdaderos fieles seguidores de su marca, como explica Kawasaki, quien se autodenomina el segundo evangelista de software de Apple y proclamó al mundo la buena nueva de que *Macintosh podía hacer a la gente más productiva y más creativa*.

No obstante, en el interior de las organizaciones y en específico de las instituciones policiales, lograr la adopción de una tecnología y por ende generar una disrupción no puede lograrse de facto, por instrucción o incluso por Ley, si bien es cierto que el nivel de compromiso del Alto Mando o de la Gerencia es de importancia para lograr que los procesos de adopción e implementación tecnológica sean más rápidos, no es este camino el único que garantizará una verdadera disrupción, el cambio de reglas o el establecimiento de un nuevo paradigma. No basta con que la tecnología resuelva un problema, es de vital importancia que su implementación y adopción sea de manera "orgánica", de forma natural, es decir, sean los integrantes usuarios de una organización quienes demanden su uso, que comprueben su eficiencia y que "deseen" tenerla.

En este sentido, se requiere no solo contar con una tecnología o una solución tecnológica que resuelva un problema, que por sí solo este proceso es complejo, sino que sean los policías quienes comprueben y perciban los beneficios de su uso, el cual está directamente relacionado con la efectividad en sus funciones, solamente de esta manera se logrará estar ante una verdadera disrupción y el impacto no solo podrá ser evaluado, sino que abrirá las puertas de un nuevo futuro.

De la experiencia en el desarrollo de tecnologías y/o soluciones tecnológicas para la operación policial, en el área de innovación tecnológica de la Dirección General Científica, se identificó la importancia de que los esfuerzos concluyeran con los procesos de implementación y adopción, lo que dio lugar a crear un nuevo paradigma interno: del laboratorio a la operación policial.

En este sentido, desde su creación el área de innovación tecnológica de la Guardia Nacional representaba un modelo disruptivo para la función policial en México, pero sin comparación directa con las labores de un centro de investigación o de centros de desarrollo tecnológico, puesto que el nuevo paradigma del laboratorio a la operación policial resaltaba la importancia de asegurar que la tecnología fuera utilizada, aprovechada, comprendida y solicitada por los policías.

[8] Kawasaki, Guy, pp. 150-180

Ante este desafío y la gran diferencia entre la perspectiva de la realidad que tiene el científico en un laboratorio del moderno edificio de la Dirección

General Científica y el personal operativo que se enfrenta a las complejidades y a la diversidad de situaciones o escenarios, donde convergen el cumplimiento de la ley, la protección de la ciudadanía y de su patrimonio, así como cuidar su integridad propia, se tuvieron que adoptar tres enfoques o roles para abordar el nuevo paradigma:

1. **Proveedores:** implicaba solamente el desarrollo de tecnologías específicas y la entrega de estas, para que los policías o agentes las utilizaran para el fin con el que fueron concebidas. Sobra decir que este modelo es viable solo cuando la tecnología alcanza el nivel de madurez y se considera un producto.
2. **Proveedores con transferencia de conocimientos:** es una evolución del modelo de proveedores que permite sumar esfuerzos para garantizar el uso correcto de las tecnologías y reducir la curva de aprendizaje/adopción que puede presentarse al usarlas. Este enfoque permite introducir nuevas tecnologías, aun cuando no hayan alcanzado el grado de productos e incluso se encuentre en fase de prototipo.
3. **Operadores:** este enfoque considera que los ingenieros o científicos serían los encargados de utilizar las tecnologías de manera conjunta en la operación policial, convirtiéndose en los especialistas que acompañarían al personal operativo en sus actividades diarias y para las cuales las nuevas tecnologías implicaban mejorar su efectividad.

En este punto, podría el lector imaginar ¿cuál enfoque es el que prevalece actualmente?, ¿cuál enfoque logró cumplir con el paradigma del laboratorio a la operación policial? Vale la pena reflexionar un poco.

Si bien es cierto que los dos primeros enfoques fueron aplicados a la par que se mejoraban las capacidades de desarrollo tecnológico en cada laboratorio, los resultados no llegaron a ser totalmente satisfactorios, básicamente porque aún se contaba con prototipos que, aunque eran funcionales, no se trataba de productos terminados y validados, mucho menos con efectividad aprobada por los policías (quienes representan el inicio y fin de nuestros esfuerzos).

Lo anterior, no fue por un error de diseño, sino porque en su mayoría los procesos de innovación o creación de tecnologías se basan en prácticas denominadas bootstrapping[7] que precisa obtener prototipos funcionales con los recursos disponibles o al mínimo costo posible como para validar una idea o solución. Ante este panorama, se decidió después de un largo debate y de resistencias internas, asumir el tercer enfoque: ser operadores, y no solo operadores sino una nueva clase de ellos.

La transición del laboratorio a la operación policial responde al compromiso de los mandos del área, pero también al de todos los ingenieros o científicos que asumieron de manera valiente y decidida a defender sus ideales, para llevar a cabo sus ideas transformadas en prototipos a la realidad del entorno policial. Sobra decir que esta transición pudo realizarse porque los ingenieros que integramos el área científica habíamos sido también formados como policías en la Academia Superior de Seguridad Pública, bajo el perfil investigador en su mayoría. Para algunos, sin pensarlo demasiado, el entusiasmo, compromiso y nuestros ideales nos habían llevado a formar una nueva clase de policías, personalmente me gusta llamarlos "policías científicos", pero también se les puede llamar: "súper policías".

Lo anterior, podría parecer presunción o carente de humildad, sin embargo, no es así, ya que solo es una forma de resumir las cualidades que son requeridas para crear disrupciones bajo el paradigma del laboratorio a la operación policial; de esta manera, los "policías científicos" o "súper policías", debían cumplir tres grandes requisitos:

- Conocimientos técnico – científicos[8]
- Conocimientos jurídicos, de derechos humanos y procedimientos policiales
- Adiestramiento en técnicas y tácticas policiales

Aunque muchas veces parece obvia, por ser un requisito de facto en las instituciones de seguridad, también se debía contar con la acreditación vigente de las evaluaciones de control de confianza, por lo que de esta manera se iniciaron procesos internos de capacitación y de adiestramiento del personal con otras unidades operativas, dando lugar a la creación de un grupo capaz de realizar operaciones tecnológicas especiales, o en el contexto del presente capítulo, lograr la implementación y adopción de tecnologías para hacer más efectiva la operación policial generando una disrupción positiva con un impacto mayor.

De esta manera y hasta la actualidad, se ha logrado crear una unidad de desarrollo tecnológico que es capaz de alinear sus esfuerzos para mejora de la efectividad policial, diseñando e integrando tecnologías específicas, y que tiene en su modelo un componente de auto sustentabilidad al crear una red colaborativa, ya que en el futuro todos los policías utilizarán las tecnologías que se han desarrollado, porque estás se convertirán en productos; y las nuevas tecnologías que hoy están en desarrollo serán operadas por el grupo especial del área científica, asegurando la efectividad y vanguardia tecnológica para realizar de mejor manera las actividades policiales, convirtiéndose en un proceso permanente de innovación tecnológica.

7 Bootstrapping es un término en Ingles empleado cada vez más en la jerga del emprendedor, que significa empezar algo sin recursos o con muy pocos. Kawasaki, Guy. pp. 100.
8 Los perfiles profesionales incluían ingenieros en electrónica, electricidad, mecánica, aeronáutica, mecatrónica y sistemas computacionales, algunos con posgrados en ciencias o ingeniería.

Lo anterior se puede representar en los siguientes gráficos, el primero muestra el proceso que inicia en el centro con el desarrollo de nuevas tecnologías y avanza en espiral hasta su adopción y uso extensivo por parte de los policías; el segundo muestra de manera descendente las etapas, desde las ideas de soluciones hasta su uso extensivo, trasladando el desarrollo tecnológico al soporte técnico del producto o tecnología.

A manera de resumen el siguiente gráfico representa la ubicación y la importancia de la creación de un grupo de policías especializados, que permitan servir de vínculo entre la operación real y el entorno de desarrollo de laboratorios:

De esta manera existía un nuevo "engrane" o eslabón que era común a dos lenguajes diferentes, el lenguaje de los científicos y el lenguaje de los policías operativos (paradójicamente siendo ambos policías), y que servía de intérprete entre la expectativa (lo que creemos desde el laboratorio) y lo que es en realidad (el entorno operativo y la condiciones en que se desempeñan las funciones policiales), trayendo consigo una serie de beneficios para ambos lados, entre los cuales destacan:

- Entendimiento de las necesidades del entorno operativo.
- Nuevas ideas de proyectos tecnológicos (o nuevas problemáticas a resolver).
- Reducción de la curva de aprendizaje de implementación tecnológica.
- Comprobación en entornos reales del desempeño de la tecnología.
- Reducción del tiempo de prueba de prototipos tecnológicos al poder llevar a campo, de manera segura, ingenieros que pueden resolver cualquier inconveniente técnico presentado (lo que resulta eficiente en un esquema de innovación bootstrapping).
- Definición de un catálogo de servicios que involucraba una tecnología específica desarrollada.
- Resultados comprobados de la aplicación de la tecnología.
- Empatía del entorno operativo con el desarrollo tecnológico y viceversa.

Este modelo es válido para su réplica en otras instituciones policiales o incluso en otras organizaciones que desean introducir esquemas de innovación intramuros, sobre todo ante la gran separación que puede existir entre los que viven creando el futuro (podríamos llamarlos innovadores, inventores, ingenieros o científicos) y los que viven en el presente, también llamados operadores; sin embargo, sobra decir que la clave está en el punto donde convergen ambos: en las decisiones que hoy estamos tomando para cambiar nuestra situación actual y dirigirnos a otra diferente o mejor.

IV. Dispositivo Táctico para la Operación Policial® (DTOP®): Caso de Éxito

El Dispositivo Táctico para la Operación Policial® (DTOP®), representa un caso de ejemplo del impacto real de la tecnología que se ha desarrollado en el área Científica de la Guardia Nacional y que ha conducido el proceso de adopción e implementación antes presentado.

El DTOP® permite al oficial de policía realizar la identificación en campo de personas con antecedentes penales, órdenes de aprehensión y de registro de personal de seguridad pública, mediante la identificación biométrica dactilar, y consulta las bases de datos criminalísticas; así como de vehículos con reporte de robo y armamento registrado; es decir, el DTOP® permite realizar la consulta de información almacenada en las bases de datos institucionales de manera rápida y sencilla para apoyo a la toma de decisiones en campo

Parte de la problemática detectada no exclusivamente en México, sino más bien en el actuar policial en general, es la capacidad que debe tener el agente de policía para tomar decisiones en su actuar diario, pues intervienen factores que se deben controlar o considerar para su correcta actuación. Adicionalmente al alto nivel de estrés, inherente a las funciones, la toma de decisiones tiene que venir acompañada del cumplimiento de atribuciones Constitucionales, protección a los derechos humanos, uso de la fuerza, seguimiento a los procesos sistemáticos de operación y demás información específica para tomar una decisión.

En este sentido, el DTOP® se desarrolló con el objetivo de proveer "al alcance de su mano" la información registrada en las bases de datos Institucionales, para que el agente de policía pueda disponer de ella de manera proactiva en sus procesos de toma de decisión, privilegiando el aprovechamiento de la información, la colaboración interinstitucional y la prevención policial. De esta forma, el agente de policía podrá contar con información de una manera rápida para evaluar de mejor manera una situación.

Como se expuso anteriormente, los procesos de adopción e implementación tecnológica son tan importantes como el desarrollo tecnológico, pues el fin último es que la tecnología sea utilizada y aprovechada, así mismo, al policía debe permitirle cumplir mejor sus funciones.

---

[9] Registros de marca 1823437, 1826927 y registro de patente MX 52359 B ante el Instituto Mexicano de la Propiedad Industrial (IMPI)

Para la implementación del DTOP® en sus primeras versiones, se participó en actividades policiales reales en puntos de inspección, aeropuertos, patrullajes en carreteras, seguridad en eventos masivos, entre otros, para validar su funcionamiento, identificar requerimientos técnicos, nuevas necesidades y en general cualquier mejora que pudiera ampliar las capacidades y éxito del dispositivo.

Durante este proceso, los resultados no se hicieron esperar, puesto que, por primera vez en México, un oficial de policía podría contar de manera rápida y sencilla con el acceso a la información registrada en las bases de datos para verificar información de personas, vehículos y/o armamento; de esta forma, se lograron resultados que permitieron:

- Cumplimentar órdenes de aprehensión.
- Recuperar vehículos con reporte de robo.
- Detectar documentación apócrifa.
- Verificar antecedentes de pertenencia en instituciones de seguridad pública.
- Verificar antecedentes penales, para orientar entrevistas policiales.
- Identificar de manera rápida la identidad de personas que habían perdido la vida, por medio de la huella dactilar.

Actualmente el Dispositivo Táctico para la Operación Policial® (DTOP®) es de uso exclusivo de la Dirección General Científica de Guardia Nacional, y para asegurar su correcta utilización se han desarrollado capacidades especiales en oficiales asignados al servicio.

Como parte del ciclo de adopción e implementación de tecnologías, el DTOP® se encuentra validado como una tecnología de impacto real en la operación, al proveer de manera eficiente de información para la toma de decisiones, es reconocido y apreciado entre las unidades operativas y se espera que en próximos años sea un producto tecnológico de uso de todos los agentes de la Guardia Nacional, de las policías Estatales y Municipales, constituyéndose en una herramienta más de trabajo colaborativo, vanguardia y aprovechamiento de la información para contribuir a la justicia y la paz de México.

V. Reflexiones Finales

El impacto que tienen las tecnologías en una institución policial está directamente relacionado con el nivel de cambio que produce, y su alineación con los objetivos institucionales, en este sentido cabe la posibilidad de que esta tecnología represente un aprovechamiento, una mejora, una innovación o una disrupción.

El DTOP® representa un progreso para la investigación. Por el desarrollo tecnológico que conllevó al ser una tecnología única en su tipo en el país y por el grado en que esta tecnología mejora sustancialmente en el actuar policial al proveer al agente de información fidedigna para la toma de decisiones, la que evita la discrecionalidad y fomenta el trabajo colaborativo, la prevención y el intercambio de información.

De tal manera que una persona señalada por la comisión de un delito, por ejemplo homicidio, y para quien la autoridad ministerial emitió una orden de aprehensión, pueda ser identificada por oficiales de la Guardia Nacional mientras conduce un vehículo y comete una falta a los reglamentos de tránsito en carreteras federales, procediendo a la detención y puesta a disposición, incluso tiempo después de cometer el delito y residiendo en un lugar lejano de donde se señalaron los hechos delictivos.

Lo anterior representa una mayor eficacia para los agentes de la Guardia Nacional, al aprovechar la información que les provee el DTOP®, y significa una respuesta del Estado Mexicano al anhelo de justicia de las víctimas, a la reducción de la impunidad y la posibilidad de que estas conductas no se sigan presentando por el mismo individuo, dándole a este último la posibilidad de un juicio justo y una reinserción social. Contribuir de esta manera es la razón de ser del área de innovación tecnológica de la Dirección General Científica.

El DTOP®, como otras soluciones tecnológicas que se están desarrollando en la Dirección General Científica, permitirán fortalecer las operaciones policiales, generando un impacto que no se medirá desde la Guardia Nacional, pues el verdadero impacto de la tecnología será trasladado a la ciudadanía, al pueblo, que ve en sus instituciones a los garantes de la libertad, los derechos humanos, la justicia y la paz. Son los ciudadanos los que se verán beneficiados de todos los esfuerzos que día a día se realizan en cada uno de los laboratorios tecnológicos de la Guardia Nacional, desde ahí visualizamos el DTOP®, así como otras tecnologías, desde ahí estamos visualizando una mejor manera de servir, ¡desde ahí estamos creando el futuro!

Fuentes de consulta

- Borghino, Mario. Disrupción. Más allá de la innovación, México, Penguin Random House Grupo Editorial, 2018.
- Kawasaki, Guy. El arte de empezar 2.0, México, Paidós México, 2013.
- SEASKATE, INC. The evolution and development of police technology, a technical report prepared for The National Committee on Criminal Justice Technology, National Institute Of Justice. NCJRS Estados Unidos de Norteamerica, 1998. En https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf
- Thiel, Peter y Masters, Blake. De cero a uno, como inventar el futuro, Colombia, Grupo Planeta, 2014.

CRIPTOMONEDAS Y BLOCKCHAIN

Lancelot García Leyva[1]

"Lo importante es no dejar de hacer preguntas, No perder jamás la bendita curiosidad". Albert Einstein.
¡A un niño no le digas! la curiosidad mató al gato.

Sumario: I. Introducción. II. ¿Cuántas divisas virtuales hay? III. Monedero electrónico-wallet. IV. Red P2P y funcionamiento. V. Blockchain. VI. Minería, prueba de trabajo y prueba de participación. VII. Discusión.

Índice de Términos: *Peer-to-Peer* (P2P), *Blockchain* o cadena de bloques, Criptomonedas, Cryptodivisas, dinero digital, Bitcoin, DeFi, Stablecoin, ICO, Altcoin, Nft, minería, monedero electrónico, *wallet*.

I. Introducción

Se dice que la curiosidad es la disposición que engendra la exploración, la investigación y el aprendizaje. Todo se complica cuando los interrogantes se trasladan al futuro. Ahora mismo se están abriendo nuevos horizontes, y se anuncian cambios enormes, todos somos conscientes que le estamos diciendo adiós a un mundo y otro se está fraguando a gran velocidad.[2] ¡Si pudiéramos ir al futuro, con que nos encontraríamos...!

De acuerdo con el Instituto Tecnológico de Massachussets, una de las 10 tecnologías emergentes que realmente cambiarán nuestra forma de vivir y trabajar, es el dinero digital (criptomonedas) el cual tendrá un impacto masivo en la privacidad financiera.[3] De acuerdo con Entrepreneur, México se encuentra entre los 6 países con más usuarios de criptomonedas en el mundo.[4]

Realizó estudios de ingeniería en electrónica en la Universidad Tecnológica de la Mixteca, Maestría en el Instituto Nacional de Astrofísica, óptica y Electrónica, Doctorado en la Universitat Politècnica de Catalunya, España. Cursó la Especialidad en Seguridad Nacional y Regional en el ECISEN. Actualmente es director de area en la Dirección General Científica de la Guardia Nacional

N. deGrasse, «Cuando ya no esté,» 22-09-2016. [En línea]. Available: https://www.youtube.com/watch?v=MmHsKnjgOC4&feature=youtu.be

[3] MIT, «Las 10 Tecnologías Emergentes.» 17 02 2021. [En línea]. Available: https://www.technologyreview.es/listas/tecnologias-emergentes/2020

[4] E staff, «Entrepreneur.» 09-07-2029. [En línea]. Available: https://www.entrepreneur.com/article/353058#:~:text=%22Seg%C3%BAn%20la%20encuesta%2C%20la%20regi%C3%B3n,de%20la%20criptomoneda%22%20se%C3%B1al%C3%B3%20Statista. [Último acceso: 14-02-2021]

Cuando se realiza la compra de un bien o la renta de un servicio por medio de tarjeta de débito o crédito, hay una entidad bancaria que respalda y valida cualquier transacción. Esto no ocurre con el dinero en efectivo (es no personal), ya que éste nos permite hacer cualquier transacción sin que nadie solicite los datos personales como nombre o apellidos para poder realizarla. Ésto significa que no hay un tercero que valide la transacción en efectivo. Ésto analizó Satoshi Nakamoto, un investigador desconocido, que en el año 2008 publicó en *The Cryptography Mailing List*, el artículo *"Bitcoin: A Peer-to-Peer Electronic Cash System"*[5]. Satoshi propuso un sistema para crear dinero digital, una moneda que no existía en forma física como papel, metal o cualquier forma conocida, una moneda basada en bits y sin que esté centralizada en la banca o en el Gobierno.

La idea de dinero virtual, es similar al dinero que tenemos en el banco, como tal, es un número el cual podemos utilizar en una transacción digital por medio de tarjetas bancarias o transferencia, la cuestión aquí, es que siempre hay una entidad que valida dicha transacción, verifica que se tenga el fondo y después se refleje en la cuenta del destinatario. Si imaginamos una transacción bancaria, el banco en ese instante de tiempo no toma el dinero físico y lo lleva al destinatario, es un número que está en una cuenta y se refleja en otra, esto cumpliendo un proceso digital, protocolos y condiciones de seguridad. Algo similar ocurre con las criptomonedas.

Sin embargo, este modelo bancario no le termina de agradar a algunos usuarios, ya que al realizar una transacción siempre debe haber una entidad bancaria que verifique que sea válida. En esta situación el banco verifica que exista ese dinero (usando tarjeta de débito) o en su caso que se tenga el crédito (tarjeta de crédito) y lo transfiere a la cuenta destino. Incluso esto es similar cuando se utiliza un sistema de procesamiento y pago que agilizan las transacciones hechas con tarjetas de débito, crédito o prepago tal como American Express, Visa y MasterCard.

En tal escenario, al pagar por internet se está obligando a proporcionar los datos personales como son nombre, tipo de tarjeta, número de tarjeta, fecha de expiración y código de seguridad. Caso contrario a cuando se realiza una compra utilizando efectivo, el dinero es no personal, y nadie necesita saber quién eres. Existen otros inconvenientes tal como la inflación, la cual depende de muchos factores socio económicos, como puede ser que el gobierno imprima nuevos billetes sin que tenga algo que lo respalde, como puede ser el oro, entre otros, generando que el dinero pierda valor.

[5] S. Nakamoto, 31 Octubre 2008. [En línea]. Available: https://bitcoin.org/bitcoin.pdf

En general, la idea de Satoshi es lo que busca solucionar, ya que principalmente pretende desvincularse de cualquier entidad Bancaria y de Gobierno, no solo dando inicio a la primera moneda virtual conocida como Bitcoin (por sus siglas BTC), si no también, ha generado toda una revolución económica y social. Así mismo, Satoshi analizó y utilizó la red Peer-to-Peer, ya que la información va de usuario a usuario, sin que exista un intermediario, sin que esté centralizada la información, proponiendo aplicar este método para que sean gestionadas las transacciones de su moneda propuesta. Sin embargo, había cosas que resolver, como ¿dónde estaría el dinero?; para ello ideo un monedero electrónico donde se encuentre el dinero virtual. Así mismo, analizó la falta de un registro global de las transacciones e ideó uno de dominio público, donde todos los usuarios pudieran conocer el historial de cada moneda.

También propuso que fuera no personal, esto quiere decir que el registro sea público, pero privado en cuanto a quién pertenece ese dinero, como el dinero en efectivo, que el dueño es quien lo tiene. Este registro público es como el estado de cuenta del banco que contiene el registro de transacciones, al cual se le nombra libro maestro. Ahí se encuentran todas las transacciones de la historia, no sólo de un usuario, sino de todos, desde que inició la moneda con la primer transacción, hasta el día de hoy. Satoshi lo ideo de esta manera ya que con ello se puede trazar el historial de cualquier moneda y sobre todo, se puede consultar en cualquier momento, en atención a que el libro maestro es público.

El pasado 3 de febrero 2021, la Exchange Binance publicó su informe "Global Crypto User Index 2021"[7]. La metodología utilizada comprende el periodo del 15 de septiembre al 25 de octubre del 2020. Ellos examinaron datos de más de 61,000 usuarios de criptomonedas (cryptos), en más de 178 países y regiones alrededor del mundo, en el cual identificaron sus actitudes, preferencias, adopción y motivación.

a) Los principales hallazgos de este estudio son:
   - El número de usuarios dentro de la plataforma se incrementó, de 5.8 millones en 2017 a 101 millones a finales del 2020.
   - Se incrementó la inversión minorista en las cryptos ya que son más accesibles debido a las plataformas como ***PayPal, LocalBitcoins, GrayScale, Binance***, entre otras.

b) De acuerdo con la afiliación de los propietarios de cryptos:
   - El 52%, las ven como una fuente de ingreso.
   - Para el 15%, representan su principal fuente de ingreso.

6 Coinmarketcap, «Todas las cryptodivisas,» 17-02-2021. [En línea]. Available: https://coinmarketcap.com/es/all/views/all/y l. currencies, «Todas las criptomonedas,» 15 -02-2021. [En línea]. Available: https://mx.investing.com/crypto/currencies.

a) Razones que tuvieron para comprar cryptos:
   - El 55% ve a las cryptos como una oportunidad de inversión a largo plazo.
   - Sólo el 31% lo hace por una oportunidad de inversión a corto plazo, y un 27% sólo tiene cryptos por FOMO[8].
     - Durante un ciclo de mercado es común escuchar la palabra FOMO (Fear Of Missing Out).
     - Los proyectos DeFi[9] son más populares en el sureste asiático, donde el 52% de los usuarios de esta región usan algún proyecto.

b) Respecto al uso que le dan los propietarios de cryptos:
   - El 39% están HODL en Bitcoin y otras cryptos.
   - Apuestas y préstamos (22%) y pagos (11%).
   - Es posible que el uso de ***cryptografía*** como medio de intercambio no se perciba como el caso de uso más importante (21%), pero ya está desempeñando parcialmente ese papel.

c) Confianza en las criptomonedas:
   - Existe una confianza casi unánime en las criptomonedas (97%) entre los usuarios de criptomonedas:
     - Monedas estables: el 78% prefiere usar monedas bancarias en lugar de monedas estables.
     - El riesgo percibido sigue siendo la última barrera para la adopción cuando se aprovecha el modelo TAM de Pavlov (2003).

"No greater fools" (no más tontos): la adopción está impulsada principalmente por la utilidad futura esperada para los activos cryptográficos.

---

6 «Global crypto user Index 2021. Crypto user profiles, attitudes, and motivations,» 03-02-2021. [En línea]. Available.

7 Coinmarketcap, «Todas las cryptodivisas.» 17-02-2021. [En línea]. Available: https://coinmarketcap.com/es/all/views/all/y l. currencies, « Todas las criptomonedas,» 15-02-2021. [En línea]. Available: https://mx.investing.com/crypto/currencies

8 El término FOMO describe el miedo a perderse un acontecimiento emocionante e interesante y el sentimiento de que los demás tienen una vida mejor y más plena. Con este término se asocia la necesidad de estar permanentemente en contacto con los demás de manera digital para saber lo que están haciendo, https://www.ionos.mx/digitalguide/online -marketing/redes-sociales/fomo/

9 DeFi es la abreviatura de finanzas descentralizadas y es un término general para los servicios financieros clásicos que son procesados por una plataforma descentralizada como blockchain. https://economia3.com/que -es-defi-camino-finanzas-descentralizadas/

10 HODL es un término que significa «hold» (conservar) y que posteriormente se convirtió en el retroacrónimo, «hold on for dear life», que en español sería algo así como «conservar (la criptomoneda) como si fuera la vida en ello», https://www.etoro.com/es/news -and-analysis/trading/hodl-heres-guidelanguage-cryptocurrency-trading/

11 Yong Varela, Luis Antonio Modelo de aceptación tecnológica (tam) para determinar los efectos de las dimensiones de cultura nacional en la aceptación de las tic Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM, vol. XIV, núm. 1, enero-junio, https://www.redalyc.org/pdf/654/65414107.pdf

IV. ¿Cuántas divisas virtuales hay?

De acuerdo con el portal Investing.com, al 15 de febrero del 2021 existen 4,473 divisas digitales o criptomonedas, con una capitalización de mercado total de $1,492,319,151,689 y un volumen en las últimas 24 horas de $209,153,479,920. La criptomoneda más relevante es el Bitcoin, que de acuerdo con Coin Dance, tiene un valor de mercado de $48,695 con un hash rate del 98.3%, para la misma fecha. En el mismo sentido de acuerdo con coinmarketcap fecha 16 de febrero del 2021, existen 8,477 Criptomonedas, 33,821 mercados, con una capacidad de mercado de $1,492,177,535,224, un volumen de las últimas 24 horas de $209,206,867,272 BTC y un a dominance de 60.5%. De acuerdo con Bitcoin México, el costo del Bitcoin para la misma fecha es de $1,058,622.10, a las 21:08 hrs.

Para calcular con precisión el precio de un Bitcoin en México, ellos utilizan un promedio ponderado. Este precio se puede utilizar para negociar transacciones en Bitcoin, ya que es el precio mas apegado al mercado mxicano.

Las DeFi se crearon a partir de las ventajas que ofrece al sector financiero, la tecnología blockchain y las criptomonedas. Son un movimiento de muy rápido crecimiento construidas sobre la blockchain de Ethereum. Las DeFi permiten realizar cambios (exchanges) descentralizados y mercados, servicios de administración de activos (principal objetivo de Ethereum), plataformas de préstamos, soluciones de pagos, wallets crypto, entre otras.

Las DeFI son tan descentralizadas como sus creadores lo establezcan. Dentro de ellas existen muchos protocolos o plataformas DeFi como:

- DAI , la criptomoneda vinculada al dólar y respaldada por la criptomoneda Ethereum, creada con esa intención desde sus inicios.
- Exchange Uniswap, que a finales del año 2020 perdió su carácter descentralizado con el lanzamiento de UNI, su token de gobernanza.
- El proyecto 0x focalizado a la creación de exchanges descentralizados.
- Ren VM, un protocolo para la interoperabilidad entre las *blockchains* de Bitcoin; o Kyber, una casa de cambio descentralizada.

---

12 Currencies, Todas las criptomonedas, 15-02-2021. [En línea]. Available https://mx.investing.com/crypto/currencies.

13 E. staff, «Entrepreneur,» 09-07-2029. [En línea]. Available: https://www.entrepreneur.com/article/353058#:~:text=%22Seg%C3%BAn%20la%20encuesta%2C%20la %20regi%C3%B3n,de%20la%20criptomoneda%22%20se%C3%B1al%C3%B3%20Statista.. [Último acceso: 14-02-2021].

14 Coinmarketcap, «Todas las cryptodivisas,» 17-02-2021. [En línea]. Available: https://coinmarketcap.com/es/all/views/all/.

15 Bitcoin México,» 17-02-2021. [En línea]. Available: https://www.bitcoin.com.mx/precios/.

16 DeFi es la abreviatura de finanzas descentralizadas y es un término general para los servicios financieros clásicos que son procesados por una plataforma descentralizada como blockchain. https://economia3.com/que-es-defi-camino-finanzas-descentralizadas/

17 B. Academy, ¿Qué es DAI?, 27-02-2021. [En línea]. Available: https://academy.bit2me.com/que-es-dai/. [Último acceso: 27-02-2021].

Plataformas como Compound , Yearn Finance , Balancer o SushiSwap , presentan una descentralización intermedia. El código fuente de esas aplicaciones es visible, sin embargo, no se puede participar directa ni indirectamente en su mejora. Aún más preocupante es que los factores de control críticos están bajo su control. Para los casos de Compound y Yearn Finance, los fundadores tienen el control absoluto del software que hace posible su funcionamiento, donde para el caso de Yearn Finance se le denomina BDFL (Benevolent Dictator For Life) benevolente dictador para toda la vida.

Las stablecoins o monedas estables generalmente cuentan con algún tipo de respaldo para darles valor en el mercado. Algunas de ellas se encuentran respaldadas por dólares, otras más respaldadas por recursos naturales como el oro, diamantes, gas o petróleo, como es el caso del Petro. Sin embargo, es muy raro que se encuentren respaldadas por una criptomoneda. Las conocidas como criptomonedas estables, como Tether o DAI, han surgido para tratar de reducir la volatilidad de monedas virtuales como bitcoin o ether.

¿Qué es una ICO (Initial Coin Offering)? es un mecanismo de financiación para obtener fondos que utilizan los proyectos basados en blockchain, con el objetivo de darle un valor inicial a una nueva criptomoneda. A menudo los proyectos inmaduros realizan una pre-ICO, primero privada y luego una pública. Actualmente, existen más de mil proyectos ICO o criptomonedas que están en etapa inicial. Una opción de dónde se pueden encontrar las ICO son la lista publicada por Investing.com, Tokenmarket, entre otros.

Existen más de mil ICOs dentro del mercado, donde realizan una campaña de búsqueda de capitalización, ahí se vende un porcentaje de criptomonedas del proyecto a los inversionistas a cambio de medios de pago del gobierno u otras criptomonedas, usualmente Bitcoin. Las ICO comparten características de las IPO y los crowdfunding. En general prometen grandes beneficios tanto para los involucrados en el desarrollo como para los posibles inversores. Sin embargo, esencialmente son una tecnología experimental que aún se desconocen muchos efectos, comportamientos y fenómenos, eso hace que, aunque sea una fiebre, muchos proyectos están destinados al fracaso y otros tantos son un fraude. Un porcentaje de las ICOs dependen de Ethereum, que en sí mismas son un mecanismo experimental, esto es un experimento encima de un "experimento".

---

18 «COMPOUND,» 22-02-2021. [En línea]. Available: https://app.compound.finance/y Compound, 22 -02 2021. [En línea]. Available: https://es.crypto-economy.com/compound/

19 «Yearn,» 22-02-2021. [En línea]. Available: https://yearn.finance/

20 «Balancer,» 22-02-2021. [En línea]. Available: https://balancer.finance/.

21 «Sushiswap,» 22-02-2021. [En línea]. Available: https://crypto.com/price/sushiswap y «SushiswapCoin,» 22 02 2021. [En línea]. Available: https://www.coindesk.com/tag/sushiswap

22 BBVA, «¿Qué son las 'stablecoins' y para qué sirven?,» 22-02-2021. [En línea]. Available: https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/. [Último acceso: 22-02-2021]

Para tomar la mejor elección de una ICO deberás, validar que el proyecto que esté lanzando una ICO esté ligado o tenga: un sitio web, un White Paper que contenga sus objetivos, la idea, mapa de ruta de su ejecución, los medios para alcanzarlos, referenciación del equipo como su experiencia relevante (podría ser validada por Linkedin).

De acuerdo con Cointelegraph el monto total de los fondos recaudados a través de las ICO en toda su existencia se acerca a los 27,000 millones de dólares, siendo más representativa del 2017 al 2019. Así mismo, Cointelegraph hace un ranking de las 10 ICO con mayor retorno de inversión, medido por ROI que mide la cantidad de retorno de una inversión en relación con el costo de dicha inversión, donde . También ver ICO Stats, la cual presenta un ranking de ICO medidas por ROI en las últimas 24 hrs., última semana y mes.

$$ROI = \frac{|Gain|investment - Cost\ of\ investment|}{Cost\ of\ investment}$$

Las 10 ICOs con el mayor retorno de la inversión de acuerdo con Cointelegraph-2019, donde se resalta que no puede haber una lista definitiva de las 10 mejores ICO de todos los tiempos, ya que el posible retorno de la inversión depende totalmente del valor actual del token de un proyecto.

Las Altcoin son monedas alternativas que se derivan del código fuente del Bitcoin, por lo que se basa en ese código fuente para generar derivaciones, bifurcaciones, en ingles forks. El Bitcoin tiene un código fuente abierto. Algunas Altcoin que existen en el mercado son Litcoin (creada en 2011), Primecoin (2013), Ethereum (30 de julio 2015), Dash (18 enero 2018), Darkcoin (2014), TRON (2017), Ripple, Monero, Neo, entre miles más. Cada Altcoin ha sido creado para un propósito o temática distinta, pretendiendo de esta manera aportar valor y a la vez le da una ventaja.

Para incrementar la información de la ICO, sobre cómo elegir, evaluar, detectar si es estafa, comunidad y medios, etapa del proyecto, inversiones de capital de riesgo.

---

23 INVESTING, 26-02-2021. [En línea]. Available: https://mx.investing.com/cryp to/ico-calendar [Ultimo acceso: 26-02-2021]
24 T. Market, 01-02-2018. [En línea]. Available: https://tokenmarket.net. [Último acceso: 26 -02-2018]
25 T. Linkedin, 26-02-2021. [En línea]. Available: https://www.linkedin.com/. [Ultimo acceso: 26 -02-2021]
26 T. Cointelegraph, 27-02-2021. [En línea]. [Último acceso: 27-02-2021].

Cada altcoin busca incorporar detalles técnicos que Bitcoin no incorporó cuando fue propuesto y sacado al mercado. Finder presenta una lista de la A a la Z, donde se puede ver la finalidad para cada altcoin, a qué sector está enfocado, su inversión, entre otros. La importancia de las altcoin, es que para el año 2019 movía el 40% del mercado de las criptomonedas; otro factor a considerar es que si una altcoin es relativamente nueva o no es muy conocida, seguramente será más difícil de comprar y tendrá menos monederos que la soporten, ver la sección III. Monedero Electrónico. De los miles de altcoin que han existido en el mercado, solo unas cuantas han logrado un crecimiento significativo como Bitcoin. Medir la capitalización de mercado de una altcoin, es una forma de conocer su aceptación en el mercado y la popularidad que va ganando. Cada altcoin tiene una "caracteristica única" que la hace mejor en su desempeño futuro.

A modo de ejemplo: Litecoin confirma transacciones más rápido que Bitcoin; Dash y Monero se enfocan al aspecto del anonimato, realizando transacciones casi imposibles de rastrear. Las altcoins también pueden variar del Bitcoin en la manera en que se extraen. Por ejemplo, el algoritmo minero de Bitcoin se llama SHA-256, mientras que el algoritmo minero de Litecoin se llama Scryrpt. Esto deriva que para una minería adecuada se requieren diferentes tipos de hardware.

Los NFT (Non-Fungible Tokens) son los activos digitales que están transformando el coleccionismo de arte y bienes digitales. Son la versión digital de los sellos, el arte o cualquier otro producto tangible o intangible al que una serie de usuarios acaban confiriendo un valor. Al contrario de lo que ocurre con las criptodivisas, los NFTs no se pueden intercambiar entre sí, ya que no hay dos NFTs iguales: tu carta de un criptogato es única (cryptokitties), ver Gráfico 4, a); o cryptopunks es única, b); como lo es una obra de arte digital o cualquier otro bien intangible. De acuerdo con Coindesk, hay una analogía entre un NFT y una entrada para un evento musical, para la entrada se tiene información acerca del comprador, la fecha, hora y lugar del evento, para los NFTs, es similar que los hace personales y únicos.

---

27 T. I. Stats, 27-02-2021. [En línea]. Available: https://icostats.com/ [Último acceso: 27 -02-2021]

28 27-02-2021. [En línea]. Available: https://es.cointelegraph.com/ico-101/how-to-choose-an-ico-toinvest-in [Último acceso: 27-02-2021].

29 Finder, The top 100+ cryptocurrency altcoins you should know about, 27-02-2021. [En línea]. Available: https://www.finder.com/cryptocurrency/altcoins [Último acceso: 27 -02-2021]

30 Finder, The top 100+ cryptocurrency altcoins you should know about, 27-02-2021. [En línea]. Available: https://www.finder.com/cryptocurrency/altcoins. [Último acceso: 27 -02-2021].

31 BBVA, «BBVA crypto gatitos gente compra masivamente,» 28-02-2021. [En línea]. Available: https://www.bbva.com/es/crypto-gatitos-gente-compra-masivamente/ [Último acceso: 28-02-2021]; y Cryptokitties, 28-02-2021. [En línea]. Available: https://www.cryptokitties.co/. [Último acceso: 28 -02-2021].

32 COINDESK, 28-02-2021. [En línea]. Available: https://www.coindesk.com/ [Último acceso: 28 -02-2021].

La mayoría de estos "tokens" pueden ser monedas, sellos, obras de arte, criptogatos, cryptopunks , entre cientos más; los cuales se basan en los estándares de la red Ethereum y de Blockchain. Eso les ha permitido que su operación sea efectiva a la hora de la compraventa, además de que los servicios de monederos como MetaMask o MyEtherWallet, que permiten interactuar con Ethereum las hacen más ágiles, versátiles y fuertes en sus transacciones.

Las características de las NFTs:

- Son activos con similitudes a las obras de arte: en el caso de una copia, el propietario puede certificar que es el dueño único y real, aún cuando se pueda fácilmente compartir en internet.

- Indivisibles: los NFT tienen un valor de entidad o token completo y no se pueden dividir en partes a diferencia de las criptodivisas. No puedes tener una fracción 1/1000 de una obra o avatar.

- No interoperables: solo puedes usar un avatar/tarjeta en el propio juego, no así en otros juegos similares.

- Indestructibles: los datos de un NFT se almacenan en la cadena de bloques a través de un contrato inteligente (*Smart Contract*), lo que hace que no se puedan destruir, eliminar o replicar.

- En los contratos inteligentes no solo se trata de almacenar electrónicamente documentación o permitir la firma electrónica, como se ha hecho hasta ahora, sino que estos programas realizan análisis y ejecutan alguna de las partes de su lógica interna. El contrato inteligente del software o programa puede definir reglas y consecuencias estrictas del mismo modo que lo haría un documento legal tradicional, pero a diferencia de los contratos tradicionales, también puede tomar información como "*input*", procesarla según las reglas establecidas en el contrato y adoptar cualquier medida que se requiera como resultado de ello: en sí son parte de la programación.

- Propiedad absoluta: el bien intangible tiene un dueño, a diferencia de servicios tradicionales de renta de música o películas.

- El 27 de febrero del 2021, el artista Ozuna lanzó una colección de 5 tokens no fungibles (NFT) llamada "Ositos" inspirados en su logotipo. Cada pieza tiene su sello de autenticidad digital con valor alrededor de 1,600 dólares. Con ello Ozuna se convirtió en el primer cantante Latinoamericano en sacar a la venta una serie de colecciones NFT.

- El coleccionista Pablo Rodríguez-Fraile, en octubre del 2020 gastó alrededor de $67,000 dólares en un videoarte NFT de 10 segundos, ***collage*** de algo más de

5,000 imágenes creadas (una por día) por el artista Bleepe. A finales de febrero del 2021 lo vendió por 6.6 millones de dólares y fue validada por blockchain.

La casa de subastas Christie's lanzó su primera venta de arte digital - un collage de 5,000 imágenes, también de Beeple- que existe únicamente como NFT. Las ofertas por la obra han alcanzado los 3 millones de dólares, y la venta se cerrará el 11 de marzo del 2021.

Verificable: mediante la blockchain se verifica el historial de quién ha comprado-vendido un NFT, quién es el propietario actual y absoluto, los datos del creador, etc., a diferencia de un arte o sello tradicional.

III. Monedero electrónico – wallet

Las wallet funcionan similar a la bolsa de valores de un país: en el caso de USA, en New York el Dow Jones presenta índice bursátil de las acciones de las empresas, mientras que el Nasdaq esta focalizado solo a las empresas de tecnología. Entonces las wallet son el lugar donde se guardan, así como desde donde se envían y reciben de "forma segura" las criptomonedas. No todas las wallet aceptan multi monedas, hay algunas que son compatibles con un solo tipo de criptomoneda, como son los casos de Cardano (nombrado deadalus wallet, open source para ada)[39] e IOTA (nombrado Trinity wallet).

---

33 Cryptopunks, 28-02-2021. [En línea]. Available: https://www.larvalabs.com/cryptopunks. [Último acceso: 28-02-2021].
34 MetaMask, 28-02-2021. [En línea]. Available: https://m etamask.io/. [Último acceso: 28-02-2021].
35 «Myetherwallet.» 28-02-2021. [En línea]. Available: https://www.myetherwallet.com/ [Último acceso: 28-02-2021].
36 B. J. Martínez «BeInCrypto.» 28-02-2021. [En línea]. Available: https://es.beincrypto.com/arti stareggaeton-ozuna-lanza-primera-coleccion-arte-digital-nft/. [Último acceso: 28-02-2021].
37 Bleepe, «Twitter.» 16-02-2021. [En línea]. Available: https://twitter.com/ChristiesInc/status/1361691513416265735?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1361691513416265735%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.xataka.com%2Fcriptomonedas%2Fque-nft-activos-digitales-que-estan-transfo. [Último acceso: 01-03-2021].
38 Bleepe, «Twitter.» 01-03-2021. [En línea]. Available: https://twitter.com/ChristiesInc/status/1365100549385957378?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1365100549385957378%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.eleconomista.com.mx%2Fmercados%2FComo-un-videoclip-de-10-segundos-de-Bee. [Último acceso: 01-03-2021].

Las wallet pudieran ser clasificadas en tres grandes categorías: las calientes, tibias o híbridas y las frías o de hardware.

- **Wallet caliente:** Son de alto riesgo porque son muy vulnerables a hackeo o robo y las puedes encontrar en las ***Exchange***, sólo se recomienda para los que hacen ***trading***. En si las criptomonedas se guardan en la ***Exchange***.

  Las ***Exchange***, son una plataforma para el intercambio de criptomonedas o por dinero fiat (dólares, euros, yen, pesos), también listan los valores de un número determinado de criptomonedas. No todas las plataformas permiten cambiar las cryptos a dinero fiat: para el caso de Bitfinex se pueden cambiar las cryptos a dólares y euros, que acepta al menos $10,000 dólares como inversión inicial. En el caso de ***Binance*** solo hace el cambio entre cryptos.

- ***Principals Exchange: Bit nex , Binance , Bitrex , Coinmarket*** , entre muchas más.
- Wallet tibia o hibrida: Son de riesgo moderado a ser hackeadas, las cuales existen para computadora, dispositivo móvil y web (url).

  Wallets: Bitcoin, Bitso, Staking, Exodus, trust, uphold, monero, trading, MyEtherWallet, coins, theta, polkadot, review, BRD, Edge, Blockstream Green, Aqua, entre muchas más.
- Como pueden ser hackeadas: si alguien ingresa físicamente a tu dispositivo o ingresa un virus en tu pc o dispositivo móvil; si pierdes el dispositivo móvil, entre muchos otros factores.

  Wallet fría o de hardware: Son las que tienen un riesgo muy bajo de que la información sea hackeada o robada, ya que se almacenan en un hardware que tu conectas principalmente a tu computadora. A ese hardware comúnmente se les denomina hardware wallet y paper
- wallet, en ambos casos se validan por un código encriptado como QR. Sorprendentemente, existe un solo reloj de wallet ***Frank Muller*** en México, está en el Estado de Jalisco.
- Las recomendaciones para el mundo de los wallet, es similar al mundo de las computadoras. Primero que se utilice una contraseña muy fuerte, utilizar palabras de recuperación (actualmente son 12 palabras) guardarla en un sitio seguro, ya que, si se pierde la contraseña, seguramente se perderá la inversión. Utilizar una doble autenticación.
- Hasta este punto se ha visto el mundo de las criptomonedas y el blockchain, en los siguientes apartados se discutirán los principales componentes técnicos de ellas.

39 IOTA, «Trinity,» 28-02-2021. [En línea]. Available: https://trinity.iota.org/ [Ultimo acceso: 28 -02-2021].
40 Cardano, 28-02-2021. [En línea]. Available: https://cardano.org/ [Ultimo acceso: 28 -02-2021].
41 Cardano, 28-02-2021. [En línea]. Available: https://cardano.o rg/ [Ultimo acceso: 28 -02-2021].
42 Cardano, 28-02-2021. [En línea]. Available: https://cardano.org/ [Ultimo acceso: 28 -02-2021].
43 IOTA, «Trinity,» 28-02-2021. [En línea]. Available: https://trinity.iota.org/ [Ultimo acceso: 28 -02-2021].
44 Coinmarketcap, «Todas las cryptodivisas,» 17-02-2021. [En línea]. Available: https://coinmarketcap.com/es/all/views/all/
45. Buybitcoinworldwide, «Best Bitcoin & Cryptocurrency Wallets,» 28-02-2021. [En línea]. Available: https://www.buybitcoinworldwide.com/wa llets/#hot-wallets. [Ultimo acceso: 28-02-2021].

IV. Red P2P y funcionamiento

Una red P2P (acrónimo de peer-to-peer), es un conjunto de ordenadores que reciben el nombre de nodos, que se conectan para compartir datos de todo tipo y en la que cada máquina (PC, ordenador, computadora) actua como cliente o servidor.

Estas redes se diferencian de la arquitectura clásica cliente-servidor, que la mayoría de infraestructuras informáticas adoptadas, donde existe un servidor (computadora central) el cual atiende las demandas de otras computadoras incluidas a su red (los clientes). Así mismo, el servidor es quien establece los privilegios que tienen sus clientes respecto al acceso de los recursos de la red, así como de la información existente-disponible en la misma. Este sistema de privilegios desaparece en una red P2P.

En una red P2P cada computadora tiene los mismos privilegios que su vecina, esté físicamente cerca o no, en otras palabras puede ser que la computadora vecina esté en la misma red doméstica o al otro lado del mundo. En una red P2P, cada nodo representa una fracción de los recursos de la red, éstos pueden ser capacidad de procesamiento, almacenamiento, ancho de banda de red a otras computadoras participantes, sin que exista una computadora central que lleve exclusivamente la operación – coordinación de todo. En si, los recursos se proporcionan y consumen por igual por cada una de las computadoras en función de sus capacidades, lo que permite que cada uno de los usuarios de dicha red pueda obtener la información que necesite de cualquier otro miembro.

Las herramientas computacionales que han utilizado este mecanismo de compartir archivos han sido Napster, Ares, Torrent (con su cryptomoneda BitTorrent), Kaza, emule, entre otros. Cuando se quiere descargar un archivo mediante una de estas herramientas, el archivo no está en un servidor central. Este archivo se encuentra en varios clientes P2P, entonces el que la requiere mediante la red P2P, va recolectando fragmentos de los demás clientes que la tienen.

Una vez que ha terminado de descargar el archivo solicitado, el solicitante se convierte en un tipo de servidor que la proporciona a otro solicitante, incluso aunque se haya terminado de descargar. Esto tiene varias ventajas, ya que se agiliza la descarga, el archivo puede estar almacenada en varios usuarios P2P, y en caso de que uno de los usuarios se desconecte, se puede seguir descargando de los demás usuarios conectados a la red P2P.

V. Blockchain

Blockchain o cadena de bloques es un sistema de grabación de información estructurado de tal manera que es muy difícil o imposible de modificar, hackear o engañar al sistema; o sí, siempre y cuando la mayoría de los participantes – mineros sea fraudulentos. Una cadena de bloques es esencialmente un libro de contabilidad digital de transacciones que se replica y distribuye a través de toda la red de sistemas informáticos participantes en la cadena de bloques.

La transacción de una criptomoneda a través de una cadena de bloques, se realiza en seis pasos como se muestra en el Gráfico 5:

1. Alguien solicita una transacción
2. La solicitud es transmitida a todos los nodos de la red P2P (conformada por computadoras).
3. Mediante un algoritmo matemático denominado prueba de trabajo en conjunto con la red de nodos P2P, validan el estatus de los usuarios, así como la transacción (mediante democracia) y el estatus de los usuarios.

    a. Una transacción verificada incluye criptomonedas, contratos, registros u otra información.
    b. Criptocurrencia – criptomoneda

        i. No tiene un valor intrínseco el cual pueda ser cambiado por otra mercancía.
        ii. No tienen una forma física ya que existe solo en la red.
        iii. Su suministro no está determinado por un banco central, la red está completamente descentralizada.

4. Esta transacción es combinada con otras transacciones para crear un bloque, que tiene un tamaño de 1 MB, alrededor de 2,000 transacciones por bloque, en un periodo de 10 minutos.
5. El bloque nuevo es añadido permanentemente a la cadena de bloques existentes.
6. La transacción es completada, entonces el valor de la transacción pertenece al solicitante.

VI. Minería, Prueba de Trabajo y Prueba de Participación

La minería de criptomonedas es aquella actividad computacional que por medio de la resolución de algoritmos matemáticos (dos), verifica tanto la emisión de nuevas criptomonedas como las transacciones realizadas en su red blockchain, que en ambos casos el minero se ve recompensado por criptomonedas.

- Algoritmo de minería o hashing algorithm, está estrechamente relacionado con el procesamiento de datos o prueba de trabajo (PoW). En gran medida el hardware minero depende del algoritmo de minado de una determinada criptomoneda. Como es el caso de los dispositivos de minado ASIC para Bitcoin (BTC), especializado para minar el algoritmo SHA-256. Ver figura 4, a). Si quieres minar ether (ETH) o zcash (ZEC), se necesita al menos una tarjeta gráfica dedicada (GPU) y una computadora una fuente de voltaje certificada. Por otro lado, para minar monero (XMR) o bytecoin (BCN), es suficiente un procesador (CPU) de la computadora. En todos los casos el minero debe lograr antes que los demás nodos, obtener la solución a dicho acertijo, y con ello anexar un bloque nuevo de transacciones a la blockchain.

- Algoritmo de consenso, el cual te permite ser parte del consenso o votación mayoritaria entre todos los miembros (nodos) de una red de criptomonedas. Una vez que se resuelve es posible determinar qué transacciones cumplen con los criterios de valides, orden de bloques en la blockchain. Este algoritmo es conocido como prueba de participación (PoS). (Ver Gráfico 6).

La prueba de trabajo al 1 de agosto de 2017, para la red de Bitcoin estaba cerca de 8 horas de procesamiento. Mientras que el hash en 100EHS.

La minería se puede realizar de manera física u "online", en el primer caso, se implementa una granja de minería, utilizando equipo muy potente y en condiciones exigentes de temperatura – enfriamiento, ya que estos equipos consumen mucha energía y emiten elevado calor, las ganancias por recompensa son mayores, ganancias constantes o predecibles y hay que hacer una inversión considerable, se necesita tener conocimientos técnicos. La segunda es a través de la renta de equipo de minería, no necesitas conocimientos técnicos, la inversión es variable dependiendo de las condiciones de renta y periodo del equipo rentado, las ganancias son menores al primer tipo de minería.

Para que opere el hardware de minería es necesario tener diferentes herramientas informáticas las cuales se identifican como software minero, de monitoreo del comportamiento de hardware y monitoreo de desempeño.

- Software minero es la herramienta informática que permite al hardware interactuar con la red de la criptomoneda a minar.
- CGMiner, se utiliza para minar Bitcoin y Bitcash, es ASIC multiplataforma escrito en C y basado en cpuminer.
- Claymore , está focalizada para la minería de ether, ethereum classic, zcash, decred y siacoin, entre otras.
- Software para monitorear el comportamiento del hardware, así como configurar las preferencias de éste.
- Para el caso de hardware de minería ASIC como el AntMiner de Bitmain, incluyen software propio desde donde se configura, así como vigila su desempeño.
- Si se mina con un GPU comúnmente se utiliza MSI Afterburner o GPUZ[46] , para configurar y vigilar el desempeño.
- Monitorear el desempeño del "rig" minero puede ser usando el programa TeamViewer , que accede el sitio web pool de minería desde donde se realiza la minería.

Para la minería de criptomonedas se requiere de una capacidad de cómputo muy grande lo que lleva a un consumo de energía elevado, tanto que llega a consumir más que países enteros, como fue expuesto por Cristian Rus el pasado 19 de enero del 2021 en TeamViewer que para la Nación de Irán se estimaba que el minado de criptomonedas provocó una subida del 7% en el consumo de electricidad. Fue tan preocupante que la empresa estatal de electricidad iraní determinó cerrar una granja de recién creación debido al gran consumo de electricidad que implicaba. Mientras que las autoridades declararon que los culpables de apagones en ese país, se debían al alto consumo de granjas mineras de criptomonedas.

46 Eobot, «Eobot,» 28-02-2021. [En línea]. Available: https://www.eobot.com/cgminertutorialesp.pdf. [Último acceso: 21-02-2021], M. Kurko, «Investopedia,» 21-02-2021. [En línea]. Available: https://www.investopedia.com/best-bitcoin-mining-software-5095403. [Último acceso: 28-02-2021] y Admin, «LinuxHint,» Mine Bitcoins with Cgminer On Ubuntu, 2018. [En línea]. Available: https://linuxhint.com/mine-bitcoins-cgminer-ubuntu/. [Último acceso: 28-02-2021].

47 MinerGate, «MinerGate,» 2014 - 2021. [En línea]. Available: https://es.minergate.com/altminers/cpuminer-multi. [Último acceso: 28-02-2021]

48 Claymore, «Github,» Claymore-Dual-Miner, 28-02-2021. [En línea]. Available

49 Bitmain, «Bitmain,» 28-02-2021. [En línea]. Available: https://www.bitmain.com/products/antminer/. [Último acceso: 28-02-2021].

50 MSI, «msi dragon center,» 28-02-2021. [En línea]. Available: https://www.msi.com/Landing/afterburner. [Último acces o: 28-02-2021].

51 TeamViewer, 28-02-2021. [En línea]. Available: https://www.teamviewer.com/es-mx/. [Último acceso: 28-02-2021].

52 C. Rus, «Xataka,» 19-06-2019. [En línea]. Available: https://www.xataka.com/criptomonedas/iran-estasufriendo-apagones-luz-a-nivel-nacional-autoridades-culpan-a-granjas-bitcoin. [Último acceso: 2802-2021].

Otro caso, sucedió el pasado 8 de febrero del 2021 en Teherán donde HardZone , reporta que ese país se quedó sin electricidad debido a un consumo de 450MW por GPUs gaming, el consumo equivalente a una ciudad de 100,000 habitantes.

¿Por qué Teherán? En este país la energía se produce a un costo de 1.8 centavos por kWh y se vende a más de 10 veces su valor al público, sin embargo, los mineros la obtienen por un precio alrededor de 2.2 centavos el kWh. Esto no ocurre ni en China, motivo por el cual los mineros se han instalado en esta nación. Este consumo eléctrico también ocasiona un problema ambiental, ya que esta actividad no hace pausas en ningún periodo de tiempo. El Centro de Finanzas Alternativas de la Universidad de Cambridge realizó un estudio donde estableció que la red de Bitcoin consume más energía (electricidad) que Finlandia, Chile, Colombia o los Países bajos. Este mismo estudio estima que la red de Bitcoin consume al menos 123.64 TWh (teravatios-hora), resaltando que una parte importante de las emisiones de CO2 es generada por la industria eléctrica.

Para tener una perspectiva nacional esto equivale al 46.14% de energía eléctrica que produce la Comisión Federal de Electricidad (CFE).

Derivado de lo anterior Ethereum está emigrando de la prueba de trabajo (proof of work) a la prueba de participación (proof of stake). La prueba de trabajo o minado es realizar cálculos computacionales muy costosos para resolver un algoritmo matemático, se recompensa al primer minero que resuelve el problema de cada bloque, entre otros, mientras que en la prueba de participación el nuevo bloque creado es elegido de manera determinística, establecida por su participación, no existe una recompensa de bloque por ello los mineros toman las tarifas de transacción (los mineros son llamados forjadores), puede ser miles de veces más rentable, red descentralizada, usuarios no anónimos, cadenas de bloques públicas, es necesario solicitar permiso para que los usuarios tengan una copia del libro mayor y para participar en la confirmación de transacciones.

Estamos en un punto donde se tiene una visión general del mundo de las criptomonedas y el blockchain, sin embargo, no se han tocado temas relevantes, como es la seguridad, las debilidades del sistema y como los hackers han aprovechado esas debilidades, el trading, entre otros.

53. HZ, «hardzone.es,» Los mineros dejan sin luz a Teherán: 450 MW consumidos por GPUs gaming, 08-02-2021. [En línea]. Available: https://hardzone.es/noticias/tarjetas-graficas/consumo-mineriacriptomonedas-teheran/. [Último acceso: 28-02-2021].
54.

VII. Discusión

Indiscutiblemente las criptomonedas han venido a cambiar nuestro mundo, han marcado una disrupción en el mundo financiero. En lo personal concuerdo con Gerry Rice, el principal portavoz del Fondo Monetario Internacional, quien dijo en febrero del 2021 que los Gobiernos deberían sacar partido a beneficios del dinero digital y abordar sus riesgos. "Las monedas digitales públicas y privadas pueden reducir el costo de hacer negocios, mejorar la productividad, la inclusión financiera y la integración del mercado".

Las Monedas Digitales de Bancos Centrales (MDBC) pueden fortalecer la resiliencia y eficiencia del sistema de pagos a menores costos, agilizar los pagos, incrementar la competencia e inclusión financiera. Los gobiernos deberían esforzarse por lograr un enfoque equilibrado frente al dinero digital para aprovechar los beneficios y abordar los riesgos, entre ellos la seguridad cibernética, tal como lo está haciendo el mundo del deporte, la música y el arte.

La historia de existencia del dinero digital ha demostrado que van ganando terreno en todas las ramas comerciales, que muchas empresas han apostado y siguen apostando por el uso del dinero digital. Hasta el punto, que Tesla ha invertido en Bitcoins. Por otro lado, a finales del 2019, Walmart indicaba que ya trabajaba en el desarrollo de una moneda digital que estaría respaldada por dólares estadounidense, de acuerdo con la solicitud de patente con número 20190236564 publicada por la Oficina de Patentes de Estados Unidos (USPTO) en la cual, la cadena detallista (retail) busca registrar "una unidad monetaria digital atando la unidad monetaria digital a una moneda normal; almacenar información de la unidad monetaria digital en una blockchain; comprar o pagar la unidad monetaria digital".

En ese mismo sentido existe un revuelo entre los clientes de McDonalds, que el 9 de marzo del 2021, referencian a la moneda física McCoin que McDonald's lanzó en el 2018 con motivo a las celebraciones de los 50 años de su icónica Big Mac. Moneda que se puso a disposición de todo el mundo la cual funcionaba como un cupón intercambiable únicamente por una Big Mac. Pareciera que dicha moneda está en proceso de digitalizarse a escala global.

En el escenario de la ciberseguridad, múltiples plataformas han sufrido ataques cibernéticos donde se han perdido muchas monedas digitales que es imposible recuperarlas (millones de dólares), incluso ciberdelincuentes han encontrado la forma de vulnerar el sistema, entre algunas formas mediante la debilidad de la prueba de trabajo. Para contrarrestar el riesgo Bitso contrató un seguro contra robo de bitcoin, litecoin y bitcoin cash, es una póliza que Bitso adquirió con Coincover, aseguradora especializada en el sector de criptomonedas y blockchain, suscrita por Lloyd's of London con el objetivo de cubrir los fondos en sus hot y warm wallets.

Fuentes de Consulta

- N. deGrasse, «Cuando ya no esté,» 22-09-2016. [En línea]. Available: https://www.youtube.com/watch?v=MmHsKnjgCC4&feature=youtu.be.
- MIT, «Las 10 Tecnologías Emergentes,» 17-02-2021. [En línea]. Available: https://www.technologyreview.es/listas/tecnologias -emergentes/2020.
- E. staff, «Entrepreneur,» 09-07-2020. [En línea]. Available: https://www.entrepreneur.com/article/353058#:~:text=%22Seg%C3%BAn%2 0la%20encuesta%2C%20la%20regi%C3%B3n,de%20la%20criptom oneda%22 %20se%C3%B1al%C3%B3%20Statista. [Último acceso: 14 02 2021].
- S. Nakamoto, 31 Octubre 2008. [En línea]. Available: https://bitcoin.org/bitcoin.pdf.
- Coinmarketcap, «Todas las cryptodivisas,» 17-02-2021. [En línea]. Available: https://coinmarketcap.com/es/all/views/all/.
- I. currencies, «Todas las criptomonedas,» 15-02-2021. [En línea]. Available: https://mx.investing.com/crypto/currencies.
- «Global crypto user Index 2021, Crypto user profiles, attitudes, and motivations,» 03-02-2021. [En línea]. Available:
- https://research.binance.com/static/pdf/Global_Crypto_Index_2021.pdf.
- «Bitcoin México,» 17-02-2021. [En línea]. Available:
- https://www.bitcoin.com.mx/precios/.
- B. Academy, ¿Qué es DAI?, 27-02-2021. [En línea]. Available: https://academy.bit2me.com/que -es-dai/. [Último acceso: 27-02-2021].
- «COMPOUND,» 22-02-2021 [En línea] Available: https://app.compound.finance/.
- Compound, 22-02-2021. [En línea]. Available: https://es.cryptoeco nomy.com/compound/.
- «Yearn,» 22-02-2021. [En línea]. Available: https://yearn.finance/.
- «Balancer,» 22-02-2021. [En línea]. Available: https://balancer.finance/.
- «Sushiswap,» 22-02-2021. [En línea]. Available: https://crypto.com/price/sushiswap.
- «SushiswapCoin,» 22-02-2021. [En línea]. Available: https://www.coindesk.com/tag/sushiswap.
- BBVA, «¿Qué son las 'stablecoins' y para qué sirven?,» 22-02-2021. [En línea]. Available: https://www.bbva.com/es/que -son-las-stablecoins-y-para-quesirven/. [Último acceso: 22-02-2021].

INVESTING, 26-02-2021. [En línea]. Available: https://mx.investing.com/crypto/ico -calendar. [Último acceso: 26-02-2021].
T. Market, 01-02-2018. [En línea]. Available: https://tokenmarket.net. [Último acceso: 26-02-2018].
Linkedin, 26-02-2021. [En línea]. Available: https://www.linkedin.com/. [Último acceso: 26-02-2021].
Cointelegraph, 27-02-2021. [En línea]. [Último acceso: 27-02-2021].
I. Stats, 27-02-2021. [En línea]. Available: https://icostats.com/. [Último acceso: 27-02-2021].
27-02-2021. [En línea]. Available: https://es.cointelegraph.com/ico -101/how-tochoose-an-ico-to-invest-in. [Último acceso, 27-02-2021].
Finder, The top 100+ cryptocurrency altcoins you should know about, 27 -022021. [En línea]. Available: https://www.finder.com/cryptocurrency/altcoins. [Último acceso: 27 -02-2021].
BBVA, «BBVA crypto gatitos gente compra masivamente,» 28 02 2021. [En línea]. Available: https://www.bbva.com/es/crypto -gatitos-gente-compramasivamente/. [Último acceso: 28-02-2021].
Cryptokitties, 28-02-2021. [En línea]. Available: https://www.cryptokitties.co/. [Último acceso: 28 -02-2021].
Cryptopunks, 28-02-2021. [En línea]. Available: https://www.larvalabs.com/cryptopunks. [Último acceso: 28 02 2021].
COINDESK, 28-02-2021. [En línea]. Available: https://www.coindesk.com/. [Último acceso: 28-02-2021].
MetaMask, 28-02-2021. [En línea]. Available: https://metamask.io/. [Último acceso: 28-02-2021].
«Myetherwallet,» 28-02-2021. [En línea]. Available: https://www.myetherwallet.com/. [Último acceso: 28 -02-2021].
B. J. Martínez, «BeInCrypto,» 28-02-2021. [En línea]. Available: https://es.beincrypto.com/artista -reggaeton-ozuna-lanza-primeracoleccion-arte-digital-nft/. [Último acceso: 28 02 2021].
Bleepe, «Twitter,» 16-02-2021. [En línea]. Available: https://twitter.com/ChristiesInc/status/1361691513416265735?ref_src=twsrc%5
Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1361691513416265735%7Ct
wgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.xataka.com%2Fcri ptomonedas%2Fque-nft-activos-digitales-que-estan-transfo. [Último acceso: 01-03- 2021].
Bleepe, «Twitter,» 01-03-2021. [En línea]. Available: https://twitter.com/ChristiesInc/status/1365100549385957378?ref_src=twsrc
%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1365100549385957378
%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.eleconomi

sta.com.mx%2Fmercados%2FComo-un-videoclip-de-10-segundos-de-Bee.
[Último acceso: 01-03-2021].
Cardano, 28-02-2021. [En línea]. Available: https://cardano.org/. [Último acceso: 28- 02-2021].
IOTA, «Trinity,» 28-02-2021. [En línea]. Available: https://trinity.iota.org/. [Último acceso: 28-02-2021].
BITFINEX, 28-02-2021. [En línea]. Available: https://www.bitfinex.com/. [Último acceso: 28-02-2021].
BINANCE, 28-02-2021. [En línea]. Available: https://www.binance.com/en. [Último acceso: 28-02-2021].
BITTREX, «Bittrex Global,» 28-02-2021. [En línea]. Available: https://global.bittrex.com/. [Último acceso: 28 -02-2021].
Buybitcoinworldwide, «Best Bitcoin & Cryptocurrency Wallets,» 28-02-2021. [En línea]. Available: https://www.buybitcoinworldwide.com/wallets/#hotwallets. [Último acceso: 28-02-2021].
Eoboot, «Eoboot.» 28-02-2021. [En línea]. Available:
https://www.eobot.com/cgminertutorialesp.pdf. [Último acceso: 21-02-2021].
M. Kurko, «Investopedia,» 21-02-2021. [En línea]. Available:
https://www.investopedia.com/best-bitcoin-mining-software-5095403. [Último acceso: 28-02-2021].
Admin, «LinuxHint,» Mine Bitcoins with Cgminer On Ubuntu, 2018. [En línea]. Available: https://linuxhint.com/mine-bitcoins-cgminer-ubuntu/. [Último acceso: 28-02-2021].
MinerGate, «MinerGate,» 2014 - 2021. [En línea]. Available: https://es.minergate.com/altminers/cpuminer-multi. [Último acceso: 28-022021].
Claymore, «Github,» Claymore-Dual-Miner, 28-02-2021. [En línea]. Available: https://github.com/Claymore-Dual/Claymore-Dual-Miner. [Último acceso: 28-02- 2021].
Bitmain, «Bitmain,» 28-02-2021. [En línea]. Available:
https://www.bitmain.com/products/antminer/. [Último acceso: 28 02 2021].
MSI, «msi dragon center,» 28-02-2021. [En línea]. Available:-https://www.msi.com/Landing/afterburner. [Último acceso: 28 -02-2021].
B. España, «Asesoramiento configuraciones Software minero,» 28-02-2021. [En línea]. Available: https://forobits.com/t/asesoramiento-configuracionessoftware-minero/4622/78. [Último acceso: 28-02-2021].
BitDegree, «BitDegree.org,» 28-02-2021. [En línea]. Available: https://es.bitdegree.org/crypto/tutoriales/rig-de-minado. [Último acceso: 2802- 2021].
TeamViewer, 28-02-2021. [En línea]. Available: https://www.teamviewer.com/es-mx/. [Último acceso: 28-02-2021].

CAPÍTULO III
ESTUDIOS DE INNOVACIÓN

INNOVANDO SOLUCIONES PARA LA SEGURIDAD PÚBLICA

Mtro. Oscar Manuel Rojas Padilla[1]
Ing. Norberto Ciprés Lugo[2]

"Estoy tan orgulloso por las cosas que no hemos
hecho como por las que sí hicimos,
la ***innovación*** es decir que no a miles de cosas."
Steve Jobs. Fundador de Apple.

Sumario: I. Introducción. II. Ejes de la innovación tecnológica. III. Innovación tecnológica para la justicia y paz. IV. Nuevos retos, nuevas oportunidades.

I. Introducción

El área de Innovación y Desarrollo Tecnológico se integra de equipos multidisciplinarios en áreas de la ingeniería, provenientes de universidades del país y centros de investigación, con los que se promueve la diversidad de pensamiento y un entorno académico más estimulante, lo que lleva a aportar una mayor perspectiva a la solución de problemas de Seguridad Pública, donde la innovación pueda tener un impacto al servicio de la sociedad y de las unidades de la Guardia Nacional.

La visión de los productos de innovación tecnológica que se desarrollan en la Dirección General Científica se hacen pensando en un México en paz, en la seguridad del pueblo, en el compromiso de transformar al país en un ambiente de tranquilidad, y la manera en cómo se desafía el cambio es haciendo tecnología de innovación, primero aprendiendo cómo funcionan las cosas y segundo inspirados para hacer que funcionen mejor.

La filosofía de "paz y seguridad", estimula la participación en los problemas de seguridad que aquejan al país, empujando los límites del conocimiento a formular soluciones prácticas, abordadas desde áreas como la ingeniería en sistemas computacionales, mecánica, eléctrica, electrónica,

[1] Ingeniero en Mecatrónica por el Instituto Politécnico Nacional con estudios de posgrado en el Instituto Nacional de Astrofísica, óptica y Electrónica, actualmente coordina el área de Innovación Tecnológica de la Dirección General Científica en la Guardia Nacional
[2] Ingeniero en Control y Automatización por el Instituto Politécnico Nacional, Certified Project Manager por el Instituto Tecnológico y de Estudios Superiores de Monterrey, Diplomado en Alta Dirección por la Universidad Autónoma de México.

diseño y comunicaciones, mediante el apoyo de universidades y centros de investigación a fin de generar redes de ciencia, transformadas en innovaciones.

A través de la innovación y la investigación tecnológica se generan nuevos productos y servicios y se incrementa el valor de los existentes, con el fin de aportar nuevas capacidades en seguridad pública, mediante la ingeniería básica y aplicada, en respuesta a las amenazas y riesgos que demanda la situación del país.

En este capítulo se abordará la metodología que ha permitido captar las necesidades sociales y materializarlas en innovaciones tecnológicas a fin de aumentar la efectividad de las iniciativas de seguridad pública, teniendo como principales ejes: la formación del capital humano, la innovación tecnológica con enfoque, una metodología práctica y dinámica, derechos de propiedad intelectual, coordinación con academias en estricto apego y respeto a la ley y derechos humanos, concluyendo con un resumen de los desarrollos tecnológicos de la Guardia Nacional, nuevos retos y oportunidades.

II. Ejes de la innovación tecnológica

La tecnología es clave para resolver problemas y abordar necesidades de una manera más eficiente; al hacerlo ha revolucionado la forma en que se piensa, se trabaja y se ha transformado la manera en que se atiende la Seguridad Pública, abriendo todo un abanico de posibilidades para dar soluciones innovadoras a los problemas sociales de México. A continuación, se describen las buenas prácticas del área de innovación y desarrollo tecnológico de la Dirección General Científica, que corresponden a experiencias en ejecución.

A) Eje uno: El capital humano

"El hecho de conseguir una gran innovación y romper con lo establecido, no es fruto de una persona o de un avance, sino de todo un colectivo que ha permitido que ocurra".
Elon Musk

La producción de tecnología se caracteriza por ser una actividad que depende intensamente del trabajo creativo del capital humano, pues los conocimientos y la información necesarios para llevar a cabo actividades de investigación, desarrollo e innovación, se obtienen a partir de la formación continua del personal. Henry Ford decía que "sólo hay algo peor que formar a

tus empleados y que se vayan: no formarlos y que se queden", por lo cual en la Dirección General Científica se trabaja de manera que el personal obtenga una formación integral, tanto en el cumplimiento de las funciones de seguridad pública como en la formación científica, pues son quienes mueven y dan valor a la Institución, y que gracias a ellas y ellos es posible cumplir con los objetivos establecidos.

La primera etapa de esta formación atiende las nuevas realidades que demanda el modelo de seguridad mexicano, regido por los principios de legalidad, objetividad, eficiencia, honradez y respeto a los derechos humanos, donde las ciencias aplicadas en el campo de la ingeniería aportan capacidades, conocimientos, habilidades, destrezas, que de la mano del talento humano que se posee, se ven traducidas en innovaciones tecnológicas de valor.

En un ambiente donde el principal objetivo es impulsar innovaciones tecnológicas se requiere de fomentar una cultura creativa en sus integrantes, basada en la libre generación y circulación de ideas, se facilite el potencial para crecer más allá de su actual nivel de competencias y donde el error sea considerado como parte del proceso de aprendizaje, todo con el objeto de motivar gente capaz de generar ideas pero, sobre todo, de materializarlas; crear la capacidad de descubrirnos y de recuperarnos cuando surge lo inesperado.

En este orden de ideas, otro intangible que añade valor a esta economía colaborativa es la pasión por desarrollar nuevas cosas. Lo que mueve a un equipo de desarrollo tecnológico se sustenta en haber estudiado una carrera en la rama de las ingenierías, pero debe reforzarse con la fuerza de voluntad de ver materializado un proyecto, pues ante adversidades inevitables como la realización de un prototipo fallido o las carencias económicas pueden derivar en falta de interés y desmotivación. Es aquí cuando resalta el hacer algo que realmente te gusta, donde se deja sentir el trabajo como una carga y pasa a ser tu felicidad, donde pasa a segundo término un salario económico por dar un beneficio social.

Otro aspecto importante como institución de seguridad pública es la disciplina, como la base de una conducta de obediencia, de un alto concepto de honor, justicia, moral y de cumplimiento a los deberes, que conjugada con el área de innovación tecnológica se vuelve sinónimo de aprendizaje continuo, implicando una predisposición a mantenerse siempre actualizados ante la incorporación de nuevas tecnologías y sus formas de uso, dando paso a incrementar la habilidad de resolver los problemas de seguridad pública con mayor prontitud.

B) Eje dos: La innovación tecnológica con enfoque

"No se crean tecnologías, se crean soluciones"

En 1899 se popularizó una leyenda urbana que cuenta que el director de la Oficina de Patentes de los Estados Unidos renunció a su cargo recomendando cerrar dicha oficina, porque pensaba que todo lo que podía ser inventado ya lo estaba. Esto da una idea de las resistencias que puede despertar la innovación, así se trate de una pujante economía industrial en franca expansión económica y territorial, gracias a la capacidad de transitar de la energía obtenida por el vapor a la generada por los combustibles fósiles y su creación suprema, el automóvil.

El conformismo o los atavismos, buscan contener los procesos de cambio para reducir el abanico de posibilidades que genera el propio proceso de innovación en tanto proceso que busca generar conocimiento y utilizarlo para crear no solo nuevos productos, servicios o procesos, sino desarrollar la capacidad de imaginar lo necesario para mejorarlas. La innovación es el motor de crecimiento y principio de sobrevivencia para las personas e instituciones.

Aún más importante es innovar con valor, ya que representa el desafío de encontrar un espacio original no explorado, partiendo de la identificación de aquellos factores que generan un valor superior para cubrir las necesidades, como ejemplo el siguiente:

Hace varios años se funda una empresa multinacional francesa de electrodomésticos, en manos de directivos profesionales, los cuales llevaban una cultura establecida y su dosis de burocracia y movimientos políticos internos, que con el tiempo sus productos se fueron enfrentando a una competencia creciente y mayor presión en los márgenes de ganancia. Más concretamente, era el caso de sus freidoras eléctricas, que no acababan de distinguirse del resto de la competencia, en un mercado que se reducía año con año en términos de valor. Reconociendo la necesidad de apartarse de esa competencia un grupo de ingenieros se propusieron darle vuelta a esa situación. Los directivos profesionales se mostraron un tanto escépticos, pues cuestionaban, ¿qué podía hacerse con una freidora de papas cuando el precio era lo único que parecía impulsar las ventas? (Kim y Mabourge, 2018)

El grupo de ingenieros razonaba de otra manera ¿Qué ocurriría si se repensaran todas las asunciones que encasillan el mercado actual?, justamente se pusieron a identificar y desafiar las asunciones del sector, procedieron y casi tuvieron una revelación al descubrir que había dos hechos que todo el mundo acepta sin cuestionar: el primero, que para hacer papas fritas había que freír y el segundo, que para freír hacía falta mucho aceite.

Estas asunciones no analizadas habían llevado al sector a ignorar toda una serie de problemas; los dos litros y medio de aceite de cocina que hacían falta suponían un gasto considerable; además, una vez caliente, ese aceite resulta dañino y hasta peligroso; sin contar que cuando acabas de freír, no es fácil deshacerse del aceite, con lo que la limpieza del aparato no resulta sencilla; y ya como colofón, con todo ese aceite, las papas fritas no son muy sanas.

Desafiando todas estas verdades y centrándose en cómo hacer papas fritas deliciosas y sanas sin necesidad de freír, resultó un aparato completamente nuevo que no implica freír nada y usa únicamente una cuchara sopera de aceite para freír un kilo de papas, con aproximadamente un 40% menos de calorías y un 80% menos de grasa que la misma porción de papas cocinadas a la manera tradicional, además el aparato es fácil de limpiar y no plantea problemas ni de seguridad ni a la hora de deshacerse del aceite usado. Obteniendo como resultado papas crujientes por fuera y blandas por dentro.

La misma idea rige el trabajo del área de Desarrollo Tecnológico de la Guardia Nacional: cuestionar los modelos tradicionales y los contextos vigentes centrándose en la innovación en valor y no solo en la innovación tecnológica, todo ello a partir de principios de proyección estratégica, con vista a mantener su viabilidad en el futuro y a atender específicamente las demandas de la ciudadanía y de las unidades operativas, esto se hace a través de una planeación pensada anticipando los cambios tecnológicos y sociales, desafiando lo existente y arriesgando la comodidad, esto con el objeto de ampliar los horizontes del conocimiento y adoptar una perspectiva anticipada y no reactiva.

Realizar innovación tecnológica con valor representa ver un problema donde nadie más se daba cuenta de que existía y tomar los esfuerzos para encontrar la solución, no se trata de ser brillante al enfrentarlo, sino de mantenerse continuamente trabajando en ello, es estar consciente de que se puede presentar el fracaso y si eso fuera, aprender rápido y mejorar es la solución.

La innovación tecnológica con valor puede venir de cualquier parte, la clave es generar espacios seguros, propicios y cómodos para compartir ideas y desarrollarlas sin temor a equivocarse, pues hasta los genios trabajan con un método de prueba y error, sin errores no hay innovación.

Por otro lado, ante un mundo globalizado y una intensa internacionalización del desarrollo de las tecnologías, además de las exigencias demandadas por la sociedad para atender los problemas de seguridad pública,

es prioritario enfocarse en la creación de valor como diferenciador y como estrategia para acortar los tiempos de desarrollo tecnológico.

Estos cambios llevan a modificar las formas de trabajo, enfocándose en aquellas actividades que involucran innovación, conocimiento (I+D) y diseño como lo muestra la siguiente curva de valor y apoyarse de otros para la manufactura y ensamble.

C) Eje tres: "Una metodología práctica y dinámica"

La tecnología avanza a un ritmo acelerado y se ha vuelto parte de la vida cotidiana, su presencia es tan común y necesaria en todos los sectores que se ha convertido en un punto atractivo para la delincuencia; ante esta problemática social que demanda una atención inmediata, se recurre a la generación de desarrollo e innovación de tecnología como parte del ecosistema que asegura la solución al problema.

A continuación se citan los criterios que se consideran en el desarrollo o innovación de un producto tecnológico, en esta institución de seguridad pública.

a) "Impacto contra complejidad"

El desarrollo e innovación de tecnología se lleva a través de un proceso cíclico, que inicia en la investigación básica y aplicada, para ser probada mediante el desarrollo de un prototipo o una versión beta, mismo que entra a un ciclo de pruebas de validación que depura diversos prototipos, para finalmente obtener un producto. Este ciclo implica la disposición de recursos económicos, materiales y capital humano, que muchas veces no se logra concretar y otras se logra, sin tener el impacto esperado.

Ante una situación donde apremia el tiempo y el presupuesto suele ser insuficiente, se recurre a la técnica de evaluar impacto contra complejidad, donde se sopesan estas dos variables:

1.- Complejidad: medida desde una alta inversion, alto tiempo de desarrollo y alta complejidad técnica.
2.- Impacto: es el grado de cambio significativo y positivo que ocurriría en la ciudadanía o personal de la institución como resultado de la implementación de la innovación.

a) Bajo impacto y baja complejidad: estos son los proyectos que no tienen un principio ni mucho menos un fin.
b) Alto impacto y alta complejidad: en estos casos es cuando se puede planear de manera anticipada basada en la predicción de hechos pasados, estos son los proyectos con visión al futuro.

c) Alto impacto y baja complejidad: este último es el que normalmente se emplea en una institución policial, que demanda soluciones inmediatas y de alto beneficio social.

b) "Identi car claramente la problemática y crear innovación en valor"

Un proyecto puede nacer por emergencia, mejora continua o necesidad, pero todos coinciden en que debe existir un objetivo claro y con ciso, además de alcances definidos, cuando se tiene esta información, es importante decretar la realización, partiendo de la existencia o no de la tecnología en el mercado. Cuando la tecnología existente cumple con las expectativas, se recurre a su evaluación, en caso contrario se inicia su desarrollo o mejora para cubrir las necesidades.

Cuando la tecnología tiene que desarrollarse o ser innovada, el objetivo es ofrecer una solución para un problema existente, de tal manera que se adapte a las necesidades solicitadas y la misma sea lo suficientemente fácil de usar, de nada servirá crear una tecnología de punta que será abandonada por no ser útil y práctica.

c) "Generación de prototipos rápidos o versiones betas"

Con el objetivo de reducir el ciclo de desarrollo y probar las ideas propuestas, se recurre a la generación de prototipos de software, hardware y diseño y manufactura mecánica, lo que permite evaluar y tomar acciones, ya sea de corrección o mejoramiento.

Esta técnica permite mostrar, reemplazar y modificar rápidamente el concepto de la idea, a fin de aclarar los requerimientos del área usuaria, además de que como desarrollador permitirá madurar la tecnología mediante ciclos controlados en acompañamiento de las diferentes áreas de desarrollo involucradas.

D) Eje cuatro: "Registro de derechos de propiedad intelectual"

El registro de los derechos de propiedad intelectual juega un papel crucial: como área de desarrollo de innovación tecnológica, es importante garantizar los derechos de exclusividad de explotación, mediante la obtención del título o certificado que el Estado proporciona. Para ello existen clasificaciones e instituciones como el Instituto Nacional del Derecho de Autor (Indautor) y el Instituto Mexicano de la Propiedad Industrial (IMPI) que se encargan de proteger y fomentar los derechos del autor.

Dentro de los beneficios que se obtienen con el título, destacan:

- La obtención del derecho exclusivo de explotación concedido por el Estado.
- Exclusividad al prohibir el uso sin su consentimiento, ya que, con el registro o publicación, informa a terceros que éste es un derecho de propiedad particular.
- Permite ejercer acciones legales de protección en contra de terceros que lo usen sin autorización. En marcas:

1. Al ser un bien intangible, puede sumarse a los activos de la institución.
2. Exclusividad al uso de la marca en todo el territorio mexicano, usar la leyenda "Marca Registrada", las siglas "M.R." o el símbolo ® y a conceder el uso a terceros mediante licencias de uso.

El registro de los derechos de propiedad intelectual es una función del Estado al nivel del fomento económico y el desarrollo del conocimiento aplicado, donde el objetivo principal es compartir con las instituciones hermanas, se vuelve un instrumento que ha permitido generar los canales seguros para compartir los avances tecnológicos. Otra de las grandes ventajas de contar con los derechos de propiedad intelectual, ha sido en el proceso de manufactura en masa, donde se ha permitido abrir la opción de fabricar con empresas privadas, con las que se tiene que compartir información sensible; esto asegura una relación estrecha y confiable. Por otro lado, esta área de desarrollo, ha sido un incentivo para mantener y mejorar la calidad, competitividad y productividad de los desarrollos tecnológicos policiales, además de obtener posicionamiento ante los cuerpos policiales, incluso del extranjero, consolidando así la confianza del Estado en la Guardia Nacional.

Al obtener un título se promueve la transferencia de tecnología, se estimula la investigación y el desarrollo y se impulsan nuevos desarrollos, además de ser un medio para reconocer la creatividad dentro de los elementos policiales.

E. Eje cinco: "Coordinación con la academia"

La innovación tecnológica requiere de ecosistemas que reduzcan las brechas del conocimiento, pues ante necesidades latentes y ciudadanos que demandan bienestar social, es necesaria la generación de redes que constituyan una colaboración científica y técnica con proyección hacia el

beneficio social, aprovechando la infraestructura y los conocimientos de las universidades y centros de I+D.

En la Guardia Nacional se trabaja en la generación de alianzas como es el caso de la Universidad Nacional Autónoma de México en específico con la Facultad de Ingeniería y el Laboratorio de Ingeniería Mecánica Asistida por Computadora y con la Universidad Tecnológica de Tula -Tepeji quienes con su colaboración permitieron la manufactura de la carcasa del Dispositivo Táctico para la Operación Policial (DTOP®), todos trabajando con un mismo objetivo: garantizar la integridad de los ciudadanos y sus bienes.

F. Eje seis: "Apego a la ley y a los derechos humanos"

Cuando se emprende el desarrollo o la innovación de alguna tecnología, se hace pensando en respetar la libertad y privacidad de los ciudadanos, mediante procedimientos transparentes que permitan establecer que el uso de la misma está dentro de los márgenes de la ley y los derechos humanos.

La incorporación de tecnología a las actividades de los policías de la Guardia Nacional, se acompaña de una vigilancia que supervisa la protección de datos personales y la privacidad de la información, además del funcionamiento y cumplimiento para el cual fueron implementadas.

III. Innovación tecnológica para la justicia y paz

En materia de tecnología, la Guardia Nacional ofrece distintas alternativas y herramientas que se pueden implementar al servicio de la seguridad pública, optimizando el proceso de prevención y respuesta a la delincuencia acorde a las nuevas tendencias y contextos sociales.

Por otro lado, los ciudadanos disponen de diversas herramientas tecnológicas para afrontar los problemas de seguridad, desde un frente de prevención o como una herramienta de denuncia anónima; sin embargo, algunas tecnologías se encuentran bastante difundidas, tanto a nivel de la ciudadanía como de policías, mientras que otras son de difícil acceso para público en general. A continuación, se describen las tecnologías de la Guardia Nacional, según su uso:

a) Para la atención ciudadana: su principal objetivo es establecer una relación estrecha entre la sociedad y la Guardia Nacional; dentro de esta categoría se encuentra el desarrollo de aplicaciones móviles, normalmente diseñadas en las plataformas Android e iOS, que bajo un equipo de ingenieros

de software, ha permitido tener un alcance no solo para la institución, sino también desarrollos para otras dependencias federales.

- GN reporta. Aplicativo móvil que permite brindar atención ciudadana mediante contacto directo con el Centro Nacional de Atención Ciudadana de la Guardia Nacional, permite reportar de forma anónima la comisión de delitos, además de expresar quejas, sugerencias o dudas.
- GN carreteras. Aplicación desde la que se puede reportar el robo de vehículos e incidentes en carreteras federales; consultar incidentes viales, sus afectaciones y posibles rutas alternas; localizar hospitales, paraderos de descanso y afluencia vehicular en casetas del área metropolitana. Los reportes son visualizados en una plataforma web por las unidades de la Guardia Nacional para ser validados y atendidos de manera oportuna.
- APP 9-1-1 Emergencias. En colaboración con el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública se cuenta con una app que permite formar una red de contactos a los que se notificará por medio de un mensaje SMS cuando el ciudadano se encuentre en una situación de emergencia, tiene tres funciones: notificación de emergencia, llamada de emergencia y botón de pánico.

c) ***Para inteligencia:*** orientadas hacia la obtención y explotación de información, que ayude a la toma de decisiones, con el fin de prevenir el actuar de la delincuencia.

- *Dispositivo Táctico para la Operación Policial (DTOP ®)*. Se compone de un smartphone y un lector biométrico de huella dactilar, integrados dentro de una carcasa dura y una suave que lo hace resistente a caídas e impactos por el uso. Esta herramienta tecnológica móvil y táctica con conectividad a la red de Internet, permite consultar mediante la huella dactilar, bases de datos de la Plataforma México y el Instituto Nacional Electoral en tiempo real y desde cualquier lugar, a fin de identificar personas con antecedentes penales y órdenes de aprehensión vigentes, además de validar la identidad del ciudadano.

c) Para análisis del fenómeno delictivo: el uso de esta tecnología permite identificar nuevas amenazas y patrones relacionados con la criminalidad.

- Sistema de Información Geográfica para la Inteligencia Operativa (GISIO). Plataforma informática que permite generar insumos de inteligencia policial, a partir de los reportes ciudadanos realizados a los números 911 y 089, además de los proporcionados por los distintos C4/C5 de las entidades; permitiendo analizar el fenómeno delictivo, desde los principales factores que lo generan, hasta su evolución y migración temporal y espacial.

d) Para equipamiento tecnológico: este tipo de desarrollos tecnológicos están orientados a satisfacer las necesidades interinstitucionales.

- Impresora 3D. Cuando se toma un objeto físico y se convierte a digital se vuelve completamente flexible de operar, se puede modificar lo que se necesita color, tamaño, forma, de tal manera que se adapte a las necesidades y se imprime al tamaño deseado. Ésto muestra las facilidades de esta tecnología "Impresión 3D". Su funcionamiento es bastante simple es un cabezal como las impresoras comunes que se mueve en sus tres ejes, depositando un material de plástico en una capa finita de acuerdo al objeto que se diseñó, después otra capa dando el volumen capa sobre capa hasta completar el objeto. Esta tecnología no solo crea impresiones en materiales plásticos, imprime en metal. En la Guardia Nacional se ocupa para imprimir piezas de drones, carcasas, cortadoras láser y cualquier proyecto en su fase de prototipo.

- Recuperador de ojivas: es un equipo mecánico cuya finalidad es la obtención de muestras de proyectiles disparados por armas de fuego de diversos calibres como: 9mm, 38 súper, 38 especial, 0.40", 0.450", 12 GA, 0.223" (ametralladora M60D) o su equivalente 5.56 x 45mm según el estándar de la OTAN, 0.308", 7.62 x 51mm y 5.7 x 28mm, para su posterior estudio del rayado del cañón sobre el proyectil, generando el registro y control de las armas asignadas a cada elemento de seguridad pública a fin de fortalecer las investigaciones ministeriales tanto del fuero común como del federal. Cuenta también con un pedestal desmontable y un sistema de disparo a distancia, los cuales son exclusivos para la ametralladora M60D.

IV. Nuevos retos, nuevas oportunidades

Con el surgimiento exponencial de nuevas tecnologías que están transformando la cotidianidad, el reto será comprender cómo afectarán el panorama social y encontrar la manera de integrarlas a las operaciones policiales.

Con la generación de grandes cantidades de información cada vez mayores y en tiempo real que se extienden por todos los rincones y ámbitos, hoy implica la implementación de técnicas de análisis y procesamiento de datos para generar conocimiento e inteligencia, esto da pie al Big Data que permite recabar desde diferentes fuentes y procesar rápidamente la misma para la toma de decisiones.

Con el avance tecnológico, se abren grandes retos pero también nuevas oportunidades, como la posibilidad del trabajo colaborativo remoto con personas de todo el mundo inmersas en el desarrollo e innovación tecnológica en Seguridad Pública, la explotación de las áreas de la biometría, sensores e inteligencia artificial que permitirán incrementar la efectividad en la prevención e investigación de ilícitos.

Otro de los grandes retos es la propuesta e implementación de políticas públicas en materia de implementación de tecnología, que permitan permear en los diferentes órganos de Seguridad Pública a fin de realizar acciones conjuntas, que inciden determinantemente en la resolución de hechos de violencia y delitos que se producen en el país.

Fuentes de Consulta:

- Kim Chan y Renée Mauborgne La Transición al Océano Azul. Editorial: Empresa Activa, Marzo 2018.
- Proméxico (2015), Mapa de Ruta Puebla Capital de Innovación y Diseño, Ciudad de México, Diseño Editorial Abracadabra.

EL PERFIL CIENTÍFICO-POLICIAL

Primera Subinspectora GN, Rosa María Richards Uribe.[1]
Primera Subinspectora GN, Héctor Barrón González.[2]
Suboficial GN, Yolanda Ramírez Roldán.[3]
Comisario GN, Mtro. Severino Cartagena Hernandez.[4]

Sumario: I. Introducción; II. Antecedentes; III. Vinculación con la comunidad científica; IV. Lecciones aprendidas en desarrollo científico. (Confidencialidad); V. Administración especializada de proyectos; VI. Enfoque colaborativo; VII. Acreditación y certificación en sistemas de gestión de la calidad en las ciencias forenses para la prevención e investigación del delito. VIII. Tendencias; IX. Certificación de competencias laborales ante conocer; X. La educación para la función científico policial: un apunte.

I. Introducción

La figura del policía como un profesional de la seguridad que se sirve del método científico se remonta a finales del siglo XIX en México y tiene como fundamento la medicina legal, la toxicología, la toma de huellas dactilares y la antropología forense. El concepto de la Dirección General Científica de la Guardia Nacional se remonta a 2010 y se articuló en un modelo único que se ha sumado a las disciplinas de la criminalística, las que atienden los llamados delitos electrónicos, que incluyen la ciberseguridad, el expansivo dominio de la ciberdelincuencia y la forensía digital.

---

[1] Doctora en Ciencias Ambientales y Maestra en Química, obtuvo la ACREDITACIÓN bajo la norma Mexicana NMX-EC-17025-IMNC-2006 y la CERTIFICACIoN bajo la norma Mexicana ISO 9001:2008. Ha publicado las obras Metodología de la Investigación, Antología del repositorio digital de la Universidad Autónoma del Estado de Hidalgo, New Organo-inorganic Materials for Water Contaminants Remediation, entre otras. Actualmente se desempeña como Subdirectora en la Dirección Funcional de Planeación y Análisis Estratégico de la Guardia Nacional.

[2] Realizó el Doctorado en Control Automático en la Universidad de Sheffield, Inglaterra y tiene una especialidad en Inteligencia Policial. En el INAOE dirigió proyectos de desarrollo tecnológico para el Fondo Sectorial CONACYT-SEMART y en la Dirección General Científica de la Guardia Nacional actualmente dirige el área de Información Delictiva.

[3] Titulada de la licenciatura en Informática por el Instituto Tecnológico de Apizaco en Tlaxcala, graduada de Maestría en Ciencias de la Educación por la Universidad de Camagüey, República de Cuba, pasante de Doctorado en Ciencias Pedagógicas por la Universidad de Camagüey, República de Cuba, cuenta además con Diplomados en el área pedagógica por Universidad de Camagüey, República de Cuba. Tiene Certificaciones, Asesor a distancia por la CUAED, Universidad Autónoma de México para el
Programa de Migrantes en Estados Unidos y Canadá en las Técnicas para la Enseñanza Aprendizaje a Distancia, certificada por el Consejo Nacional Normalización y Certificación de Competencias Laborales CONOCER en dos Estándares de Competencias Labor.

[4] Encargado de la Dirección de Planeación y Análisis Estratégico en la Dirección General Científica. Dirigió el Centro de Atención Psicológica y Estrés Pos Traumático de la entonces División de Fuerzas Federales. Fue Director General de la Academia Superior de Seguridad Pública de la entonces Policía Federal. Profesor en la maestría y especialidades que imparte la Guardia Nacional, con Maestría en planeación y segnal.

El modelo, por último, se fortaleció con las atribuciones y equipamientos necesarios para la innovación tecnológica al servicio de las diversas unidades que componen a la institución policial. El resultado fue un modelo cuya integración se resume en tres términos: criminalística, cibernética e innovación. Una combinación singular, que no tiene parangón en las policías científicas del mundo, donde la criminalística y la medicina legal siguen su propia tradición respecto de las disciplinas relacionadas con la cibernética y la computación, ni qué decir de la innovación.

El modelo de la policía científica ha ido evolucionando de una forma característica a lo largo del tiempo, en consonancia con la evolución del conocimiento y la práctica de lo policial, aunque sin perder de vista la esencia de la profesionalización que le dio origen, con la diferencia de que añade a la formación inicial en academia la especialización técnico científica que demanda los requisitos de una prevención y atención ordenada y sistemática del delito, enriqueciendo así el perfil y los requisitos para ser policía.

La seguridad y el bienestar de la ciudadanía se encuentran ante una fuerte carrera contra el tiempo. La delincuencia mantiene una dinámica orientada hacia la tecnificación. De hecho, la delincuencia cibernética ha sido fuente para la formación de organizaciones criminales distintas de la delincuencia organizada convencional, que al igual que ésta busca optimizar sus recursos y mantener la subsistencia de sus negocios ilícitos. Para nadie resulta extraña la idea del uso de drones como herramientas de transporte de explosivos y drogas, o el reclutamiento de especialistas en química para la elaboración de estupefacientes. Por ello, los cuerpos de seguridad deben estar aún más preparados para afrontar líneas delictivas emergentes e innovadoras, y mantenerse actualizados constantemente.

Como preámbulo a lo que hoy es la Dirección General Científica de la Guardia Nacional, se vislumbró proveer a los cuerpos de seguridad de recursos altamente especializados para combatir el delito. Mediante el uso de metodologías científicas, se daría certeza a las actividades de investigación, prevención y reacción de los cuerpos policiales, mediante la adecuación de tecnología, la estructuración de protocolos mejor elaborados y la caracterización de delitos emergentes.

Más allá de las herramientas tecnológicas que se puedan llegar a utilizar en el resguardo de la Seguridad, los recursos humanos son el factor clave para poder lograr una robusta institución policial basada en el conocimiento científico. Sin embargo, el perfil del personal que conforma la Dirección General Científica de la Guardia Nacional requiere ser multidimensional, es decir, formado a través de tres perspectivas diferentes.

como servidor público, como policía y como especialista tecno-científico. Cada uno de estos aspectos proporciona un perfilamiento profesional muy particular que atiende una necesidad crítica en el área de seguridad pública.

El presente capítulo ofrece algunos conceptos en torno al perfil científico policial, con base en las experiencias de formación de recursos humanos para la policía científica en las tres áreas que conforman la Dirección General Científica; con base en los principios de la conceptualización, experimentación, replicabilidad y comparabilidad del conocimiento que hoy demanda la prevención y persecución de los delitos en un contexto global, profesional y de respeto a los derechos humanos, con base en el contexto nacional en torno al perfil científico policial que se debe ofrecer al desarrollo de la convivencia social.

Con esa finalidad se abordarán tres dimensiones de la formación de recursos humanos para la policía científica: la vinculación con la comunidad científica del país, la certificación y acreditación de los procedimientos críticos, así como la certificación de competencias laborales para hacer frente a los requisitos de permanencia del cuerpo policial.

III. Antecedentes

De acuerdo al artículo 40 de la Ley General del Sistema Nacional de Seguridad Pública,[5] las Instituciones de Seguridad tienen la obligación de actualizarse en el empleo de métodos de investigación que garanticen la recopilación técnica y científica de evidencias. Mientras que el artículo 47 establece que las academias de profesionalización policial deberán capacitar en materia de investigación científica y técnica a los servidores públicos.

Esto es comúnmente empleado en la generación de un perfil policial especializado en investigación, en criminalística y ciencias forenses. Tal como ha sido históricamente aplicado en países como España y El Salvador. En México se intentó formar una policía científica, con la diferencia quizá de que en la experiencia de México, los servicios forenses se redujeron prácticamente a la identificación de personas y quedaron adscritos a las Procuradurías, lo que les dificultó aportar a la profesionalización policial en México, hasta la creación de la División Científica en la otrora Policía Federal, hoy inserta en la Unidad de órganos Especializados por Competencia de la Guardia Nacional como Dirección General Científica.

[5] Ley General del Sistema Nacional de Seguridad Pública. Diario Oficial de la Federación. Última reforma 27 de mayo de 2019.

Específicamente, la Dirección General Científica tiene la atribución de aprovechar y movilizar los conocimientos y herramientas científicas y técnicas en la investigación para la prevención de los delitos, y la de implementar los mecanismos que impulsen la investigación científica en áreas de oportunidad que deriven en metodologías y herramientas para la modernización continua de las diversas unidades de la Institución.[6]

Esa es quizá la diferencia entre el trabajo científico policial y el trabajo policial estándar. Mientras que el primero demanda del método científico y sus resultados aportan al avance del conocimiento, el trabajo estándar suele ser de carácter deductivo (las famosas preguntas de oro). Lo anterior, no solo implica hacer uso de herramientas metodológicas para la investigación de delitos, sino hacer uso del método científico para la generación de conocimiento, nuevo o aplicado, en un campo particular de estudio. Esto implicaría la generación de un perfil particular, capaz de elaborar hipótesis, analizar diversas fuentes de información, formular preguntas de investigación científica, implementar innovaciones tecnológicas, todo mediante estrictos estándares metodológicos.

El policía científico no solo buscará la solución de delitos específicos, sino la continua mejora de la actuación policial en dos sentidos: el uso racional de la fuerza en un sentido persuasivo y ante todo, la prevención, mediante un estricto marco jurídico científico y tecnológico. Por lo que para ser reconocido, y respetado en su campo de aplicación, deberá recorrer un camino encuadrado en las fronteras del conocimiento, como lo demuestra el hecho de que la práctica policial no puede prescindir de los avances en campos como las neurociencias, la inteligencia artificial o la ciencia de datos, por solo mencionar algunas ramas del conocimiento científico que dan cuenta del nivel de especialización al que tiende el conocimiento y la práctica policial.

Mientras que las neurociencias expanden el conocimiento del fenómeno criminal, la relación víctima-victimario o las respuestas al estrés y el trauma, la inteligencia artificial se dirige a la generación de algoritmos y modelos quereplican diversos niveles y expresiones de la conducta e incluso de la experiencia humana; finalmente, la ciencia de datos ofrece agregados de información cuyo procesamiento y elaboración dan cuenta de la ingeniería social que moldea percepciones y valores y permite el análisis del comportamiento de utilidad tanto para la comisión como para la corrección de las conductas antijurídicas y antisociales. Se trata de dominios capaces de generar sus propios principios, bases teóricas, líneas de desarrollo y aplicaciones dentro del quehacer policial, y que se han expandido en forma exponencial, por no decir explosiva, en la última década.

[6] Reglamento de la Ley de la Guardia Nacional. Diario Oficial de la Federación. 29 de junio de 2019.

Este reconocimiento se logra a lo largo de tres etapas, dos de ellas de carácter epistemológico y una de carácter institucional.[7] En la primera etapa, el policía científico proviene de otras disciplinas, tales como derecho, medicina, criminología o ingeniería. Estos especialistas empiezan a combinar sus talentos para resolución de problemas específicos. La segunda etapa continúa con la generación nuevos marcos teóricos, sustentados en la singularidad de estas actividades y en la creciente interacción del campo técnico científico con las conductas criminales, abarcando la formación de nuevas formas de victimización y de la tercera etapa involucraría el reconocimiento institucional y la consolidación de redes que fortalezcan esta nueva área de conocimiento. El quehacer científico policial requiere de la capacitación en competencias básicas, la actualización en las diversas disciplinas, así como de la especialización en la frontera de las diversas áreas del conocimiento. Sin embargo, se considera necesaria la integración con el conjunto de la comunidad científica y sus instituciones rectoras.

III. Vinculación con la comunidad científica

En el año 2013, la otrora Policía Federal estableció un convenio con el Consejo Nacional de Ciencia y Tecnología, a fin de constituir el Fondo Sectorial para la seguridad pública, cuyas Reglas de Operación estaban fundamentadas en la Ley de Ciencia y Tecnología. Con este instrumento se buscaba atender las demandas prioritarias en Seguridad Pública, a través de la interacción con las Instituciones de Educación Superior y los Centros de Investigación de Alta Especialización en México, seleccionadas por Convocatoria Pública. Durante el periodo de 2014 al 2020 inclusive, lograron consolidarse cuatro proyectos de desarrollo tecnológico relacionados con herramientas de inteligencia y ciberseguridad. También se dio pauta para la implementación de proyectos de capacitación especializada en áreas de ciberseguridad y criminalística.

Anteriormente se establecieron otros acuerdos de una naturaleza similar, tales como los Fondos Sectoriales SEMAR-CONACYT y SEDENA CONACYT, los cuales buscaban la generación de infraestructura tecnológica propia, que fortaleciera las capacidades de estas instituciones en sus actividades de Seguridad Nacional.

La amalgama entre la comunidad científica y la seguridad pública requirió de un enfoque muy particular, determinado principalmente por las características de la operación policial. De dicha experiencia, se generó una base de conocimiento y aprendizaje altamente fructífero, que podría reperfilar el desarrollo científico nacional.

[7] Nagel, Christof, Vera, Antonio. Policie science as an emerging scientific discipline. International Journal of Police Science and Management. April, 2020.

IV. Lecciones aprendidas en desarrollo científico. (Confidencialidad)

El trabajo policial gira alrededor de la protección de los derechos de los ciudadanos y sus bienes, siendo la investigación y persecución de los delitos el fin de la actuación policial. Por ello, las necesidades científicas y tecnológicas de la seguridad pública giran alrededor de delitos como secuestro, extorsión, narcotráfico, trata de personas, pornografía infantil, fraude cibernético, entre otros.

Los grupos delictivos relacionados con estos delitos continuamente se mantienen informados, implementando sus propios métodos de generación de inteligencia, para identificar las vulnerabilidades de las instituciones de seguridad. Por ello, fue prioritario garantizar la confidencialidad de la información sobre la tecnología derivada de estos desarrollos.

Si bien el desarrollo del pensamiento libre y la publicación de artículos en revistas arbitradas son esenciales para la comunidad científica, era importante establecer también un esquema de trabajo, que no perjudicará la operación policial. Junto con la implementación de instrumentos como cartas de confidencialidad, minutas controladas y generación de reportes con información pública, se estableció un esquema basado en el mapeo funcional entre dominios separados, mediante acompañamiento especializado.

El dominio establecido por el contexto policial era primero analizado por especialistas científico-policiales, los cuales realizaban un mapeo de las funciones requeridas para un desarrollo tecnológico hacia un co-dominio más restringido. Esta nueva base de información era utilizada por los Centros de investigación para el desarrollo de la tecnología, sin perjudicar la funcionalidad del sistema y el resultado final.

V. Administración especializada de proyectos

En lo que se refiere a la Seguridad Pública, cada día que transcurre durante un proyecto de desarrollo tecnológico, se generan nuevos secuestros, se publican nuevos sitios donde fomentan la trata de menores, se realizan ataques continuos a las infraestructuras críticas. Por ello, uno de los factores críticos en el desarrollo tecnológico es el tiempo para generar resultados, a lo que el personal de las instituciones de seguridad está habituado. Las instituciones científicas trabajan a un ritmo diferente, lo que podría implicar una incompatibilidad determinante para el éxito de los proyectos. Para lo anterior se determinó tomar algunas consideraciones importantes:

1. Por parte de la institución se designó un equipo de policías científicopoliciales capaces de establecer los requerimientos funcionales y establecer un enfoque modular efectivo para cada desarrollo, de acuerdo a su transferencia a la aplicabilidad policial a corto plazo. Se tomó como base el estándar IEEE-830 (Especificación de requerimientos de software), y se realizaron adecuaciones, de manera gradual, orientadas a SysML, con el fin de establecer con claridad sistemas de alto impacto.
2. Se generó un proceso de seguimiento del proyecto, tomando como base el estándar ISO/IEC 25040 (Proceso de evaluación de productos software). Para lo cual se estableció un protocolo de calidad, basado en los requerimientos funcionales, y acordados entre ambas partes. El protocolo fue utilizado para medir cada desarrollo, acorde a su madurez tecnológica, a lo largo del proyecto.
3. Se estableció una administración compartida del proyecto, las divergencias ocurridas por la diversidad en las dinámicas institucionales, las dependencias administrativas, la especificación semántica de los componentes logísticos-tecnológicos y la cultura laboral fueran mitigadas, mediante una continua interacción interinstitucional.

VI. Enfoque colaborativo

Conforme la línea de desarrollo científico-colaborativo ha ido madurando en forma gratificante, los proyectos de profesionalización altamente especializada, como maestrías y doctorados en Centros de Investigación, se mantienen como áreas de oportunidad. Esto debido a la exigencia científica que se requiere para realizar un grado de estudios superior en ciencias exactas, y por el otro, la demanda laboral que se exige en la Institución, que busca garantizar el bienestar de la ciudadanía.

Para ello es requerido que, en lugar de que sea una Institución proveniente del sector científico la que coordine el plan de estudios, debe ser una entidad de seguridad la que establezca la dinámica académica, donde colaboren los centros de investigación en la generación de un cuadro formativo complementario, acorde a los paradigmas científico- policiales.

[8] IEEE 830-1998 - IEEE Recommended Practice for Software Requirements Specifications. Publicado 1998-10-20

La colaboración institucional especializada implicó dos aspectos importantes que deben ser resaltados. El primero, es la posibilidad de que el trabajo conjunto científico-tecnológico lleve a redireccionar el trabajo científico en los centros de investigación, abriendo un amplio espectro de problemas complejos que puedan definir nuevos programas de estudio, líneas de investigación y novedosos perfiles profesionales.

Por otro lado, esta experiencia colaborativa también permitió vislumbrar que el perfil técnico del personal de la Dirección General Científica, se ha ido complementado fuertemente con el quehacer policial. El científico policial tiene a su alcance problemas altamente complejos que lo activan a mantenerse actualizado, creativo, propositivo y altamente especializado, en un área donde la comunidad científica tradicional aún es pionera.

El Centro de Evaluación de la Dirección General Científica se crea por instrucción y con el objetivo de mantener la permanencia del Certificado Único Policial de sus integrantes, en trabajo coordinado de la Entidad de Certificación.

La Dirección General Científica de la Guardia Nacional tiene acreditados Estándares de Competencia en funciones específicas en las que las y los integrantes de grupos prioritarios han sido evaluados. La meta principal es que a las y los integrantes se les otorgue el certificado por la demostración de haber adquirido la competencia en una función.

El proceso que se realiza en el Centro de Evaluación consiste en recibir los listados de Grupos Prioritarios, identificarlos y ubicar de manera coordinada con las áreas la función en la cual se van a evaluar, así como constatar que se lleve a cabo la alineación que deben recibir las candidatas y candidatos a certificación.

A través del apoyo de coordinación de la Entidad de Certificación el requisitado de portafolios de evidencias, las evaluaciones y la emisión del juicio de competencias se desarrollan de manera objetiva. La solicitud de la Entidad de Certificación para realizar Grupo Dictamen con expertos en las funciones evaluadas se realiza posterior a las evaluaciones.

I. Acreditación y certificación en sistemas de gestión de la calidad en las ciencias forenses para la prevención e investigación del delito

La concepción de creación de una policía con conocimientos, aptitudes y actitudes en el área Científica en puestos estratégicos del medio de seguridad pública federal en México, fue una gran vertiente para establecer el objetivo de brindar la aplicación de mecanismos, lineamientos, políticas, protocolos y procedimientos que permitan demostrar los principios fundamentales del método científico y tecnológico para realizar las funciones que desarrolla una Institución policial, la cual tiene la finalidad de la prevención e investigación de delitos.

El perfilamiento del personal científico, obedece a la importancia de establecer herramientas capaces de demostrar la confiabilidad y confianza del manejo de las solicitudes de las autoridades competentes para la prevención e investigación de los delitos en las ciencias forenses, mismo que genero la necesidad de establecer una línea de excelencia y calidad en los procesos, por tanto, se inicia con el diseño, aplicación e implementación de sistemas de gestión de la calidad con los matices forenses. Motivo por el cual, se visualizó la Acreditación, que es el formalismo internacional de dar un protocolo de verificación mediante una entidad de acreditación nacional o internacional (ema[9], ANAB , ILAC , IAF , etc.), tiene como objetivo reconocer la evidencia enla competencia técnica, que brinda la validación de entendimiento de los conocimientos, aptitudes, actitudes ante un dictamen. La confiabilidad de estos organismos de certificación de laboratorios es ver el grado de evaluación de la conformidad que está establecida en las NOM´s, las NMX, normas internacionales u otras especificaciones, prescripciones o características.

---

[9] Entidad mexicana de acreditación, a.c., es la primera entidad de gestión privada en nuestro país, que tiene como objetivo acreditar a los Organismos de la Evaluación de la Conformidad que son los laboratorios de ensayo, laboratorios de calibración, laboratorios clínicos, unidades de verificación (organismos de inspección) y organismos de certificación, Proveedores de Ensayos de Aptitud y a los Organismos Verificadores/Validadores de Emisión de Gases Efecto Invernadero (OVV GEI) Productores de Materiales de Referencia y la autorización de Buenas Prácticas de Laboratorio de la OCDE www.https://www.ema.org.mx/portal_v3/index.php/que -es-ema

Ofrece servicios de acreditación para agencias de ensayos forenses desde 1982 y es el proveedor de acreditación bajo las normas ISO para las agencias forenses de los Estados Unidos con más años en el mercado. WWW.https://anab.ansi.org/es/forensic -accreditation

Es la organización internacional para organismos de acreditación que operan bajo la ISO / IEC 17011 y que participan en la acreditación de organismos de evaluación de conformidad, incluyendo laboratorios de calibración (que utilizan ISO / IEC 17025), laboratorios de ensayos (que utilizan ISO / IEC 17025), laboratorios clínicos (que utilizan ISO 15189) y organismos de inspección (que utilizan ISO / IEC 17020). https://www.https://ilac.org/language -pages/spanish/

El Foro Internacional de Acreditación (IAF por sus siglas en Inglés) es el máximo foro mundial de organismos de acreditación y organismos interesados en Evaluación de la Conformidad (organismos de certificación) en las áreas de sistemas de gestión, productos, servicios y personal. Está integrado por más de 70 organismos de acreditación de 67 economías y por 6 Organismos Regionales. https://www.ema.org.mx/portal_v3/index.php/iaf

Este modelo de trabajo con sistemas de gestión de la calidad fue adoptado por países como Estados Unidos, Inglaterra, México, Colombia, China, Rusia, Alemania, entre otros, con la finalidad de generar la estandarización de su trabajo forense bajo el establecimiento de definiciones, criterios, guías y normas a utilizar.

En los laboratorios forenses (diversas disciplinas bajo los criterios cuantitativos o cualitativos) se aplican los criterios de ISO 17025 "Requisitos generales para la competencia de los laboratorios de ensayo y de calibración" o ISO/IEC 17020 "Evaluación de la Conformidad - Requisitos para el funcionamiento de diferentes tipos de unidades (organismos) que realizan la verificación (inspección)". La aplicación de estas normas internacionales tiene la finalidad de obtener la acreditación, que refleja que el nivel de trabajo y experiencia es equiparable contra cualquier otro laboratorio a nivel mundial igualmente certificado.

La confianza generada en la aplicación de estos criterios, ha impulsado la generación de nuevos grupos de trabajos de discusión, uno de los más importantes a nivel internacional es el comité técnico TC 272 en materia de ciencias forenses, que genera la interpretación y revisión de la ISO 21073 de ciencias forenses.

Otro punto de gran relevancia a considerar, es el inicio de la transformación de la administración de justicia de la aplicación del sistema penal en materia forense. El cual considera el cumplimiento de los requisitos legales en cuanto a la capacidad de recepción, análisis y/o actividades derivadas de los procesos criminalísticos en el esclarecimiento del hecho delictuoso bajo la conducción y mando del Ministerio Público o autoridad competente.

Todos estos requisitos legales del manejo de la cadena de custodia derivados en el Acuerdo A/009/15, del Código Nacional de Procedimientos Penales y Guía Nacional de Cadena de Custodia, se hacen referencia de la importancia del deber y manejo de un proceso de calidad en todo servidor público y más aquellos que tengan contacto directo con los indicios, vestigios, evidencias, objetos, instrumentos o productos del hecho delictivo.

En consecuencia de la búsqueda de la con[illegible]anza en los dictámenes periciales u opiniones técnico cient[illegible]cas se solicitó firmemente que el personal este altamente capacitado bajo perfiles de capacidades y aptitudes, ya que el papel que desempeñará cada uno de los expertos será una parte fundamental en la impartición de justicia.

Una Norma Mexicana (NMX) en un instrumento de referencia para determinar la calidad de los productos y servicios. https://www.eedvim.com.mx

Es un comité técnico de la ISO que trabaja en temas relacionados con las ciencias forenses. https://www.ema.org.mx

La necesidad de contar con laboratorios que cuenten con tecnología, instalaciones adecuadas, personal, capacitación continua y laboratorios acreditados nos brinda generar la más alta competencia a nivel mundial y demostrar que los resultados son confiables, mismos que serán presentados y considerados en un caso o juicio.

Siguiendo está inercia, se da origen a la generación de un sistema de gestión de la calidad basado en normas internacionales, bajo el entendimiento en materia de calidad y técnicos especializados (disciplina forense), del cual se obtuvo los siguientes resultados:

La obtención de esa acreditación ha permitido brindar la confianza de los resultados en el procesamiento metódico del ADN mediante el análisis e interpretación de datos para validar la obtención de perfiles genéticos de personas, con la finalidad de obtener la identificación genética de restos humanos.

Otro logro, que tiene en consideración para la homologación de sus actividades en el análisis de drogas que es un tema muy importante por ser un delito contra la salud, se trabajó para la obtención de la licencia sanitaria.

La importancia de esta Licencia, es que el responsable sanitario deberá informar los riesgos que implica el uso y manejo de sustancias tóxicas, corrosivas o irritantes y, en su caso, fuentes de radiación ionizante; así como material infectocontagioso y los inherentes a los procesos de las muestras, con el fin de que cumplan con las normas de seguridad correspondiente y utilizar el equipo de protección personal. Además de llevar a cabo la vigilancia de los estándares para el análisis de drogas.

Dentro de los alcances en calidad, la necesidad de dar seguridad en el trabajo de la cadena de custodia y después del lugar de Procesamiento del lugar de intervención dirigió los esfuerzos a buscar la Certificación en ISO 9001.

Acuerdo por el que se establecen las directrices que deberán observar los Servidores públicos que intervengan en materia de cadena de custodia.
https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015

Nuevo Código publicado en el Diario Oficial de la Federación el 5 de marzo de 2014 http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_190221.pdf

https://www.criminalistasforenses.org.mx/docs/cadena-de-custodia_guia-nacional.pdf

El área de Criminalística de la Dirección General Científica de la Guardia Nacional inicia el proceso de certificación de Cadena de Custodia en el año 2015, manteniendo la misma durante cuatro ciclos anuales hasta el año 2019.

La ampliación en la Certificación ISO 9001:2015 "Sistemas de Gestión de la Calidad" en el alcance de la certificación del Proceso de Cadena de Custodia, desde el procesamiento del lugar de la intervención, hasta su entrega a los laboratorios para su análisis forense. (Gráfico 1)

En virtud de que los servicios forenses, realizan estudios que juegan un papel importante en la investigación de delitos, tales como la lucha contra el terrorismo, identificación de víctimas en catástrofes, estudios de filiación (paternidad, adopciones irregulares, fosas, etc.). Se estableció el reto, desarrollar una ampliación de alcance en certificación con la perspectiva del lugar de intervención.

Permitiendo ser el pionero entre las instituciones responsables de Seguridad Pública con más conocimiento y experiencia en el procesamiento del lugar de intervención, que se equipara con el procesamiento de la escena del crimen, con la intención del desarrollo homologado de los criterios, documentos y procedimientos en este tema.

Con la finalidad de garantizar la confiabilidad en la aplicación de los procedimientos de recepción, canalización a las diferentes especialidades forenses, almacenamiento temporal y entrega de los indicios y/o evidencias a las autoridades solicitantes, que se realiza con base en los niveles de legalidad, confiabilidad, transparencia y profesionalismo conforme a las normas, guías lineamientos nacionales e internacionales del sistema de cadena de custodia.

La transición hacia el Sistema Penal Acusatorio en México va de la mano de grandes retos en materia forense a nivel nacional, uno de ellos es la implementación y seguimiento de normas de calidad nacionales e internacionales.

VIII. Tendencias

En este contexto, los cambios hacia este nuevo sistema de justicia apuntan a que sólo los dictámenes emitidos por laboratorios de análisis forense acreditados o en vías de estarlo podrían ser tomados como válidos en las investigaciones criminalísticas y penales, ante Ministerios Públicos y jueces, con el fin de resolver hechos punibles.

Lo anterior se establecerá a través de un esquema coordinado, que parte de un ejercicio de autodiagnóstico, sistematizado a través de las auditorías internas en gestión de calidad.

Mediante el establecimiento de directrices claras, tales como:

- Establecer los procesos, procedimientos y mecanismos, que permitan coordinar y supervisar la operación de los servicios científicos y técnicos, que brinda la Dirección General Científica, de conformidad con los requerimientos establecidos por las áreas de la Guardia Nacional para el cumplimiento de sus funciones.
- Coordinar la atención de solicitudes de autoridades competentes y las áreas que integran la Institución, en el ámbito de su competencia, para proporcionar auxilio en la búsqueda, preservación y obtención de indicios y evidencias, así como medios de pruebas, que resulten en la investigación de delitos.

Para dar cumplimiento a los requisitos de servicio o de producto científico dentro de sus atribuciones establecidas en el marco normativo, da respuesta a la Guardia Nacional y autoridades competentes (Juez, Ministerio Publico, Fiscalías, etc.).

La información aquí trabajada, expresada en la Ley Federal de Transparencia y Acceso a la Información Pública, se vuelve información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, por lo que no puede ser informada expresamente al público durante su tratamiento interno.

Cuando la autoridad realice una solicitud de la información mediante los portales legales de transparencia, la Alta Dirección o el personal designado se pondrá en contacto con la autoridad competente (Ministerio Publico, Juez, etc.).

Derivado que solo las solicitudes giradas para requerir un análisis de laboratorios son realizadas por las autoridades solo con ellos se mantendrá la comunicación, y será únicamente de lo solicitado y de su información conforme a lo pactado al inicio del servicio.

La conducción de todas sus actividades bajo el apego del **Acuerdo A/009/15** por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.

La aplicación de métodos para el manejo de los indicios y elementos de prueba, conforme a la normatividad aplicable de cadena de custodia.

Finalmente, del convenio general de colaboración entre el **FONDO SECTORIAL CONACYT-SEGOB-CNS,** No. Folio **C-S-101772 - CONACYT SEGOB CNS 2017-5,** con la finalidad de obtener la capacitación especializada en diversos temas en materia de calidad que son de gran certidumbre en los laboratorios forenses.

Se brindó la capacitación y reafirmaron las habilidades de los siguientes temas:

- Conocimiento, entendimiento y aplicación de los puntos contenidos para la certificación ISO 17025:2017 "Requisitos Generales para la Competencia de los laboratorios de ensayo y calibración".
- Formación de Auditores Internos en Sistemas de Gestión en ISO 17025: 2017.
- Certificación de Auditores Internos en Sistemas de Gestión en ISO 17025: 2017.
- Conocimiento, entendimiento y aplicación de los puntos contenidos para la certificación ISO 9001:2015 en "Sistemas de Gestión de la Calidad".
- Certificación ISO 9001:2015 en Sistemas de Gestión de la Calidad.
- Gestión de riesgos aplicado a Sistemas de Gestión bajo la ISO 3100:2018.
- Construcción de indicadores y desempeño.
- Formación de Auditores Internos en Sistemas de Gestión en ISO 9001:2015 "Sistemas de Gestión de la Calidad".
- Conocimiento, entendimiento y aplicación de los puntos contenidos de ISO 19011:2011 - Sistemas de gestión- Directrices para la auditoría de sistemas de gestión.
- Directrices para evaluar el desempeño del SGC y el cumplimiento de los requisitos de los sistemas de gestión con base en las normas de gestión ISO 19011:2018.

Se desarrollaron las aptitudes, actitudes y habilidades necesarias, para vigilar y dar seguimiento al Sistema de Gestión de la Calidad, que se ha implementado para los servicios forenses que brindan el apoyo a la policía con capacidades científicas.

El cual brinda la confianza de generar auditorías internas, con bases en la planificación, las buenas prácticas de auditoria y las competencias del auditor líder. Además de reforzar el análisis de la evaluación de la eficacia y las oportunidades de mejora del proceso, que tiene por finalidad brindar el soporte de credibilidad de los resultados.

En el marco del Fondo Sectorial CONACYT-CNS para la Seguridad Pública, en 2017 se definió la Convocatoria 2017-5 "Certificación de competencias". El objetivo era el fortalecimiento de recursos humanos mediante cursos de especialización y certificaciones en materia de ciberseguridad y criminalística, con la participación, tanto de instituciones públicas como privadas.

Estos cursos fueron dirigidos a la alta especialización requerida por parte del personal de la Dirección General Científica de la Guardia Nacional para atender delitos que se encuentran en el borde de la tecnología, mediante la integración de diversos métodos formales para aumentar la eficiencia en las pruebas de seguridad y la corrección eficiente de las fallas y debilidades identificadas.

La continua capacitación en estos campos de conocimiento conlleva:

- Orientación metódica para el desarrollo de las disciplinas de computación e investigación para probar y validar los sistemas de seguridad de la información.
- Promoción y apoyo en el diseño de tecnologías diversas asociadas a la seguridad de la información, así como incremento en el uso apropiado de tecnologías de la información, en particular en la verificación y validación de la efectividad de los sistemas, dispositivos y procedimientos de ciberseguridad.
- Aseguramiento e incremento de la productividad al aumentar la confiabilidad en la continuidad de los sistemas y en la seguridad de la información.
- Incremento del conocimiento en ciberseguridad, riesgos, amenazas al documentar y comunicar los resultados de cada actividad y prueba de seguridad realizada.

IX. Certificación de competencias laborales ante conocer

Hasta el año 2011, el único mecanismo para la permanencia del personal policial lo representaban los controles de confianza. A partir de ese año se instaura la evaluación del desempeño que año con año se aplica en función de la relación de dependencia jerárquica que cada integrante tiene con su respectivo superior. De esto surge un cambio cualitativo con la emisión, en 2017, del Certificado Único Policial.

El Certificado Único Policial es el mecanismo integrador de los requisitos de permanencia que añade al secular control de confianza y la evaluación del desempeño, la integración de competencias laborales específicas que el policía debe refrendar periódicamente. De acuerdo con el *Manual para la Capacitación y Evaluación de Competencias Básicas de la Función para los Integrantes de las Instituciones de Seguridad Pública:*

> *El proceso de evaluación por competencias es esencialmente de recolección, procesamiento y valoración de información orientado a determinar en qué medida el personal operativo ha adquirido el conocimiento y dominio de una determinada competencia o conjunto de competencias a lo largo del proceso formativo, por lo que deberán establecerse acciones de capacitación y evaluación en diferentes momentos para conocer el grado, manejo y avance de los sustentantes.*

La entonces Policía Federal a través de su Entidad de Certificación y Evaluación (EC), operada por la Coordinación del Sistema de Desarrollo Policial (SIDEPOL), acreditada por el Consejo Nacional de Normalización y Certificación de Competencias Laborales (CONOCER) para capacitar, evaluar y certificar las competencias laborales del personal, y con la finalidad de promover en las diferentes unidades administrativas el cumplimiento de la obtención del Certificado Único Policial, a partir del 05 de septiembre de 2017 conformó el Centro de Evaluación de la hoy Dirección General Científica, como Unidad Administrativa acreditada a propuesta de la Entidad de Certificación y Evaluación de Competencias; esto para evaluar con fines de certificación, las competencias de las y los integrantes de la entonces División, con base en cualquiera de los Estándares de Competencia registrados por la Dirección General Científica.

- EC0509 "Aplicación del censo biométrico para la obtención de las Características Individuales".
- ECO 757 "Búsqueda de información en la red pública de internet para la investigación policial".

En un sistema formalizado se desarrolla el siguiente conjunto de acciones para el servicio del centro de evaluación de la Dirección General Científica de la Guardia Nacional:

A) Las áreas programan con anticipación con el Centro de Evaluaciones, actividades de evaluación; solicitan al Centro de Evaluación el acceso para el desarrollo de capacitación y evaluaciones de los estándares de Competencia vigentes de la Dirección General; el personal que tendrá acceso es el asignado con figura de supervisor y evaluador, con sus respectivos candidatos; cada una de las actividades serán coordinadas y registradas por el coordinador del Centro de Evaluación; las áreas deberán informar al coordinador del Centro de Evaluación de manera inmediata cualquier situación que se presente con los

supervisores, evaluadores y candidatos; los supervisores informarán al Coordinador las situaciones emergentes que se presenten en las evaluaciones; las áreas son las responsables de llevar el control del estatus de su personal certificado y reportarlo al Centro de Evaluación.

B) Cada año se identifica al grupo prioritario que recibirá la actualización en su estándar de competencia para la permanencia de acuerdo El contar con un registro propio permite a la Guardia Nacional que el Sistema Nacional de Seguridad pública considere como válidas las competencias registradas, para no someterse al régimen que abarca a las demás policías del país (primer respondiente, policía de investigación y sistema penitenciario).

Lo anterior implica una significativa responsabilidad de mantener actualizado al personal además de contar con evaluadores que transmitan las tres grandes áreas del saber competencial: conceptual (saber conocer), procedimental (saber hacer), y actitudinal (saber ser) dentro del campo específico de conocimiento que abarcan las competencias así registradas.

X. La educación para la función científico policial: Un apunte

Ninguna elaboración en torno a la formación de recursos humanos para la policía científica puede verse completa sin añadir un comentario dirigido a la educación científico policial. Como se ha corroborado en las páginas anteriores, la formación del personal dentro de la Dirección General Científica de la Guardia Nacional, requiere de capacitación y especialización, así como el desarrollo de competencias generales y específicas para el desempeño de su labor.

Durante 2019, cuadros que habían estudiado la licenciatura en ciencias policiales desarrollada por la institución, pudieron ver colmado su anhelo de pertenecer a la Dirección General Científica. Este interés genuino por aportar desde el conocimiento que brindan los estudios superiores a la prevención y la persecución de los delitos, da cuenta de la acreditación del área científica y su aporte, real y potencial, a la solución de los problemas de la seguridad en el país. Sin embargo, una efectiva formación de cuadros científicos demanda que se alcancen grados académicos con maestría y doctorado dentro del dominio de las atribuciones de la propia Dirección General Científica de la Guardia Nacional.

Anteriormente nos referíamos a la ciencia de datos, las neurociencias y la inteligencia artificial como áreas de conocimiento emergentes que reclaman la formación de especialistas que actualicen métodos y sistemas; incorporen metodologías disciplinarias a sus distintos campos de trabajo, y que permitan dilucidar el modus operandi de posibles bandas criminales guiadas por la instrumentación de ingenios y sistemas de punta, pero también empresas y gobiernos del extranjero dedicados a vulnerar infraestructuras y sistemas sensibles para sus propios intereses. En este campo se han intentado

propuestas de universalización del conocimiento que permitan al personal dedicar un periodo de tiempo mínimo de dos años a la especialización del conocimiento científico.

Por este motivo resulta indispensable la identificación de cuadros que profundicen y perfeccionen el conocimiento en estas y otras ramas, como genética y genómica, ciencias de la computación, las diversas ramas de la ingeniería para la operación de laboratorios y talleres, y en general todo aquello que, dentro de un plan bien establecido, aporte a la expansión del saber científico aplicado a la prevención y la investigación, incluso a la inteligencia policial.

Sin embargo, diversos factores conspiran contra la materialización de este propósito. El primero es la carencia de recursos humanos suficientes que faciliten la distracción de sus tareas para dedicarse a estudios de posgrado en ciencia básica e ingeniería. Un factor adicional es, hay que decirlo, la permanencia en el trabajo.

Es necesario desarrollar instrumentos normativos que obliguen a la futura o futuro posgraduado a permanecer en la institución dedicado tanto a compartir el conocimiento adquirido, como proceder a su aplicación empírica en las unidades y laboratorios para la prestación de los diversos servicios, además de enriquecer con el conocimiento especializado así adquirido, las capacidades para la investigación, el desarrollo de infraestructura, laboratorios y servicios acordes al estado del arte en la ciencia, la tecnología y la innovación.

Que la institución produzca su propio capital humano y desarrolle competencias de alta especialización requerirá del compromiso voluntario, y al mismo tiempo vinculante, que devuelvan a la institución lo invertido en la formación de ese y otros cuadros, al tiempo de motivarlos para crecer en la estructura, funciones y carrera institucionales.

Éste es quizá el mayor desafío que enfrenta el desarrollo científico policial para mantenerse en la frontera del conocimiento mediante la formación de cuadros especializados, que complementarán las tareas de incesante desarrollo de protocolos, métodos y sistemas en los distintos laboratorios y talleres con que cuenta la Dirección General Científica de la Guardia Nacional.

En este contexto la Guardia Nacional aportará a la cultura policial en su conjunto y permitirá proyectar las categorías, conceptos, lógica y método científico al quehacer policial para el desarrollo institucional y en los órdenes de gobierno Estatal y Municipal en materia de seguridad pública e investigación científica.

Fuentes de Consulta:

- LinziWilson-Wilde (2018), The international development of forensic science standards — A review, Elservier, Forensic Science International, Volume 288,July 2018, Pages 1-9
- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (2017) Manual para la Capacitación y Evaluación de Competencias Básicas de la Función para los Integrantes de las Instituciones de Seguridad Pública, consultado en:https://www.gob.mx/cms/uploads/attachment/file/ 237940/Manual_para_la_ capacitacion_y_evaluacion_de_competencias_basicas.pdf
- Acuerdo A/009/15 PGR. Por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia. D.O.F 12/II/2015.
- Código Nacional de Procedimientos Penales.
- Guía Nacional de Cadena de Custodia.
- ISO/IEC 17025:2017 Requisitos generales para la competencia de los laboratorios de ensayo y de calibración. Tercera edición 2017-11, Versión corregida 2018-03
- ISO/IEC 9000:2015. Sistemas de gestión de la calidad – Fundamentos y vocabulario.
- ISO/IEC 9001. Sistemas de gestión de calidad-Requisitos. Quinta edición 2015-09-15
- ISO/IEC 19011. Directrices para la auditoría de los sistemas de gestión. Tercera edición 2018-07
- ISO/IEC 31000:2018: Gestión del riesgo (Traducción oficial) Segunda edición 2018-02
- ISO/IEC 27001 - Information security management systems – Requirements.

VIGILANCIA Y PROSPECTIVA TECNOLÓGICA

Dr. Juan Carlos Rivera Dueñas[1]
Mtra. Beatriz Olivia Sánchez Flamenco[2]

Sumario: I. Introducción; II. Monitoreo tecnológico III. Evaluación tecnológica; IV. Vinculación estratégica. V. Ingeniería de procesos técnico-operativos. VI. Consideraciones finales.

I. Introducción

El desarrollo tecnológico es un fenómeno social que se manifiesta no solo con el surgimiento de productos innovadores orientados a la resolución de problemas y necesidades; sino que también propicia la creación de nuevos procesos, paradigmas vanguardistas, y hasta campos de estudio emergentes que van redefiniendo a la misma sociedad, de modo que la innovación tecnológica no solo es el resultado tangible de una larga cadena de procesos cognitivos, también es el catalizador que, de manera estratégica, hace converger recursos de diferente índole, encaminados a la materialización de una visión al futuro.

Bajo este marco de trabajo se elaboró el andamiaje conceptual que dirigiría el Modelo de Innovación Tecnológica para la Operación Policial (Fig. 1), conformado por tres pilares principales: el primero tiene en la investigación científica y el desarrollo la columna vertebral del modelo, constituyendo las bases científicas y tecnológicas que conformarán productos innovadores, mediante el uso de herramientas metodológicas estrictas.

El segundo es la implementación de nuevos procesos policiales, que mediante el acompañamiento técnico profesionalizado, llevaría a la asimilación tecnológica y la reingeniería de estos procesos. El tercer pilar se encuentra anclado en la vigilancia y prospectiva tecnológica que, como si fuera el sistema visual de una entidad compleja, proveería un amplio panorama situacional, que permita dirigir de forma activa y consciente, las actividades del resto del modelo.

---

[1] Con Doctorado en Control de Sistemas del Posgrado de la Facultad de Ingeniería de la UNAM, fue escritor y editor de artículos para la revista "Robotica" de la Cambridge University Press de Inglaterra. Durante su estancia en la Policía Federal y la Guardia Nacional de 2010 a 2020 se generaron más de sesenta proyectos de desarrollo y reparación de infraestructura policial; así como proyectos de infraestructura tales como la Maestría en Seguridad Hemisférica del Sistema de Desarrollo Policial, el Laboratorio Nacional de la Guardia Nacional y los convenios de colaboración con el sector académico.
[2] Cursó la licenciatura en Periodismo con diplomado en Periodismo Político por el Centro de Estudios Universitarios de Periodismo y Arte en Radio y Televisión, cuenta con 10 años de experiencia en materia de Seguridad Pública enfocada a la Ciencia y a la Tecnologica, por la cual ha tenido diversos cargos como la Jefatura de Departamento de Vinculación con la Industria, Encargada de la Subdirección de Especialidades y Difusión y Vinculación Tecnológica; culminando con la Dirección de Monitoreo y Evaluación Tecnológica para la Operación Policial

Lo que el modelo representa es en realidad un ciclo de gestión tecnológica enfocada a su aplicabilidad en Seguridad Pública. Que si bien, las actividades involucradas en los tres ámbitos antes descritos, es la Vigilancia y Prospectiva Tecnológica la que permite establecer un plan estratégico de implementación; proveyendo de información relacionada, no solo acerca de la tecnología que puede ser utilizada de manera efectiva para requerimientos de seguridad pública; sino que también acerca de los mayores retos tecnológicos a mediano y largo plazo, los riesgos y las amenazas latentes por parte de la delincuencia, así como las tendencias y los nuevos desafíos científicos que puedan ser aprovechados para el beneficio del estado. Esto tiene la finalidad de plantear la implementación tecnológica desde el punto de vista costo-beneficio, considerando el tiempo de vida útil de la misma, temporalidad operativa, nivel de especialidad o conocimientos necesarios para su operación, limitantes e impactos socioculturales, por mencionar algunos factores.

Durante la formación y consolidación de la Dirección General Científica, la vigilancia y prospectiva tecnológica se fue implementando como un paradigma activo. Esto quiere decir que busca interactuar con los agentes determinantes del contexto técnico-policial, a fin de identificar con claridad las condiciones óptimas de evolución tecnológica en la operación policial. Esto se ha logrado mediante la implementación de cuatro principales actividades a ser desarrolladas a lo largo de este capítulo:

- Monitoreo tecnológico
- Evaluación tecnológica
- Vinculación estratégica
- Ingeniería de procesos técnico-operativos

II. Monitoreo Tecnológico

Con el objetivo de plantear alguna mejora tecnológica dentro de las instituciones, se debe iniciar con un diagnostico donde se establezca claramente la línea base sobre la cual debemos medir el estado en el que nos encontramos. Esto se realiza mediante un monitoreo, que debe ser realizado de manera estratégica, que pueda servir como el termómetro que nos ayude a identificar el grado de capacidad tecnológica para atender acciones de seguridad pública.

Tomando en consideración el estándar Directrices para la implementación de un proceso de Vigilancia Tecnológica GT-004-INMC-2012, donde se establece que el monitoreo debe ser un proceso continuo, permanente y dirigido por objetivos claros, se debe tomar en consideración que hay tres ámbitos a considerar en esta actividad para utilidad de la Guardia Nacional:

- Las capacidades tecnológicas actuales de las Unidades Administrativas.
- La oferta del mercado con productos con madurez tecnológica validada.
- Tendencias innovadoras y emergentes provenientes de centros de investigación.

Lo anterior se logra mediante un continuo análisis interno para identificar vulnerabilidades y mejores prácticas, y por otro lado, mediante un análisis externo sobre las posibles funcionalidades disponibles por actores externos.

a) Análisis interno de requerimientos tecnológicos

Mediante la creación de un Grupo de Trabajo en Monitoreo y Evaluación Tecnológica, conformada por representantes de cada una de la Unidades Administrativas, de logró la identificación de áreas de oportunidad dentro de la institución. De esta forma, y bajo un acompañamiento personalizado de especialistas técnicos, se busca la estrategia de solución más adecuada, no solo en términos tecnológicos, sino en términos de prestaciones táctico-policial basadas en mejores prácticas.

Para la identificación de mejores prácticas se realiza un análisis de las funciones y objetivos que persiguen las actividades policiales, así como los recursos humanos, materiales y financieros que requieren. Lo anterior nos da el contexto de escenario de operación de la misma y nos ayuda a plantear los posibles escenarios que resuelve la actual estrategia de operación; así como los riesgos, compromisos y resultados que derivan de ella. Se busca como otras instituciones atienden dichas actividades, qué tecnologías emplearon y como las implementaron; esto con la finalidad de poder estructurar una comparativa, analizar los posibles escenarios y evaluar el impacto de su implementación en la Guardia Nacional. La identificación de mejores prácticas policiales es una actividad poco solicitada institucionalmente, pero con un amplio impacto operativo a largo plazo.

[4] Secretaría de Economía (2012) "Declaratoria de vigencia de la Norma NMX-GT-004-IMNC-2012". Diario Oficial de la Federación, 17 de diciembre de 2012 (https://www.dof.gob.mx/nota_detalle.php?codigo=5282554&fecha=17/12/2012). Consultado el 01 de febrero de 2021.

b) Análisis externos de prestaciones técnicas

El monitoreo al exterior se realiza planteando con claridad indicadores que permitan ser la métrica de trabajo para discriminar, clasificar y priorizar información para la toma de decisiones, en materia de vigilancia tecnológica. Estos indicadores no solo deben cubrir aspectos de infraestructura, sino también logísticos, científicos, prácticos y funcionales.

Los indicadores de bienes tecnológicos permiten dar un seguimiento a los parámetros de confiabilidad en infraestructura tecnológica; uno de ellos es la vida útil de la tecnología el cual nos permite establecer semáforos de actualización, mantenimiento y proyección de gasto de adquisición; un indicador de nivel de riesgo operativo nos permite estar preparado para los imprevistos e incidentes derivados de las operaciones especializadas con riesgos de pérdida de tecnología. Esto aunado a los indicadores propios de los servicios brindados por las áreas operativas, permite hacer una evaluación costobeneficio de las tecnologías y su factibilidad de eso.

Los indicadores de tendencias tecnológicas y científicas están determinados por el origen y las bases técnicas que los sustentan. Los avances técnicos científicos de los centros de investigación solo pueden ser monitoreados mediante una participación activa de la Guardia Nacional con dichas instituciones, manteniendo y actualizando un registro de las líneas de investigación más importantes, capacidad científica asociada al Sistema Nacional de Investigadores y resultados más prometedores capaces de ser implementados en la actuación policial. Otro indicador de tendencias es el grado de madurez tecnológica que se ha alcanzado a través de estos paradigmas emergentes, esto con el objetivo de mantener un balance entre el tiempo de implementación y el impacto institucional.

III. Evaluación Tecnológica

¿Por qué evaluar la tecnología desde el punto de vista operativo y con características técnicas comparables a los métodos empleados ya por la industria para la implementación de tecnología?, ¿Por qué hacerlo si existen los lineamientos y normativa para la adquisición de bienes?. La respuesta es crucial, las tecnologías tienen características técnicas más allá de lo que las normas y estándares nos indican.

La infraestructura tecnológica es solo una parte tangible de la materialización de un proceso policial, el cual determina condiciones muy particulares del uso del equipamiento tecnológico. Estas condiciones involucran características ambientales en el momento de una acción policial, el adiestramiento y las habilidades del personal, la disposición física y temporal para una intervención, entre otros. Un sistema de vigilancia aérea comercial, ya validada bajo ciertos estándares de producción, debe ser evaluado sobre el

ambiente donde se espera utilizar, determinar si la información que proporciona es la requerida para operaciones a las que la Guardia Nacional requiere. Sistemas de vigilancia aérea con origen extranjero no necesariamente tiene el mismo desempeño funcional ante un escenario nacional.

De este ejemplo podemos ver claramente que la función policial define el tipo de equipamiento que se requiere; estos factores son contemplados en las normas y estándares para los procesos de adquisición, pero no son claros o no nos brinda información de que tanto aportaran a la eficiencia del personal al momento de realizar sus labores o cuanto estrés puede soportar dicho equipamiento de acuerdo con los escenarios de operación o factores climáticos de temperatura y humedad. Pueden ver que dichos factores dependen de conocimiento específico sobre la función policial, los riesgos a los que se somete el personal y el equipamiento; por lo cual la evaluación se vuelve un factor importante para el cumplimiento de objetivos y para la planeación adecuada de la infraestructura tecnológica de las instituciones policiales.

Bajo este contexto, el proceso de evaluación mantiene una continua interacción con el proceso de monitoreo tecnológico, a fin de realizar una adecuada adopción tecnológica integrándose bajo una cadena de acciones coordinadas (Gráfico 4). Las áreas de monitoreo establecen enlaces con instituciones científicas, empresas proveedoras de servicios y venta de equipamiento; con la finalidad de establecer comparativas de las tecnologías, mediante pruebas de laboratorio y pruebas en campo, que permitan pasar a pruebas operativas en escenarios reales, y con ello saber cuáles son las tecnologías que presentan las mejores prestaciones.

Con base en los requerimientos operativos de las áreas usuarias se pueda seleccionar a las mejores y establecer opiniones técnicas que permitan orientar a las áreas operativas sobre los alcances de las tecnologías y líneas prospectivas de planeación con base en sus decisiones; y con ello impactar en los procesos de actualización. Mediante el monitoreo se recolectan las mejores prácticas, internas y externas, y se integran de forma que exista una adecuación optima con el contexto operativo-policial de la institución. Esto genera finalmente un conjunto de parámetros que deberán ser considerados en la etapa de evaluación. La evaluación no solo es aplicable para tecnología comercial, sino innovaciones desarrolladas por la comunidad científica, o desarrollos tecnológicos propios.

Existen diversos tipos de evaluación y muchas más metodologías para realizarla, en función de la aplicación, requerimientos operativos y tiempo de vida útil; así como criterios técnicos como por ejemplo normatividad eléctrica, mecánica, de software, de equipos de protección y todas aquellas que las instituciones consideren aplicables para la adquisición, compra, uso y manejo de los equipos tecnológicos en los centros de trabajo con la finalidad de prevenir y evitar accidentes o enfermedades de trabajo; derivadas de la

exposición a algún agente, material o forma de uso que no sea adecuado. En el caso de la Dirección General Científica, la metodología establecida obedece a validar claramente las expectativas operativas de la Guardia Nacional.

a) Protocolos de evaluación y calidad

Las pruebas deben seguir estrictos protocolos, tanto en laboratorio como en campo, considerando previamente un análisis de requerimientos técnico-operativos de las áreas usuarias de la Guardia Nacional, focalizando a alcanzar el mejor balance costo-beneficio.

Para ello se toma como referencia el Modelo de Evaluación de Calidad proporcionado en el estándar ISO 25010. En este modelo se determinan las características de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado, tales como las funcionalidades, el desempeño, la portabilidad, la seguridad, entre otras. Con el objetivo de cubrir las propiedades de todo producto tecnológico, el modelo es solo utilizado como guía base para generar los protocolos particularizados a cada tecnología, en base al conjunto de requerimientos y banco de buenas prácticas.

Dado que la observación depende de la persona que interpreta la realidad, por lo que para mitigar los sesgos o mal interpretaciones, las pruebas realizadas bajo un estricto seguimiento de protocolos. Las evaluaciones de laboratorio se enfocan en comprender los objetos de estudio para poder diferenciar su comportamiento bajo posibles escenarios y así obtener información técnica que permita establecer los límites tecnológicos de las ofertas comerciales o desarrollos tecnológicos.

Las pruebas de laboratorio nos permiten caracterizar la tecnología, midiendo y analizando cada parámetro por separado, estableciendo hipótesis sobre posibles condiciones y comprobando finalmente cada escenario.

[5]Estandar ISO/IEC 25010 Modelo de Evaluacion de Calidad del Producto de Software. Consultado el 01 de febrero de 2021. https://iso25000.com/index.php/normas-iso-25000/iso-25010.

b) Pruebas de Laboratorio

El análisis de esa información nos permite establecer conclusiones sobre la tecnología; pero por si misma no permite decidir la mejor de ellas.

c) Pruebas de Campo

Las pruebas de campo nos permiten medir las funcionalidades tecnológicas bajo escenarios cercanos a la operación; así como la respuesta que dichas tecnologías tienen ante posibles situaciones de estrés, brindando información sobre los límites y destrezas del conjunto de características de las tecnologías que lo integran. Un ejemplo son las pruebas de campo realizadas a vehículos aéreos no tripulados, los cuales consisten en conocer los alcances de altitud, comunicación, radios de giro y características de destreza y estabilidad ante perturbaciones ambientales. Pero aunque el análisis podría brindarnos información para realizar una selección o recomendación, aún no es completo ya que los factores de usabilidad real no han sido evaluados.

d) Pruebas operativas

Estas pruebas nos permiten evaluar que tan intuitiva, flexible y adaptable es la tecnología desde el punto de vista de la usabilidad, la portabilidad y el tiempo de reacción del equipo ante situaciones de estrés del usuario. En el caso de la evaluación de un dron, por ejemplo, se evalúa la capacidad del sistema de vuelo, no solo para adecuarse a las condiciones climáticas, sino también a las vulnerabilidades del usuario, grado de pericia y posibles agentes externos, que pretendan obstaculizar la misión a cumplir.

IV. Vinculación Estratégica

La vinculación y colaboración con desarrolladores, busca encontrar áreas de oportunidad en las que los intereses comunes potencialicen las acciones operativas institucionales en materia de tecnología para la seguridad.

La vinculación científica-policial se ha definido como un proceso conformado por una serie de etapas que lleven a consolidar a la Guardia Nacional, mediante la Dirección General Científica como una entidad líder en el ámbito científico-tecnológico.

a) Redes científicas y tecnológicas

La primera etapa involucra la creación de redes de colaboración, mediante actividades y proyectos específicos. Durante los años, 2015 y 2017, algunas líneas de trabajo de la Dirección General Científica convergen con áreas prioritarias establecidas por el Consejo Nacional de Ciencia y Tecnología, por lo cual Mandos Policiales empiezan a formar parte de grupos temáticos conformado principalmente por cuerpos de académicos y científicos reconocidos nacional e internacionalmente; tal como lo fue la interacción que se presentó con la Red Temática en Ciencias Forenses. De la misma forma, durante 2016 y 2017, la Red Temática de Lengua Natural organizó sesiones especiales donde personal de la Dirección General Científica y científicos provenientes de diferentes centros nacionales de investigación compartieron experiencias y conocimientos en temas como la identificación de perfiles delictivos en las redes sociales.

Por otro lado, el personal altamente calificado de la Dirección General Científica, al estar en una institución policial, genera un perfil muy particular, que le permite aplicar conocimientos altamente especializados en situaciones críticas. Dicho perfil resulta de gran relevancia para la valoración de la viabilidad de proyectos científicos; por lo que personal de la Dirección General Científica formó parte de los Comités de Evaluación del CONACYT, entre 2016 y 2018. Con ello, la institución empieza a hacer presencia en la comunidad, no solo como una institución altamente especializada para la Seguridad Pública, sino como un actor capaz de participar activamente en la redefinición científica del país.

b) Fortalecimiento de infraestructura científico-tecnológica

Un paradigma en la administración pública federal y particularmente en las instituciones policiales, es que la colaboración interinstitucional en materia tecnológica, son muy poco común. Las dependencias que se vinculan formalmente con las instituciones o desarrolladores tecnológicos para fines tecnológicos en materia de capacitación, infraestructura tecnológica, o análisis de información, regularmente es a través de un esquema de servicios; es decir, en el sentido de recibir asesoría, adquisición de bienes o peticiones de información. Una estrategia diferente es la vinculación para la generación de socios estratégicos.

En esta segunda etapa, se buscan diferentes esquemas de colaboración con empresas, desarrolladores, academia y centros de investigación, para incrementar el capital científico y tecnológico de la Institución. Para lo anterior, la DGC ha implementado diversos protocolos para la atención y colaboración con instituciones nacionales e internacionales; desde acuerdos, convenios, mecanismos de enlace de información, acceso a plataformas de otras instituciones y mecanismos de financiamiento de proyectos de desarrollo tecnológico e innovación.

Para ello, se hace uso de uno de los resultados del proceso de monitoreo tecnológico, el cual es la identificación de necesidades tecnológicas, con el fin de generar una cartera de proyectos que dirija de forma estratégica la vinculación interinstitucional.

Supongamos que del monitoreo de tecnología y evaluación tecnológica se identificó que no se ha desarrollado tecnología enfocada al reconocimiento automático de imágenes en internet para actividades de investigación en delitos cibernéticos. Sin embargo, si existen instituciones académicas que se dedican al desarrollo de algoritmos de identificación de rostros. Para ello se puede establecer una vinculación para tener acceso a esa tecnología mediante convenios donde no se tienen esquemas de financiamiento de instituciones gubernamentales o académicas más allá de la contratación de servicios.

Entre las primeras estrategias implementadas de colaboración con centros de investigación, para fortalecimiento tecnológico fue en 2013, cuando por primera vez, una institución policial formaba parte del Registro Nacional de Instituciones y Empresas Científicas y Tecnológicas. De esa forma, la Dirección General Científica se asoció con la Universidad Iberoamericana con el fin de proveer requerimientos para el desarrollo de un sistema aéreo de vigilancia autónoma. De esta forma, se proveían de líneas de investigación a centros de investigación e instituciones de investigación superior, para el desarrollo de nuevos investigadores que solventarán problemas de alta prioridad nacional. Al mismo tiempo, el resultado de estos proyectos era la generación de tecnología de la cual la Institución será beneficiada.

Un segundo enfoque fue la generación de un Fondo totalmente dedicado al fortalecimiento de la Seguridad Pública, a través de un Convenio con CONACYT. En tal esquema, el presupuesto en materia de seguridad se priorizaba en función de las necesidades y requerimientos operativos, con base en los planes de trabajo de las áreas de la Institución. Tanto CONACYT como la Institución proporcionaban el financiamiento para proyectos científicotecnológicos, los cuales eran asignados por Convocatoria Pública y desarrollados por los Centros de Investigación.

La cartera de proyectos para vinculación era entonces valorizada mediante parámetros de alineación multidimensional, tal como es presentado en el Gráfico 8. A partir de esta evaluación se realiza una priorización de proyectos para ser financiados. El modelo de alineación está conformado por cuatro ámbitos:

- Alineación estratégica
- Función Policial
- Costo económico
- Impacto en la operación policial.

La vinculación con entidades privadas, asociaciones civiles o entidades reguladoras pueden llevar a proyectos de alta envergadura, con impacto a nivel nacional. El mercado comercial de las tecnologías juega un papel básico en este ámbito. Supongamos que la institución tiene requerimientos de comunicaciones a lo largo del país para poder establecer su interoperabilidad entre las distintas instituciones; para lo cual existen varias estrategias para resolver esta necesidad. Una opción es la contratación de un sistema de interoperabilidad a nivel federal el cual deberá de poder resolver la intercomunicación de distintas instituciones como protección civil, policías, fiscalías, ejército, marina, entre otras. Esto implica múltiples desafíos técnicos, ya que cada institución emplea diferentes tecnologías de comunicación y diferentes protocolos de seguridad de información.

Otra opción es crear lineamientos y normativas de cumplimiento estatal y federal que permitan la interoperabilidad basada en estándares y protocolo de comunicación. Lo anterior implica que los tres órdenes de gobierno deberán ponerse de acuerdo en los esquemas de comunicación y establecer acuerdos al respecto. Un último escenario de aplicación es la realización de un análisis técnico entre las necesidades, territorios y tecnologías ofertadas en el mercado comercial, para establecer los canales de comunicación, usuarios y alcances; esto con la finalidad de establecer acuerdos y contratos de servicios que contemplen los requerimientos de interoperabilidad y con ello reducir los riesgos de la implementación de las tecnologías y maximizar la explotación de la misma.

c) Liderazgo científico e innovador

La tercera etapa de vinculación estratégica plantea que la institución desarrolle una estructura autosustentable, capaz de crear conocimiento, gestionar el capital tecnológico creado y adoptado, innovar protocolos, herramientas metodológicas y paradigmas científico policiales, que impacten en la óptima asimilación tecnológica de las instituciones de seguridad.

Este modelo ya es aplicado en algunos países, tal es el caso del *Center for Applied Science and Technology* en Reino Unido, el cual se origina como *Scientific Development Branch* del Ministerio del Interior. Este departamento de innovación tecnológica, dedicada primeramente al desarrollo de sistemas de identificación y monitoreo, desarrolla vínculos con centros de investigación y actores de la iniciativa privada, a fin de perfilarse como una entidad líder en investigación aplicada. Finalmente, se integra al Laboratorio de la Defensa y Tecnología, donde es capaz de crear capital científico y tecnológico propio.

V. Ingeniería de procesos técnico-operativos

Las actividades policiales requieren de herramientas y procesos de vanguardia eficientes y confiables para ser realizadas con éxito. Con la incorporación de nuevas tecnologías, se espera que las actividades institucionales se realicen con mayor eficacia; sin embargo, la asimilación tecnológica implica altos riesgos en el uso adecuado de herramientas, la correcta interpretación de información y el adecuado cumplimiento de normativas y estándares en herramientas innovadoras. Por ello se requiere monitorear constantemente cada nuevo proceso, herramienta o servicio tecnológico para establecer mecanismos de mejora continua.

En la DGC se han realizado actividades de apoyo interinstitucional para el establecimiento e implementación de mejores prácticas policiales, industriales e institucionales. La intención es la creación de estándares de actuación policial en materia de tecnología, macroprocesos policiales que involucran la participación de múltiples áreas en la Guardia Nacional, subprocesos al interior de cada una de ellas, así como protocolos y procedimientos de operación que permitan estandarizar la información, así como evaluar la eficiencia y eficacia de las operaciones policiales.

Esta actividad de análisis permite mantener actualizada a las instituciones en temas tales como estructura orgánica, planeación y crecimiento de las áreas, políticas y manejo de cargas de trabajo, entre otros. El análisis de procesos policiales nos permite hacer reingeniería de las instituciones y mantenerlas actualizadas conforme a los cambios sociales y necesidades de seguridad que se presenten.

Con ello, se ha propuesto el Modelo de Mejora Tecnológica Institucional (Gráfico 10), el cual está basado en CMM (Capability Maturity Model) y establece una trayectoria de reacondicionamiento de procesos, que deberán recorrer las áreas operativas, para asegurar la eficiencia tecnológica de los procesos operativos.

El modelo plantea una guía base para construir un sistema de calidad orientada en la asimilación gradual y optimizada de la tecnología y la innovación, dentro de las actividades de prevención e investigación policial.

- La base del modelo está establecida con el reconocimiento inicial de procesos y tareas dependientes de la tecnología policial. Con ello, se debe caracterizar a partir de los resultados que genera, y evaluado a través de directrices de control interno en cada área operativa.
- La segunda etapa de este modelo está dirigido con la generación de Procesos Sistemáticos Operativos (PSO) que permitan la repetitividad de resultados y mitigar el sesgo de los operadores de la tecnología.

- Mediante protocolos definidos por las áreas de evaluación tecnológica, se deben plantear claramente puntos de verificación del proceso, a fin de supervisar la adecuada realización de una tarea, e identificar posibles áreas de oportunidad. El resultado podría ser utilizado por el proceso de monitoreo y vinculación para solventar vulnerabilidades en la ejecución del PSO.

La etapa final del modelo obedece a la optimización de los PSO, mediante una adecuada asimilación tecnológica, y de mejores prácticas, mediante la continua ejecución del proceso de evaluación tecnológica.

Si bien, se ha plasmado la asimilación de tecnología y mejores prácticas técnico policiales, es importante también considerar que existe una transición inherente en el cambio de cultura tecnológica, el cual deberá ser analizado y solventado bajo una adecuada comunicación dentro de la operación diaria. Esto lleva a un cambio de paradigma sociocultural al que el personal policial deberá someterse de forma consciente y con convicción.

Con el internet y las redes sociales, la dinámica de interacción humana se agilizó y la evolución de la sociedad fue sometida a un impulso acelerado, que en tan solo 30 años ha cambiado las formas en las que se relacionan las personas. La seguridad no ha sido una excepción, y presenta grandes retos, tal como lo es la ciberseguridad. Los protocolos de actuación, procesos de operación de evidencias y atención a la ciudadanía han evolucionado para convertirse en metodologías con mecanismos de evaluación más cuantitativas, en donde la experiencia de los peritos es considerada como estratégica. De la misma forma, deberá ir evolucionando cada actividad policial, fortalecida mediante una nueva cultura tecnológica.

VI. Consideraciones finales

La ciencia descubre nuevas formas de entender el mundo constantemente y el conocimiento humano crece con ella, los ecosistemas sociales evolucionan en función de los factores y patrones generados por la interacción humana. Por eso es necesario construir esquemas de colaboración y procesos operativos que permitan atender las necesidades de la ciudadanía de forma eficaz y eficiente, este en sí es un proceso tecnológico permanente que en las organizaciones gubernamentales mexicanas tiene grandes áreas de oportunidad.

En la Guardia Nacional se afinan los procesos tecnológicos especializados desde varias aristas. Pero existen también procesos operativos de servicios y mantenimiento de la infraestructura tecnológica y de comunicaciones que son el sistema nervioso de una institución donde se requiere de una planeación metódica y prospectiva en función de las nuevas tecnologías que se desarrollan, se comercializan y se implementan en las áreas operativas y administrativas de la institución.

VISIÓN PROSPECTIVA DE LA INVESTIGACIÓN CIENTÍFICA EN LA GUARDIA NACIONAL

Mtro. Oliver González Barrales[1]

Sumario: I. Introducción. II. La cuestión del método científico. III. La ciberseguridad y su operación con el método científico. IV. El nuevo espíritu del tiempo. V. Ciencia y prospectiva VI. Enfoque colaborativo; VII. Acreditación y certificación en sistemas de gestión de la calidad en las ciencias forenses para la prevención e investigación del delito. VIII. Tendencias; IX. Certificación de competencias laborales ante Conocer; X. La educación para la función científico policial: Un apunte.

I. Introducción

La ciencia aplicada a la función policial desde su origen buscaba integrar a la investigación policial los principios de las llamadas ciencias exactas, incluyendo la química y, sobre todo, los avances de la biología y la medicina, acrisolando el pensamiento científico en la disciplina de la criminalística, que desde finales del siglo XVIII aportaba conocimiento para la resolución de casos criminales.

Más tarde, surgida del pensamiento positivista europeo y su visión en torno de dirigir el progreso a través de una mejor interacción y concienciación, de la criminología se propuso desarrollar una ciencia del castigo con base, de acuerdo con su creador, Giovanni Lombroso, en la observación de los comportamientos antisociales ocurridos en cárceles y hospitales. El enfoque plasmado en la nueva disciplina se fijó la misión de descubrir y sistematizar las leyes del comportamiento delictivo para en última instancia prevenir el delito mediante la identificación de perfiles criminales cuyos rasgos característicos permitan identificar el *modus operandi*.

Independientemente del grado de acierto de sus fuentes formativas, contar con una policía científica ha simbolizado los esfuerzos por dotar a la función policial de rigor, orden y un indeclinable sentido de búsqueda de la verdad objetiva; podemos afirmar, sin temor a equivocarnos que resulta necesario profesionalizar al personal policial en el uso de métodos,

[1] Ingeniero en Sistemas Computacionales y Maestro en Tecnologías de la Información y Administración por el Instituto Tecnológico Autónomo de México (ITAM), certificado en ISO27001:2013, Auditor Líder, Sistema de Gestión de la Seguridad de la Información; CISM, Administrador General de la Seguridad de la Información y Hacking ético OPST OSSTMM. Cuenta con alrededor de 20 años de experiencia en el Sector de Seguridad Pública en el Gobierno Federal, permitiendo alcanzar diversos logros como lo es el desarrollo del modelo homologado de policía cibernética, semanas nacionales de la ciberseguridad, lanzamiento de campañas de concientización en ciberseguridad a nivel nacional y certificaciones de procesos en la entonces División Científica de la Policía Federal.

herramientas, impulsar el desarrollo del talento humano y el refuerzo de sus capacidades en la frontera del conocimiento científico, enfocando sus actuaciones en procedimientos objetivos para determinar las causas del delito, dirigiendo sus investigaciones a la generación de resultados de valor probatorio penal, y lo más relevante generar conocimiento para la prevención del delito.

Hace casi un siglo, en México, alrededor del año 1923, se intentó por primera vez la constitución de una policía científica mediante la creación de la Escuela Técnica de Policía, plantel del cual egresaron unos 400 técnicos que formarían una estructura de profesionistas dedicados a la criminología, las técnicas de investigación policial y la identificación de personas, todo ello a cargo de un profesorado integrado por criminólogos, médicos y fotógrafos.

Desafortunadamente, por apremios de la época se resolvió contar con una policía menos formada, de modo que las aspiraciones originales de formar una policía científica quedaron reducidas a la función pericial forense de identificación de personas, a cargo de las instancias de procuración de justicia, que sin duda es una tarea relevante para la impartición de justicia, dista mucho de la formación de una policía que aplique la ciencia y la técnica con una visión holística en favor de la seguridad en nuestro país.

Tendrían que pasar décadas para que en 2010 se creara la División Científica de la extinta Policía Federal, cuyo establecimiento se consagró en 2011 al alojarla en el edificio que actualmente ocupa, en la alcaldía Álvaro Obregón de la Ciudad de México, con el propósito de ser el primer cuerpo policial orientado al fortalecimiento de la función policial en nuevo entorno, con nuevos riesgos por la evolución tecnológica y en la perspectiva del sistema penal acusatorio en México.

Con el cambio radical en el fortalecimiento de los cimientos constitucionales, con el propósito de construir un cuerpo policial civil que dé certidumbre en la carrera policial y una formación que perdure a largo plazo se crea la Guardia Nacional, que impulsa el desarrollo de una Guardia Nacional Científica a través de la Dirección General Científica adscrita a la Unidad de órganos Especializados por Competencia, que recibe la estafeta en la carrera por consolidar el conocimiento científico y tecnológico en el ejercicio de la función policial con el entusiasmo de resarcir la deuda que por décadas se ha tenido con la ciudadanía en materia de seguridad.

La Dirección General Científica tiene la encomienda de usar y aplicar los conocimientos y el herramental científico para la investigación especializada del delito, proporcionando servicios técnicos y científicos en colaboración y coadyuvancia con la autoridad de procuración e impartición de justicia, en conjunto con las direcciones generales de inteligencia, antidrogas e investigación.

Más allá de la descripción formal de sus atribuciones, la policía científica aporta a la Guardia Nacional la plena participación en el sistema penal acusatorio, generando elementos de prueba apegados al protocolo nacional de cadena de custodia para la identificación de personas, las capacidades en materia de ciberseguridad, prevención de la ciberdelincuencia y el desarrollo tecnológico para la función policial.

Con el aporte de la Dirección General Científica, la Guardia Nacional refuerza el enfoque multidimensional en la atención del delito, con ello no solo se atienden las conductas criminales tradicionales, que dicho sea de paso han evolucionado junto al desarrollo tecnológico, ampliando el alcance de los tentáculos de la delincuencia, también se atienden las conductas criminales que nacen con la evolución tecnológica, es decir, los llamados ciberdelitos, aquellas actividades delincuenciales que no existían en épocas de nula conexión o interacción en línea.

La prevención e investigación de los delitos cibernéticos incluye tanto la modalidad de ciberseguridad para evitar la afectación de infraestructuras críticas que inciden en el funcionamiento de la industria, los servicios, las finanzas y la economía, como la ciberdelincuencia, esto es, los delitos que se materializan a través del medio electrónico, como el comercio ilícito, el lavado de activos, el fraude, pero también la trata de personas y el abuso de menores a través de la pornografía infantil.

Con más de 24 especialidades, en el ámbito de la criminalística, tanto de campo como de laboratorio, la Guardia Nacional atiende temas relevantes en nuestro país como el de personal desaparecidas, mediante uso científico del ADN, el análisis de sustancias para la identificación de tráfico ilícito de drogas mediante instrumentos y personal especializado en química, así como análisis de documentos, análisis de balístico, análisis de datos biométricos como huella y voz, entre muchas otras capacidades para la prevención e investigación del delito, resaltando la adaptación de la criminalística en el nuevo entorno operativo, el ciberespacio, realizando también análisis cibercriminológicos que aportan evidencia y líneas de investigación a efecto de que la autoridad ministerial lleve a buen puerto las carpetas de investigación correspondientes.

La innovación tecnológica es transversal y necesaria, con el desarrollo de productos y servicios que no solo fortalecen las capacidades de la Guardia Nacional en el ciberespacio y en el ejercicio de la ciencia aplicada a la función policial, si no que también fortalecen el ejercicio de las funciones de la Guardia Nacional en sus diferentes tareas, como la seguridad en carreteras, las operaciones encubiertas, o las investigaciones encargadas por la autoridad ministerial. La innovación tecnológica de la Guardia Nacional ha trascendido a otras instancias relacionadas con la seguridad de nuestro país, como en el fortalecimiento de la seguridad en los penales federales por medio del análisis del espectro radioeléctrico para la prevención de comunicaciones prohibidas, o bien en la mejora tecnológica del sistema base del Registro Público Vehicular,

así como, diversas acciones que abonan a la prevención de los delitos, colaborando en la investigación, la obtención de información, el levantamiento topográfico por medio de drones y diversas acciones de detección y vigilancia para prevenir situaciones de riesgo a la seguridad de la información y de las personas.

El fortalecimiento de la ciberseguridad, la prevención y combate al cibercrimen es uno de los desafíos más importantes que enfrenta México y el mundo, con impacto directo en la seguridad pública, seguridad ciudadana y Seguridad Nacional, se asocia a conductas delictivas relevantes como el lavado de dinero, la pornografía infantil, trata de personas, robo de identidad, comercio ilegal y la afectación a las infraestructuras críticas como la del sector financiero, energético, y el de salud, entre otros.

Con la experiencia de más de una década de policía científica, se mantiene viva una pregunta: a la vuelta de los años ¿qué tan científica es la policía científica?, a ella trataremos de dar respuesta en el contexto de la Guardia Nacional.

II. La cuestión del método científico

Voltaire, en *Zadig o el Destino* (Eco: 1992) nos describe los primeros planteamientos del conocimiento con aspiraciones científicas: Zadig, legendario ciudadano de Bagdad en la época del esplendor del conocimiento árabe:

> "buscó la felicidad en el estudio de la naturaleza. «No hay mayor ventura, decía, que la de un filósofo que lee en ese gran libro que Dios ha puesto ante nuestros ojos (subrayado nuestro). Las verdades que descubre son suyas; alimenta y eleva su alma, vive tranquilo; nada teme de los hombres» [En] una casa de campo a orillas del Éufrates. Allí no se entretenía en calcular cuántas pulgadas de agua corrían en un segundo bajo los arcos un puente, o en si caía una fracción cúbica más de agua en el mes del ratón que en el del cordero. No ideaba hacer seda con telarañas, ni porcelana con botellas rotas, sino que estudió sobre todo las propiedades de animales y plantas, y adquirió pronto una sagacidad que le descubría mil diferencias, allí donde los otros hombres no ven más que uniformidad".

Zadig no sería un ingeniero ni un artesano, sino un filósofo, o más propiamente, un naturalista, que a través del entrenamiento que proporciona una observación dedicada, le permitiría emprender la lectura de las sutiles diferencias que caracterizan los fenómenos del medio que nos rodea, con la finalidad de profundizar en la comprensión de sus causas. El objetivo, con base en el personaje de Voltaire, sería dominar la gramática del gran libro que ofrece

la naturaleza. Sin ningún problema la ciencia podía ser un ejercicio derivado de un ejercicio autodidacta, eso sí, pleno de rigor y disciplina.

La idea de ciencia que predominaba en estos primeros tiempos consistiría en la capacidad de generar un conocimiento que dieran cuenta de la armonía del mundo. Eso sí: aceptando la intervención del azar como un rasgo característico de los acontecimientos de la naturaleza, pero también en las interacciones humanas.

Es a partir de la física de Newton que el conocimiento científico establece por primera vez un equilibrio entre naturaleza y ciencia (Cowles: 2020) fraguando así la primera revolución científica, concepto según el cual cada nueva etapa del conocimiento genera una ruptura con el anterior: Kuhn acuña el término paradigma para expresar tanto lo que desaparece como lo que surge, y que eventualmente estará llamado a desaparecer. Hoy el término se ha vuelto sinónimo de contexto, de patrón, y de todo lo que se da por establecido.

Como consecuencia de los dos conceptos anteriores –revolución científica y paradigma–, Cowles añade el "espíritu del tiempo", esto es, que para el protagonista del avance de la ciencia se generará una "tensión esencial" consistente en tender un conjunto de compromisos intelectuales y manipulativos entre el modelo o régimen anterior y el que rompe con aquél.

Más importante aún es que una vez alejados de Zadig y la observación como medio de representar la armonía del mundo, en esta etapa surge el "método científico"; caracterizado por el énfasis no solo en el descubrimiento, el hallazgo o la invención, sino la invención del método mismo, donde "la verdadera novedad, lo que rompe con la antigua civilización" radica en que la mente se ha vuelto el instrumento del conocimiento y no solo el órgano donde se da respuesta a los enigmas que el ser humano encuentra.

Lejos del científico como generador de invenciones producto de su genio, el científico metódico gira alrededor de una comunidad compartida de discurso, acorde al paradigma y espíritu de su tiempo, lo que permite a la ciencia estabilizar a los individuos que se comprometen con ella. Sin método el quehacer científico no puede establecerse. En cambio, su existencia asegura que la ciencia se vuelva "simple, universal, natural y poderosa"; pero, y, sobre todo, neutral (Cowles: 2020, p. 19).

El enfoque en el método más que en los resultados, siguiendo a John Stuart Mill, significa que la revolución del conocimiento se ha instalado en la mente humana, convertida en instrumento del descubrimiento científico como medio para alcanzar su cabal perfección. El mecanismo de este cambio se encuentra en el concepto de hipótesis, objeto limítrofe entre la inducción y la deducción, siendo esta última la fuente de la que emanará la conjetura que guiará la indagación científica siempre y cuando se sustente en la lógica, la duda metódica y el rigor del pensamiento.

Como señala Schulz (2015: 113), el pensamiento humano ha generado modelos de cognición cuya finalidad es "reducir el error" mediante la perfilación de un "pensador ideal" cuyos principios pueden ser tres: el cartesiano basado en la duda metódica, el lógico formal, que a partir de premisas válidas extrae conclusiones que también lo son. Por último, el de la "diligencia debida" que presta atención a "pruebas y contrapruebas" objetivas para soslayar las ideas preconcebidas. El problema es que en la vida real al pensamiento "Le desagrada la duda radical, no depende de la lógica formal. No es diligente a la hora de acumular pruebas, menos aún contrapruebas, y no podría funcionar sin ideas preconcebidas.

Entrado el siglo XIX y una vez que se ha trascendido la fase naturalista, el pensamiento científico abandonará la perspectiva confirmatoria para volverse contraintuitivo, de modo que las leyes que formalizan sus hallazgos y descubrimientos que desafían el sentido común. De la generación espontánea pasando por el flogisto como causa del fuego a la teoría del éter -en la que se defendía la afirmación de Aristóteles de que la naturaleza le tendría horror al vacío- los experimentos de Michaelson y Morley condujeron a la aceptación de que la luz es al mismo tiempo partícula y onda que se esparce en forma longitudinal en el vacío, por lo que no requiere de un medio para diseminarse.

Volviendo a la generación espontánea como origen de la vida o la teoría del flogisto como causa del fuego en el siglo XVII, cuando el concepto de la combustión no se encontraba cabalmente desarrollado a nivel de la química, la ciencia no deja de desafiar el sentido común y la observación ingenua, a través de protocolos estrictos que dan forma metódica a la indagación y no se quedan con conocimiento adquirido. Las teorías científicas plantean la inversión del razonamiento, de modo que nuestros referentes convencionales, conformistas y de sentido común, ante todo se critican, revisan, transforman o superan

Finalmente, el conocimiento científico demanda de habilidad imaginativa. Unas veces apreciada y hasta sobrevalorada, de la imaginación suele desconfiarse por rebasar las fronteras de la comprensión humana. Pero sin una imaginación que guíe la curiosidad no puede haber la formulación de hipótesis y la generación de teorías. Tampoco la proyección de previsiones, algo fundamental para el rol predictivo y prospectivo que aporta la ciencia. Solo la imaginación permite emplear el pasado como llave para indagar en el futuro.

Los paradigmas producto de las revoluciones científicas entendidos como "lo que los miembros de una comunidad científica comparten" no solo están hechos de modelos y conceptos nuevos, sino también de creencias y valores que comparten los miembros de esa comunidad. De modo que luego de generar novedades, el paradigma dará paso a la formulación de convenciones, de las que pueden derivar sesgos cognitivos cuyas limitaciones de comprensión pueden frenar la expansión del propio conocimiento.[1]

III. La ciberseguridad y su operación con el Método Científico

Vivimos en un mundo hiperconectado, hoy día, los procesos sustantivos de las empresas e instituciones son soportados por las tecnologías de las información y comunicación; hoy si no estás conectado, si no inviertes en capacidad de procesamiento de información, si la "nube" no forma parte de tu arquitectura tecnológica, simplemente "no existes" como empresa o institución, ya que el diferenciador en términos de eficiencia y eficacia es la tecnología, y esto es una carrera constante, que está en marcha y que avecina grandes cambios tecnológicos que proveerán grandes beneficios en términos económicos y de bienestar, pero que también, dejaran al descubierto grandes vulnerabilidades; tecnologías de punta como el internet de las cosas, la tecnología 5G, *EdgeComputing*, criptomonedas, entre otras.

En el ámbito personal y profesional, cada ciudadano de nuestro país depende de una u otra forma de las tecnologías de la información y comunicación, computadoras personales, teléfonos inteligentes, redes sociales, correos electrónicos, banca en línea, plataformas comerciales, entra otras. En México, alrededor de 85 millones de personas están conectadas a internet, lo que vuelve a este escenario, en un ambiente paralelo al escenario real, actualmente es común referirse a ese escenario como "ciberespacio", que sin duda hoy día representa un recurso del estado mexicano, es un espacio, donde se genera economía, comunicación, conocimiento, recreación, impulsa la democracia y la libertad de expresión.

Este ambiente complejo de interconexión genera grandes volúmenes de información, el big data, que representa un gran reto para los Estados, para las empresas y para las instituciones, ya que genera un nuevo poder, el "ciberpoder", es decir a las instancias que logran procesar grandes volúmenes

[1] Hay una historia verdadera de dramatización muy exitosa, la plasmada en el filme "La verdad oculta", se aborda el diagnóstico de los exjugadores de fútbol americano, quienes ven reducida su esperanza de vida debido a la encefalopatía crónica traumática, derivada de malformaciones en el tejido cerebral ocasionadas por la exposición prolongada al impacto del golpeo en el fútbol americano en la región encefálica. Lo que interesa a nuestros propósitos es la descalificación que sufre el personaje que encarna al Dr. Bennet Omalu, médico legista que a pesar de haber reunido a nivel patológico pruebas de lesiones que explican la presencia del proceso degenerativo, se enfrenta al más influyente sector de la profesión médica que refuta sus resultados confiada en que las modernas técnicas de imagenología no revelan daño alguno a nivel cerebral.

de datos para generar información acorde a sus objetivos (inteligencia) tendrán una gran ventaja frente a sus competidores.

Desafortunadamente, las tecnologías de la información y comunicación permiten también realizar actividades delincuenciales, el ciberespacio genera diversas condiciones para que los delincuentes lleven a cabo sus operaciones con gran facilidad, desde fraudes, extorsiones, robo de información, espionaje, lavado de dinero, adoctrinamiento, trata de personas, pornografía infantil, afectaciones a infraestructuras críticas para desestabilizar la situación política y económica de los Estados, afectaciones a la soberanía mediante invasiones blandas o guerras psicológicas, es decir actores extranjeros que pueden alterar la percepción de los ciudadanos a través de campañas de información falsa vía redes sociales, afectación de los procesos democráticos, entre otros.

La Dirección General Científica, ha dedicado gran parte de su tiempo a entender el nuevo entorno operativo, el ciberespacio, cuáles son los alcances de la cibercriminalidad, la ciberseguridad, la integración de la variable tecnológica en el crimen convencional, la delincuencia organizada, la delincuencia organizada transnacional, los actores políticos, la propiedad intelectual y la competencia en términos comerciales.

En resumen, podemos aseverar que existen dos enfoques, uno, las actividades delincuenciales que afectan el estado de la información y las tecnologías mismas, tales como los ataques de *ransomware, malware*, y ataques de denegación de servicio, entre otros; dos, las actividades delincuenciales que se potencializan con el uso de la tecnología, tales como, fraude, extorsión, comercio ilícito, trata de personas, pornografía infantil, entre otros.

Son tres los principios que rigen la seguridad de la información: el primero es su objeto fundamental mantener la confidencialidad de la información generada por un usuario o compartida por él solo a personas autorizadas; en segundo es la integridad, que supone que la información es auténtica y circula sin riesgo de errores o corrupción; el tercero es el principio de disponibilidad: la información debe estar disponible para el o los usuarios en todo momento que la necesiten, siguiendo los protocolos necesarios.

Existen al menos seis niveles de ataques que preocupan a la ciberseguridad (figura 1): hacker amateur y actores no maliciosos; 2) grupos criminales y hacktivistas, 3 y 4) crimen organizado y cibermercenarios. 5) y 6) naciones atacantes. Cada nivel está caracterizado por las herramientas que usan y un modus operandi característico. Es un postulado común que el 80 por ciento de los ataques y ciberdelitos ocurren por colaboración inconsciente de la víctima, de modo que pueden evitarse con medidas básicas de atención, lo que demanda un esfuerzo consistente de prevención, concientización y reglas de convivencia conocidas como civismo digital.

En clave del método científico y el avance de la ciencia, expresado en términos de ruptura con una condición, interpretación o estado de cosas que le ha precedido, se puede decir que la ciberseguridad asociada al ciberespacio como ámbito de la convivencia y la interacción basada en la conexión en red configura una revolución científica que se verifica en el ámbito tecnológico, a través de la computadora de escritorio, portátil, las tabletas y el teléfono inteligente, teniendo como vía de interacción el Internet en general y las redes sociales en particular.

Por primera vez los datos han dejado de pertenecer a quienes los generan; para su estudio, control y aprovechamiento se les incorpora a bases de datos de actores geopolíticos por derecho propio, las grandes compañías que tienen el monopolio de los datos a nivel mundial. Los datos son considerados por su relevancia en la economía como el nuevo petróleo en la era de la información, son vital para todo ámbito de competencia, por ello, la ciberdelincuencia genera métodos sofisticados para afectar el estado de la seguridad de la información con diversos fines, monetizando sus actividades ilícitas.

La ciberdelincuencia es un fenómeno, que hoy día representan un reto para la ciencia, ha crecido en herramientas, conocimiento y capacidad financiera, representa uno de los más importantes riesgos para las naciones.

En este tramo de aprendizaje de la Dirección General Científica, con más de 10 años de experiencia en el ámbito de la ciencia aplicada, tecnología y ciberseguridad, le ha permitido analizar la evolución de la cibercriminalidad, a través del estudio de hechos históricos, el comportamiento actual y el análisis prospectivo, que ha permitido emprender acciones que impulsan la construcción de capacidades para que México tenga las herramientas necesarias para prevenir e investigar estas conductas ilícitas.

Para dimensionar el riesgo que representa la ciberdelincuencia, tomaremos como ejemplo la evolución de los ataques del tipo ***ransomware,*** mejor conocidos como secuestro de archivos, que generan mecanismos de extorsión; para entender su evolución y su impacto a la seguridad pública y nacional, es imprescindible entender su anatomía, desde el aspecto técnico, pasando por el modelo de negocio criminal y cuáles son los principales actores que componen hoy día el ecosistema del ransomware y cuáles son las acciones que se están realizando a nivel internacional y nacional, cuáles serían las afectaciones futuras si las condiciones de los grupos criminales dedicados al ***ransomware*** y en general a la ciberdelincuencia siguen en ascenso.

Iniciemos desde lo más básico, ¿qué es el ***ransomware***?, es un tipo de ***malware***, un código malicioso desarrollado por expertos en desarrollo de software y expertos en criptografía, como en todos los casos, hay delincuentes de diferente perfil, por supuesto que también los hay aprendices que cometen muchos errores, que dentro del mismo código del ***ransomware*** ponen la llave de

descifrado, pero los hay también con capacidades sofisticadas, el objetivo más elemental de este software malicioso es identificar archivos en la computadora de la víctima para después cifrarlos, y solicitar un pago por el rescate de esos archivos, es decir, enviar la llave de descifrado para regresar los archivos en el estado normal en el que se encontraban, por esa razón se le conoce como secuestro de archivos.

Veamos ahora, ¿desde cuándo existe el *ransomware*?, se tiene registros que el primer *ransomware* surgió en 1989, es decir poco más de tres décadas, se trató de un código malicioso tipo troyano que se le conocía como AIDS o PC *cyborg* que modificaba el archivo autoexec.bat, un archivo de procesamiento por lotes que se ejecutaba al iniciar la computadora, después de 90 sesiones, el código malicioso cifraba los nombres de los archivos volviendo inutilizable el sistema, después pedía un pago de 189 dólares como supuesto pago de renovación de licencia.

Este *ransomware* se distribuía en disquetes con información que hablaba del SIDA, el pago se debía hacer en una cuenta que radicaba en Panamá, casi 20 años después vimos al virus del policía que bloqueaba las computadoras infectadas y solicitaba el pago fraudulento de una multa por que el usuario supuestamente había estado viendo contenido pornográfico. 8 años después vimos el ataque mundial de *WannaCry* que explotaba una vulnerabilidad en los sistemas *Windows* conocida como eternal blue, que utiliza un *exploit* del mismo nombre, aprovechó una vulnerabilidad en el protocolo SMB para compartir archivos e impresoras, recientemente tenemos otros *ransomware* más sofisticados como *Ne_lim* que pone al descubierto todas las capacidades que han desarrollado los delincuentes informáticos y que hoy día ha llamado la atención de las autoridades de seguridad nacional en todo el mundo.

Quien diría que un "inofensivo" ataque cibernético realizado hace más de tres décadas, lograba defraudar a los usuarios por un monto de 189 dólares por medio del engaño. 33 años después esa misma técnica, ese mismo legado delincuencial ha puesto en jaque a las principales potencias en el mundo, generando afectaciones severas en servicios esenciales como el de salud, financiero y energético, extorsionando a empresas e instituciones con sumas exorbitantes, ejemplo de ello, es la suma que reportó las autoridades de Estados Unidos del primer trimestre del año 2021, que oscila en los 600 millones de dólares, que se han pagado a los ciberdelincuentes producto de los ataques de ransomware, además de las afectaciones económicas ocasionadas por paralizar los procesos sustantivos automatizados por la tecnología. Algunos de las afectaciones más conocidas son: ataque a Colonial Pipeline que paralizó el suministro de combustible al sector de aviación en el noreste y gran parte del sur de Estados Unidos y diversos efectos colaterales, y la afectación del sistema de salud en el Reino Unido, entre otros; en México se han registrado diversos

ataques de *ransomware*, los importantes, el que afectó los sistemas informáticos de PEMEX, y el de la lotería Nacional, entre otros.

Es importante conocer la historia, para entender la situación actual y poder hacer prospectiva, que nos espera en los próximos años, observando cómo han evolucionado los criminales, como han explotado esta línea de ataque y de doble extorsión para generar mayores daños y tener elementos más contundentes para obligar a las empresas e instituciones a pagar cuantiosas sumas de dinero, afectando seriamente las infraestructuras críticas. Pero lo más grave el empoderamiento serio de los criminales, que hoy día tienen el poder económico necesario para realizar ataques de alto impacto, amenazas persistentes avanzadas y que además son patrocinados en muchos casos por Estados.

Veamos cuales son los vectores de ataque más utilizados, el hacker crea exploits, un exploit es un software desarrollado para explotar vulnerabilidades específicas, hay un mercado muy importante de este tipo de software que incluso presenta consolas de interacción con el usuario para hacer más fácil su uso, los exploits se envían por correo electrónico como archivos adjuntos, sitios web comprometidos, sitios oficiales, que han sido comprometidos y utilizan un ataque que se le conoce como drive by download, que refiere a descarga involuntaria del usuario, o lo más sencillo utilizar sitios web apócrifos para engañar al usuario a interactuar con el sitio y descargar código malicioso, o bien por redes sociales enviando enlaces engañosos para que los usuarios le den clic y descarguen el código del *exploit*.

También los *exploits* puede atacar directamente a servidores o computadoras vulnerables expuestos en internet.

En el caso de interacción con los usuarios los usuarios son atraídos para ejecutar los *exploits* a través de ingeniería social, una vez instalados los *exploits* en los sistemas vulnerables, permiten después ser el puente para instalar todo tipo de *malware* en este caso *ransomware* o bien para poder controlar el sistema infectado remotamente para diversos fines.

Ahora vamos a hablar de la evolución del modelo de negocio criminal, esto es relevante para saber por dónde se están moviendo las amenazas del tipo *ransomware* y en general las amenazas cibernéticas que cada vez más buscan monetizar rápidamente sus ganancias, ahora se ha configurado una trama interesante y muy dañina que potencializa las operaciones de los cibercriminales, requiere de atención coordinada debido a que están creciendo en capacidades, por ello urge más cooperación nacional e internacional, mejores marcos jurídicos, profesionalización de las diversas autoridades para prevenir y combatir este tipo de delincuentes, de lo contrario los niveles de extorsión y daños puedan derivar en afectaciones físicas más allá de afectaciones económicas.

En el 2010 los delincuentes solicitaban el rescate a través de un servicio de SMS premium, utilizaban los servicios que había a disposición para extender las actividades de monetización de las actividades ilícitas. Lo obtenido se llevaba a un sistema de billeteras electrónicas tipo *PayPal*, lo que les permitía enviar los recursos a otros países, hasta que esto se empezó a regular. Las ganancias ilícitas en ese momento en realidad eran moderadas al igual que el número de víctimas.

A partir de 2013 la misma delincuencia empezó a utilizar el *bitcoin* como mecanismo de pago para los rescates, obteniendo cantidades moderadas por ataque, pero un número de víctimas a escala global. Asimismo, los delincuentes diseñaron un programa de afiliación denominado *ransomware* as a service, un modelo de colaboración basado en la división y especialización del trabajo en el que unos desarrollaban el código malicioso, otros los *exploits*, otros más los sistemas de reconocimiento dentro de la red, y así hasta la negociación del rescate.

A partir de 2016, los delincuentes, además del *bitcoin*, empezaron a utilizar bases de datos para categorizar víctimas aprovechando el big data para procesamiento de información, mercados precategorizados de credenciales y accesos, y un enfoque colaborativo de monetización para realizar incluso doble o triple extorsión, logrando un impacto global, con objetivos específicos y en masa.

En la actualidad los delincuentes cibernéticos cuentan con suficientes recursos técnicos y económicos para adquirir vulnerabilidades día 0 y hacerles daño a objetivos específicos de alto perfil.

De acuerdo con este modelo, para entender la anatomía del *ransomware* hay que ver a los principales actores del modelo criminal; hoy día hay cinco principales actores que se describen a continuación:

1. Intrusos: roban y venden accesos e información confidencial.
2. Comercializadores: fabrican el *ransomware* y lo venden. Generan modelos de colaboración *ransomware as a service* y ocasionalmente llegan a operar solos. Los *Maze y Netwalker* son los primeros grupos criminales que desarrollaron los mecanismos de comercialización que dividen el trabajo y las ganancias. El 30 por ciento de las ganancias las obtienen los comercializadores, pero los que tienen a la víctima cautiva, los intrusos, se llevan el 70 por ciento de las ganancias. El ataque de Avalon que permitió a las víctimas recuperar sus recursos seguramente obedece a que en el mecanismo de colaboración algo salió mal entre ellos, lo que permitió a las víctimas recuperar la información. De modo que este modelo de negocio ilícito no está exento de contradicciones.

3. Secuestradores: hacen el reconocimiento de la red, identifican los segmentos y cómo se pueden mover de forma lateral. Las redes se dividen en subredes y el reconocimiento consiste en verificar cuantos segmentos tiene la red para ganar privilegios de acceso. Para ello compran costosas licencias de software de ciberseguridad, o bien vulneran bases de datos de empresas que se dedican a producir componentes de ciberseguridad.

   Una vez obtenidos los privilegios los delincuentes van identificando la información que es sustancial para la víctima. No se van a distraer en un archivo de *Word,* sino que buscarán elevar la fuerza de la extorsión, esta información la van a robar en primer término y luego a cifrar.

4. Grupo de extorsionadores: se contrata para intimidar a la víctima. Ellos han hecho un trabajo de inteligencia indagando el sector en que se desenvuelve la empresa o institución objetivo, su situación contable y administrativa, sus procesos críticos, todo lo que les permitirá hacer la labor de intimidación más fuerte. Por ejemplo, si la empresa cotiza en bolsa se expone a sanciones del mercado por no acreditar el buen manejo de la información. De ahí es que resuelven estimar el rescate requerido y exigirlo.

5. Mezcladores o *mixers*: son los encargados de ocultar las operaciones de criptoactivos ante las autoridades, sobre todo en la conversión de dinero electrónico a dinero fiduciario, impidiendo saber a donde llegó el recurso. En esa especie de licuadora virtual se ponen muchas transacciones de criptoactivos, incluyendo las que se quieren ocultar, se mezclan o entrelazan para confundir las criptooperaciones, de tal forma que dificulta las investigaciones de las policías.

Lejos ha quedado la imagen del ataque cibernético como expresión del joven idealista que ha desarrollado la habilidad suficiente para vulnerar un sistema, normalmente perteneciente a una empresa o institución, y que actúa como si del ejercicio de una libertad o de un acto de rebeldía contra las élites dominantes se tratara, en principio carente de ideología, pero dotado de un herramental cibernético artesanal y poderoso. No es que la imagen del *hacker* como un inconforme que se muestra desafiante ante el orden haya desaparecido, solo que el *hackeo* como acto de justicia ciudadana hace tiempo que ha pasado a la historia para convertirse en una forma delictiva más. (Baricco: 2019)

En cambio, el saldo de los últimos treinta años arroja el empoderamiento exagerado de la delincuencia a nivel mundial; por lo mismo, sorprende, por tanto que desde el inicio de la computación personal no se haya puesto el suficiente interés en la concientización del usuario acerca de la ciberseguridad, un modelo de negocio que no ha dejado de adaptarse al cambio tecnológico, si no es que a dirigirlo, como ocurre con el fenómeno de las criptomonedas, y en todo caso, marcando pautas y señalando tendencias.

El siguiente paso puede ser, nada descartable, que, en su búsqueda de formas más dañinas para presionar a sus víctimas, los atacantes desarrollen la capacidad para generar afectaciones físicas de envergadura que puedan derivar en desastres y pérdida de vidas.[1]

La ciberseguridad en general comprende dos grandes ámbitos: la protección de infraestructuras críticas y el combate al delito cibernético. En ellos se verifica el método científico en el sentido abordado aquí: se observa una problemática ante la cual se debe actuar; se formulan hipótesis en forma colegiada y coordinada en la mayor parte de los casos; se observa la dinámica del cambio y se actúa en un sentido de prevención y protección.

Un área de relevancia son los CERT, instancias que fortalece la seguridad cibernética de empresas, instituciones e infraestructuras, cumplen una función vital de alerta para afrontar requerimientos de seguridad de la información. La Dirección General Científica contiene un CERT coordinador para prevenir, contener, alertar y responder. Periódicamente generamos un análisis de las diferentes amenazas, se mantiene una colaboración internacional que nutre los insumos de información necesarios para la generación de alertas tempranas que son enviadas a los administradores de sistemas para la prevención y contención de ataques cibernéticos.

La colaboración internacional permite realizar investigaciones en apego al marco legal, bajo mando y conducción del ministerio público, que reditúa en el ejercicio de impartición de justicia en casos complejos donde la tecnología es usada como medio o como fin para la comisión de delitos. Estas acciones de impacto a la seguridad con visión multidimensional llevan la rúbrica de la Guardia Nacional. Incluso, hay casos en los que por su tipo no se requiere que la víctima presente denuncia, el personal mismo de la Guardia Nacional se constituye ante la autoridad ministerial a denunciar con una intensión proactiva y en favor de las víctimas para iniciar una carpeta de investigación, como en los casos de pornografía infantil, se apoya a la víctima, se colabora con el ministerio público e incluso se comparece ante el juez. La idea es lograr la aplicación severa de la ley.

[1] Como se sugiere en la producción francesa "Caja Negra" (2020) de Yan Gozlan, thriller psicológico en el que la indagación de un accidente aéreo termina explicándose más por la intrusión informática que por el error humano o la acción terrorista

IV. El nuevo espíritu del tiempo

El discurso cibernético ha avanzado posiciones para una interpretación de la mente humana que se fueron generalizando y popularizando en lo que se denomina la teoría computacional del cerebro, según el cual las operaciones bioeléctricas a nivel neurológico resultarían parangonables a los estímulos que hacen funcionar a una computadora, al menos a nivel del cálculo y la memoria, en la condición actual ha habido una reafirmación de esa creencia, cuya seducción ha sido difícil de superar, al grado incluso de que pueden ser los algoritmos de las computadoras los que, habiendo registrado la información relativa a las prácticas y hábitos de las personas, e incorporando mecanismos de ingeniería social, han logrado "programar" las percepciones y reacciones de la gente; y así como un algoritmo puede programar la prestación de un servicio o la elección de una ruta óptima para transportarse, no ha faltado quien se incline hacia una especie de "gobierno del algoritmo" como solución a temas como la movilidad y el remedio a la contaminación ambiental.

Sin embargo, los avances en neurociencias han avanzado de manera notable en la comprensión de los fenómenos cognitivos y emocionales, así como su interacción, para mejorar la comprensión de los errores humanos que rodean las fallas cibernéticas. En otras palabras, la gran mayoría de las personas considera que la protección de la información es una tarea demasiado lenta y farragosa como para prestarle atención. Muchas cultivan el hábito de mantener saturado su correo electrónico porque les sirve como archivo histórico. El caso más reciente a finales de 2021 ha sido la comprobación de que también la mensajería *WhatsApp*, considerada como el último reducto de la privacidad en red, podía ser también intervenida por la delincuencia. El revuelo que ha levantado esta situación solo refleja el olvido de que también *WhatsApp* es una red social y que debe ser configurado el nivel de seguridad por parte del usuario, principalmente la verificación en dos pasos.

Un resultado hoy corriente de la ciencia de datos se verifica en la ingeniería social. En la era de los metadatos su conocimiento puede condicionar las percepciones de conglomerados de personas. Los datos hacen factible saber inclusive a nivel del inconsciente las prácticas más habituales y los valores que éstas traducen, ello ha dado paso a estrategias y maniobras de ingeniería social que gracias a esos registros consiguen en muchos casos incidir y orientar conductas irracionales a partir de la explotación de las emociones más primarias. La escasa o falsa conciencia de nuestra relación con las redes se traduce así en prácticas nocivas en el largo plazo, lo que acentúa las vulnerabilidades de los sistemas, procesos y patrimonio.

Para las finalidades de este apartado lo que interesa es que la ciencia de datos ha configurado así una revolución científica y un paradigma asociado a ella, el concepto de ciberespacio y la necesidad de la ciberseguridad. Hoy como nunca, la ocasión hace al ladrón, ya que la posesión de determinado conocimiento técnico puede condicionar la posibilidad de incurrir en acciones delictivas como el robo de datos e identidad. De ahí que para vérselas con el paradigma actual sean indispensables la concientización,la educación cívica digital y la actualización en los riesgos cibernéticos a manos de divulgadores científicos acreditados. Esto es una necesidad apremiante.

No solo ello, dentro de esta revolución científica se plantea otra más:¿puede el método científico ser influido por el estado actual de la ciencia de datos? Al parecer, sí: en un artículo reciente (Tingley: 2021) se observa que la aplicación de la ciencia de datos a dominios que forman parte de la vida cotidiana puede arrojar resultados sorprendentes y cuestionar nuestra idea de la ciencia. En una renombrada revista científica se divulgó el hallazgo de que el café puede ser un buen aporte a la salud cardiovascular, contrario a la versión de que puede estar asociado a la hipertensión, así como a determinadas formas de cáncer. Al parecer la mala fama del café obedece al sesgo que impone el que su consumo es también muy socorrido por personas que fuman. lo que habría influido en la mala valoración de la bebida.

Un resultado así de sorprendente dice la autora, no fue producto de la aplicación del método científico a partir de la formulación de hipótesis o teoría alguna. Bueno: tampoco las observaciones que condujeron a la teoría de la evolución venían precedidas por una hipótesis concreta, sólo que mientras la teoría de la evolución se construyó sobre una dedicada colección de observaciones, el conocimiento actual es el resultado de calcular millones de datos sobre el consumo del café, a los que se ha añadido información sobre el metabolismo humano y otras variables que hubiera sido imposible abordar sin contar con las capacidades de procesamiento actuales. El mundo "datificado" de hoy produce información útil no solo para la ingeniería social, sino también para la comprensión de fenómenos encuadrados en la experiencia cotidiana.

En el paradigma clásico del método científico el carácter errático del comportamiento humano, la fuerza de hábitos condicionantes de la conducta, y la dificultad de medir los comportamientos habituales a partir de la experiencia empírica configuraban variables que solían desafiar el estudio formal de nuestras prácticas más cotidianas, al dificultar la formalización de hipótesis basadas en su consistencia lógica y coherencia interna. Ese problema metódico parece haber dejado su lugar a la preocupación por la calidad de los datos utilizados y la consistencia del algoritmo con el que se procede a ordenarlos y correlacionarlos.

Por otra parte, el hallazgo de que el café puede contribuir a la salud cardiovascular no era el propósito de la investigación, sino identificar el grado en el que los hábitos –incluso autodestructivos– tienen en la salud cardíaca en una población como la estadounidense, donde una de cada cinco personas desarrolla alguna enfermedad cardiovascular, mientras que la mitad de la población bebe café a diario.

El asunto es que el desconocimiento general que asocie los componentes de la dieta humana con el desarrollo de fallas cardiacas y otras enfermedades degenerativas, con el auxilio de la inteligencia artificial a nivel de "*machine learning*" permitió determinar los beneficios potenciales de abordar las complejas interrelaciones de modificar la ingesta de algunos alimentos, dando con el hecho de que tanto la evaluación de la salud cardiovascular en su conjunto como el control de la arterioesclerosis podrían verse beneficiadas por el consumo de café, aunque falta por saber el nivel óptimo de ingesta de la bebida.

El caso es que alcanzar tal resultado no requirió formular una hipótesis sino del procesamiento libre de un conjunto de datos disponible; por lo que ahora corresponde evaluar determinados factores de riesgo, a nivel de la clínica, lo que podría llevar a recomendar el consumo de café para atenuarlos, generando un estilo de vida determinado. Todo ello a partir de determinar la relación de causalidad que se establezca entre el consumo de café y la salud cardiovascular.

De modo que la ciencia de datos y su cuidado como activo de la sociedad, representa una gran oportunidad para el trabajo en materia de salud y política social en general. Sin embargo, de acuerdo con el Foro Económico Mundial, en el ciberespacio se puede generar múltiples amenazas, lo que requiere hacer músculo y atender las áreas de oportunidad, capacitación y certificación de por medio; ante todo, coordinación. La figura 2 identifica riesgos globales en cinco ámbitos: crisis climáticas, sistemas de salud bajo tensión, un mundo inestable, la estabilidad económica la cohesión social –cierto: la economía devuelta al funcionamiento de la sociedad y no solo de las finanzas– y lo que es materia del presente trabajo: la fragmentación digital.

La fragmentación digital está compuesta de once variables: economía y sociedad digital, gobernanza de la Internet, cuarta revolución industrial, medios y entretenimiento, ciberseguridad, comunicación digital, Internet de las cosas, electrónica, multinacionales emergentes, 5G, y tecnologías de la información. La tecnología ha dejado de ser neutra y se erige en un actor crítico en la estabilidad y la gobernanza mundial. Lo anterior implica la formación de técnicos y especialistas, pero también el desarrollo de ciencia original para detectar y conjurar riesgos para el gobierno, las instituciones, la industria y la economía en general.

V. Ciencia Prospectiva

En la medida que la ciencia de datos actualiza los postulados del método científico, la participación de la ciencia en la prevención y el combate al delito crece en importancia. no es la primera vez que se intenta el estudio científico del delito y sus fuentes. Sin embargo, sí puede serlo para perfeccionar las tareas de prevención, investigación y combate al fenómeno delictivo.

De hecho, nada impide considerar que el desarrollo de capacidades técnico-científicas con el aporte de la ciencia de datos pueda beneficiar con su aporte el espíritu del tiempo actual. La seguridad es una cuestión muy seria, que no deja de plantear desafíos. Por tanto, el abordaje con un enfoque de riesgos se vuelve crítico en la labor de mantener la viabilidad de las sociedades.

Conforme ha evolucionado la tecnología también han evolucionado los métodos para la comisión del delito; de acuerdo con numerosas proyecciones, en poco tiempo la problemática de la ciberseguridad y el ciberdelito abarcará el espectro de lo punible en una proporción dominante. Se requiere por tanto contar con la producción de ciencia para la función policial.

Ya nos hemos referido a la ciencia de datos; ésta, junto con la inteligencia artificial, seguramente irá intensificando los desafíos, al igual que las oportunidades, para devolver la tranquilidad a la ciudadanía. Ciertamente se requieren una visión amplia de la gobernanza, y un espíritu proactivo, anticipatorio e integral para desarrollar estrategias y alcanzar los resultados que demanda el avance de la sociedad.

En los más diversos medios ha proliferado la idea de profundizar en el alcance prospectivo de la elaboración científica, como medio para reducir la incertidumbre reinante, desviar el curso de las tendencias y generar soluciones de política eficaces. Los modelos de gobernanza convencionales están exigiendo el desarrollo de habilidades que penetren en la conjetura de lo que puede ocurrir.

Con base en el modelo prospectivo desarrollado por la Guardia Nacional, el enfoque prospectivo balancea el diagnóstico de la situación presente con la prevención de riesgos y amenazas, al tiempo de proyectar situaciones de baja probabilidad y alto impacto. Los escenarios prospectivos suelen ser de dos tipos: exploratorios, esto es, evaluativos del rumbo futuro, y normativos, esto es, que dicten hacia donde se tiene que marchar para orientar una tendencia o de plano romperla. La conjetura escenarial se basa en el principio prospectivo de posibilitar un futuro o estado de cosas.

En situaciones como la actual, en la que debemos prepararnos para un mundo que seguramente extrañará la normalidad como la conocíamos; que no tolerará muchos de los factores que han saturado la economía y el ambiente, y que nos demandará ser muy cuidadoso de la herencia que habremos de dejar a las generaciones que nos sucederán.

Fuentes de Consulta

Baricco, Alessandro (2019), The Game, Anagrama, México.

Eco, Umberto (1992), Los Límites de la interpretación, Lumen, Barcelona, Consultado en: http: //mastor.cl/blog/wpcontent/uploads/2011 /12/Eco_Umberto - Los_limites_de_la_interpretacion.pdf

Cowles, Henry (2020) The Scientific Method. An evolution of Thinking from Darwin to Dewey. Harvard University Press. Cambridge

Gozlan, Yann, (2020), "Caja Negra", Duración: 131 min; Producción: Francia, 2021 ; Reparto: Pierre Niney, Lou de Laâge, André Dussollier; Guion: Yann Gozlan, Niney es experto analista capaz de escuchar los sonidos que nadie oye en las grabaciones de una caja negra, lo que le permite discernir los motivos que originan un accidente aéreo, al parecer ligado al internet de las cosas. • Kostopoulos, George (2017), Cyberspace and Cybersecurity, Routledge, London.
https://books.google.com.mx/books?hl=es&lr=&id=gQA7DwAAQBAJ&oi=fnd&pg=PT20&dq=cybersecurity+and+cyberspace&ots=mIFAm0ANbz&sig=JSuXbWyPVEtQQ9Trw6Jwfkj8#v=onepage&q=cybersecurity%20and%20cyberspace&f=false

Kuhn, Thomas S. (1979: 2011) La estructura de las revoluciones científicas, Fondo de Cultura Económica.

Landesman, Peter (2015) "La verdad oculta". Película interpretada por Will Smith en el papel del Dr. Bennet Omalu, narra la historia de los hallazgos de un médico legista relacionados con la encefalopatía crónica traumática, cuyas demostraciones de microscopía óptima se confrontan al paradigma de la imagenología electrónica avanzada, y a un sector de la ciencia médica que rechaza sus conclusiones defendiendo de paso la práctica y la propaganda relacionada con ese deporte. Otra figura que se exalta en el filme es la del científico-activista y su indeclinable compromiso con la verdad, cuya búsqueda lleva al personaje a desafiar a poderosas comunidades de la profesión e intereses creados.

Schulz, Kathryn (2015) En defensa del error. Un ensayo sobre el arte de equivocarse, Siruela, Madrid.

Stevens, LauraM., Erik Linstead, Jennifer L. Hall, and David P. Kao (2021) , "Association Between Coffee Intake and Incident Heart Failure Risk: A Machine Learning Analysis of the FHS, the ARIC Study, and the CHS", en Circulation: Heart Failure, Vol. 14, no. 2; consultado en:
https://www.ahajournals.org/doi/10.1161/CIRCHEARTFAILURE.119.006799. • Tingley, Kim (2021), "Is Coffee Good for Us? Maybe Machine Learning Can Help Figure It Out", en; The New York Times Magazine, 24 de marzo de 2021 , consultado en: https://www.nytimes.com/2021/03/24/magazine/coffeeheartmachine - learning.html.

World Economic Forum (2020), Global Risks Report, consultado en:
https://www.weforum.org/global -risks

CAPÍTULO IV
POLÍTICA CRIMINAL Y CIBERSEGURIDAD

POLÍTICA CRIMINAL EN LA CIBERSEGURIDAD
RETOS Y PERSPECTIVAS

Dr. Alejandro Carlos Espinosa[1]

Sumario: I. Introducción. II. Política Criminal. III. Ciberseguridad. IV. Política Criminal y Ciberseguridad en México. V. Posibles escenarios y respuestas institucionales frente a los ciberdelitos. VI. Conclusiones.

I. Introducción

En este artículo se analiza a la Política Criminal y a la Ciberseguridad, se toman conceptos importantes de dichas materias, así como algunos ciberdelitos; se aborda el Caso Olimpia y la penalización de ciberdelitos.

Se señalan las diferencias entre política criminal y criminológica y se hace un análisis del estado de cosas que priva frente a esta novedosa expresión delictiva generalizada en todos los ámbitos de la sociedad que impacta en el perfil, *modus operandi* y el surgimiento de *novos* delitos con escenarios de realización oculta que exigen una respuesta del Estado.

La necesidad de atender fenómenos transgresores del orden de los que incluso algunos ni siquiera han nacido como tipos penales, esto es, nos encontramos ante la ausencia de tipo en la dogmática y ley penal, o bien frente a casos de atipicidad ante la vertiginosa evolución de los tipos penales.

Por ello, desarrollar estudios sobre política criminal y ciberseguridad en México, es una exigencia que invita al desarrollo de capacidades institucionales, del fortalecimiento y en algunos casos creación de ciberpolicías y ciberinvestigaciones profesionales.

II. Política Criminal

El diccionario de la Real Academia de la Lengua Española señala que política o políticas son las "orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado"[2] y por criminal "perteneciente o relativo al crimen"; "que implica o conlleva crimen".[3]

---

[1] Doctor en Política Criminal, Director de Investigación Académica de la Guardia Nacional, Miembro del Sistema Nacional de Investigadores Nivel-1, Profesor concursado en las materias Derecho Militar y Derechos Humanos de la Facultad de Derecho de la UNAM, miembro de número de la Academia Mexicana de Criminología, ex Juez Ad hoc de la Corte Interamericana de Derechos Humanos, autor de los libros Derecho Militar Mexicano, Derecho Procesal Penal Militar y coautor de la obra Jurisdicción Militar, Estudio Latinoamericano de los Modelos de Justicia y Coordinador del libro Anticorrupción en la Seguridad Pública publicado por la Guardia Nacional.

[2] Cf r. Diccionario de la Real Academia de la Lengua Española. Política. 2021. https://dle.rae.es/pol%C3%ADtico#Ta2HMYR

[3] Cf r. Diccionario de la Real Academia de la Lengua Española. Criminal. 2021 https://dle.rae.es/criminal?m=form

[4] CALDERON CEREZO, Angel y CHOCLÁN, José Antonio. Derecho penal tomo I, 2ª edición, Editorial Bosch, 2011. p.33. España.

De lo anterior, se señala que la política criminal tiene como sujetos de acción a los gobernados, motivo de la reflexión Político-Criminológica, tanto del Estado como en relación con las personas en sus diferentes condiciones y roles, esto con base en la ideología expresada en planes y programas de la gestión, con el propósito de lograr niveles aceptables de seguridad pública y permitir la consecución de los objetivos nacionales, así como la preservación y desarrollo de las instituciones del Estado.

Por su parte, Calderón Cerezo y Choclán Montalvo respecto de la Política Criminal señalan que:[4]

> *"La Política Criminal se ocupa de la reforma del Derecho Penal vigente (del derecho como debería ser). A diferencia de la dogmática que tiene por objeto la interpretación de un texto previamente dado, la Política Criminal se preocupa de desarrollar nuevas concepciones de los fines jurídicos penales. Esta ciencia asume las conclusiones de la dogmática jurídico penal y se sirve de los logros empíricos de la Criminología. Por ello, la Política Criminal actúa de puente entre la Dogmática y la Criminología".*

Otra lectura igualmente importante es la del Observatorio de Política Criminal de Colombia que, en el 2015, adoptó, tras importantes trabajos y análisis, la definición dada por la Corte Constitucional de Colombia en la sentencia C-646 de 2001, de la siguiente manera:[5]

> *"La política criminal es el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción".*

Para Eugenio Raúl Zaffaroni: [6]

> *"Si bien se mantiene un concepto tradicional, conforme al cual la política criminal es un discurso legitimante del poder punitivo, lo cierto es que incluso en ese empleo la expresión no puede ocultar su tensión interna, porque la política criminal no puede eliminar totalmente su potencial crítico. Si bien existen discursos político criminales legitimantes, que aceptan como verdades meras a firmaciones apriorísticas (como las que encierra cualquier teoría positiva de la pena), todo cambia cuando, partiendo de datos de la realidad, se construye como una valoración general del modo de encarar desde el poder la conflictividad criminalizada y, por ello, de ejercer el poder punitivo. Desde esta perspectiva, su función tampoco se limita al legislador, pues el juez también toma decisiones*

[5] Cfr. Corte Constitucional de Colombia en la sentencia C-646 de 2001. https://www.corteconstitucional.gov.co/relatoria/2001/C-646-01.htm

políticas (porque expresa una decisión de poder estatal) y, por ende, el dogmático no puede quedar al margen de estas valoraciones".

Las formas en que se expresa la política criminal son diversas y suelen ser desde simples hasta complejas, por ejemplo, la transformación de los espacios a través de su recuperación para la recreación y el deporte hasta de orden legislativo que implica profundas transformaciones a la norma sustantiva y adjetiva penal. Unas y otras generan cambios dirigidos a la convivencia social que con la llegada de la tecnología se hizo complejo y aparejó retos y cambios para lograr el control y el deseado orden en las relaciones de las personas sin afectar derechos.

Igualmente puede ser económica a través de modelos de desarrollo que estimula una determinada actuación de la población o bien a través de multas y sanciones económicas, así como estrictos procesos de reparación del daño que condicionen soluciones alternas al conflicto penal para reconstruir el tejido social.

Por lo que hace a las administrativas tiene que ver con la administración de las prisiones, la incorporación de la tecnología, el razonamiento probatorio o los candados para obtener beneficios penales en el caso de incurrir en conductas señaladas como delito, para de esta manera lograr el adecuado acondicionamiento institucional.

De acuerdo con Armando Juárez Bribiesca[7]:

"las decisiones político-criminales comprenden todas las áreas de las políticas públicas vinculadas con el fenómeno de la criminalidad. Debiendo el Estado cumplir con su deber de prevenir la comisión de los delitos, no solo a través del diseño de implementación de un Sistema Penal eficiente, sino que, además, mediante la adopción de políticas sociales orientadas a incluir positivamente en los diferentes factores que convergen en la producción de la criminalidad".

La visión de política criminal como tradicionalmente se le conoce, se ha transformando en una lectura humanista y de prevención del delito, el jurista Aleman Claus Roxin en su obra Política Criminal y Sistema del Derecho Penal, referente a que las políticas públicas en materia de Seguridad Ciudadana, "siempre deben partir sobre la base de la prevención del delito, como primer paso a seguir, y no a la represión o reinserción, como segundo y tercer paso respectivamente, de lo contrario, se trasgrede la lógica de lo más favorable".

---

[6] Zaffaroni, Eugenio Raul. Derecho penal, Editorial Porrua, p. 148. 2001. Mexicotencia C -646 de 2001. ttps://www.corteconstitucional.gov.co/relatoria/2001/C -646-01 .htm

El paso está dado por importantes sectores del humanismo en el Derecho Penal y la función social al iniciar el cambio de una política criminal centrada en el endurecimiento y la represión con lógicas limitativas y que socavan al gobernado a una visión libertaria de respeto y humanidad sustentada en la prevención de conductas antisociales y delictivas, es decir, se muta de la represión a la prevención.

La humanización de los procedimientos penales y la construcción de tipos penales cargados de respeto a los Derechos Humanos, ahora deben convivir con la inteligencia artificial, la avalancha tecnológica, el cambio de paradigma en las relaciones humanas, los novedosos comportamientos de la sociedad y la dependencia de las Tecnologías de la Información y Comunicación (TIC´s), de las que destaca la telefonía celular como instrumento del delito a partir de su masificación, por ejemplo en 2020 se contabilizaron 88.2 millones de usuarios de teléfono celular (75.5% de la población de seis años o más). Dan cuenta de una nueva realidad.

Lo señalado *up supra* es un botón de muestra para advertir un nicho de oportunidad delictiva con capacidades que le permiten ser verdaderas oficinas móviles o bien centros de operación criminal.

III. Ciberseguridad.

Para contextualizar el tema de la Ciberseguridad y su nexo con la política criminal o criminológica, según corresponda en cada supuesto, es menester abordar el concepto de Ciberespacio, el cual se entiende como el ámbito intangible, de naturaleza global, soportado por las tecnologías de la información y comunicaciones (TIC´s), que es utilizado para la interacción entre individuos y entidades públicas y privadas[8].

Para Pierre Lévy el ciberespacio "*designa el universo de redes digitales como un mundo de interacción y aventura, es el espacio de con ictos globales y una nueva frontera económica y cultural*"[9]. La prevención del ciberdelito es una tarea constitucionalmente asignada a los tres niveles de gobierno a través de sus respectivos sistemas de seguridad pública que confluyen en el Sistema Nacional de Seguridad Pública.

Fernández MacGregor señala que la Ciberseguridad "es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque. Esto incluye soluciones tecnológicas como el uso de programas anti-virus o la actualización periódica de software; además de buenas prácticas en el uso de las tecnologías de la información, así como no abrir archivos de direcciones de correos que provienen de fuentes desconocidas".

[7] Juárez Bribiesca, Armando y Medina Ramírez, Marco Antonio. (2011) Política criminal (México-Chile). Revista Mexicana de Justicia. UNAM, México
https://revistas.juridicas.unam.mx/index.php/reformajudicial/article/view/8806/10857

Para la ciberseguridad, es importante identificar que existen los ciberataques, mismos que son las acciones informáticas que se utilizan para vulnerar las tecnologías de la información, así como copiar, borrar, reescribir, sustraer toda aquella información que existe en el ordenador de la víctima, lo que se potencializa tratándose de información confidencial y de transferencia de recursos.

Machín Nieva señala los siguientes ciberataques más comunes.

a) Código malicioso o malware: su fin principal es dañar el funcionamiento correcto de cualquier equipo informático, ya sea inutilizando el sistema operativo o haciéndose con el control de la memoria.

b) Virus: es un programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.

c) Troyano: es un software que suele aparentar ser inofensivo o incluso realizar tareas necesarias para el usuario, pero que en realidad su objetivo es el robo o destrucción de la información acumulada en el dispositivo.

En el marco del programa Sectorial de la Secretaría de la Defensa Nacional 2020 – 2024, está ponderado el objetivo de hacer eficiente la operatividad de las Fuerzas Armadas (Ejército y Fuerza Aérea), en este sentido es el ciberespacio un tema más o menos novedoso que exige la atención institucional al ser la información el actual derrotero de la inteligencia. (SEDENA, 2020 - 2024).

En la actualidad la ciberseguridad es un tema de primera línea, al ser la información el punto de partida para las relaciones de carácter global quepermite comunicar, negociar o dominar las fuerzas en el mundo, esto se potencia frente a los antagonismos que exigen coordinación, rapidez, eficiencia y certeza.

---

9 Cfr. CODENAL, Glosario de términos unificados de seguridad nacional. México, 2018.

10 Cfr. Lévy, Pierre. ¿Qué es lo virtual? Paidós. España. 1999. P. http://cmap.upb.edu.co/rid=1R3QGX5B9170HLS8-6ZNQ/Levy%20Pierre%20-%20Que%20Es%20Lo%20Virtual.pdf

Cfr. Fernández Macgregor, B. Rafael. Perspectiva de ciberseguridad en México. McKinsey & Company. 2018. https://consejomexicano.org/multimedia/1528987628_817.pdf

Cfr. Machín Nieva, Gazapo Manuel. La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea Revista UNISCI, núm. 42, octubre, pp. 47-68 Universidad Complutense de Madrid. España. 2016. https://www.redalyc.org/pdf/767/76747805002.pdf

Tal es el caso, que en un mismo momento, prácticamente a segundos de haber ocurrido, el mundo está informado de diferentes hechos, verbigracia la pandemia, los noticieros, las nuevas formas de trabajo en casa, la transformación de la educación y la reinvención de los negocios en nuevas condiciones donde las altas tecnologías y redes de información, las ventas en línea e incluso aspectos lúdicos entre personas de diferentes países.

En este sentido se han potenciado las relaciones sociales a distancia con personas que no sabemos a ciencia cierta quienes son y es factible enfrentar depredadores sexuales particularmente con personas vulnerables como lo son los menores de edad, de ahí que la explotación sexual infantil sea un tema de gran actualidad, así como muchas expresiones delictivas dentro de las que destacan el fraude, la extorsión y el robo de identidad.

IV. Política Criminal y Ciberseguridad en México

La Oficina de Naciones Unidas contra la Droga y el Delito (UNODOC) señala que no existe una definición exacta sobre ciberdelincuencia, pero las que existentes coinciden en los siguientes elementos: se considera como un acto que infringe la ley y que se comete usando las tecnologías de la información; la principal finalidad es atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito; no tiene barreras físicas o geográficas.

Por lo que hace al ciberacoso, el Instituto Nacional de Estadística y Geografía (INEGI) vía el Módulo sobre Ciberacoso (MOCIBA) señala que:

En México el Caso Olimpia (Olimpia Melo Cruz), se considera paradigmático, en virtud de que con motivo del mismo se penalizo la violación a la intimidad sexual.

Olimpia cuenta que, cuando tenía 18 años un video de ella con contenido sexual se compartió a través de las redes sociales hasta viralizarse; se encerró en su casa aproximadamente ocho meses e intento suicidarse tres veces.

Posteriormente, entendió que ella al igual que otras mujeres eran victimas de una violencia, así que decidió acudir a la procuración de justicia, pero no existía una ley que penara la acción de compartir contenido intimo sin autorización. Esto como lo expresa el principio de legalidad en materia penal que establece: *nulum poena sine legem, nulum poena sine tipo, nulum poena sine conducta*.

Cfr. Oficina de Naciones Unidas contra la droga y el delito. UNODOC. Modulo I. Introduccion a la Ciberdelincuencia2020 https://www.unodc.org/e4j/es/cybercrime/modul_e-1/key-ssues/cybercrimein-brief.html. Cf r. Latto, Nica. ¿Qué es el ciberdelito y cómo puede prevenirlo? 2021. España https://www.avast.com/es-es/c-cybercrime#topic-1

Así que, se encargo de estudiar el tema, ya como activista y con el apoyo de organismos no gubernamentales impulso una reforma la cual penalizaba la violación a la intimidad sexual.

Debe señalarse que la "Ley Olimpia" no es una ley como tal sino, que se trata de una propuesta que planteaba reformas en materia de delitos contra la intimidad, difusión de contenido íntimo sin consentimiento, ciberacoso, así como a la Ley de acceso de las mujeres a una vida libre de violencia, para que las instituciones se encargaran de concientizar a los ciudadanos sobre los derechos sexuales y la violencia digital.

A nivel federal, el primero de julio de 2021, mediante Decreto se adicionó al Título II de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia el capítulo IV Ter denominado "De la Violencia Digital y Mediática", compuesto por los artículos 20 Quáter, 20 Quinquies y 20 Sexies .

La violencia digital está definida en el artículo 20 Quárter como:

> *"...toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia".*

Además de lo anterior, se toman en cuenta todos aquellos actos que afecten la "intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación".

También nos define qué son las tecnologías de la información y la comunicación: aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos.

Esta ley señala, que la violencia digital será sancionada en los términos del Código Penal Federal.

Modula sobre Ciberacoso (MOCIBA). Instituto Nacional de Estadística y Geografía (INEGI). 2020. México. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf

El Diccionario de la Real Academia de la Lengua Española señala que viralizar "es adquirir carácter de conocimiento masivo un proceso informático de difusión de información"

Animal Político. BBC News Mundo. Ciberacoso Ley Olimpia. 2019.
https://www.animalpolitico.com/bbc/ciberacoso-ley-olimpia-video-sexual-historia/2019

Idem

El artículo 20 Quinquies define a la violencia mediática como:

> *"...todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las mujeres y las niñas, produzca o permita la producción y difusión de discurso de odio sexista, discriminación de género o desigualdad entre mujeres y hombres, que cause daño a las mujeres y niñas de tipo psicológico, sexual, físico, económico, patrimonial o feminicida"*.

La violencia mediática la puede ejercer cualquier persona física o moral, utilizando algún medio de comunicación, con la finalidad de atentar contra la seguridad, libertad, salud e integridad de las mujeres.

Por su parte, el artículo 20 Sexies señala que "en caso de existir la violencia digital o mediática la administración e impartición de justicia deberán de ordenar de manera inmediata, a través de correo electrónico o escrito, las medidas de protección a la víctima, para que las empresas, redes sociales, páginas electrónicas, etcétera, interrumpan, bloqueen, destruyan o eliminen el contenido difundido".

El 15 de Junio de 2018, se publicó en el Diario Oficial de la Federación la adición al Código Penal Federal de un Título Séptimo BIS con un Capítulo I y un artículo 199 Septies.

Este capítulo se denomina "Comunicación de Contenido Sexual con Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen la Capacidad para Resistirlo".

> Artículo 199 Septies.- Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.

Cámara de Diputados. Ley General de Acceso de las Mujeres de las a una vida libre de violencia. 2021. México.
http://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV_010621.pdf
Idem.

El primero de Junio de 2021, se publicó en el Diario Oficial de la Federación la adición de un Capítulo II denominado "Violación a la Intimidad Sexual" al Título Séptimo Bis denominado "Delitos contra la Indemnidad de la Privacidad de la Información Sexual", compuesto por los artículos 199 Octies, 199 Nonies y 199 Decies al Código Penal Federal.

El artículo 199 Octies señala que: Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.

Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.

Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.

Por su parte, el artículo 199 Nonies, a la letra dice: Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no correspondan con la persona que es señalada o identificada en los mismos.

El artículo 199 Decies señala las agravantes, entendidas como la "circunstancias modificativas de la responsabilidad que determina un aumento de la pena correspondiente al delito por suponer una mayor peligrosidad del sujeto o una mayor antijuridicidad de su conducta.

Cámara de Diputados. Código Penal Federal. 2021 México

Idem.

Cfr. Diccionario panhispanico del español jurídico. Agravante. 2020. https://dpej.rae.es/lema/agravante

Cámara de Diputados. Código Penal Federal. 2021. México.

Finalmente, en México la Estrategia Nacional de Ciberseguridad reconoce que las tecnologías de la información son parte del desarrollo político, social y económico, en razón de que cada día aumenta el uso del internet en el país, por lo que existen riesgos que se relacionan con su uso y un aumento de ciberdelitos.

La Estrategia Nacional de Ciberseguridad señala que los riesgos y amenazas en el ciberespacio constituyen un ataque a la dignidad humana, integridad de las personas, reputación, economía, así como afectación de las instituciones públicas, seguridad pública e incluso seguridad nacional.

La Estrategia pretende articular acciones de ciberseguridad para individuos, empresas e instituciones públicas, así mismo establece colaboración y cooperación de diversos sectores, da a conocer los riesgos y amenazas en el ciberespacio, desarrolla capital humano para actuar contra la ciberseguridad y promueve al uso adecuado de las tecnologías de la información.

V. Posibles Escenarios y respuestas institucionales frente a los Ciberdelitos

Sin darnos cuenta el mundo entero se ha introducido en un universo digital y de internet en donde cada vez más personas de todas las edades, segmentos sociales y culturales, ideologías y formas de pensamiento se involucran en las aldeas digitales, de suerte que un número muy importante de habitantes del planeta han comenzado a vivir dos mundos: el real y el virtual.

El maremágnum de experiencias y oportunidades que ofrece la vida digital ha aparejado transformaciones conductuales, sociales, culturales y políticas al ofrecer nuevas experiencias para vivir a bajo costo en la ciberealidad o dicho de otra forma, en la realidad virtual, al grado que una persona puede alegrarse o deprimirse en función de *likes* o comentarios positivos o negativos e incluso frente a acciones como el ser bloqueado, entre otras.

Con la anterior reflexión se pretende demostrar que sí existe un impacto emocional, social, político y cultural en razón de lo que ocurre en ese mundo alterno, al que cada vez más personas deciden pertenecer, con lo que atendiendo a la facilidad de ocultar la identidad, las tentaciones de dar rienda suelta a patologías, conductas antisociales y delitos, es recurrente.

Cfr. Estrategia Nacional de Ciberseguridad. 2018. México. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Na cional_Ciberseguridad.pdf
Idem.

En este orden de ideas, el uso impropio e incorrecto del internet abrió, sin duda, la puerta grande para entrar al mundo de los ciberdelitos, en este sentido, dio paso a un nuevo tipo de delincuente que ya no necesita interactuar socialmente de forma física para desplegar conductas transgresoras de los vienes jurídicos tutelados de otro, ahora lo puede hacer desde el confort de su sillón, sentado frente al computador y sin que se conozca su identidad, con una amplia gama de posibilidades para la comisión de ilícitos de muy diversa índole, por que así como en la vida real los delitos más recurrentes son los patrimoniales, esa misma tendencia se expresa en lo virtual a partir de los fraudes, extorsión y suplantación de personas, sin que sea menor la existencia de delitos de violación a la intimidad, acoso y hostigamiento sexual virtual.

Existen graves peligros en todos los ámbitos con la llegada de los ciberdelitos, así por ejemplo, los riesgos son latentes para las familias, empresas, la información del Estado, trámites burocráticos, fraudes bancarios e incluso en los ámbitos de seguridad pública, interior del Estado y nacional.

Por otra parte, las amenazas del crimen organizado por internet han sido estudiadas y analizadas por el Centro Europeo de Ciberseguridad de EUROPOL y por ejemplo destaca el hecho de que Reino Unido subraye que la ciberdelincuencia creciente rebasa a la delincuencia común en el número de eventos, victimas, así como daños económicos y materiales.

VI. Conclusiones

La Política Criminal y la Ciberseguridad, son expresiones importantes de la actual situación tecnológica en México, en atención de su impacto transversal en la seguridad.

Por lo que su armonización y tratamiento legislativo tendrá un impacto favorable en las acciones que para prevenir los delitos cibernéticos implemente la administración pública en sus diversos niveles de gobierno y dará elementos a los juzgadores y fiscalías para que en el tramo de sus respectivas responsabilidades allanen el camino de acceso a la justicia a los gobernados.

Es necesario impulsar políticas que pasen de la lectura criminal o represiva a la criminológica o preventiva que permitan el acceso a la justicia, la reparación del daño de la victimas, la reconstrucción del tejido social y en su caso el castigo de los ciberdelincuentes que cometen hechos delictivos en internet, en virtud de que, la mayoría quedan impunes, por la limitación de las denuncias, la falta de capacidad de las instancias del sistema de justicia penal, por ejemplo el fortalecimiento de la policía cibernética en todos los cuerpos policíacos del país y la ausencia o carencia de una legislación acorde con la realidad delictiva on line.

Las áreas de oportunidad para desarrollar conocimiento científico social frente a los ciberdelitos es un reto de las políticas públicas, así por ejemplo, habrá que desarrollar técnicas de razonamiento probatorio, ajustes procesales y doctrinarios en materia de teoría de la prueba, reformas procesales, creación de tipos penales acordes a la nueva realidad y el desarrollo de una educación del manejo de las herramientas virtuales para la prevención de los delitos por parte de las instituciones de seguridad y justicia.

Las dependencias del gobierno, en tanto órganos del estado responsables de la información de los ciudadanos y de proporcionar servicios públicos a éstos, debe desarrollar capacidades en el ciberespacio en dos sentidos: para logar internamente la ciberseguridad de las instituciones y en paralelo para hacer un frente de ciberdefensa de los intereses del Estado.

Fuentes de consulta

- Animal Político. BBC News Mundo. Ciberacoso Ley Olimpia. 2019. https://www.animalpolitico.com/bbc/ciberacoso -ley-olimpia-videosexual-historia/2019
- Díaz, N. M. (2021). Ciberseguridad. Ciudad de México: CODENAL
- Diccionario de la Real Academia de la Lengua Española. Político. 2021. https://dle.rae.es/pol%C3%ADtico#Ta2HMYR
- Diccionario de la Real Academia de la Lengua Española. Criminal. 2021. https://dle.rae.es/criminal?m=form
- Diccionario panhispánico del español jurídico, Agravante. 2020. https://dpej.rae.es/lema/agravante
- Cámara de Diputados. Código Penal Federal. 2021. México. http://www.diputados.gob.mx/LeyesBiblio/pdf/9_010621 .pdf
- Cámara de Diputados. Ley General de Acceso de las Mujeres de las a una vida libre de violencia. 2021. México.
- http://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV_010621 .pdf
- CODENAL. (2018). Glosario de Términos Unificados de Seguridad Nacional. Ciudad de México: CODENAL.
- Corte Constitucional de Colombia en la sentencia C-646 de 2001.
- https://www.corteconstitucional.gov.co/relatoria/2001/C -646-01 .htm
- Estrategia Nacional de Ciberseguridad. 2018. México. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
- Fernández Macgregor, B. Rafael. Perspectiva de ciberseguridad en México. McKinsey & Company. 2018.

https://consejomexicano.org/multimedia/1528987628 -817.pdf

Juárez Bribiesca, Armando y Medina Ramírez, Marco Antonio. (2011) Política criminal (México-Chile). Revista Mexicana de Justicia. UNAM. México. https://revistas.juridicas.unam.mx/index.php/reformajudicial/ article/view/8806/10857

Latto, Nica. ¿Qué es el ciberdelito y cómo puede prevenirlo? 2021. España. https://www.avast.com/es -es/c-cybercrime#topic-1

Lévy, Pierre. ¿Qué es lo virtual? Paidós. España. 1999. P.

Machin Nieva, Gazapo Manuel. La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea Revista UNISCI, núm. 42, octubre, 2016. pp. 47-68 Universidad Complutense de Madrid. España.

https://www.redalyc.org/pdf/767/76747805002.pdf

Marín Gutiérrez, Francisco. Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción. Documento de Opinión IEEE 78/2021. PP. 8 y 9.

http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO78_2021_FRANMAR_Ciber.pdf

Módulo sobre Ciberacoso (MOCIBA). Instituto Nacional de Estadística y Geografía (INEGI). 2020. México.

https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf

Oficina de Naciones Unidas contra la Droga y el Delito. UNODOC. Módulo 1. Introducción a la Ciberdelincuencia. 2020.

https://www.unodc.org/e4j/es/cybercrime/module -1/key- issues/cybercrime-in-brief.html

TENDENCIAS, RETOS Y DESAFÍOS DE LA CIBERSEGURIDAD Y LOS CIBERDELITOS EN LA 4ª REVOLUCIÓN INDUSTRIAL

Mtro. Jacobo Bello Joya[1].

Sumario: I. Evolución histórica. II. Megatendencias tecnológicas. III. Puntos de inflexión tecnológicos (Tipping Points). IV. Los nuevos modelos de negocio en la cuarta Revolución Industrial (Start-Up). V. Tendencias, retos y desafíos de la ciberseguridad y los ciberdelitos en la cuarta Revolución Industrial. VI. Consideraciones finales.

I. Evolución histórica

A) Era moderna de la humanidad, las revoluciones industriales

Las Revoluciones Industriales marcan el periodo de la época moderna de la humanidad, mas del 90% de los inventos de la humanidad ocurrieron en los últimos 150 años, estas revoluciones industriales enmarcan un período histórico de transformaciones económicas y sociales, que desencadenó cambios sin precedentes para las sociedades de todo el mundo y se han caracterizado por fuertes transformaciones sociales y económicas, a continuación exploraremos las características y evolución de cada una de ellas.

B) Primera y Segunda Revoluciones Industriales (*muscle power*)

La Primera Revolución Industrial, que se inició en Inglaterra durante la segunda mitad del siglo XVIII, es quizás uno de los eventos más decisivos en la historia de la humanidad, se caracteriza por sus avances en el sector textil: la máquina de hilar y en el sector siderúrgico: el uso del hierro y del ferrocarril, que junto a la máquina de vapor, estimuló la siderurgia y el comercio y la movilidad de familias enteras que migraron del campo a las ciudades en busca de mejores condiciones de vida, al llegar a esas enormes ciudades, los únicos trabajos que encontraban disponibles era en las minas o en las grandes fábricas y, una vez contratadas, las personas permanecían ahí gran parte de sus vidas.

[1] Actualmente es el Titular de la Guardia Cibernética en la Dirección General Científica de la Guardia Nacional, cuenta con dos maestrías una en Dirección Estratégica de las Tecnologías de Información y Comunicación en la Universidad de Texas y en Sistemas de Información por la Fundación Arturo Rosenblueth, curso las especializaciones en Tecnologías de Información en la Universidad de Georgetown y la especialización en Redes y Teleinformática en la Universidad Anáhuac, y cuenta con mas de 25 años de experiencia en puestos directivos en áreas de Tecnologías de la Información y Comunicación.

La segunda Revolución Industrial fue un periodo de importantes cambios industriales, sociales y económicos que surgieron tras la primera etapa de la Revolución Industrial iniciada en Gran Bretaña. Ésta se desarrolló entre los años 1870 y 1914, en la cual se empezaron a utilizar fuentes de energía mas eficientes como la electricidad y el petroleo, creándose nuevas fuentes de trabajo y nuevas industrias a partir de una serie de inventos y descubrimientos, como el telégrafo, el teléfono, la máquina de escribir, la máquina de coser, la fotografía, el cine, el automóvil y el avión, entre muchos otros. La producción sistemática desarrollada durante la segunda Revolución Industrial tuvo como consecuencia la aceleración de la producción, logrando mayor competitividad en el mercado lo que, a su vez, incrementó el desempleo debido a la sustitución de empleados por maquinarias.

La primera y segunda Revoluciones Industriales se han caracterizado por la mecanización de las tareas rutinarias y que requieren de esfuerzo físico, por ello son también identificadas como la revoluciones del "*Muscle Power*".

C) Tercera y cuarta Revoluciones Industriales (*muscle mind*)

La tercera Revolución Industrial se inició a finales de la década de 1960. Generalmente se le conoce como la revolución digital o del ordenador, porque fue impulsada por el desarrollo de los semiconductores, la computación mediante servidores tipo "*mainframe*" (década de los 70´s), la informática personal (década de los 80´s) y la internet (década de 1990). Se resalta con especial énfasis el desarrollo de los sistemas informáticos basados en un inicio en sistemas computacionales centralizados que han migrado al computo personal basado en redes de comunicaciones de área amplia, metropolitana y local (WAN-MAN-LAN) que junto al desarrollo de la internet, constituyen un soporte vital a los diversos sectores de la sociedad en la automatización de procesos de negocio y de gobierno, así como de los ciudadanos en su vida diaria. Se ubica su culminación de forma conjunta con el siglo XX.

La cuarta Revolución Industrial comenzó a principios de este siglo y se basa en la revolución digital. Se caracteriza por un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina.

La Industria 4.0, un término acuñado en la Feria de Hannover de 2011, ha revolucionado las cadenas de valor globales, mediante la creación de "fábricas inteligentes"; la cuarta revolución industrial genera un mundo en el que sistemas de fabricación virtuales y físicos cooperan entre sí de una manera flexible en todo el planeta. Esto permite la absoluta personalización de los productos y la creación de nuevos modelos de operación. La cuarta revolución industrial, no obstante, no solo consiste en máquinas y sistemas inteligentes y conectados, su alcance es más amplio, se producen avances en ámbitos que van desde la secuenciación genética hasta la nanotecnología, y de las energías renovables a la computación cuántica. Es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la cuarta revolución industrial sea fundamentalmente diferente de las anteriores.

La tercera y cuarta Revoluciones Industriales se han caracterizado por la automatización de los procesos, la generación de la era de la sociedad de la información y del conocimiento y de la inteligencia artificial como un aliado en la vida diaria de las personas, por ello son también identificadas como la revoluciones del "*Muscle Mind*".

D) Componentes y características de la cuarta Revolución Industrial

En este apartado se identifican indicadores y conceptos que han sido reconceptualizados en la cuarta Revolución Industrial, así como los pilares que han motivado un cambio acelerado en la sociedad hoy día tecnificada, con un enfoque orientado a las personas, en modelos de negocio que buscan la desintermediación y la creación de las empresas llamadas "Unicornios".

- Pilares de la industria 4.0
  - Innovación disruptiva
  - Modelo diferenciado de negocio
  - Tecnología I4.0

Hallar o diseñar algo que la humanidad no había previsto y cuyo uso resulta en la solución de un problema es lo que se define como innovación disruptiva, las industrias tradicionales y "exitosas" son desafiadas por nuevas organizaciones que, a través de la innovación disruptiva, apalancada en nuevas tecnologías, transforman los sectores existentes. Innovación disruptiva es aquella que conduce a la aparición de productos y servicios que utilizan preferiblemente una estrategia disruptiva (que produce ruptura brusca) frente a una estrategia sostenible y generalmente planeada a largo plazo.

La transición de la tercera Revolución Industrial a la cuarta Revolución Industrial ha llevado consigo a una evolución de paradigmas, buenas prácticas y adopción tecnológica que se esta integrando de forma gradual en la vida diaria.

La cuarta Revolución Industrial es única, debido a la creciente armonización e integración de muchas disciplinas y descubrimientos distintos. Se fusionan tecnologías fundacionales como el internet y el blockchian, con tecnologías disruptivas para crear innovaciones tangibles que dejaron de ser ciencia ficción. Hoy, por ejemplo, las tecnologías de fabricación digital pueden interactuar con el mundo biológico. Algunos diseñadores y arquitectos ya están combinando el diseño por ordenador, la fabricación aditiva, la ingeniería de materiales y la biología sintética para crear sistemas que involucran la interacción entre micro organismos, nuestro cuerpo, los productos que consumimos e incluso los edificios que habitamos.

La Inteligencia Artificial (IA) está presente por doquier, desde vehículos que se conducen solos y drones, hasta asistentes virtuales y software de traducción. Esto está transformando nuestras vidas. La IA ha logrado avances impresionantes, impulsada por el aumento exponencial de la potencia de cómputo y por la disponibilidad de grandes cantidades de datos, desde el software utilizado para descubrir nuevos fármacos hasta los algoritmos que predicen nuestros intereses culturales. Muchos de estos aprenden del rastro que nuestros datos dejan en el mundo digital, lo cual da por resultado nuevos tipos de "aprendizaje de máquina" y el descubrimiento automatizado que les permite a los robots y ordenadores "inteligentes" autoprogramarse y encontrar soluciones óptimas a partir de principios básicos.

La cuarta Revolución Industrial generará, en igual medida, grandes beneficios y grandes retos. Una preocupación particular es la desigualdad exacerbada. Los desafíos planteados por la desigualdad creciente son difíciles de cuantificar dado que la gran mayoría de nosotros somos consumidores y productores, y la innovación y la disrupción afectan a nuestros niveles de vida y bienestar tanto de manera positiva como negativa.

El consumidor parece ser el gran ganador de la cuarta revolución industrial que ha hecho posible nuevos productos y servicios que aumentan prácticamente sin costo alguno la eficiencia de nuestras vidas como consumidores. Pedir un taxi, encontrar un vuelo, comprar un producto, realizar un pago, escuchar música o ver una película; cualquiera de estas tareas ahora se puede realizar de manera remota. Los beneficios de la tecnología para todos los que consumimos son incontrovertibles. Internet, el teléfono inteligente y las miles de aplicaciones están volviendo nuestra vida más fácil y, en general, más productiva. Un dispositivo sencillo como una tableta, que usamos para la lectura, la navegación y la comunicación, posee el poder de procesamiento

equivalente a cinco mil ordenadores de escritorio de hace treinta años, mientras que el costo de almacenamiento de la información baja exponencialmente.

I. Mega tendencias Tecnológicas

La conectividad digital impregna todos los aspectos de la vida diaria, desde la forma en que las personas interactúan hasta el ecosistema económico, la toma de decisiones políticas y las nuevas habilidades necesarias para conseguir un trabajo. La pandemia ha provocado una mayor dependencia de los recursos en red generando que las personas sean más interdependientes, mientras que a un gran número de personas les preocupa si los prestadores de servicios y contenidos (OSP´s) – facebook, twitter, youtube, amazon, gmail, whatsapp, tiktok, por mencionar algunos – pueden lograr el equilibrio adecuado entre privacidad, seguridad y confianza.

Al mismo tiempo, la creciente digitalización está impulsando al sector privado a cambiar el paradigma de ofertas basadas en productos a ofertas basadas en servicios; si bien estas ofertas están altamente automatizadas y estandarizadas, estas son personalizadas a través de la fusión de la Inteligencia Artificial que explota una cantidad exorbitante de información personal principalmente por un dispositivo celular. La perfecta integración de los mundos físicos y digital a través de sensores, actuadores, hardware y software integrados en red cambiará no solo los modelos industriales, estos ya se reflejan en la vida diaria en el hogar. En resumen, el mundo está a punto de experimentar una tasa de cambio exponencial a través del auge de las nuevas tecnologías que impulsan nuevos modelos de negocio y estilos de vida.

III. Puntos de Inflexión Tecnológicos (Tipping Points)

Como parte de la agenda de trabajo del Foro Económico Mundial, en marzo de 2015, el "Consejo de la Agenda Global sobre el Futuro del Software y la Sociedad" lanzó la encuesta Puntos de Inflexión Tecnológicos (Tipping Points). Se determinaron 21 "puntos de inflexión", a efecto de identificar los cambios tecnológicos que afectan a la sociedad en general, y evaluar el impacto de estos cambios en nuestra sociedad con la finalidad de prepararse para los cambios que se avecinan.

Con el objetivo de proporcionar una instantánea de las expectativas de una comunidad de más de 800 ejecutivos y expertos del sector de tecnología de la información y las comunicaciones, la encuesta preguntó a los encuestados cuál era su percepción de cuándo ocurrirían estos puntos de inflexión, ofreciendo rangos de fechas desde "ya ha sucedido" hasta "20+ años".

Los resultados se analizaron y cotejaron en dos formatos principales. En primer lugar, se utilizó un sistema de medias ponderadas para calcular el año promedio en el que se espera que ocurriera cada punto de inflexión. El cronograma resultante se presenta en la siguiente tabla y va de 2018 a 2027, reflejando las percepciones solo de aquellos que pensaron que el cambio ocurriría en algún momento.

En segundo lugar, para obtener una visión más global del cambio trascendental dentro de la próxima década, se agregó el porcentaje de personas que respondieron "10 años" o menos para cada punto de inflexión.

Si bien la Metodología "Tipping Point" es un ejercicio que busca identificar cómo las nuevas tecnologías impactan a una sociedad de forma positiva así como de forma negativa identificando los posibles riesgos de ciberseguridad; se convierte en una herramienta útil para que el sector privado identifique los riesgos de ciberseguridad de sus nuevos modelos de negocio basados en tecnologías disruptivas

Con la finalidad de hacer palpable el ejercicio metodológico de evaluar los posibles impactos que el uso de las tecnologías pueden ocasionar a una sociedad, a continuación se presenta el análisis de algunos puntos de inflexión (tipping points) considerando sus posibles impactos positivos, negativos e incluso aquellos que generan incertidumbre.

Almacenamiento para todos (2018)

90% de las personas cuentan con almacenamiento ilimitado y gratuito

- Se estima que el 90% de los datos a nivel mundial fueron creados en los últimos 2 años
- Las empresas privadas duplican cada año su cantidad de información
- Los proveedores de servicios y contenidos en internet ofrecen almacenamiento gratuito a sus usuarios como parte de su oferta de servicios / valor (Google Drive, Box, Copy , Dropbox, One Drive) Þ Ley de Moore aplicable al almacenamiento

- Posible Impacto Positivo

• La empresa privada se vuelve más eficiente
• Mejores servicios Gubernamentales
• Las capacidades de desarrollo humano crecen al extender las limitaciones humanas de memoria
• Disponibilidad y permanencia de la información

- Posible Impacto Negativo

• Robo de datos

- Acceso no autorizado a información
- Riesgos en la integridad de la información

Posible Escenario Incierto

- Memoria eterna , nada se borra
- Incremento de la generación, distribución y consumo de "contenidos"

Un trillón de sensores conectados a Internet (2022).

Es económicamente factible conectar cualquier cosa a Internet.
Los sensores inteligentes ya están disponibles a precios muy competitivos.
Todas las cosas serán inteligentes y estarán conectadas a Internet.
Nuevos servicios basados en el incremento de capacidades analíticas.
Todos los productos conectados a una infraestructura de comunicación ubicua y los sensores en todas partes permitirán a las personas percibir por completo su entorno.

Posible Impacto Positivo

- Aumento de la productividad
- Menor costo de entrega de servicios
- Cambio en los mercados laborales y habilidades
- Creación de nuevas líneas de negocios
- Digital Twin: datos para el monitoreo, control y predicción
- Las cosas perciben su entorno y reaccionan de manera autónoma
- Generación de conocimiento adicional

Posible Impacto Negativo Privacidad

- Pérdida de empleos de bajas habilidades
- Hackeos y problemas de seguridad
- Mayor complejidad / Pérdida de control

Posible Escenario Incierto

- Los bienes se rentan por uso
- Modelos de negocios basados en el valor de los datos
- Nuevos negocios de venta de datos
- Distribución masiva de infraestructura de IoT
- Altas tasas de cobertura: utilización en autos, máquinas, herramientas, equipo, infraestructura
-

Primer teléfono móvil implantable disponible comercialmente. (2023).

- Implantes podrán detectar parámetros de enfermedades y enviar datos al centro de monitoreo del hospital
- Implantes que liberan medicamentos curativos automáticamente

- Tatuajes y Chips implantables que permitirán ubicar, identificar, realizar pagos, comunicar pensamientos o estado de ánimo a un dispositivo.

Posible Impacto Positivo

- Reducción de personas desaparecidas
- Aumento de la salud de las personas
- Ancianos autosuficientes
- Mejoras en la toma de decisiones
- Reconocimiento de imágenes y disponibilidad de datos personales

Posible Impacto Negativo

- Riesgos a la Privacidad
- Acceso no autorizado a la información
- Disminución de la seguridad de los datos
- Cambios en la forma de interrelaciones personales
- Incremento de las distracciones (trastorno por déficit de atención)
- Posible Escenario Incierto
- Mayor longevidad de vida
- Cambios en la naturaleza de las relaciones humanas
- Cambios en las interacciones humanas
- 10% de los lentes para lectura conectados a Internet (2023)
- Lentes inteligentes con acceso a Internet
- Conectividad a dispositivos preferentemente al smartphone
- Transmisión y recepción de video en tiempo real
- Aplicaciones: Multimedia – Juegos – Comunicación – Información – Salud

Posible Impacto Positivo

- Información tiempo real para toma de Decisiones
- Ayudas visuales para realizar actividades: fabricación-cirugías prestación de servicios
- Habilidades para las personas con discapacidad

Posible Impacto Negativo

- Riesgos a la Privacidad
- Acceso no autorizado a la información
- Distracción mental que causa accidentes
- Trauma de experiencias inversivas negativas
- Aumento de adicción y aislamiento

Posible Escenario Incierto

- Un nuevo segmento creado en la industria del entretenimiento
- Mayor información inmediata

80% de las personas tendrán una presencia digital en Internet (2023)

De una presencia digital básica (# de celular, mail y web personal) a una presencia digital extendida (Facebook, Twitter, LinkIn, Instagram, Snapchat)

La Persona Digital evolucionara a Ciudadano Digital con derechos y obligaciones en el entorno virtual en el mundo conectado y a través de la presencia digital, las personas podrá buscar y compartir información, expresar ideas libremente, encontrar y ser encontrado, y desarrollar y mantener relaciones prácticamente en cualquier parte del mundo.

- Posible Impacto Positivo
  - Incrementa la transparencia
  - Incremento de la interconexión entre individuos y grupos
  - Aumento de la libertad de expresión
  - Difusión / intercambio de información más rápido
  - Uso más eficiente de los servicios del gobierno

- Posible Impacto Negativo
  - Riesgos a la Privacidad
  - Acceso no autorizado a la información
  - Aumento robo de identidad
  - Bullying / acoso en línea
  - Difundir información inexacta (la necesidad de manejo de reputación)

- Posible Escenario Incierto
  - Herencias digitales / huellas
  - Publicidad más dirigida
  - Información y noticias más específicas
  - Perfiles individuales
  - Identidad permanente (sin anonimato)
  - Facilidad para desarrollar un movimiento social en línea (grupos políticos, grupos de interés, pasatiempos, grupos terroristas)

90% de las personas usando Smarthphone (2023).

- En 1985 la supercomputadora Cray-2 era la máquina más veloz del mundo.
- En 2011 el Iphone 4s tenía un poder equivalente a la Cray-2
- En 2015 el Apple Watch tiene poder equivalente a 2 Iphone 4 s
- Actualmente existen poco más de 5,000 millones de números de teléfonos móviles activos

- Posible Impacto Positivo
  - Mayor participación económica de ciudadanos "última milla"
  - Acceso a educación, la salud, servicios de gobierno, oportunidades de empleo y comercio
  - Mayor Democracia

- Posible Impacto Negativo
  - Sitios cerrados en ciertos países/regiones donde no se permite acceso libre a internet

- Posible Escenario Incierto
  - 24/7 – siempre en línea
  - Estar en todo lugar, en todo momento
  - Impacto ambiental por manufactura

10% de los vehículos son autónomos (2026).

Tesla, Google, Audi y otras empresas han desarrollado con éxito vehículos autónomos.

Los vehículos autónomos pueden ser más eficientes y seguros que aquellos conducidos por seres humanos, además de reducir la contaminación y el tráfico.

Departamento de transporte de UK está cambiando su regulación para habilitar carreteras y vías primarias

- Posible Impacto Positivo
  - Mayor seguridad y eficiencia / menor contaminación.
  - Movilidad para gente de edad avanzada o con discapacidades motrices.
  - Más tiempo para enfocarse en el trabajo o contenidos multimedia

- Posible Impacto Negativo
  - Hacking/cyberattacks
  - Perdida de trabajos (taxistas y choferes)
  - Disminución de ingresos por multas (GOB)
  - Menos propietarios de autos
  - Seguros más caros si conducen personas

- Posible Escenario Incierto
  - Desarrollo de la industria automotriz

10% de las transacciones del Producto Interno Bruto (PIB) almacenado en Block chain (2027).

- La tecnología de *blockchain* permite establecer transacciones de confianza en forma distribuida, sin necesidad de tener una autoridad intermedia que valide dichas transacciones
- Ello reduce significativamente los costos de transacción.
- A diferencia de otras tecnologías, ésta es una tecnología fundacional que modifica de raíz la manera como realizamos transacciones de valor en Internet.

Posible Impacto Positivo

- Mayor inclusión financiera en los mercados emergentes, a medida que los servicios financieros en la cadena de bloques ganan masa crítica
- Desintermediación de instituciones financieras, ya que se crean nuevos servicios e intercambios de valor directamente en la cadena de bloques.
- Una explosión de activos negociables, ya que todo tipo de intercambio de valor se puede alojar en la cadena de bloques.
- Mejores registros de propiedad en los mercados emergentes y la capacidad de convertir todo en un activo negociable.
- Contractos y servicios legales cada vez más vinculados al código vinculado a la cadena de bloques, para ser utilizado como depósito de garantía irrompible o
- Contratos inteligentes diseñados programáticamente
- Mayor transparencia, ya que ***blockchain*** es esencialmente un libro mayor global que almacena todas las transacciones.

Posible Impacto Negativo

- Desconfianza de los usuarios ante una tecnología disruptiva
- Posibilidad de *hack* regla 51 %

Posible Escenario Incierto

- Mecanismos alternos de formalización de transacciones financieras y comerciales e incluso inmobiliarias.

II. Los nuevos modelos de negocio en la 4ª Revolución Industrial (Start- Up)

Las Startups son empresas o emprendimientos que se centran en un solo producto o servicio que los fundadores quieren llevar al mercado. Por lo general, estas empresas no tienen un modelo de negocio completamente desarrollado y, lo que es más importante, carecen del capital adecuado para pasar a la siguiente fase del negocio. Las empresas emergentes (startups) suelen ser empresas en línea u orientadas a la tecnología que pueden llegar fácilmente a un gran mercado. Para operar una pequeña empresa, por otro lado, no necesita un gran mercado para crecer. Solo necesita un mercado y debe poder llegar y servir a todos aquellos dentro de su mercado de una manera eficiente.

Esta nueva modalidad de modelos de negocio han sido de tal impacto que hoy día su éxito se mide en lo que denominan empresas "Unicornio". La primera vez que se utilizó el término fue en noviembre de 2013, de la mano de Aileen Lee, fundadora de Cowboy Ventures; Unicornio se define como una compañía tecnológica que alcanza un valor de mil millones de dólares, se utiliza este término "Unicornio" puesto que se podrían comparar a estos animales mitológicos, una fantasía que parece imposible de encontrar. A continuación se presentan ejemplos de nuevos modelos de negocio, que consideraron procesos de innovación disruptiva y el uso de tecnologías emergentes.

Características predominantes:

Los nuevos modelos de negocio consideran relaciones Peer to Peer, es decir evitan intermediarios y ponen en contacto al usuario que demanda el servicio con el oferente del producto o servicio.

Se rompen paradigmas pasados proponiendo nuevos paradigmas (disruptivamente innovadores) que están soportados por tecnología emergente.

La relación inversión – ganancia deja de ser lineal para convertirse en una relación exponencial.

El surgimiento acelerado de estos nuevos modelos de negocio disruptivos y que utilizan las tecnologías de la denominada cuarta Revolución Industrial, tiene una relación directa con brechas generacionales: los ***Baby Boomers*** y Generación X en contra parte con los Generación Y (***Millenians***) y Generación Z. Los primeros son individuos que aspiran a un plan de retiro y pensión; generalmente permanecen en sus lugares de trabajo por lo menos 7 años y en una gran mayoría logran su jubilación en un solo trabajo; acostumbran planear sus actividades laborales de forma anual así como en su vida personal; su enfoque sistémico es integral (análisis-especificaciones funcionales-diseñodesarrollo-pruebas-liberación); generalmente las inversiones en negocios son lineales (si se invierte en x1 se obtiene una ganancia de y1, subsecuentemente hasta xn – yn; se inclinan por soluciones ERP/GRP.

Tipos de Delitos Cibernéticos:

El surgimiento de los delitos cibernéticos inicia de forma simultánea con la denominada cuarta Revolución Industrial a principios del año 2000, siendo de tal magnitud que en Europa se formaliza en 2001 el Convenio de Budapest en respuesta a la creciente ola de delitos cibernéticos.

- ***Primera Generación**, aquellos delitos que utilizan a las tecnologías como medio (fraude, extorsión, amenazas, suplantación de identidad, otros). El perfil del delincuente es de "delincuencia común".*
- ***Segunda Generación**, aquellos delitos que tienen como fin la tecnología (DDOS, Malware, Ransonware, Hijacking, acceso ilícito a sistemas, otros). El perfil del delincuente es con conocimientos técnicos especializados.*
- ***Tercera Generación**, son aquellos que fusionan las dos primeras generaciones, un claro ejemplo es el malware WannaCry, se efectúa una extorsión sustentada en un secuestro y cifrado de información. El perfil del delincuente es generalmente "delincuencia organizada".*
- ***Cuarta Generación**, a principios del 2021 el Foro Económico Mundial en su análisis global o de riesgos, señala como amenaza la concentración de grandes volúmenes de información por unas cuantas empresas. La siguiente generación de delitos cibernéticos son aquellos que harán uso de estos grandes volúmenes de información para con ello apalancar sus conductas delictivas.*

En contra parte los individuos generación Y – Z, son conscientes que el mundo cambia rápidamente, por ello conceptualizan al "mundo líquido" (término utilizado para denotar que los cambios son tan rápidos que es como si quisiéramos retener agua en nuestras manos); están acostumbrados a planear su día y en algunas ocasiones lo que harán el fin de semana; muchos de ellos son impulsores de estilos de vida como el YOLO (*you only live once* – aprovechar el momento – *Carpediem*); laboralmente permanecen en promedio de 1 a 2 años; viajar y recorrer el mundo es una prioridad; en lo sistémico han adoptado el uso de metodologías "Ágiles" y desarrollo incremental; en lugar de pensar en automatizar todos los procesos de negocio, su enfoque es holístico funcional, es decir, se ha promovido el desarrollo de las denominadas APPs (aplicaciones que te resuelven un requerimiento específico); por último, su capacidad del cambio los ha hecho proponer nuevos modelos de negocio "exponenciales", es decir la inversión principal se concreta en un software, pocos empleados, infraestructura mínima necesaria que es capaz de generar ganancias a tasas de rendimiento 100 veces mayor a las tradicionales.

V. Tendencias, retos y desafíos de la ciberseguridad y los ciberdelitos en la cuarta Revolución Industrial

El desarrollo económico, político y social derivado de la cuarta Revolución Industrial sin lugar a dudas ha traído beneficios a la humanidad, sin embargo la creciente digitalización de la sociedad y de la cual se ha exponenciado por la pandemia COVID-19 nos presenta retos y desafíos que sin lugar a duda marcaran una tendencia en los próximos años.

Principales tendencias:

- *Rasonware* se ha convertido en la amenaza de *malware* más sobresaliente superando al robo de datos privados y los troyanos bancarios que afecta a ciudadanos e instituciones.
- El constante incremento de usuarios de telefonía celular ha generado *malware* con mayor complejidad muy similares a los de una computadora personal.
- Se presenta un número cada vez mayor de redes oscuras en Internet (*Darknets*) para el intercambio de material con pornografía infantil, aunque las redes P2P siguen siendo las más comunes para este fin.
- El robo de datos personales y la usurpación de identidad cada vez adoptan mecanismos mas sofisticados como el *spoofing* telefónico.
- El uso de plataformas de cifrado de punto a punto así como el uso de pagos de forma anónima ha generado una escalada de servicios de transmisión en vivo con contenidos de abuso infantil. Los principales objetivos están en regiones con niveles de pobreza infantil, fácil acceso para los menores de edad a la tecnología y limitadas medidas de protección.

La cantidad de víctimas menores de edad con fines de explotación sexual se ha incrementado utilizando redes sociales.

- La ampliación del uso de tarjetas con Chip y PIN continuarán disminuyendo la actividad fraudulenta del uso de tarjetas electrónicas de forma presencial, sin embargo, el ataque a cajeros automáticos evolucionará.
- Los fraudes en línea sin presencia de la tarjeta (pagos electrónicos) continuarán creciendo para la compra de artículos, boletos de avión, hospedajes y alquiler de autos.

- Se observó un aumento en el número y calidad de *phishing* haciendo más difícil identificarlo, los fraudes por venta de flotillas de autos de empresas privadas e instituciones de gobierno seguirán.
- Grupos profesionales seguirán evolucionando las técnicas de BEC a fin de aumentar el número de objetivos y causar pérdidas significativas.
- Los ataques de denegación de servicios (DDoS) continuarán creciendo en intensidad y complejidad mediante la presencia de SAAS servicios "software as-a-service" en Internet (Nube).
- Las empresas que almacenan datos financieros seguirán siendo uno de los objetivos principales de los cibercriminales.
- Los datos siguen siendo un producto clave para los cibercriminales aunque ya no sólo con el fin de obtener ganancias financieras directas sino para el fraude sofisticado e incluso la extorsión.
- El intercambio de pago entre criminales utilizando criptomonedas es cada vez más frecuente, incluso se ha convertido en la solución estándar para los pagos de extorsión, ya sea como consecuencia de ***ransomware*** o ataques *CryptoLocker*.
- El uso de cifrado por los delincuentes para proteger sus comunicaciones o los datos almacenados representa un reto considerable para la aplicación de la ley, por la dificultad de acceso a la evidencia. Este es un tema transversal que afecta a todos los ámbitos de la delincuencia.

Principales retos:

- Armonización Legislativa: avance en la tipificación de los ciberdelitos para la investigación legal de los mismos, que facilite el intercambio de información internacional y operaciones coordinadas.

Estadísticas e indicadores de ciberdelitos: es necesario disponer de información estadística de los ciberdelitos con base en la tipificación de los mismos, para generar estrategias y política pública.

- *Deep Web* y redes P2P: acceso libre de usuarios con navegación anónima. Gran mercado ilegal de operaciones: narcotráfico, armas, sicarios, pederastia, entre otros.

- CriptoMoneda: moneda virtual que permite realizar transacciones financieras en internet sin una autoridad central o bancos, permitiendo el anonimato en la comisión de delitos.

- Cultura cívica: uso responsable de los servicios de internet y aprovechamiento de los mismos para el desarrollo de un país.

- Identidad virtual: Proteger la identidad en el internet con mecanismos de autenticación biométrica, así como la protección de las grandes bases de datos con información de datos personales biométricos.

- Ataques cibernéticos cuyo objetivo es afectar las infraestructuras críticas informáticas e industriales de un país.

- Profesionalización del Cibercrimen. Una investigación sobre los mercados de robo de datos y la relación entre compradores y vendedores se destaca por su relevancia:
  - Los ciberdelincuentes implementan estructuras bien definidas y utilizan las mejores prácticas de mercadeo, tales como, encuesta de satisfacción al cliente, incluso dan de baja vendedores con opiniones negativas, son verdaderos negocios en línea que tiene sus departamentos de servicio al cliente.
  - La investigación resalta el reto al que se enfrentaran las autoridades, haciendo hincapié en que el coeficiente intelectual de los que dirigen estos negocios en la red está por arriba del promedio.

Redes de Bots. Es una de los mecanismos utilizados por los ciberdelincuentes para controlar de manera remota a equipos de cómputo con la finalidad de realizar actividades ilícitas tales como propagación de código malicioso, envío de correo SPAM, robo de información, ataques de denegación de servicio, espionaje, entre otros.
Colaboración Internacional. Establecer canales de comunicación para el intercambio de información oportuna. Ej. Convenios de colaboración COMJIB (Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de Ciberdelincuencia) y el convenio de Budapest.

Consideraciones finales

Prevención de delitos cibernéticos: se requiere un esfuerzo coordinado de todos los sectores de la sociedad, por ello el establecimiento y consolidación de asociaciones público privadas será un factor fundamental para consolidar la cultura de la prevención a través de campañas nacionales que sirvan como catalizador para incrementar la cultura de ciberseguridad, el cibercivismo. El reducir la brecha digital en términos de cobertura de servicios de internet a la par de civismo digital, promoverá la democracia digital y el fortalecimiento de las Policías Cibernéticas de las Entidades Federativas es una de las prioridades nacionales.

Investigación de delitos cibernéticos: a efecto de consolidar el sistema de persecución del delito se considera relevante contar con un código penal nacional que homologue las tipologías penales y con ello posibilite la armonización legislativa a nivel internacional, a través de la celebración de convenios y se fortalezcan los mecanismos de colaboración internacional (Tratados de Asistencia Legal Mutua – MLAT); así como el acceso transfronterizo de evidencia digital y la formación en materia de ciberdelincuencia para instituciones policiales, ministeriales y judiciales

Por último y no menos importante la gestión de incidentes cibernéticos: la implementación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos para los activos de información críticos a cargo de las Entidades Federativas, el sector privado y organismos autónomos que garantice la prestación de los servicios esenciales del país; la creación de los Centros de Ciberinteligencia para el intercambio de información de amenazas cibernéticas a nivel internacional, permitirá anticipar y atender de forma eficaz y oportuna los incidentes; la formación de Equipos de Respuesta Institucionales y Sectoriales y consolidación del CERT-MX; y la implementación de una plataforma de análisis de *malware* (MISP) para el intercambio de información a nivel nacional, así como la puesta en operación de un sitio Web del CERT-MX en gob.mx a efecto de fortalecer la proximidad ciudadana, no permitirá como nación ser un país más resiliente

ENTREVISTA

Nota: las entrevistas no son parte de la obra; se trata de información complementaria proporcionada por los expertos en seguridad para enriquecer su interpretación

GRUPOS DE TRABAJO DE LA INTERPOL PARA LA UNIDAD DEL CIBERCRIMEN DE LAS AMÉRICAS

Entrevista a Mariano Manfredi.
Interpol.

Severino Cartagena Hernández (DGC). SCH. Mariano: usted es un veterano no solo del trabajo en Ciberseguridad sino inclusive de su Institucionalización. ¿Es correcto que actualmente funge como vicepresidente del grupo de trabajo de Interpol de jefes de Ciberseguridad de las Américas?

Mariano Manfredi. MM. Así es. Bueno el grupo de trabajo de Interpol para la Unidad del cibercrimen de las Américas ya tiene más de 10 años, yo me incorporé hace 4 años y desde el 2019 me eligieron vicepresidente, junto con el Jefe de la Unidad Cibernética de Belice que es el presidente. Lo que se intentó institucionalizar fue la necesidad de creación, apoyo y entrenamiento de las capacidades policiales en investigación de Cibercrimen.

El grupo de trabajo no pertenece a Interpol en sí mismo, sino que es un grupo consultor de Interpol; celebra una o dos reuniones al año, que por la pandemia se volvieron virtuales, donde todos los jefes que atienden el cibercrimen exponen su problemática, sus necesidades, en cuanto a capacitación, operatividad y capacidades que tienen. Al final de las reuniones lo que se hace es una recomendación de Interpol, sobre lo que necesitan las Unidades de las América para seguir desarrollando sus capacidades.

Aparte se coordinan algunas operaciones a nivel regional; por ejemplo, el año pasado tuvimos la operación alianza que trataba sobre casos de venta de tarjetas de crédito, otra operación que fue en simultáneo con otros países en materia de Criptohaking, más una operación preventiva y de puesta en conocimiento de la problemática de investigación delictual. Ahí había un convenio con grandes empresas de Ciberseguridad, que eso es lo bueno del grupo de trabajo, lo que permite muchas alianzas del sector público con el privado.

Recién actuamos en el post crimen, en el post hecho, algo que está bien inculcado en el grupo de trabajo; el acercamiento del sector público con el sector privado, por eso generalmente en las reuniones participan empresas muy reconocidas en el sector de la Ciberseguridad. Hay un intercambio, un buen negocio donde todos ganan: nosotros del lado del sector público, porque nos nutrimos de la información y del día a día que ellos tratan, y ellos nos contactan por cualquier situación que le suscite y que necesiten en materia de colaboración de alguna agencia de la aplicación de la ley.

En el grupo no solo están los jefes de la Unidad de Cibercrimen, también es un poco ampliado; tratamos de acercar al sector de la justicia, a los fiscales especializados en cibercrimen, en reuniones de muy buen contenido donde los actores intercambiamos ideas, experiencias, capacidades, metodologías. Este último año el grupo estuvo mucho más dinámico, tuvimos reuniones casi todos los viernes donde invitamos al sector privado no solo de la industria sino que para redes sociales, a *Facebook,* a *Whatsapp,* a *Twitter*, en fin, se trata de ver cómo entre todos podemos cooperar y soslayar un poco la burocracia que hay en las comunicaciones policiales y en las comunicaciones con la justicia.

Acercándose esos tres actores en la misma mesa se logra mucha dinámica y se alcanzan buenos resultados con la rapidez necesaria que conlleva la investigación de un ciberdelito, no sólo se consigue trabajar en conjunto sino que se consigue recomendarle a la Dirección de Cibercrimen de Interpol un plan para el año venidero, del que surgen operaciones conjuntas, capacitaciones, coberturas de alguna necesidad puntual que la mayoría de los países necesiten. También hay mucha iniciativa para estandarizar protocolos y procesos más homogéneos de investigación, esa es la finalidad que tiene el grupo en sí.

SCH. Las ciberinvestigaciones transforman con su dinámica lo policial, inclusive el mismo sentido del resultado cambia de manera importante. ¿Qué nos diría usted al respecto para abundar en este detalle tan importante?

MM. Yo antes de entrar a la Policía Judicial de la Ciudad de Buenos Aires, en el ámbito del Ministerio Público, fui Policía Federal. El cambio de investigador criminal, de ese policía que antes salía a investigar a la calle y que se nutría de los informantes y los cateos, ha cambiado diametralmente: hoy el investigador policial necesita salir de los institutos de formación policial con cierta formación particular en el ámbito de la investigación de los ciberdelitos, no tiene que ser un analista de sistemas, pero sí una persona con los conocimientos básicos como para entender conceptos de la materia. Un ejemplo es el secuestro de la evidencia digital, otro, conocer la dinámica de los ciberdelitos, los actores.

Quienes hemos sido policías por muchos años nos damos cuenta que el cambio es abismal, más aún teniendo en cuenta que el 90% de los delitos tienen un componente que requiere cierta experiencia en el manejo de la digitalidad. Yo creo que el criminalista policial ya no es el último actor de la investigación como antes sí lo era. Hoy ese criminalista debería tener un perfil de investigador, porque no todo está resuelto en la forensia digital, hay muchas cosas que requieren una experticia particular. Un perito forense que sepa un poco de investigación en fuentes abiertas puede concluir su dictamen con

información más consistente y más certera. Y lo mismo para el investigador criminal, quien debe conocer los términos de la criminalística forense digital porque él es el que va a hacer valer esa prueba bien recolectada. Esto es algo de lo que los Institutos de Formación Policial adolecen en la materia.

SCH. Todo esto que está usted comentando hace a la idea de una Policía Científica que es un poco reflexionar en cómo la ciencia aporta a la actividad policial y como la misma actividad policial puede volverse científica.

MM. Tomemos de ejemplo las series policiales, la actividad de esos criminalistas va más allá del análisis criminalístico de la cuestión, fíjese como el concepto de un grupo interdisciplinario a partir de una tarea criminalística. O sea que el criminalista tiene su equipo, tiene su policía que va averiguar su caso en la calle, tiene su espacio de búsqueda en fuentes abiertas, tiene su espacio informático, ¿cómo se homogeneizó todo ese grupo? arrancando del factor criminalístico.

La Policía Científica debería ser eso, no solamente tener una función criminalística académica, más allá de la función del criminalista que es importantísima, creo que el factor de la criminalística y de la investigación hoy tienen que ir de la mano porque no todo está resuelto en la digitalidad: hay redes sociales nuevas, artefactos, sistemas computacionales nuevos que generan nuevos programas y que a su vez nos van a generar el hallazgo de nuevas pruebas, que es la finalidad. Yo creo que la actividad policial dio un vuelco de 180 grados a partir de la pericia digital. El perito forense informático necesita saber un poco más de solo el manejo académico informático de la cuestión.

SCH. Es ciencia pero no es ciencia académica, debe fluir en la interdisciplinariedad y también en esta colaboración múltiple en red.

MM. Usted conocerá la rigidez de un forense informático, pero hoy el mundo tiene una vertiginosidad que no podemos esperar que la industria provea de los elementos necesarios para hacer una pericia informática. No podemos esperar sus tiempos, debemos resolver los casos y eso encuadra un poco en el concepto de Cibercrimen de Andrés Velázquez, quien dice: "hay que pensar fuera de la caja". Al criminalista le cuesta mucho pensar fuera de la caja, fuera de los protocolos o de los procedimientos.

La criminalística trata por supuesto de usar procedimientos dentro del margen de la ley, que sean repetibles y que si están bien justificados, que si están bien descritos y si se puede comprobar lo que se hizo.

Pensar fuera de la caja y salir a innovar con herramientas hasta propias supone incorporar la innovación en los sistemas policiales, hoy se necesita mucha innovación y desarrollo.

SCH. Eso que usted comenta es muy importante porque aquí en la GN, la DGC tiene precisamente un área de innovación que también está desarrollando capacidades y sistemas para hacer frente a las nuevas modalidades del crimen en general.

MM. Si pero ahí de vuelta, no tenemos que caer en el error del pensamiento policial tradicional porque a veces las áreas de innovación hacen esto, desarrollan nuevas capacidades, y eso está bien, pero desde mi punto de vista un sector de innovación en el ambiente de la investigación criminal debería ser la rueda de auxilio de aquella investigación que se trunca por alguna barrera de desconocimiento de los actores. La innovación significa que debería haber un ***big bang*** permanente de cómo el criminalista y el policía pueden resolver una situación inédita con la ayuda del sector de la innovación, al que se encarga resolver ese problema, y pensar qué desarrollo llevar adelante para su aplicación a las situaciones particulares. Últimamente me han dicho que hay sectores de innovación que están desarrollando un predictor del delito, pero ese no es el problema que tienes hoy, el problema es tan básico que a veces esas oficinas de innovación lo que tienen que hacer es ser justamente una rueda de auxilio válida para la investigación criminal, son los que tienen que pensar soluciones y desarrollarlas, sobre todo cuando no están resueltas en el sector privado.

SCH. Ahora que comentó usted el tema del *Criptohaking*, escuchaba yo en otra parte que el problema del *Criptohaking* es que el delito no siempre queda bien configurado porque resulta que el equipo de cómputo fue solamente utilizado como medio para cometer un delito en otra parte pero no contra el interés del huésped, como una especie de cono de sombra. ¿Eso es correcto?

MM. Esa fue una gran discusión en la última reunión del grupo de trabajo presencial, con fiscales incluso; si hay el bien jurídico protegido está difícil de exponer, hemos llegado hasta a desarrollar teorías hablando con los fiscales y podría llegar a configurarse hasta un robo de la energía eléctrica que alimenta el equipo por un tercero; o bien puede ser un acceso no autorizado a un sistema informático porque el intruso no tiene la autorización necesaria para utilizar el recurso informático de la víctima o del equipo que está haciendo el minado ilegal. Podría ser una utilización indebida de una infraestructura informática que no necesariamente comprende grandes servidores, puede ser mi laptop.

Lo único que puede decirse es que todo ese minado no autorizado produce un corto de energía eléctrica, porque hasta ahora objetar el acceso ilegítimo al equipo de cómputo, la autenticación de la infraestructura informática es algo difícil de comprobar. Pero si en algún momento eso genera una demanda mayor de la energía eléctrica podría ser un robo a la energía eléctrica. Pero esto fue una tormenta de ideas que hasta me pareció gracioso.

Por eso la campaña que hicimos con el grupo de trabajo era más preventiva que otra cosa, era detectar y avisar a la víctima que está siendo víctima de *criptohaking*.

SCH. Precisamente esta dificultad para definir el bien jurídico, nos llevan a otro tema de discusión, que en el mundo del ciberdelito más nos vale proteger, prevenir y concientizar porque para investigar está más difícil. ¿Es así, hay un margen de improbabilidad en la solución de un caso? ¿Cómo se perfila el caso criminal en el marco de la Ciberseguridad?

MM. Yo tengo un pensamiento propio, yo creo que las agencias de la aplicación de la ley no son los organismos encargados de la prevención, yo creo que hay una dispersión de esfuerzos cuando un organismo de aplicación de la ley se mete en la prevención. No digo que esté mal, si nosotros hablamos del camino para que se produzca un crimen digital, hay muchos eslabones antes, que ya configuran subdisciplinas en sí mismas. La Ciberinteligencia es la primera disciplina que se debería manejar a nivel país o a nivel región, después en la cadena sigue la ciberseguridad, de modo que si la ciberinteligencia no pudo anticipar las nuevas modalidades delictivas hay que ver lo que está pasando porque Ciberseguridad que no la pudo parar, mitigar, mucho menos prevenir, hasta que terminó consumándose.

Es en este punto donde entramos las agencias de la aplicación de la ley, que a partir de ese eslabón deberían dedicar todo su esfuerzo, porque yo creo que no sé México pero por ejemplo Colombia tiene un departamento de prevención de ciberdelitos con muchos recursos dedicados a la prevención cuando es precisamente la investigación lo que nos exige dirigir nuestras capacidades a la investigación una vez que el delito se ha consumado. Considero que para la prevención hay otras áreas específicas que deberían de tener la capacidad necesaria para hacer campañas de prevención.

Una vez que se ha presentado un riesgo o un ataque, el CERT tiene que difundir un boletín de seguridad, pero antes el organismo de inteligencia tendría que haber dicho al CERT qué es lo que está pasando a nivel mundial, anticipando que en México y en Argentina nos va a pasar esto, para tomar las prevenciones necesarias y prevenir a todo el universo informático de lo que puede pasar. Yo creo que sí es necesario apostar por la prevención pero hacerlo

en el lugar donde tiene que estar, porque prevención después de lo que ya pasó, ya no es prevención propiamente dicha.

SCH. ¿No es un llamado a la protección.

MM. No digo que este mal, pero campañas publicitarias por parte de la policía o la justicia diciendo que están ocurriendo ciertos hechos, ¡está bárbaro! Pero en si es llamarlo prevención a eso.

SCH. En el trabajo de la ciberinteligencia usted ha comentado que las categorías forenses en lo que se refiere a los indicios, los vestigios del hecho criminal en este caso a nivel de forense digital tienen tanto valor como en el mundo físico, y por tanto la víctima tendría que ser muy cautelosa de no actuar cuando ha sido objeto de un ataque. ¿Qué habría entonces que decirle al público cuando se enfrenta a una situación de esta naturaleza?

MM. Lo primero es que denuncie, yo creo que tomamos conocimiento de una íntima parte de los que realmente ocurre.

SCH. ¿Hay mucha cifra negra?

MM. Más allá de cifra negra, dígame usted de las diez personas que conoce que les ha pasado algo, ¿cuantos fueron a denunciar a las autoridades? Entonces ahí si hay que concientizar, ahí si somos nosotros, la policía y la justicia, quienes necesitamos que nos den trabajo, porque teniendo más denuncias, sabiendo de más hechos podemos abordar los casos con mejor calidad y rapidez, de otro modo, cuando nos enfrentamos a un hecho desconocido nos tenemos que poner a estudiar, hacer consultas, aprender sobre la marcha.

En cambio, cuanto más nutridos estemos de los hechos que varían día a día, porque todos los días surge un *modus operandi* nuevo, por tanto resulta válido hacer esas campañas, decir a la gente que si le pasa algo, por más íntimo que sea lo denuncie; denunciar no cuesta nada y se puede hacer por cualquier medio, *twitter*, una página web, un *WhatsApp,* o la policía.

Hoy la accesibilidad de la justicia tiene muchos caminos, ya no es como antes que tenías que ir a una fiscalía o una comisaría; hoy hay que concientizar a la población de que denuncie, aunque sea algo íntimo, aunque el daño patrimonial sea menor o no se haya consumado aún, yo creo que toda esa información nutre al investigador criminal, le ayuda a estar al día en los modus operandi; poder entender por qué por ejemplo, hace dos meses en Ecuador hubo una gran filtración en uno de los bancos más grandes de Ecuador, está

bien, en unos días no sucedió nada pero Ecuador estaba bajo una campaña de asedio, de phishing con todos esos datos de las filtraciones.

Sin embargo, la gente denuncia muy poco. Si la gente hubiera empezado a dar aviso a las autoridades de lo que estaba sucediendo les hubiera dotado de mayor claridad para poder llevar a cabo una remediación certera, rápida y eficiente. Yo creo que lo más importante es decirle a la gente que denuncie.

Lo segundo es que si te pasa algo, no hagas nada más que denunciar, para eso estamos nosotros que somos los profesionales en la materia, porque también te puedes encontrar que la víctima ha alterado la prueba o se ha hecho parte del delito sin darse cuenta al quererse defender o queriendo mitigarlo erróneamente, por ahí termina hasta el propio denunciante cometiendo un ilícito.

SCH. ¿Cómo encubrimiento o borrado de pruebas?

MM. El no denunciar es ya una forma de encubrimiento.

SCH. Pero sin embargo los informáticos no parece que estén muy receptivos a la posibilidad de cometer un error así, o que los pueda llevar a una situación peor que la que quieren remediar.

MM. Yo creo que, por el contrario, y basado en la experiencia de esto del acercamiento con el sector privado, hoy las grandes empresas de la Ciberseguridad también cambiaron su dinámica, no quieren perder productos ni clientes, por lo que han adoptado la metodología de atacar al atacante, hackearlo, sin darse cuenta que al hacerlo se la pasan cometiendo algún tipo de ilícito.

SCH. Uno se imagina las bandas del crimen organizado, su organización, su territorialidad, su esquema de lealtades, etcétera; y cuando piensa uno en la criminalidad cibernética más bien imagina uno como lobos solitarios, como genios incomprendidos o justicieros o reivindicadores. ¿Cómo es la organización criminal?

MM. Yo las comparo con una empresa multinacional muy bien organizada y estructurada, en el crimen organizado cibernético no hay un solo lobo solitario. La dinámica del ataque cibernético empieza con intentos persistentes de ingresar a los sistemas de una gran empresa, que factura millones de dólares y que tiene miles de clientes. El grupo agresor se introduce a los sistemas informáticos, se queda adentro, hace inteligencia e información

y luego ve qué delito se va a cometer –porque los hackers no cometen los delitos, solo hacen el ataque persistente.

Cuando hablamos de organizaciones de ataques persistentes, estamos hablando de verdaderas infraestructuras criminales. La inteligencia lo que hace es saber qué delito va a ser más redituable que otro, empieza la filtración de información al grupo que después se va a encargar de cometer el delito porque ellos son especialistas en otras cosas.

SCH. Hay una clara división del trabajo entonces.

MM. Claro después está el grupo que va a llevar a cabo la estafa, esos son expertos en distintas técnicas en intrusión a servidor del correo, el ***man in the middle***, que consiste en engañar a un usuario para que confíe en un intermediario que a la postre resulta un delincuente informático. Pues bien, para lograrlo hay que sacar una radiografía de una gran empresa para saber qué actor de esa empresa habla sobre qué tema, cómo habla, qué términos utiliza, ahí hay mucha inteligencia respecto al armado de ingeniería social; los ingenieros sociales ejecutan el engaño mimetizándose con los sitios que frecuenta el usuario, que pueden parecer clientes o proveedores, hasta lograr que se desvíen millones de dólares, después empieza otra etapa que es la del dinero, hay que abrir la cuenta bancaria, allí necesitan otros actores, no tanto que sepan de informática, más bien que sepan de formación de sociedades mercantiles en países donde no es muy común formar una sociedad. Desde la apertura de cuenta bancaria necesitas una infraestructura compleja basada en el conocimiento económico financiero.

Después tienes el último rango que son las "mulas", nadie va a una ventanilla a depositar un millón de dólares, o sea que para cada tipo de delito hay un conjunto de actores especializados y cuando las investigaciones te van abriendo se cae en la cuenta que esas mismas organizaciones criminales buscan empresas dedicadas a giros específicos, la que ataca empresas marítimas se especializa en empresas marítimas, lo mismo la que actúa en el sistema financiero. Por ello yo creo que hay quizás un cartel mucho más repartido geográficamente.

Bueno la multijurisdiccionalidad que hay en cualquier delito cibernético hoy, es una organización muy grande, lo que imposibilita una buena investigación.

SCH. Entonces hay que trabajar también con mucha dinámica y con un buen enfoque hacia la cooperación, estar pendientes de lo que otras áreas nos pueden dar.

En México por ejemplo tuvimos una experiencia con el *WannaCry*, ejerció una afectación muy limitada por que oportunamente el CERT australiano nos puso sobre aviso de donde estaba la vulnerabilidad y como nos podía afectar para hacer la divulgación y actuar oportunamente para detenerla, de manera que el *WannaCry* tuvo un impacto marginal en México, sin embargo en otros países si tuvo mucha repercusión.

MM. Ese un ejemplo del eslabón de la cadena que yo comento, ahí prevaleció la prevención de manera rápida pero ¿qué falló, que no vimos cuando pasó lo del *WannaCry*, cuál era su finalidad? Falló la inteligencia, la finalidad no era el cobro de algún rescate, más bien fue disparar el precio de *BitCoin*, entonces si todos los organismos encargados de aplicación de la ley hubiéramos tenido información de inteligencia, no solo de prevención como la que mandó el CERT australiano, ya hubiéramos actuado con más celeridad y sabiendo a donde estaba direccionada la campaña del *WannaCry*, podríamos haber prevenido, induciendo a los afectados a no pagar porque no era esa su finalidad.

SCH. Es un ejemplo interesante para dar cuenta de los alcances y limitaciones de las actuales cadenas de trabajo en la investigación policial.

MM. Yo creo que con una buena información de inteligencia todos hubiéramos actuado con gran celeridad a su vez llevando tranquilidad, acuérdense cuando quiere prevenir con campañas de prevención lo que genera es caos, genera miedo, genera temor colectivo, genera un montón de cosas.

SCH. Entonces propicia el fenómeno de la profecía autocumplida, es decir; ante el pánico y el miedo cometes más errores y probablemente te vuelves más vulnerable ante la organización criminal.

MM. Claro, todos fuimos atrás del doble factor de autenticación hasta que apareció el sim swap, (o clon del código SIM del usuario de un equipo) ¿y ahora, que hacemos?

SCH. ¿No funciona el doble factor de autenticación?

MM. Si te hago *sim swap* ya tengo todos tus dobles factores de autenticación para la identificación de todas las redes y para hacer un montón de cosas. Para mí este recurso de la delincuencia es el resultado del doble control de autenticación, el *sim swap* no tiene otra cobertura, ¿para qué quiero robar tu línea telefónica? para robarte *whatsapp*, el *Facebook*, el *instagram*, tu

cuenta bancaria. El fondo del *sim swap* es el robo del doble factor de autentificación.

SCH. Entonces el doble factor de autenticación no es la panacea, también puede estar expuesto. Que interesante porque esto desafía nuestra sabiduría convencional y también las medidas preventivas que se sugiere a la gente tomar en la prevención del delito electrónico. Entonces el doble factor de autenticación también puede generar una nueva vulnerabilidad.

MM. Yo creo que el *sim swap* nace para el tema del doble factor de autenticación.

SCH. Entonces seguimos rodeados por la cibercriminalidad.

MM. Yo creo que sí, ellos sólo piensan en eso. Volvemos a las estructuras criminales, para mí están muy bien organizados, están permanentemente produciendo inteligencia de nuevas vulnerabilidades y nuevos *modus operandi* que llevan a cabo otros. Este es su negocio, ellos investigan, encuentran vulnerabilidad o encuentran *modus operandi* nuevo y lo venden a una organización, yo no creo que sea un lobo solitario que encuentra algo y hace algo por que sí.

Hay mucho dinero, el costo que tiene llevar adelante un BIC con todos los factores que tiene un BIC es interesante. Por eso a veces me llaman y consultan porque hubo una estafa y que necesitan depositar 60 mil dólares, y digo no; eso es algo local porque por 60 mil dólares nadie vulnera una infraestructura para un BEC.

SCH. Pareciera que cobran demasiado poco.

MM. Todos los actores algo se tienen que llevar. Al final del día es su trabajo.

SCH. Hay mucha estrategia en ello.

MM. De hecho hace muchos años fui al NECMEC y en una reunión charlando no recuerdo con quien me contaba esto nosotros nos encontramos con un *groomer* (el pederasta que se encarga de enganchar a los menores con propósitos de abuso para la pornografía infantil) pero el fondo en cuestión son galpones (bodegas) llenos de gente con el *groomer* haciendo *packs* para vender.

SCH. Y mucha gente inclusive inocente se ha metido también es ese compromiso de los packs para obtener un poco de dinero.

MM. Yo hablaba de galpones con 200 personas en la India haciendo *grooming* para armar *packs* para consumo personal; nosotros los policías nos encontramos con el *groomer* torpe, con el que incurre en algún error, pero el 90% son organizaciones que se dedican a recolectar imágenes de menores para la venta, no para consumo propio. No hay duda que es crimen organizado y hay que enfocarlo como tal, y hay veces que nosotros por querer resolver el caso nos quedamos con el crimen local y no pensamos más allá de nuestra frontera.

SCH. Eso nos devuelve a la pregunta del principio: cómo es que la investigación cibercriminal ensancha las fronteras de lo policial y obliga a tener un mayor enfoque en una formación colaborativa y en un rediseño de las estrategias de investigación.

MM. No hay más fronteras geográficas. La fronteras que tenemos hoy son de las empresas de servicios, no son geográficas, hoy hay que traspasar la frontera de *Facebook*, de *Google*, de grandes prestadores de servicios electrónicos que son los que tienen la información que nosotros les damos, la frontera geográfica, la cooperación de justicia entre países es superficial; hoy la frontera que necesitamos pasar son las empresas de servicio electrónico que cuentan con la información que nosotros necesitamos para poder investigar los crímenes que se cometen en nuestra jurisdicción y en la de los países que están involucrados. No hay más fronteras geográficas, esto de la pelea por la jurisdiccionalidad de los datos, de quién es el dueño del dato, el dueño del dato *Facebook*, el dueño del dato *Google*, son para estados ya algo impuesto.

SCH. La misma idea de jurisdicción cambia.

MM. Yo les decía a *Facebook*: ustedes quieren tener más soberanía que un estado, ¡cómo puede ser! Y es así, en realidad la soberanía es su usuario que es el negocio de ellos.

SCH. Ahora la privacidad es la soberanía.

MM. *Apple* no vende más teléfonos, vende privacidad, teléfonos lindos, el producto es la privacidad el teléfono es el medio, hay que hacerlo lindo porque me gusta tener un teléfono lindo, vistoso, caro, que sea rápido. Pero el producto es otro.

SCH. ¿Y si esta en caja negra *Apple*, es efectivamente tan impenetrable?

MM. Yo he ido a presentaciones de empresas que ofrecen vaciarte el iphone con un solo clic, así que no hay privacidad.

SCH. Otro mito que vuela en pedazos.

MM. Pero no me lo contaron, lo vi, lo probé, existe y ahí están los que lo tienen. Otro mito, el *WhatsApp* es indescifrable, si mientras está en el aire pero cuando está en tu teléfono las llaves de tus aplicaciones están en tu teléfono. Cuando aterrizó en tu teléfono ya no lo es más.

SCH. Por tanto está tan expuesto como cualquier otro recurso o archivo que está en tu teléfono.

MM. Sólo hace falta que este dentro de tu teléfono ya con eso basta.

SCH. Con más razón hay que pugnar por una capacidad y una organización que persiga con eficacia estas expresiones de la criminalidad dado que el avance tecnológico también plantea una evolución de las vulnerabilidades que también se ven sometidas las personas por el uso de la tecnología.

MM. Si, pero las empresas son inteligentes, qué difícil va a ser para los estados ir contra la privacidad de las personas, porque cuando nosotros reclamamos algo a *Facebook*, a *Apple*, ellos toman como bandera, como producto principal la privacidad, lo que equivale a la muralla china, en legislación va acompañada de providencias contra violar la privacidad de los usuarios, cuán difícil va a ser conseguir una herramienta legal para vulnerar el derecho a la privacidad de las personas, entonces hicieron un gran estudio de marketing y un gran trabajo las empresas. Por eso sostengo que el producto de esas empresas es la privacidad. Y no solo porque las personas buscan privacidad, sino porque es lo más difícil de soslayar incluso legalmente. De hecho, hay tres conceptos donde levantan la barrera fácilmente: un ataque terrorista, un riesgo inminente de vida o un riesgo físico a menores de edad, si uno se sale de esos tres carriles se estrella con la muralla china, cuyos creadores cuando la levantaron le dejaron tres puertitas.

Yo me imagino que han cambiado el modelo de negocios. Hoy todos compiten por la garantía de privacidad, no importa si la interface es fea o linda solo se busca la privacidad. Es el gran nicho de negocio. Nuestras vidas están en las comunicaciones.

SCH. La perspectiva de la Ciberseguridad ofrece también un nuevo prisma desde donde ver la más corriente cotidianidad hasta los más grandes cambios estratégicos en el mundo.

MM. Por ejemplo en reunión con el enlace de la fuerza de la ley de Uber, un ex policía, ustedes pueden recibir información de Uber para resolver un atentado, sí pero me preguntan qué chofer de Uber hay en todos lados, que chofer de Uber había alrededor de una coordenada y ese tipo seguro que llevó a alguien, vio algo, y el policía convencional no tiene eso en la cabeza, no pasa por su mente ni buscar testigos en redes sociales, mandar un *twit*, ¿alguien vio algo en este accidente?, necesitamos localizar al conductor, no vamos por la burocracia, un comunicado de prensa, la televisión, la radio que ya nadie mira televisión ni escucha radio y seguimos usando los canales convencionales.

Lo que hizo Europol con el reconocimiento de objetos de imágenes de explotación sexual infantil, esta almohada es de tal hotel que queda en tal lugar, entonces las instituciones también tienen que poner rigidez y ver a través del prisma que dices, la nueva realidad.

SCH. Es con ese horizonte abierto el que dejaríamos a nuestro lector pendiente, al borde del asiento para esperar el siguiente capítulo. No hay espacio para la certeza, cualquier forma de tranquilidad nos remite a una zona de confort que como todas es absolutamente ilusorio.

MM. Pero aparte no nos podemos negar al avance tecnológico, lo que pasa en el mundo digital tiene consecuencias en el mundo real, y lo que pasa en el mundo real tiene consecuencias en el mundo digital, pero ya se mezcló.

SCH. ¿Qué ha hecho este año el coronavirus con esta mezcla de la realidad material y la virtualidad?

MM. Es invisible para nuestros ojos. Yo creo que la pandemia ha generado muchas oportunidades al cibercrimen porque nos empujó a la digitalidad; yo por ejemplo para no tocar dinero, uso "Mercado Pago", y como yo así millones de personas, más la gente que no estaba preparada para la vida digital que se vio obligada a utilizarla: el jubilado, el retirado, el pensionado, la persona mayor que tiene que lidiar con el banco en línea, que no tiene idea de cómo hacerlo; todo eso cambio lo ordinario.

La guerra cibernética que no vemos para la gran competencia de los laboratorios mundiales y los ataques permanentes, la digitalidad nos empujó a eso, ya no más mundo digital y real, hoy vivimos la digitalidad, tomamos el transporte pagando con una tarjeta, tiene circuito cerrado de televisión, el

vehículo tiene geoposicionamiento; ni qué decir de los automóviles, estamos rodeados de digitalidad, no hay manera de eludirla.

SCH. Será uno de los factores que condicionarán este hecho de que la normalidad nunca volverá a ser la misma.

MM. Nunca volverá a ser la misma, para las nuevas generaciones, para bien; para las generaciones intermedias nos aguantamos pero para las generaciones grandes es un cambio radical. Es un choque generacional tecnológico de esa talla, nada más que ahora va mucho más rápido, y nos acostumbramos al cambio tecnológico porque todos los días nos pega algo nuevo.

La conclusión que te daría es que no existe más la zona de confort, ahora tenemos que estar en un estado vigilante permanente, estar más atentos; no podemos pretender que se sabe todo; nadie sabe nada, no hay más expertos en ninguna materia, el avance es tan vertiginoso en todas las áreas que decir que eres un experto en algo, es imposible. El cambio del conocimiento es permanente.

DINÁMICA Y TRANSVERSALIDAD DEL CIBERDELITO

Entrevista a Adrián Eduardo Acosta. Interpol.

Severino Cartagena (DGC). (SCH). Adrián, tú que estás en Interpol, donde tienes una participación importante en la formación y capacitación policial en estos temas de ciberseguridad, quisiera captar tu sensibilidad respecto de temas que están muy vivos en este momento.

Adrián Eduardo Acosta. (AEA). Si, yo tengo 16 años en Interpol, Secretaría General, más 9 años en Interpol Argentina, entonces son 25 años en completo con Interpol.

SCH. Los mismos 25 años que lleva el internet en nuestras vidas, ¿no?

AEA. Si, más o menos.

SCH. Y en ese periodo has sido testigo y quizás seguramente actor en las diferentes etapas de evolución del ciberdelito y por tanto de las necesidades de seguridad informática en el mundo. ¿Cómo podrías resumir en etapas este compromiso creciente con la ciberseguridad en general y con el ciberdelito en particular?

AEA. Evidentemente cuando aparece internet y empieza a evolucionar y la gente lo empieza a utilizar cada vez más, en principio para un tema de entretenimiento o laboral, con el tiempo evolucionó y se transformó en un tema cultural, de cambio de costumbres, al grado que internet ha influido en el cambio de costumbres en la sociedad global. Eso ha implicado también que los delitos cada vez sean más complejos y cada vez más prioritarios. Durante muchos años se habían tratado como delitos prioritarios, como el narcotráfico, la trata de personas, el terrorismo. Pero desde el año 2001 es un parteaguas, ya que a partir de entonces la ciberseguridad ha ido tomando relevancia creciente a nivel mundial. Al principio el cibercrimen era considerado un delito menor en general y cuando yo empecé a trabajar el tema, en Interpol había oficiales de otras áreas delictivas y todavía no se daba demasiada importancia porque el del Cibercrimen era un dominio que correspondía a los delitos de alta tecnología.

Sin embargo, en la medida en que fue pasando el tiempo, el cibercrimen fue cobrando cada vez mayor relevancia hasta afectarnos a todos. Dicho en otros términos, empieza a ser transversal a todas las áreas de investigación criminal;

entonces no solamente se habla de un cibercrimen puro, sino que se vuelve transversal en temas como los delitos económicos, al igual que los delitos contra menores, y desde luego el ciberterrorismo, que se implanta también como un área importante. Con el tiempo, la trata de personas también ejerce su influencia a través de las redes sociales.

De modo que todos los delitos empiezan a tener un contexto en el área tecnológica, entonces desde distintas perspectivas, como el lavado de dinero, lo mismo el narcotráfico o la corrupción, que antaño se investigaban de manera convencional dentro del crimen organizado, para incorporar ahora también el área de la tecnología. Piénsese tan solo el lavado de dinero, en el que las criptomonedas o criptoactivos que cada vez tienen más valor y cada vez también tienen más importancia. Bueno, pues el movimiento de los activos toma la misma relevancia en el ámbito del crimen organizado y el narcotráfico.

Entonces cuando yo empecé a trabajar en el área del Cibercrimen, el contexto era mucho menor y menos prioritario; pero ya en 2010, y sobre todo en 2011 y 2012 empieza a tomar una prioridad a nivel mundial hasta alcanzar hoy en día su lugar entre los delitos más prioritarios. A pesar de este comportamiento del cibercrimen, sin embargo todavía hay países de nuestra región e incluso países con menos nivel de desarrollo que no ven el cibercrimen como una amenaza, privilegiando otros delitos a pesar de que muchos otros delitos que todavía se consideran amenazas tienen un componente tecnológico detrás que demanda desarrollar capacidades de investigación y, habría que añadir, la investigación legislativa dirigida a tipificar los delitos para poderlos combatir correctamente.

SCH. Suele decirse que lo específico de la ciberseguridad son los ataques cibernéticos y, en general, los delitos o situaciones que son específicos al mundo del ciberespacio. ¿Cómo han evolucionado estos delitos, cuáles son sus formas más características que ustedes han encontrado sobre todo de este último año tan peculiar?

AEA. La ciberseguridad es un área que también está recibiendo cambios, la ciberseguridad se dedica de una forma proactiva a darle seguridad a los sistemas, de que nadie se va a introducir, nadie va a introducir un *malware* y muchas otras cosas más allá de los ataques cibernéticos. Sin embargo, esos ataques siguen teniendo objetivos delictivos en diferentes áreas, como pueden ser: robar información, secuestro de una máquina para pedir un rescate y

muchos otros más, cuya proliferación introduce cambios en la forma de entender la ciberseguridad.

Me explico, ya no solamente se puede pensar en el cibercrimen puro, en esos delitos que afectan al normal funcionamiento de los sistemas informáticos, sino que también, empiezan a tener objetivos delictivos diferentes ángulos; por tanto, la ciberseguridad no solamente se enfoca en el objetivo de mantener funcionando los servicios informáticos, un enfoque que a todas luces resulta parcial. Ahora se trata de desarrollar un objetivo general; por lo tanto, hay que estar preparados para todo, más importante aún es el hecho de que por más que los cibercrimenes puros tienen que estar legislados, la verdad es que los criminales van evolucionando y van creando nuevos métodos que a los países se les hace difícil encuadrar legalmente y ese es otro desafío: el de estar actualizando la legislación constantemente. Por ejemplo en mi país, Argentina, al igual que muchos otros de Latinoamérica una modalidad delictiva "el *criptohaking*" resulta muy difícil de encuadrar, debido a que consiste en instalar un *malware* en una página web o en un *router* para que las personas que abran esa página empiecen a hacer minería de datos o a resolver un algoritmo criptográfico para criminales que quieren obtener algún criptoactivo. La víctima se convierte en cómplice involuntario de un delito que resulta muy difícil de encuadrar ya que, a pesar de que está claro que es algo ilegal, no está claro cuál es la ilegalidad; entonces tenemos que, además de asegurar los servicios para que ese *malware* no sea instalado, a través de la ciberseguridad también se debe tener un contexto mucho más amplio del objetivo.

SCH. Y si existe un amplio vocabulario de expresiones que hacen precisamente a la comisión de estos delitos, el *phising*, el *malware*, el *ransomware* son expresiones que de inmediato nos remiten a la realidad de la ciberdelincuencia. ¿Y cómo se comporta la ciudadanía ante estas realidades del fenómeno delictivo que tarde o temprano pueden comprometerlos?

AEA. Efectivamente existe ya un nuevo vocabulario en todo esto y realmente se está aprendiendo muchísimo todos los días, y no solamente la sociedad en general o cuando se es víctima y se aprende directamente del momento, sino que también los mismos aplicadores de la ley empiezan a tener una reeducación de toda esta nueva variedad delictiva; entonces, las policías, los fiscales, los jueces, en tanto organismos de aplicación de la ley, empiezan a aprender un nuevo vocabulario y a entender todo este nuevo contexto. Pero, además, el asunto no se queda solamente en aprender un vocabulario y que significa su contenido en una amplia variedad de delitos como pueden ser el *Grooming,* el *Phising,* el *Pharming,* sino que ahora puede verse que hay aspectos técnicos que se enseñaban ingeniería y áreas técnicas, y que hoy ya es común para todas las áreas que participan en la investigación criminal y en la aplicación de la ley, por ejemplo: que es una Dirección IP, de eso antes solo se hablaba en áreas tecnológicas, mientras que hoy lo tiene que saber todo el mundo, desde la abogacía hasta las áreas humanísticas y sociales.

En resumen, la terminología tecnológica ya forma parte de la sociedad, no es un vocabulario exclusivo del área tecnológica. A mí me ha tocado tomar exámenes en universidades a profanos del área tecnológica que sabían perfectamente qué era una dirección IP, un bite, terminología que de ser exclusiva de las áreas precisas de informática ahora representan conocimientos generales. Al respecto, estamos conscientes de que los organismos de la aplicación de la ley dentro de sus academias necesitan tener ya un conocimiento de esta tecnología y de estos delitos.

Estamos conscientes de que al policía desde la academia, desde la primera instrucción que recibe, hay que enseñarle cómo incautar un teléfono, un reloj inteligente, una computadora y demás dispositivos de almacenamiento electrónico. Como antaño enseñábamos a los estudiantes a incautar un arma introduciendo un lápiz, ahora hay que enseñar también como incautar un dispositivo de almacenamiento de un equipo electrónico.

En resumen, hay todo un cambio cultural en la sociedad y en los organismos de la aplicación de la ley y que hay que empezar a aplicar.

SCH. Cada vez más el punto crítico de atención es precisamente lo cotidiano, lo que tiene que ver con la convivencia, lo que vive el público día a día, cada persona, la manera de relacionarse con la tecnología se vuelven crípticos precisamente para tener una buena seguridad informática. Sin

embargo, este último año las personas han experimentado como nunca un contacto no solo frecuente sino vital con la tecnología y eso las expone a situaciones donde se pueden exponer a que sean víctimas de un delito. ¿Cómo ha sido esto desde la perspectiva tuya y de la institución a la que representas?

AEA. Evidentemente esta situación de pandemia y aislamiento en algunos países ha potenciado el uso de estas tecnologías, hasta la gente que no quería ser parte de estas tecnologías tuvo que adaptarlas y usarlas porque era necesario; había gente que no quería tener redes sociales ni hacer videollamadas; sin embargo, esto ha hecho que la sociedad en general se vuelque para eso. Por ejemplo, hoy al acto de festejar un cumpleaños a través de la plataforma de videoconferencia, le han puesto nombre "Zoomcumpleaños", incorporándola de este modo a su vida normal.

El caso es que mucha gente no estaba preparada y consciente de los riesgos que se corren en el uso de la tecnologías de uso cotidiano, incluso de las plataformas de videoconferencia, lo cual, sumado a eso los criminales también vieron esta oportunidad que ya se dedicaban a hacer este tipo de delitos, a tener más gente conectada, tener mucha más gente en línea mucho más tiempo vieron una gran ventana de oportunidad y empezaron a cometer más delitos entonces realmente se vieron incrementado los delitos cibernéticos en el año pasado y por supuesto se han mantenido este año también, el home office también ha potenciado eso y básicamente el que la gente estuvo mucho más tiempo conectada ha potenciado los crímenes, entonces en general a nivel mundial han crecido y hablamos de delitos como el phising que se ha mantenido presente durante el año pasado y este año y que han crecido en forma exponencial.

SCH. Ese es el tema, el crecimiento exponencial de estas situaciones delictivas, en México se ha vivido con el delito de abuso sexual infantil o con la pornografía infantil que desde 2019 a 2020 creció en más de 16% por ejemplo. Desde 2010 no ha dejado de crecer. ¿Cómo es la incorporación a esta modalidad delictiva y cómo qué perfil destacarías tú del ciberdelincuente?

AEA. en este caso en particular de lo que es material de abuso sexual infantil por supuesto tiene un perfil definido, el pedófilo, el abusador, otros tipos de delitos también tienen perfiles pero esos ya son delitos económicos, buscan ganancias económicas en este caso de material de abuso sexual infantil no se buscan ganancias económicas sino se busca obtener estas imágenes y nuestra

región particularmente fue la única región que destacó el crecimiento de este delito, entonces realmente es algo muy llamativo, tenemos que prestarle atención y un área prioritaria para no solo detener a estas personas que distribuyen este material sino también a los que producen y recatar a las víctimas.

Entonces, el nuevo cambio de paradigma que está haciendo Interpol no solamente es arrestar a quien distribuye este material, sino también rescatar a la víctima es una prioridad para nosotros, detrás de esas imágenes existe una víctima y hay que rescatarla de ese ambiente y de ese abuso.

SCH. En una plática que diste por ahí por octubre y que recogió oportunamente YouTube, decías que los ciberdelitos son los que más crecen a nivel global. ¿Cómo podemos aterrizar esta idea para poder ampliarla más?

AEA. El cibercrimen es el delito que más crece a nivel mundial, evidentemente; primero por las estadísticas pero por qué tiene que ver con la sociedad, la sociedad cada día se vuelca más por usar la tecnología y ha habido un cambio cultural, un cambio de comportamientos del ser humano en general por ejemplo; buscar pareja hoy se hace a través de plataforma, antes había que ir a bailar, había que salir a tomar algo, hoy en día ni siquiera eso, los jóvenes y no tan jóvenes buscan pareja a través de plataformas del teléfono, y van seleccionando a su pareja como si fuera una galería comercial; entonces esos grandes cambios culturales que no nos hemos dado cuenta pero que los estamos viviendo es lo que produce que también los criminales empiecen a cambiar.

Por otro lado, la ventana de oportunidad para la delincuencia ha dejado de estar en la puerta de un banco, porque ya hay medidas de seguridad perimetral para evitar que se robe a la gente que va a un banco a retirar dinero, entonces la ventana de oportunidad la tienen sin causar mucha violencia a través del delito tecnológico. De hecho, la información personal que guardamos nosotros, al igual que la información de las empresas se han transformado ambas en un activo muy importante para el ser humano, eso produce que la información sea como oro para los delincuentes. Hay varios factores que influyen en esto, sumados a que hoy vivimos los efectos de un cambio que inició en 2009. Hace 11 años, la internet no manejaba elementos de valor sino solo información; pues bien, ahora la información es un elemento de valor para la gente, hoy en día existen los criptoactivos como el BitCoin y esos

son elementos de valor que se utilizan a través de internet, entonces también se suma eso a todo este ámbito delictivo.

SCH. El valor material de la información en internet ha cobrado valor por sí mismo.

AEA. Al grado de que las empresas prefieren quizá que les roben dinero a que les roben información, los delincuentes saben eso y por eso este crecimiento del cibercrimen. También hay otros temas que a causa del vacío legal que dificulta tipificarlos, reciben multas o condenas leves o inexistentes. Esa es realmente esa ventana de oportunidad que aprovecha la delincuencia: la falta de legislación, a lo que se suma la falta de una cooperación internacional que impida a los cibercriminales cometer un delito en un país y estar en otro. Normalmente un ciberdelincuente no va a cometer un ciberdelito en el país en el que reside.

Tenemos que empezar a cerrar esa ventana con concientización, con prevención y para los organismos de aplicación de la ley con mecanismos de cooperación internacional mucho más efectivos.

SCH. ¿Cómo concientizar al público?

AEA. La verdad es una tarea titánica de concientizar a la sociedad global, se necesita la ayuda de todo el mundo, de los que ya sienten que saben cómo cuidarse hasta los que no saben; realmente hay que ser escéptico pero no paranoico; usar la tecnología adecuadamente y estar atento a que si te llega un correo con un adjunto que no sabes de dónde viene lo mejor es no abrirlo. Pero, al mismo tiempo, no dejar de usar el correo; es como usar el cajero automático, yo me fijo a qué cajero voy a entrar, si veo algo sospechoso y ponerme atento a todo eso; pero tengo que sacar dinero, no puedo ser tan paranoico de no acudir a un cajero electrónico. Se trata de ser un poco más precavido con la tecnología y saber cuáles son los riesgos que ya sabemos que existen.

El desafío está en que los estados, los organismos y la empresas privadas se comprometan con la concientización, porque el estado es un partícipe necesario importante pero también el sector privado debe tomar conciencia de lo sucedido, desde todos estos ámbitos hay que trabajar.

SCH. ¿Cómo les fue en su campaña de prevención, qué medios usaron y qué contenidos y cuál fue el resultado en el agregado de la prevención y la concientización?

AEA. Saber cómo nos fue realmente es muy difícil de calcular, si tuvimos éxito o no, me imagino que ya teniéndolo con una potencial víctima que haya tomado conciencia, ya es un éxito pero uno quiere tener un éxito mucho más profundo; sin embargo, nosotros hicimos campañas en varios ámbitos que duraban una semana y tuvimos el apoyo de las fuerzas policiales y de la aplicación de la ley de cada país.

Interpol, Europol, hicieron mucho de estas campañas pero siempre en inglés en este caso la hicimos en español y en inglés para los países del Caribe y de América y realmente quienes nos ayudaban a distribuir estas campañas eran los organismos de la ley de cada país. Hicimos algunas infografías y un video por cada uno de los delitos que hemos hecho de esta campaña; mínimo hay dos infografías y un video por cada campaña y la idea era en ese mes de la Ciberseguridad poder estar presentes y concientizar de esos delitos, sin embargo, todavía se siguen difundiendo, por más que interpol haya hecho la campaña de una semana no quiere decir que se ha terminado ahí, el éxito sería que esos videos, esas infografías sigan circulando, sigan ayudando a tomar conciencia y prevención de esos delitos.

Algo más, en el ámbito de la prevención, nosotros como organismo de aplicación de la ley o como policías no estamos muy acostumbrados en nuestra región latinoamericana a hacer prevención, nosotros somos más reactivos e investigamos los delitos una vez que ocurrieron; tratar de localizar a los delincuentes y de alguna manera hacer cumplir con la ley; sin embargo, ese concepto también está cambiando un poco porque ya el policía necesita ser más proactivo en esos delitos cibernéticos, quizás en otros delitos es imposible pero en delitos cibernéticos.

Conclusiones

AEA. El núcleo central de cada fuerza policial tiene que ceder el uso de esa tecnología y rodeando esa tecnología, que puede ser la base de datos, el *Big Data*, el *machine learning*, rodeando ese núcleo central tienen que estar la investigación, la inteligencia, la prevención, la capacitación más y más lejos, la logística, por supuesto que la administración, el bienestar de la gente, pero el núcleo ya no puede seguir siendo algo secundario, sino que tiene que ser la tecnología y ya no se puede considerar tecnología como un satélite fuera de todo ese núcleo central de la policía como algo de apoyo, sino que tiene que ser algo central, a todo esto de las fuerzas policiales.

SCH. Pues muchísimas gracias por tu tiempo para esta entrevista. Seguimos en contacto para el aterrizaje documental de tus conceptos a fin de nutrir esta obra que desde luego va a tener mucha relevancia al integrar este tan valioso testimonio.


GUARDIA NACIONAL
JUSTICIA Y PAZ

Guardia Nacional y Policía Científica
Estudios sobre Ciberseguridad, Criminalística,
Innovación y Política Criminal
Primera edición
Este libro se terminó de imprimir en Junio de 2022 en
los talleres de Grupo Espinosa. En su composición se utilizaron tipos
Montserrat. Tipo de impresión Offset, las medidas 16.5 × 22 cm. Los
interiores se imprimieron en papel bond ahuesado de 75 gramos y
los forros en cartulina Couché de 270 gramos

GUARDIA NACIONAL Y POLICÍA CIENTÍFICA
ESTUDIOS SOBRE CIBERSEGURIDAD, CRIMINALÍSTICA, INNOVACIÓN Y POLÍTICA CRIMINAL

Guardia Nacional y Policía Científica es un libro vanguardista con visión de futuro capaz de identificar que el mundo actual se transforma a una velocidad sin precedente. Junto con los grandes cambios en beneficio de la sociedad, aparecen nuevos retos en materia de seguridad pública en donde la delincuencia avanza y las instituciones deben dar respuestas.

La obra destaca el combate de los delitos contra la integridad de las niñas, niños y adolescentes en el ciberespacio; analiza la tortura como uno de los grandes flagelos, muestra la Policía Científica de México y realiza aportes para la identificación de casos.

El libro estudia la importancia y obtención de la evidencia; aborda el impacto de la tecnología en las operaciones policiales y observa las nuevas relaciones comerciales y de negocios lícitos e ilícitos a través de criptomonedas y blokchain y del perfil científico policial.

Trata el tema de vigilancia y prospectiva tecnológica por lo que la