Propuesta de implementación del banco de evidencia digital al servicio de la investigación criminal en el laboratorio de informática forense del centro cibernético policial

Luis Fernando Atuesta Zárate
Steven Jones Chaljub

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

PROPUESTA DE IMPLEMENTACIÓN DEL BANCO DE EVIDENCIA DIGITAL AL SERVICIO DE LA INVESTIGACIÓN CRIMINAL EN EL LABORATORIO DE INFORMÁTICA FORENSE DEL CENTRO CIBERNÉTICO POLICIAL

ALUMNO: LUIS FERNANDO ATUESTA ZÁRATE[1]

DIRECTOR: STEVEN JONES CHALJUB

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

[1]Administrador Policial, Profesional en Criminalística, Especialista en Investigación Criminal, Oficial de la Policía Nacional de Colombia con 22 años de experiencia en Investigación Criminal; 10 de ellos como investigador de delitos relacionados con las Tecnologías de la Información y las Comunicaciones; ESDEG; COL; ; ORCID 0000-0001-5857-5665; luis.auesta@correo.policia.gov.co; 3203004023.

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

PROPOSAL TO IMPLEMENT A DIGITAL EVIDENCE BANK AT THE SERVICE OF CRIMINAL INVESTIGATION IN THE FORENSIC COMPUTER LABORATORY OF THE POLICE CYBER CENTER

ALUMNO: LUIS FERNANDO ATUESTA ZÁRATE

DIRECTOR: STEVEN JONES CHALJUB

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

Aceptación del Trabajo

Agradecimientos

Gracias, desde el fondo de mi corazón a nuestro creador, por la vida que nos regalas; a mis padres Luis e Hilda por su esfuerzo que nunca termina y ser mi ejemplo de superación; a mis hijas Valentina, Mariana y María José por ser mi soporte, mi luz, mi más importante y hermosa motivación para seguir creciendo.

Gracias a mi Policía Nacional, con todo honor y orgullo, Dios y Patria, especialmente a los expertos del Centro Cibernético Policial por toda su asesoría y apoyo; al Ministerio de Tecnologías de la Información y las Comunicaciones por la financiación de este importante proceso educativo y al magnífico equipo de trabajo de la Escuela Superior de Guerra que hace parte de la Maestría en Ciberseguridad y Ciberdefensa, quienes han hecho posible este sueño.

Resumen

Para la presentación de esta monografía, cuyo objetivo consiste en proponer la implementación de un banco de evidencia digital al servicio de la investigación criminal en el Laboratorio de Informática Forense del Centro Cibernético Policial - CECIP, se han abordado conceptos como la ciberseguridad, cibercrimen e investigación criminal, realizando una descripción y análisis de los principales patrones y vectores de ataque que actualmente afectan a los ciudadanos en entorno digital, como también los procedimientos y capacidades actuales de los laboratorios de informática forense con los que cuenta la Dirección de Investigación Criminal e Interpol – DIJIN, para posteriormente realizar un diagnóstico con relación a la capacidad real de almacenamiento, análisis y correlación de evidencia digital como aporte en el apoyo a la administración de justicia, utilizando para ello la aplicación de instrumentos de recolección de información como lo son las encuestas a diferentes peritos en informática forense e información formal estadística del Centro Cibernético Policial.

La anterior información será el insumo para presentar una propuesta tecnológica detallando impacto y resultados esperados, de tal forma que se logre sustentar la importancia de implementar la iniciativa sugerida. Concluyendo que con la implementación propuesta se incrementarán los resultados estratégicos y operacionales que contribuirán en la toma de daciones en el marco del apoyo a la administración de justicia.

Palabras claves: Evidencia Digital, Análisis y Correlación, Hiperconvergencia, Malware

Abstract

For the presentation of this proposal, whose objective is to propose the implementation of a digital evidence bank at the service of criminal investigation in the Forensic Informatics Laboratory of the Police Cybernetic Center - CECIP, a description and analysis of the Current capacities of the forensic computer laboratories that the Directorate of Criminal Investigation and Interpol - DIJIN have in order to subsequently carry out a diagnosis of the capabilities of analysis and correlation of Evidence Material Elements in said laboratories through the application of information collection instruments such as it is the surveys and formal statistical information from the different laboratories.

The above information will be input to present a technological proposal for the CECIP to face the expected impact and results in such a way as to sustain the importance of implementing the suggested initiative. Concluding that with the suggested implementation, the strategic and operational results that will contribute to citizen security plans and programs will be increased, managing to minimize the criminal factors and phenomena that threaten stability and security in the Colombian territory.

Keywords: Digital Evidence, Analysis and Correlation, Hyperconvergence, Malware

Tabla de contenido

Introducción

Durante los últimos años, el fenómeno de cibercrimen y la materialización de conductas delictivas utilizando el ciberespacio como centro de acción según Robles (2015), se ha constituido en una realidad incuestionable que viene afectando seriamente el desenvolvimiento de los Estados, las sociedades y por ende sus instituciones, convirtiendo el Internet en un nuevo campo de batalla con millones de potenciales víctimas en el mundo.

Es así que este crecimiento exponencial a nivel internacional ha mostrado cifras alarmantes que preocupan a todas las naciones, tal como lo muestra el estudio realizado por Cyber Defense (2019), destacando que cada día se bloquean más de 24,000 aplicaciones móviles maliciosas de las diversas tiendas virtuales, en tal sentido, el costo promedio de los ataques de malware en 2017 fue de $ 2.4 billones de dólares, el sector de la salud ha sido uno de los más afectados ya que el 75% de su industria fue infectada con malware en algún momento, indicando además que el 38% de los archivos maliciosos llegaron en formatos utilizados por el conjunto de productos de Microsoft Office.

De manera complementaria, durante el año inmediatamente anterior, los ataques de ransomware crecieron más del 350% (Cobb, 2018), los costos por los daños que causaron aumentarán a $ 10 mil millones de dólares en 2019, siendo una empresa víctima de un ataque de ransomware cada 13.275 segundos. De continuar esta tendencia de crecimiento del cibercrimen, donde el malware se convierte en el principal vector de ataque a nivel global, se estima que el costo de los daños por delitos cibernéticos alcance los $ 5 billones de dólares para el año 2020 (Cyber Defense, 2019).

Esta situación se hace mucho más grave con el incremento del uso de los medios digitales, las tecnologías de la información y las comunicaciones, la penetración y uso masivo

de las redes sociales y en general la digitalización de la sociedad, ya que proporcionalmente aumentan las amenazas cibernéticas que se expanden planetariamente, lo cual atenta contra la seguridad digital de los ciudadanos del mundo y de todos los sectores de la sociedad actual, cuyos procesos esenciales dependen en gran medida del uso del internet y por ende de medios digitales.

Al situarse en el ámbito local, Colombia no ha sido ajeno a este fenómeno, como lo muestran Ceballos, Bautista, Mesa y Argáez (2019), los delitos informáticos más denunciados son el Hurto por Medios Informáticos con un total de 31.058 denuncias y el Uso de Software Malicioso (malware) con 2.387 casos en los últimos 5 años.

Particularmente, para el año 2019 la Policía Nacional de Colombia atendió 14.561 incidentes cibernéticos, emitió 16.322 alertas de ciberseguridad, realizó 605 capturas en relación con la ley 1273/2009 denominada "de protección de la información y los datos" y recibió 23.896 denuncias (Centro_Cibernético_Policial, 2020) mostrando los delitos de esta ley como conductas criminales en crecimiento.

Los datos expuestos anteriormente ofrecen una clara radiografía del alcance e impacto del cibercrimen, su incidencia a nivel global y local representa uno de los principales delitos económicos actuales (Lewis, 2018). Todos los estudios sobre tendencias de cibercrimen advierten un incremento importante de los ataques mediante el uso de malware y ataques de ransomware, especialmente dirigidos al sector financiero, phishing dirigido y personalizado y robo de datos personales (Enjoy Safer Technology, 2018) desplazando el peligro al uso de dispositivos móviles, obligando a los entes investigadores a la actualización de recursos, procedimientos y herramientas tecnológicas que permitan identificar el modus operandi de estas organizaciones cibercriminales, así como ampliar la cobertura para atender los cambios

continuos a los que se ve enfrentando por las diversas modalidades delictivas que se presentan a nivel Nacional.

Sin duda, el panorama descrito constituye un grave problema y motivo de preocupación para ciudadanos, empresas y gobiernos, por lo cual, la Policía Nacional debe potencializar su capacidad operativa y de investigación cibercriminal en cabeza de la Dirección de Investigación Criminal e INTERPOL, a través del fortalecimiento del Centro Cibernético Policial y sus ocho Laboratorios Regionales de Informática Forense a nivel nacional. Más cuando en el año 2019 estableció que la capacidad de evidencias analizadas fueron 228 Teras con un nivel de correlación de 0% (Ceballos, Bautista, Mesa, y Argáez, 2019).

En este sentido, siendo notable el amplio crecimiento de evidencia digital recolectada producto de acciones cibercriminales, surge la reflexión y se genera el interrogante de la pertinencia de ¿Cuál sería el modelo de banco de evidencia digital al servicio de la investigación criminal en el Laboratorio de Informática Forense del Centro Cibernético Policial, que apoye la toma de decisiones en el marco de investigaciones contra el cibercrimen en Colombia?

Aspecto importante para el Centro Cibernético Policial teniendo en cuenta que permitirá:

- Definir los procedimientos y capacidades de almacenamiento, procesamiento, análisis y correlación actuales y necesarios para la implementación del Banco Nacional de Evidencia Digital.
- Identificar las características de los principales patrones y vectores de ataque

que afectan la ciberseguridad los distintos sectores de la sociedad.

- Correlacionar evidencias de distintos laboratorios regionales de informática forense a nivel nacional.

En tan sentido, la implementación de un banco de evidencia digital, a partir de la integración de equipos de alta tecnología y medios de comunicación, que fortalezca y centralice la capacidad de almacenamiento y procesamiento (sistema de hiperconvergencia) de evidencia digital, pero que además garantice la correlación de alta disponibilidad y su análisis desde el punto de vista criminal, permitiría dar respuesta integral a los requerimientos judiciales, identificando patrones de cibercrimen asociados a estructuras criminales, mediante el desarrollo de investigaciones en todos los campos y eventos, o amenazas de ciberseguridad, con calidad, oportunidad, impacto, confidencialidad y capacidad de apoyo a la toma de decisiones de la administración de justicia del país.

Objetivo general

Proponer la implementación del banco de evidencia digital al servicio de la investigación criminal en el Laboratorio de Informática Forense del Centro Cibernético Policial.

Objetivos específicos

- Identificar las características de los patrones y vectores de ataque que afectan la ciberseguridad de los distintos sectores de la sociedad.
- Analizar los procedimientos de almacenamiento, procesamiento, correlación y análisis de evidencia digital de los laboratorios de informática forense de la Policía Nacional de Colombia.
- Establecer las capacidades de almacenamiento, procesamiento y correlación actuales y necesarios para el Banco Nacional de Evidencia Digital de los laboratorios de informática forense de la Policía Nacional de Colombia.

Contexto del fenómeno

Mediante el razonamiento deductivo que incluye la inferencia lógica de los documentos ya existentes en materia de ciberseguridad, podemos referenciar el estado del arte de las principales agencias a nivel mundial dedicadas a la persecución del ciberdelito, entendiendo esta doctrina no solo como un modelo de articulación y cooperación internacional, sino también como un modelo exitoso frente a la pandemia que refiere hoy a nivel mundial los delitos derivados del mal uso del Internet.

Como aspecto fundamental es necesario aclarar las diferencias conceptuales entre Seguridad Informática, Seguridad de la Información y Ciberseguridad, esto nos permitirá dar claridad al estado del arte en materia de ciberseguridad y su rol fundamental cuando abordamos los conceptos de evidencia digital. En tal sentido, la diferencia entre los términos genéricos de seguridad informática y seguridad de la información como lo propone (Valencia, 2018) se da en función del tipo de recursos sobre los que actúa, mientras que la primera se enfoca en la tecnología propiamente dicha, en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información, como activo estratégico de la organización.

Entre tanto, cuando hacemos referencia a ciberseguridad, entendemos que está asociada al ciberespacio y a la infraestructura que la soporta; en este escenario se articulan conceptos definidos por la ITU (Unión Internacional de Telecomunicaciones), definiéndola como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Por otra parte, ISACA (Information Systems Audit and Control Association) establece que cuando se habla de Ciberseguridad se enfoca en la protección de activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Por último, la norma ISO /IEC 27032:2012 referencia la Ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, software y servicios en internet.

Estas definiciones interactúan sobre el ciberespacio, donde convergen las tecnologías de la información y comunicaciones, escenario de confrontación y atención para las agencias de estado encargadas de la persecución penal por comportamientos contrarios a la ley; en esta materia desde el año 1996 el Comité Europeo para los Problemas Criminales (sus siglas en inglés, CDPC) decidió crear un comité de expertos que tratara exclusivamente asuntos de delitos informáticos. Este comité logró la firma del primer tratado internacional en asuntos de delitos informáticos en el año 2001 conocido como el Convenio de Budapest o Convenio sobre la Ciberdelincuencia, al cual nuestro país se adhirió (Congreso, 2018) mediante la ley 1928 del 24 de Julio de 2018.

En este sentido, se han creado diferentes agencias e instituciones para liderar la lucha contra la cibercriminalidad, como modelos internacionales de cooperación se destaca el Centro Europeo Contra la Ciberdelincuencia "EC3 de EUROPOL" el cual se inauguró en el año 2013 y nace con el objetivo de responder con la máxima celeridad ante los retos en materia de seguridad en la red. Desde el "EC3" se despliega la política en materia de lucha

contra la cibercriminalidad que define el EMPACT (notesdeseguretat, 2019) (por sus siglas en Inglés European Multidisciplinary Platform Against Criminal Threats), método establecido por la Unión Europea para afrontar las más importantes amenazas vinculadas a la delincuencia organizada, esta política se define desde la Secretaría General del Consejo de Europa cada cuatro (04) años y actualmente está vigente para el periodo 2018-2021, estableciendo diez (10) prioridades, siendo precisamente el Cibercrimen una de las más importantes (Council_of_european_union, 2017).

En complemento de lo anterior, la Organización Internacional de Policía Criminal INTERPOL como la agencia internacional más grande del mundo en materia de cooperación policial, con más de 170 países articulados, ante el crecimiento de la sofisticación, complejidad y velocidad en que viajan los delitos en Internet, inauguró en el año 2015 El Complejo Mundial para la Innovación (CMII)—Global Complex for Innovation (IGCI) en Singapur, desde donde se coordina la lucha global contra el cibercrimen; este Centro de Fusión en Ciber, se consolida como el cuerpo internacional encargado de filtrar y analizar millones de datos sobre delitos en las redes informáticas con el apoyo de la empresa privada y la academia mundial.

Estas iniciativas se unen con los proyectos y programas de la UNODC (Oficina de Naciones Unidas Contra la Droga y el Delito) con sede en Viena, Austria mediante "El Programa Global sobre Cibercrimen" (United Nation, 2020) el cual brinda asistencia técnica enfocada para el desarrollo de capacidades, prevención y sensibilización, cooperación internacional y análisis sobre el fenómeno, principalmente en países en desarrollo. El programa lo lidera la Subdivisión de Delincuencia Organizada de la UNODC y el programa de Ciberseguridad del CICTE (Comité Interamericano Contra el Terrorismo) de la OEA

(Organización de Estados Americanos) el cual está consolidado como líder regional en la provisión de iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en las Américas. El programa se centra en 03 pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación (Organización de Estados Americano, 2020).

Nuestro país no es ajeno a estos avances normativos, por lo cual, a continuación se describe el marco normativo que ha permitido regular derechos, conductas, uso de las tecnologías de la información, donde cada una de las que se describe a continuación se consideran parte esencial para el desarrollo de actividades investigativas a la hora de combatir los fraudes informáticos, la pornografía infantil, los delitos de alta tecnología y los delitos que utilizan las tecnologías de la información como medio en su actuar criminal:

- Constitución Política de Colombia. La constitución política, también llamada Carta magna o Carta Fundamental, es la ley máxima y suprema de un país o estado. En Colombia esta constitución se modificó por última vez en 1991, luego de durar más de 100 años con la constitución de 1886.
- Ley 527 de 1999, (Comercio Electrónico) "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones". Esta ley resulta importante ya que protege la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como lo son, entre otros, el intercambio electrónico de datos, internet, correos electrónicos, telegrama en

su momento, telefax, etc.

- Ley 599 de 2000, "Por la cual se expide el Código Penal". Importante mencionar que se crea el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Llama la atención la tipificación del "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa." Siendo esta básicamente la primera norma contra el cibercrimen en el país.
- Ley 679 de 2001, "Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores", modificada por la Ley 1336 del 21 de julio de 2009. Se convierte en la primea Ley que busca la protección contra la explotación sexual de nuestros niños, niñas y adolescentes, quienes actualmente se han convertido en uno de los principales blancos y objetivos del cibercrimen ante el exponencial uso de las redes sociales y la prematura entrada de los niños a este mundo digital.
- Ley 906 de 2004, "Por la cual se expide el Código de Procedimiento Penal". Mediante el cual se definen claramente las fases o etapas del proceso penal en Colombia (fase inicial, de investigación y juicio), donde juegan un papel fundamental los productos entregados a la administración de justicia por parte

de los laboratorios de informática forense, para la efectiva toma de decisiones en el marco de la investigación criminal.

- Ley 1150 de 2007, "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos". La importancia de esta Ley esta soportada en que da vida y es el punto de partida de la contratación pública del país, mediante el uso de plataformas electrónicas, buscando principalmente la transparencia en estos procesos contractuales.

- Ley 1437 de 2011, "Por medio de la cual se expide el Código de Procedimiento Admirativo y de lo Contencioso Administrativo". Este tiene como finalidad proteger y garantizar los derechos y libertades de las personas, la primacía de los intereses generales, la sujeción de las autoridades a la Constitución y demás preceptos del ordenamiento jurídico, el cumplimiento de los fines estatales, el funcionamiento eficiente y democrático de la administración, y la observancia de los deberes del Estado y de los particulares. Es decir, regula las actuaciones y procedimientos administrativos a la luz de los principios consagrados en la constitución política de nuestro país.

- Ley 1273 de 2009, "De la Protección de la Información y de los Datos". Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y

las comunicaciones. Su importancia claramente radica, entre otras, a la tutela jurídica de la información y los datos, consignando allí 09 conductas tipificadas como delitos, destacándose la violación de datos personales, el uso de software malicioso, el hurto informático y la transferencia no consentida de activos. Esta Ley nos armonizo a nivel global frente a la regulación de los delitos cibernéticos en el mundo, que si bien es cierto hoy requiere ajustarse a las nuevas tendencias de cibercriminalidad, fue en su momento uno de los grandes pasos en materia normativa ciber del país.

- Ley 1336 de 2009, "De lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes". Determina tres conductas fundamentales contra la explotación sexual de nuestras niñas, niños y adolescentes, la primera de ellas el turismo sexual para quien lo dirija, organice o promueva (4 a 8 años de prisión), la pornografía infantil para quien produzca, difunda, ofrezca, compre, almacene, transmita, exhiba contenidos de este tipo (10 a 20 años de cárcel) y algo muy importante, la extinción del derecho de dominio a los establecimientos que faciliten el turismo y explotación sexual. Como se evidencia, esta ley es severa frente a los abusos de los menores a través de internet, tipificando el almacenamiento y trasmisión de contenidos con material sexual.
- Ley 1453 de 2011, "Por medio de la cual se reforma el código Penal, El código de Procedimiento Penal, El código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad". Se destaca la sanción frente a la manipulación de equipos terminales móviles, no solo en su parte física, sino en su parte lógica. Frente al trabajo de los peritos en

informática forense, el artículo 236 de esta ley, faculta al fiscal para ordenar la aprensión, retención y recuperación de la información contenida en dispositivos electrónicos y de esta manera, descubrir, analizar y custodiar la información recuperada, para ser aportada como evidencia física contra el imputado, indiciado o condenado, básicamente soporta jurídicamente el trabajo técnico de los peritos en los laboratorios de informática forense.

- Ley 1621 del 17 de Abril de 2013. Conocida como Ley de Inteligencia y Contrainteligencia, "por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". Faculta a los organismos de inteligencia y contrainteligencia a utilizar medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información.
- Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Que se constituye en el primer tratado internacional vinculante en materia penal, que establece herramientas legales para perseguir penalmente aquellos delitos cometidos ya sea en contra de sistemas o medios informáticos, o mediante el uso de los mismos. Es importante tener en cuenta que a partir de junio de 2020, Colombia se adhirió formalmente a dicho tratado, lo cual implica un nivel de compromiso mayor ante los retos de carácter internacional en el intercambio de información y evidencia digital.
- Decreto Ley 019 de 2012, "por el cual se dictan normas para suprimir

o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública". Conocido como Ley anti tramites, donde se regulan y suprimen diligencias innecesarias que solo causan perdida de dinero y tiempo a los colombianos, busca en efecto hacer del entorno digital un medio eficaz para los ciudadanos y su interacción con las entidades del gobierno nacional, por lo cual resulta importante generar un ambienta más confiable y seguro.

- Decreto 2573 de 2014, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones". Pues bien, aquí se determina el marco general para la formulación de las políticas públicas que rigen el sector de las tecnologías de la información y las comunicaciones, la inversión en el sector y el desarrollo de estas tecnologías. Resulta igualmente interesante que define los principios y conceptos sobre la sociedad de la información y además crea la Agencia Nacional del Espectro.

Este marco normativo muestra el interés del Estado colombiano en generar mecanismos integrales para la persecución de los delitos que utilizan las tecnologías de la información y las comunicaciones como medio y/o como fin de los mismos, buscando no solo la sanción penal, sino también la modernización de los sectores, la profesionalización de las agencias de ley y la confianza ciudadana en el entorno digital.

Aunado a lo anterior, se desprenden los documentos de política pública CONPES (Consejo Nacional de Política Económica y Social), en los cuales para el año 2011 se genera el CONPES 3701, definiendo la política de ciberseguridad y ciberdefensa del país y creando las instituciones encargadas para tal fin, entre ellas, el Equipo de Respuesta a Incidentes de

Colombia (colCERT), el Comando Conjunto Cibernético (CCOCI) y el Centro Cibernético Policial (CCP). Este documento se basó en tres acciones principales: I) adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar, generar recomendaciones para afrontar las amenazas y los riesgos que se presenten; II) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad, y III) fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.

Complementando esta política fue necesario realizar un ajuste para el año 2016, por tal motivo se creó el documento CONPES 3854 denominado "CONPES de Seguridad Digital", el cual se enfocó en la gestión de riesgos de seguridad digital con el fin de promover un entorno digital confiable y seguro, que maximice los beneficios económicos y sociales de los colombianos, impulsando la competitividad y productividad en todos los sectores de la economía, bajo los siguientes principios: I) salvaguardar los derechos humanos y los valores fundamentales de los individuos, II) adoptar un enfoque incluyente y colaborativo, III) asegurar una responsabilidad compartida entre todos los actores involucrados, y IV) adoptar un enfoque basado en riesgos, que permita a los individuos el libre, confiable y seguro desarrollo de sus actividades en el entorno digital (MinTic, 2016).

Finalmente, el pasado 01/07/2020 fue aprobada la versión oficial del Documento Conpes 3995 "Política Nacional de Confianza y Seguridad Digital" (CONPES, 2020) el cual formula como objetivo establecer medidas para ampliar la confianza y seguridad digital, de manera que Colombia sea una sociedad incluyente y competitiva en el futuro, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado

del país.

En términos generales, el propósito es el de desarrollar capacidades suficientes y adecuadas para gestionar riesgos asociados con el uso de nuevas tecnologías, y para ello se parte del hecho de la necesidad de formular y actualizar estrategias y políticas relacionadas con la seguridad nacional. Este plan considera, entre otros, las directivas para el diseño, estructuración y presentación del proyecto de implementación del CSIRT (Computer Security Incident Response Team), un plan de implementación de autenticación digital, un programa para fortalecer la provisión de bienes y servicios en materia de seguridad digital y un programa de desarrollo de competencias y capacidades para abordar y gestionar riesgos asociados con el uso de tecnologías emergentes como Internet de las Cosas, Computación en la nube, Inteligencia Artificial y Big Data, entre otros.

Estas políticas públicas definieron la ruta de actuación del Gobierno Nacional para enfrentar los riesgos y amenazas en el ciberespacio, permitiendo la creación de entidades, generación de roles y funciones alrededor de la Ciberseguridad y Ciberdefensa, así como la participación de todos los actores involucrados en la definición de seguridad digital del país.

En virtud de lo anterior y dando alcance a los compromisos y responsabilidades adquiridas, la Policía Nacional en cabeza de la Dirección de Investigación Criminal e INTERPOL, creó el Centro Cibernético Policial como unidad especializada de la institución en prevención, atención y judicialización de estructuras criminales dedicadas al cibercrimen, para lo cual orienta sus esfuerzos en los siguientes aspectos:

- Prevención: mediante la articulación de esfuerzos en el C4 (Centro de Capacidades para la Ciberseguridad de Colombia), donde convergen el punto de atención 24/7 llamado CAIVIRTUAL, plataforma virtual de atención y reporte de

incidentes cibernéticos y el observatorio del delito, lo cual permite la generación de alertas tempranas y documentos de interés a los diferentes sectores de la sociedad.

- Unidad Judicial: a cargo del cumplimiento a las órdenes de policía judicial emanadas por los diferentes despachos judiciales, a través de cuatro líneas de investigación, fraude financiero, delitos contra la seguridad ciudadana, pornografía infantil y delitos de alta tecnología.
- Articulación Interagencial: a cargo de dinamizar y fortalecer los vínculos y acuerdos de cooperación con los diferentes sectores público privados del país, como también de carácter internacional desplegando estrategias como la designación de un oficial de enlace permanente desde el año 2014 ante el Centro Europeo Contra la Ciberdelincuencia "EC3 de EUROPOL" en cumplimiento a la ley 1582 del 2012, por medio de la cual se aprueba el "Acuerdo de Cooperación Operativa y Estratégica Entre la República de Colombia y la Oficina Europea de Policía". Esta capacidad de articulación y despliegue operacional le otorgó a la Policía Nacional ser la responsable del punto de contacto 24/7 del Convenio de Budapest, suscrito por el Gobierno Nacional mediante la Ley 1928 del 2018, para lo cual la institución debe contar con las herramientas legales y jurídicas necesarias, como también con el componente técnico y humano debidamente capacitado con el fin de garantizar efectivos resultados contra la ciberdelincuencia.
- Laboratorio de Informática Forense: unidad responsable del peritaje informático mediante la identificación, recolección, preservación y análisis de evidencia digital. Para lo cual existen ocho laboratorios regionales a nivel nacional.

En tal sentido, y ante el incremento y globalización del uso de las Tecnologías de la Información y las Comunicaciones TICs, que afecta directamente en el aumento y proliferación de las amenazas cibernéticas, situación que va en contra de la ciberseguridad del Estado colombiano, de sus ciudadanos, y los diferentes sectores de la sociedad que utilizan el ciberespacio para el cumplimiento de su objeto social, al interior de la Policía Nacional se viene desplegando la Directiva Operativa Permanente 038 del 13 de noviembre de 2019, "Parámetros de Actuación Policial para el Despliegue de la Estrategia Integral de Ciberseguridad – ESCIB", mediante la cual se fijan las directrices y parámetros institucionales para propiciar espacios seguros para el acceso a las tecnologías de la información y las comunicaciones a los ciudadanos, así como prevenir, atender e investigar los fenómenos delictivos que atentan la convivencia y seguridad ciudadana en el ciberespacio, bajo un enfoque de corresponsabilidad.

Este documento se convierte en la hoja de ruta institucional para dar respuesta a la evolución de los fenómenos, las expresiones de criminalidad y la conflictividad social, con el fin de satisfacer las necesidades de los cibernautas en materia de ciberseguridad, a través del desarrollo de las siguientes iniciativas:

- Proteger derechos fundamentales y humanos de los cibernautas.
- Desplegar las capacidades de la Policía Nacional, para contrarrestar los fenómenos que atenten contra la convivencia ciudadana en el ciberespacio bajo un enfoque de ciberseguridad.
- Desarrollar las acciones necesarias para alinear la ciberseguridad como fuente fundamental para la economía digital y el comercio electrónico en Colombia,

fomentando el acceso a las tecnologías de la información y las comunicaciones en un entorno seguro.

- Articular las capacidades del Estado, para realizar las actividades pertinentes que contribuyan a un desarrollo integral de los Niños, Niñas y Adolescentes de Colombia, estableciendo los mecanismos idóneos de protección en entornos digitales y contribuyendo en la formación de los mismos.
- Garantizar la estabilidad del estamento gubernamental e institucional, a través del fortalecimiento de las capacidades de prevención y anticipación frente amenazas informáticas.
- Actualizar los mecanismos y capacidades de la Policía Nacional para garantizar el acercamiento y satisfacción del ciudadano como víctima del cibercrimen, logrando el esclarecimiento de los actos delictivos para contribuir con la consecución de una paz estable y duradera.
- Desarrollar acciones de impacto que contribuyan a la prevención del ciberdelito y a la educación ciudadana y de los entes de policía y gubernamentales para la consolidación de una cultura de ciberseguridad.
- Fortalecer las alianzas de cooperación policial con agencias y entidades internacionales para una articulación efectiva en el cumplimiento de objetivos estatales en la fomentación de las Tecnologías de la Información y las Comunicaciones TIC'S.
- Para el cumplimiento de estas responsabilidades, resulta de vital importancia contar con laboratorios de informática forense, dotados de tecnología de

punta, que brinden la capacidad de almacenamiento y procesamiento de evidencia digital, pero que además garanticen la correlación y su análisis desde el punto de vista criminal, para dar respuesta a los requerimientos judiciales con calidad, oportunidad, impacto, confidencialidad y capacidad de asesoramiento al mando institucional. De esta manera la institución contribuye con la administración de justicia, cosa que impacta al ciudadano dado que también se materializa su derecho humano a la administración de justicia, y si es víctima, su derecho a la verdad y justicia.

Descripción y análisis de las capacidades actuales de los Laboratorios de Informática Forense del Centro Cibernético Policial

Estructura Actual

Los laboratorios de informática forense buscan apoyar acertadamente las autoridades judiciales, a través del desarrollo de la investigación criminalística, atendiendo las solicitudes de identificación, recolección, preservación y análisis de evidencia digital, dando respuesta oportuna según los tiempos establecidos en las órdenes a policía judicial, de igual forma apoyando las diligencias judiciales que requieran las autoridades judiciales competentes.

La principal finalidad de los laboratorios de Informática Forense es apoyar acertadamente la Investigación Criminal, mediante el desarrollo del Proceso de Segundo Nivel de la Dirección de Investigación Criminal e INTERPOL "Desarrollar Investigación Criminalística", dando despliegue al desarrollo de cuatro procedimientos así: Tratamiento y Análisis de Evidencia Digital, Recolección de Datos Volátiles, Extracción de Información a Equipos Terminales Móviles y Realizar Imágenes Forenses, procedimientos, que cumplen con las normas internacionales, para el estudio forense de la evidencia digital.

Es de anotar que los laboratorios de informática forense de la Dirección de Investigación Criminal e INTERPOL se encuentran incluidos en el Grupo de Disciplinas Forenses según la resolución 05839 de 2015 (Ministerio de Defensa Nacional, 2015).

1.12.5	**Jefatura de Policía Científica y Criminalística**	**(JECRI)**
1.12.5.1	**Área de Ciencias Forenses**	**(ARCIF)**
1.12.5.1.1	Grupo de Identificación Humana	(GRIHU)
1.12.5.1.2	Grupo de Disciplinas Forenses	(GUDIF)
1.12.5.2	**Área de Respuesta Antiterrorista e Incidentes NBQRE**	**(CIARA)**
1.12.5.2.1	Grupo Antiexplosivos Antiterrorista	(GRANT)
1.12.5.2.2	Grupo Rastreo de Armas	(GRURA)

Figura 1. Que describe la estructura actual donde se encuentran ubicados los laboratorios de informática forense de la DIJIN, tomado de la resolución 05839 de 2015 – DIJIN.

Los laboratorios de Informática forense se encuentran distribuidos a nivel nacional por regionales de policía, ocho en total, en cada una de ellas se hace el despliegue de un laboratorio con hardware y software de última tecnología, y con el acopio de las normas y procedimientos que se manejan a nivel central para brindar una respuesta oportuna a los requerimientos de las autoridades judiciales competentes, así:

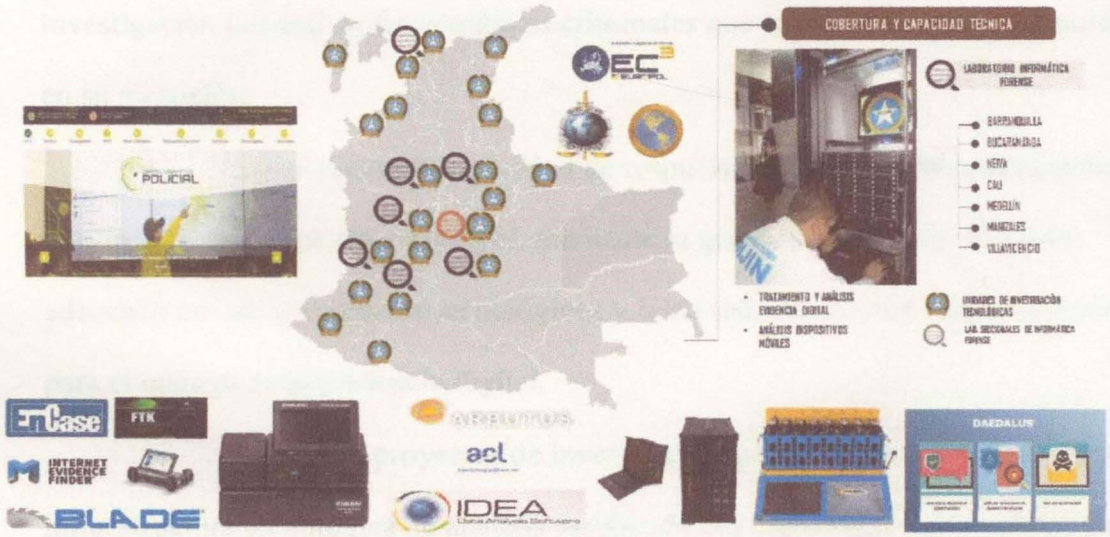


Figura 2. Descripción gráfica de donde se encuentran ubicados los laboratorios de informática forense de la Dirección de Investigación Criminal e INTERPOL

En ese orden de ideas los laboratorios de informática forense se encuentra en las ciudades de Bogotá, Barranquilla, Bucaramanga, Cali, Manizales, Medellín, Neiva y Villavicencio, cada una de éstas comprende un determinado número de departamentos, las

autoridades judiciales que se encuentren en estos lugares pueden realizar los requerimientos respectivos para el análisis de los EMP y/o EF según corresponda. Siendo el laboratorio del nivel central, la dependencia encargada de liderar y coordinar el proceso de Investigación Criminalística desarrollado por los laboratorios regionales de Informática Forense nivel nacional. Cumpliendo las siguientes funciones:

- Desarrollar el proceso de investigación Criminalística mediante la identificación, recolección, preservación y análisis de la evidencia digital.
- Realizar el análisis a dispositivos de almacenamiento digital con fines forenses, bajo la coordinación de la Fiscalía General de la Nación y otras autoridades judiciales.
- Fortalecer la capacidad de la Policía Nacional para apoyar la investigación judicial de las conductas criminales que involucren medios tecnológicos en su ejecución.
- Administrar la capacidad de respuesta de los ocho laboratorios de informática forense a nivel nacional, mediante la gerencia del talento humano, adecuado uso de los recursos tecnológicos y la estandarización de los procedimientos para el manejo de la evidencia digital.
- Presentar proyectos de inversión que permitan mantener actualizada la infraestructura tecnológica de análisis forense de la Policía Nacional de Colombia.
- Coordinar con la Dirección Nacional de Escuelas la capacitación y formación de Peritos en Informática forense de la Policía Nacional.
- Realizar seguimiento a las innovaciones tecnológicas en la materia,

informando a la alta dirección en procura de garantizar la continua modernización de la Policía Nacional.

- Generar mecanismos de cooperación policial internacional que faciliten el intercambio de información en mejores prácticas, experiencias exitosas y técnicas aplicadas a la informática forense por cuerpos policiales homólogos; así como la participación activa en encuentros y seminarios internacionales.
- Servir de órgano consultor de los laboratorios de Informática Forense de las regiones de Policía para su organización y funcionamiento.
- Propiciar estrategias que permitan la certificación y acreditación continua del laboratorio de informática forense y sus funcionarios.

Entre las actividades que desarrolla el Laboratorio de Informática Forense se encuentran:

- Brindar un servicio de Policía oportuno, con calidad y que acate la constitución y la ley, suministrando un apoyo efectivo, con altos estándares de calidad a las autoridades judiciales y administrativas.
- Adoptar los procedimientos y normas internacionales para el funcionamiento de los laboratorios de informática forense.
- Apoyar en forma el desarrollo de las investigaciones judiciales, con la calidad de los peritajes informáticos.
- Garantizar los principios técnicos científicos (Disponibilidad, No repudio, Integridad, Observancia) para el manejo de la información electrónicamente almacenada.

- Garantizar la cadena de custodia de la EF y/o EMP durante el análisis forense en el Laboratorio de Informática Forense.
- Realizar el tratamiento y análisis de la Evidencia Digital, según lo establecido en el procedimiento respectivo.
- Realizar la Imagen forense de la EF y/o EMP, siguiendo los pasos para la adquisición de una copia exacta bit a bit.
- Realizar con la ayuda de hardware forense especializado en el análisis forense para dispositivos móviles, la extracción de Información a Equipos Terminales móviles.
- Peritaje Informático en el Laboratorio de Informática forense (informe de Laboratorio).
- Trabajo de campo en informática forense en apoyo a diligencias judiciales (Informe de Campo).
- Importancia del Laboratorio de Informática forense: El laboratorio de informática forense es la unidad líder en peritaje informático a nivel nacional, para lo debe contar con los siguientes componentes:
- Herramientas en hardware, que permitan la realización de imágenes forenses y el tratamiento y procesamiento de la evidencia digital.
- Herramientas en software, especializadas en el análisis de la evidencia digital, identificación y clasificación de contenido de internet, reconocimiento de software malicioso y recuperación de información.
- Herramientas forenses para el análisis de dispositivos móviles, y

nuevas tecnologías.

- Laboratorios especializados para la recuperación de discos duros con daño físico, análisis de malware, FDA.
- Personal de peritos informáticos con la preparación, conocimientos y experiencia necearía para dar respuesta a los requerimientos de las autoridades judiciales competentes.

Herramientas existentes:

La dotación del laboratorio de informática forense contiene a nivel de software:

HARDWARE
01 teléfono celular.
02 computador portátil forenses última tecnología (Alta capacidad de almacenamiento, procesamiento, memoria RAM) para trabajo de campo.
2 máquinas forenses de última tecnología (Alta capacidad de almacenamiento, procesamiento, memoria RAM).
01 impresora portátil.
02 cámara fotográfica de alta resolución.
01 cámara filmadora para acompañamiento diligencias judiciales.
03 kit de bloqueadores forenses contra escritura.
01 equipos forenses para el análisis de dispositivos móviles.
01 equipos de clonación de dispositivos de almacenamiento.

Tabla 1. Descripción de hardware utilizado en el laboratorio de informática forense del servicio de investigación criminal.

SOFTWARE
02 licencias de software para análisis y tratamiento de evidencia digital.
01 licencias para análisis de dispositivos móviles.
02 licencias para análisis de contenido web en dispositivos de almacenamiento.
01 licencia de software para análisis de malware.
01 licencia para rompimiento de contraseñas.
02 licencias de software para ofimática.
02 licencias de software antivirus.
01 licencias para virtualización de sistemas operativos.
01 licencias para la realización de borrado seguro.
02 licencias de software para tratamiento de evidencia digital portable.

02 licencias de software para la recolección de datos volátiles.

Tabla 2. Descripción de software utilizado en el laboratorio de informática forense del servicio de investigación criminal

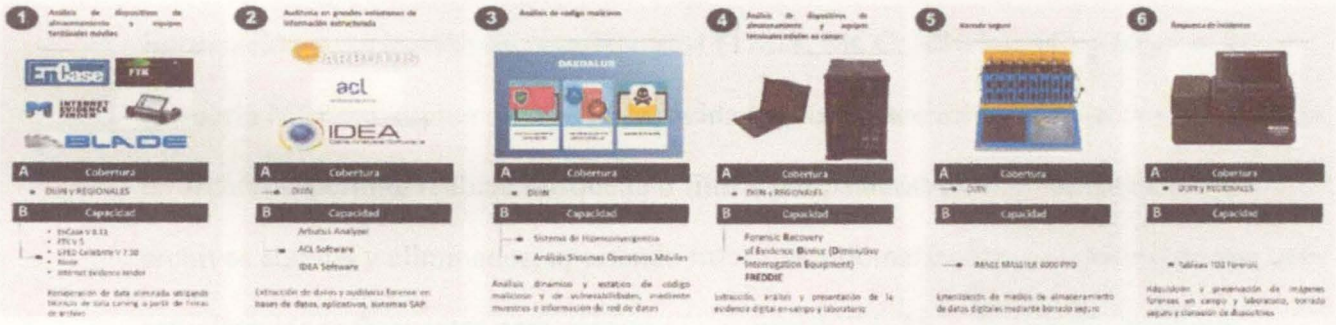
Información con base en las licencias actuales con las que cuentan los laboratorios de informática forense

A nivel central, el laboratorio de informática forense:

Cuenta con software que le permite realizar auditoria sobre información estructurada (bases de datos) y no estructurada.

Administra una plataforma para análisis de software malicioso, a través de un sistema de hiperconvergencia con el que puede emular diferentes entornos de trabajo de los principales sistemas operativos en ambientes controlados, en los que se realiza análisis estático y dinámico de las muestras.

Definición de tecnología actual utilizada por los laboratorios de informática forense de la Policía Nacional:



A nivel gráfico se puede mostrar:

Figura 3. Descripción gráfica de los equipos especializados que actualmente se encuentran ubicados los laboratorios de informática forense de la Dirección de Investigación Criminal e INTERPOL

1. Software Forense EnCaSe, FTK, IEF, Blade y ARBUTUS: Son herramientas de Software Forense fundamentales en la actividad pericial, las cuales permiten realizar adquisición de imágenes forenses y procesamiento de evidencia digital, búsqueda de información empleando diferentes filtros por palabras claves, recuperación de archivos activos y eliminados, búsqueda de artefactos de internet y correos electrónicos, entre otros. Preserva los archivos exportados como resultado del análisis forense en un formato válido garantizando la integridad de la evidencia a efectos legales y validados por los tribunales en estrados judiciales, la información obtenida puede ser exportada en diversos formatos de archivo para ser aportada en la actividad pericial.

2. UFED Cellebrite: Herramienta de hardware y software para realizar extracción de información de equipos terminales móviles y tablets (soporte de dispositivos con sistemas operativos Android, iOS y BlackBerry®, incluyendo teléfonos con chipsets chinos), datos de aplicaciones, contraseñas, mensajería instantánea, contactos, SMS's y MMS's, correos electrónicos, calendario, imágenes, archivos de audio y de video, tonos de llamada, registros de llamadas, detalles del teléfono (IMEI/ESN), ICCID y IMSI, información de ubicación de la tarjeta SIM (TMIS, MCC, MNC, LAC) y tarjetas de memoria Microsd, brinda diferentes capacidades de extracción física, lógica y del sistema de archivos, permite realizar búsqueda o filtros por palabras claves, recuperación de archivos activos y eliminados, aportando informes automatizados. Así mismo cuenta con actualizaciones frecuentes para asegurar la compatibilidad con los nuevos teléfonos introducidos en el mercado.

3. Análisis dinámico y estático de código malicioso y vulnerabilidades mediante muestras e información de red de datos.

4. Equipo FREDDIE: Se convierte en un elemento indispensable en la actividad de Informática Forense, ya que es un computador robusto y portátil con grandes capacidades de procesamiento para cualquier desafío forense. Posee memoria ampliable a 64 GB y ranuras para hasta cuadro discos duros de estado sólido para las principales aplicaciones de software forense de la actualidad. Su desempeño minimiza los tiempos de transferencia de datos para el trabajo en campo o en laboratorio. Es de resaltar que posee varias opciones de arranque de software optimizado en torno a múltiples núcleos, velocidad de reloj, memoria, potencia y velocidad. Este se convierte en el elemento fundamental del perito para atender cualquier requerimiento con la total autonomía de trabajar sobre cualquier condición, ofreciendo las mejores capacidades de respuesta. Así mismo, cuenta con bloqueadores forenses, que permiten al perito la adquisición de una mayor cantidad de datos de dispositivos de almacenamiento digital, a una mayor velocidad de transferencia, con soporte de más tipos de medios, sin disminuir la facilidad de uso o portabilidad en campo. Este dispositivo permite la multitarea (dos trabajos forenses activos a la vez – imágenes forenses), ofreciendo un amplio soporte de sistemas de archivos, que contribuirá al efectivo desempeño del perito frente a los diferentes Elementos Materiales Probatorios que tenga que trabajar en campo o en laboratorio.

5. Borrado seguro, esterilización y clonación de dispositivos de almacenamiento de datos digitales, que permitan asegurar las buenas practicas, en torno al protocolo empleado por el funcionario de policía judicial en pro de salvaguardar la información con su respectiva cadena de custodia.

6. Tableau TD3 Forensic, el cual permite la respuesta inmediata y en el lugar de los hechos de incidentes, adquisición y preservación de imágenes forenses en campo y

laboratorio, borrado seguro y clonación de dispositivos.

Solución de hiperconvergencia:

El Centro Cibernético Policial, obtuvo la capacidad de adelantar análisis avanzados de muestras de software malicioso, que hoy en día permiten generar detallados reportes de secuencia de comportamiento, clasificación de amenazas y catalogación de firmas entre otros, del tipo estáticos y dinámicos en plataformas PC y de equipos terminales móviles, además de generar escenarios de simulación para el malware colectado de tal forma que se puede estudiar en ambientes diferentes al extraído, esto con el fin de atender la amenaza y generar estrategias de prevención a futuros ataques y capacidad en la investigación criminal para la Policía Nacional.

Esto permitió fortalecer de manera eficaz y oportuna la acción judicial, la protección y conservación del acervo probatorio y la capacidad de identificar, recolectar, preservar, analizar y presentar la evidencia digital, con el fin de controlar y desarticular las personas y organizaciones delincuenciales que atentan contra la ciberseguridad ciudadana; apoyados en el empleo de las mejores prácticas y uso de recursos tecnológicos especializados en materia de informática e investigación digital forense, mediante la virtualización de las capacidades de análisis del Laboratorio de Informática Forense, con una infraestructura hiperconvergente que optimizó los tiempos y recursos en adquisición y análisis de la evidencia digital.

La solución de hiperconvergencia consta de los siguientes elementos:

- Hardware para el servidor appliance
- Software para el servidor appliance
- Software para análisis de software malicioso

- Una (1) consola de administración
- Tres (3) estaciones para analistas

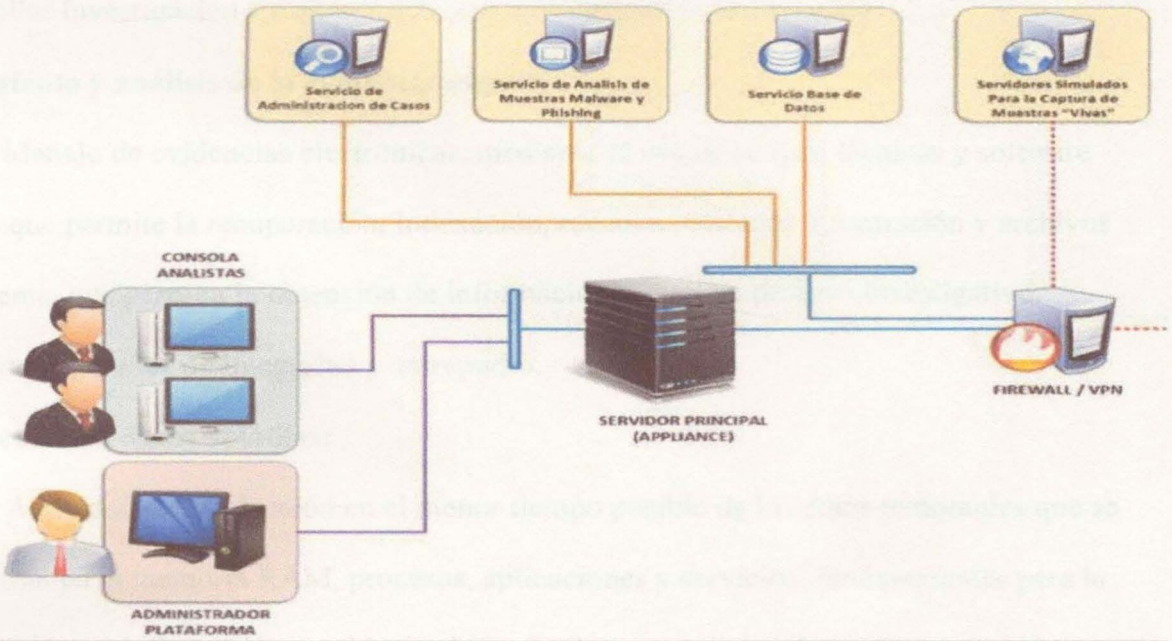


Figura 4. Descripción gráfica de topología de red de solución de hiperconvergencia.

Todos estos equipos especializados generan reportes con hallazgos susceptibles de correlación que actualmente no tiene la Policía Nacional.

Procesos y procedimientos aplicados

La principal finalidad de los laboratorios de Informática Forense es apoyar acertadamente la Investigación Criminal, mediante el desarrollo del Proceso de Segundo Nivel de la Dirección de Investigación Criminal e INTERPOL "Desarrollar Investigación Criminalística" (Ministerio de Defensa Nacional, 2015) dando despliegue a al desarrollo de los siguientes procedimientos, que cumplen con las normas internacionales, para el estudio forense de la evidencia digital.

Actualmente los laboratorios de informática forense de la Policía Nacional de Colombia con el fin de estandarizar la actuación científica de sus peritos, han definido 4 procedimientos (Planeación_DIJIN, 2020) que dependen estructuralmente del proceso Desarrollar Investigación Criminalística, como se definen a continuación:

Tratamiento y análisis de la evidencia digital:

Manejo de evidencias electrónicas, mediante el uso de scripts, técnicas y software forense que permite la recuperación, indexación, reconstrucción de información y archivos del sistema, que permita la obtención de información útil en un proceso investigativo, aplicando principios de integridad y no repudio.

Recolección de datos volátiles:

Actividad de recolección en el menor tiempo posible de los datos temporales que se encuentran en la memoria RAM, procesos, aplicaciones y servicios, fundamentales para la preservación de información en el lugar de los hechos, cuando los dispositivos electrónicos que cuentan con sistema operativo se encuentren activos (encendidos).

Extracción de información a equipos terminales móviles:

Data obtenida de dispositivos de comunicación móvil, que cuentan con capacidad de almacenamiento, procesamiento, funciones multimedia, comunicación, navegación en internet entre otras características, con la finalidad de ser aportada como E.M.P y E.F, en apoyo a procesos investigativos de autoridades competentes.

Realizar imágenes forenses:

Corresponde a la obtención de una copia física (bit a bit) o lógica de dispositivos de almacenamiento digital vinculados en un proceso investigativo, con la finalidad de tener una réplica del dispositivo original a analizar, evitando daños o cambios no intencionados. Esta

adquisición se realiza mediante el uso de herramientas forenses debidamente licenciadas y reconocidas por la comunidad técnico-científica.

Diagnóstico de capacidades de análisis y correlación de EMP en laboratorios de informática forense de la DIJIN

EMP recepcionados y analizados

A continuación, se describe de manera estadística el volumen de Elementos Materiales Probatorios recolectados y analizados en el último año (Laboratorio_Informática, 2020) con un Total Nivel Nacional de 228.140 GB = 228 Teras. Seguidamente, se desagrega por laboratorio:

CANTIDAD		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	264	RESUELTA	255
CANTIDAD DE TELEFONOS	529	CANCELADA	1
CANTIDAD SIM CARD	535	PRORROGADA	2
CANTIDAD MICRO SD	176	VIGENTE	6
CANTIDAD CD/DVD	123	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	102	TOTAL O.T.	264
CANTIDAD DVR	11		
CANTIDAD DISCOS DUROS	125		
CANTIDAD DE REGISTROS DE BD	0		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	151		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	3781		
TOTOAL GB ANALIZADAS	110.680		

Tabla 3. *Laboratorio de Informática Forense Nivel Central*

Información recopilada de la información recepcionada y analizada por el laboratorio central ubicado en la ciudad de Bogotá.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	115	RESUELTA	112
CANTIDAD DE TELEFONOS	250	CANCELADA	0
CANTIDAD SIM CARD	243	PRORROGADA	0
CANTIDAD MICRO SD	112	VIGENTE	3
CANTIDAD CD/DVD	1	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	7	TOTAL O.T.	115
CANTIDAD DVR	2		
CANTIDAD DISCOS DUROS	13		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	4		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	19		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	135		
TOTAL GB ANALIZADAS	30.413		

Tabla 4. Laboratorio de Informática Forense de la Región 2

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 2.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	81	RESUELTA	81
CANTIDAD DE TELEFONOS	167	CANCELADA	0
CANTIDAD SIM CARD	171	PRORROGADA	0
CANTIDAD MICRO SD	63	VIGENTE	0
CANTIDAD CD/DVD	14	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	15	TOTAL O.T.	81
CANTIDAD DVR	0		
CANTIDAD DISCOS DUROS	17		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	1		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	0		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	16		
TOTAL GB ANALIZADAS	15.003		

Tabla 5. Laboratorio de Informática Forense de la Región 3

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 3.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	144	RESUELTA	144
CANTIDAD DE TELEFONOS	276	CANCELADA	0
CANTIDAD SIM CARD	266	PRORROGADA	0
CANTIDAD MICRO SD	108	VIGENTE	0
CANTIDAD CD/DVD	6	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	15	TOTAL O.T.	144
CANTIDAD DVR	2		
CANTIDAD DISCOS DUROS	2		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	18		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	6		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	58		
TOTAL GB ANALIZADAS	16.714		

Tabla 6. Laboratorio de Informática Forense de la Región 4

Información recopilada de la información recepcionada y analizada por el laboratorio

Regional 4.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	152	RESUELTA	146
CANTIDAD DE TELEFONOS	122	CANCELADA	0
CANTIDAD SIM CARD	116	PRORROGADA	0
CANTIDAD MICRO SD	90	VIGENTE	6
CANTIDAD CD/DVD	170	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	4	TOTAL O.T.	152
CANTIDAD DVR	0		
CANTIDAD DISCOS DUROS	9		
CANTIDAD DE REGISTROS DE BD	1		
CANTIDAD USB	2		
TAMAÑO Y PESO DE BD EN MB	31		
OTROS ELEMENTOS	0		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	452		
TOTAL GB ANALIZADAS	10.924		

Tabla 7. Laboratorio de Informática Forense de la Región 5

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 5.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	832	RESUELTA	832
CANTIDAD DE TELEFONOS	43	CANCELADA	0
CANTIDAD SIM CARD	44	PRORROGADA	0
CANTIDAD MICRO SD	15	VIGENTE	0
CANTIDAD CD/DVD	0	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	1	TOTAL O.T.	832
CANTIDAD DVR	13		
CANTIDAD DISCOS DUROS	14		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	4		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	0		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	33		
TOTAL GB ANALIZADAS	15.892		

Tabla 8. Laboratorio de Informática Forense de la Región 6

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 6.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	68	RESUELTA	68
CANTIDAD DE TELEFONOS	0	CANCELADA	0
CANTIDAD SIM CARD	0	PRORROGADA	0
CANTIDAD MICRO SD	13	VIGENTE	0
CANTIDAD CD/DVD	298	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	60	TOTAL O.T.	68
CANTIDAD DVR	2		
CANTIDAD DISCOS DUROS	0		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	0		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	0		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	315		
TOTAL GB ANALIZADAS	13.286		

Tabla 9. Laboratorio de Informática Forense de la Región 7

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 7.

2019			
CANTIDAD ELEMENTOS ANALIZADOS		ESTADO O.T.	CANTIDAD
NÚMERO DE ORDENES DE TRABAJOS	113	RESUELTA	113
CANTIDAD DE TELEFONOS	220	CANCELADA	0
CANTIDAD SIM CARD	223	PRORROGADA	0
CANTIDAD MICRO SD	60	VIGENTE	0
CANTIDAD CD/DVD	58	VENCIDA	0
CANTIDAD COMPUTADORES (PORTATILES,TODO EN UNO Y CPU)	7	TOTAL O.T.	113
CANTIDAD DVR	6		
CANTIDAD DISCOS DUROS	2		
CANTIDAD DE REGISTROS DE BD	0		
CANTIDAD USB	1		
TAMAÑO Y PESO DE BD EN MB	0		
OTROS ELEMENTOS	0		
CANTIDAD DE IMAGENES FORENSES REALIZADAS	351		
TOTAL GB ANALIZADAS	15.228		

Tabla 10. Laboratorio de Informática Forense de la Región 8

Información recopilada de la información recepcionada y analizada por el laboratorio Regional 8.

De manera complementaria en lo comprendido del año 2020, en el laboratorio de informática forense del nivel central, se han analizado muestras de archivos ejecutables que pertenecen a sistemas operativos; Windows (85%) y Linux (15%), que se han extraído de diferentes casos nacionales y en los cuales se ha identificado como principal vector de ataque

programas maliciosos (Backdoor, Botnet, Downloader,Launcher, Rootkit, Scareware, Spam-sendingmalware, Worm o virus) con características especiales como; invisibilidad-evasión, persistencia, escalamiento de privilegio y robo de credenciales. Además se han identificado documentos maliciosos creados por atacantes para explotar vulnerabilidades en el procesamiento de documentos y software de renderizado como Adobe (Reader / Acrobat) y Microsoft Office (Word, PowerPoint, Excel), convirtiéndolos en un reto para la Ciberseguridad y para los procedimientos de análisis forense.

Extensiones:

Entre las extensiones más utilizadas para la distribución de software malicioso en Windows, se han identificado; .exe, .bat, .tmp, .bin, .sys y .rtf, las cuales interactúan directamente con el sistema de archivos y las llaves de registro.

Técnicas Identificadas:

Entre las técnicas más destacadas que se han identificado, está la ofuscación de la estructura de los archivos analizados, entre los que se destacan las librerías para interactuar con los componentes físicos de los dispositivos; comprometiendo la información personal de los usuarios mediante invasión de elementos como el teclado, cámara, mouse, micrófono etc.

Otra técnica encontrada es la de exfiltración de datos por medio de conexiones remotas en la que los ciberdelincuentes habilitan puertos de escucha en los sistemas para transferir y recibir datos sin que el usuario se percate de ello.

También se identifican técnicas de Phishing para suplantación de plataformas bancarias, ya que utilizando formularios web para capturar datos y mediante funciones programadas, envían los mismos a correos electrónicos y bases de datos locales. Muchos de estos sitos se alojan en servidores virtualizados adquiridos en Deep Web; logrando con esto

un nivel de anonimato difícil de rastrear e investigar.

Otra técnica identificada es la inyección de procesos en memoria popular en los sistemas operativos Windows, consistente en instaurar procesos de carga automática en la memoria primaria, que permite al ciberdelincuente monitorear el estado del sistema; software y hardware, estableciendo piezas de código previamente programadas donde establece condiciones en que se realiza el ataque.

Aplicación de instrumento

Con el fin de lograr la recolección de información útil para la presente propuesta se utilizó el instrumento de recolección "Encuesta" teniendo como población lo Jefes de los Laboratorios de Informática Forense y los Peritos de Informática Forense que son quienes continuamente realizan actividades de recolección y análisis de evidencia digital obteniendo los siguientes resultados.

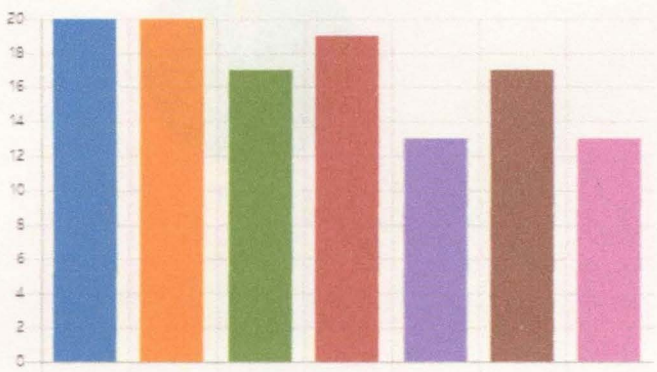
La prueba fue resuelta por 24 personas entre las cuales se encuentran los Jefes de los 8 Laboratorios de Informática Forense y los peritos de adscritos a dichos laboratorios buscando que haya una objetividad en la aplicación de la encuesta.

2. Describa su cargo en unidad en que labora

Más detalles

3. ¿En qué tipo de investigaciones participa?

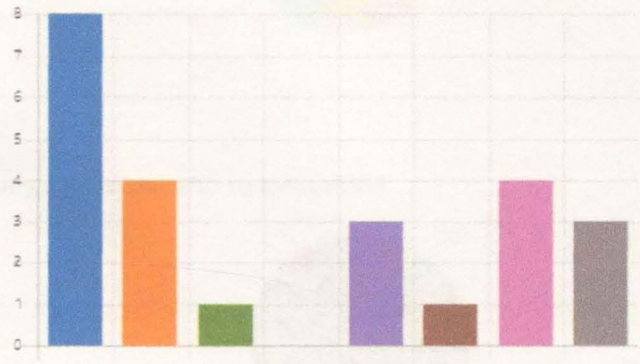
Más detalles



10. ¿Cuál es el motivo de que estas actividades sean tan laboriosas ? (seleccione tres como máximo)

Más detalles

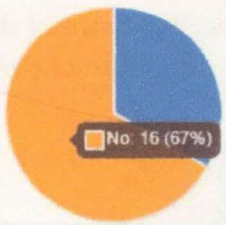
La cantidad de datos	8
La complejidad de los análisis	4
La complejidad de los datos	1
La dependencia de terceros	0
La falta de conocimientos esp...	3
La escasa calidad de los datos	1
La integración de resultados p...	4
Otro	3



11. ¿Actualmente existe alguna plataforma que permita correlacionar distintas evidencias digitales de distintos laboratorios de informática forense?

Más detalles

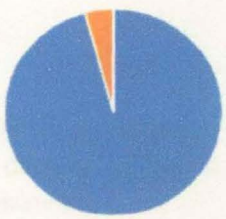
Si	8
No	16



13. ¿Dada la capacidad de almacenamiento actual, por cuánto tiempo se puede almacenar en su laboratorio de informática forense evidencia?

Más detalles

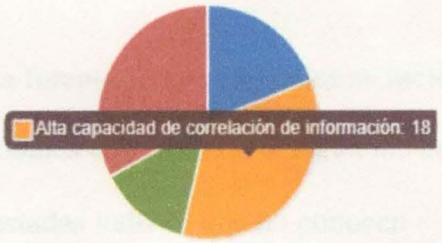
Menos de un año	23
De uno a tres años	1
De tres a cinco años	0
Más de cinco años	0



17. Seleccione dos propiedades deseables en una herramienta de correlación y análisis de evidencia digital

Más detalles

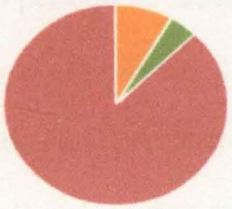
Tiempos de respuesta mínimos	10
Alta capacidad de correlación ...	18
Gran capacidad de almacena...	7
Visualización de los resultados	17



14. En TB cuantas evidencias recolectan y analiza por año su laboratorio

Más detalles

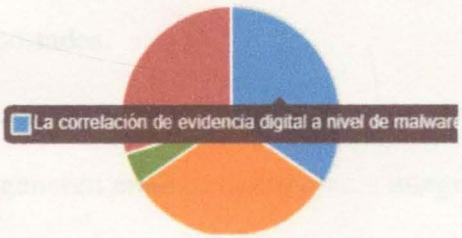
Menos de 1TB	0
Entre 1TB y 3TB	2
Entre 3TB y 5 TB	1
Más de 5 TB	21



15. En un futuro cercano, desde el punto de vista de forense digital ¿a cuáles de las siguientes actividades cree que la tecnología aportará mayores ventajas? (seleccione 2)

Más detalles

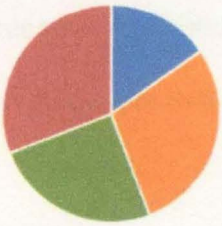
La correlación de evidencia di...	15
El análisis de grandes volúme...	14
Análisis de Kernel de sistemas ...	2
Correlación de de evidencia g...	13



16. A su parecer, ¿cuáles de las siguientes características son las más importantes para una herramienta de análisis o búsqueda simultánea en distintas fuentes de información para orientar la investigación? (Seleccione dos como máximo)

Más detalles

Gran capacidad de almacena...	8
Capacidad de correlación de e...	15
Capacidad de visualización de...	13
Automatización de procesos	16



Análisis cuantitativo:

Fueron encuestados 24 peritos de informática forense, entre los cuales se incluyen los jefes de los laboratorios de informática forense regionales encontrando el siguiente análisis:

- El 67% de las personas encuestadas indican que no conocen herramientas de correlación de evidencia digital.
- El 96% de los encuestados manifiestan que por la capacidad actual, sólo se pueden almacenar evidencias digitales por un periodo no superior a un año.
- Un 63% de los encuestados evidencia la importancia de correlacionar evidencias digitales como punto de apoyo a la administración de justicia.
- El nivel de correlación de evidencias digitales actual es NULO.

Análisis cualitativo:

- Esta pregunta permitió establecer que los peritos analizan evidencia digital relacionada con múltiples delitos, los cuales a su vez pueden ser correlacionados a nivel de las evidencias aportadas.
- De esta forma se identifica una necesidad de contar una plataforma que pueda procesar gran cantidad de datos que generen análisis complejos e integren resultados de manera masiva.
- Lo que demuestra que cada vez más se incrementa el análisis de evidencias digitales por cada laboratorio requiriéndose aumentar la capacidad de análisis de la misma.
- Para los peritos en informática forense se hace necesario contar con herramienta de Análisis y de correlación de información que muestre coincidencias de

manera automatizada.

Propuesta tecnológica para el CECIP – Banco Evidencia Digital

Como se ha mostrado a través del concepto del laboratorio de informática forense a nivel de definición, características, estructura, capacidades y funciones, encontramos que el nivel central cuenta con unas capacidades más robustas con relación a los laboratorios regionales, existen capacidades limitadas de almacenamiento y procesamiento, siendo además totalmente descentralizado, sin que exista capacidad de análisis correlacionado de evidencia digital, lo cual, ante el considerable volumen de información que recolectan, resulta un despropósito no estar integradas estas capacidades, ocasionando que el nivel de explotación sea mínimo como aporte al proceso de Desarrollo de Investigación Criminalística y por ende a la administración de justicia.

Por tal razón se hace necesario contar con una solución tecnológica que permita dar respuesta a los desafíos actuales de almacenamiento, correlación y análisis de evidencia digital, soportado en un sistema de hiperconvergencia.

En este sentido, la Dirección de Investigación Criminal e INTERPOL a través de la implementación de un "BANCO NACIONAL DE EVIDENCIA DIGITAL" en el Centro Cibernético Policial, no solo verá reflejado el aumento de la capacidad de almacenamiento y procesamiento, sino lo más importante, la correlación y análisis de evidencia digital, dando respuesta a requerimientos judiciales, atención de casos e investigaciones en todos los campos y eventos o amenazas de ciberseguridad, con calidad, oportunidad, impacto, confidencialidad y aporte significativo a la administración de justicia en el marco de la investigación criminal.

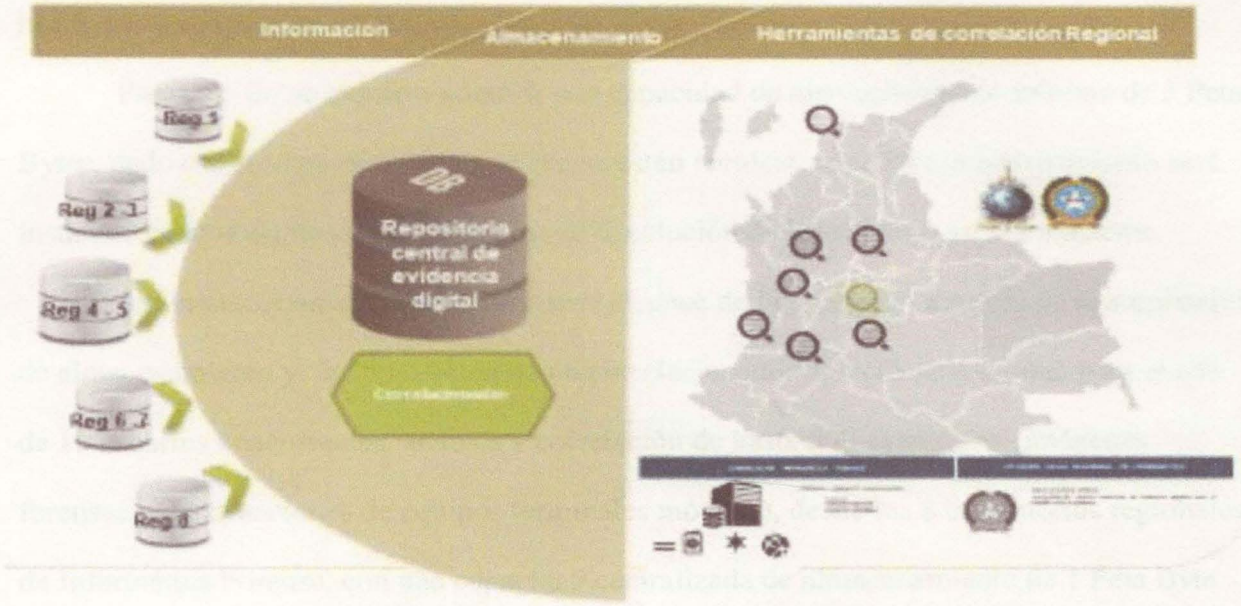


Figura 5. Propuesta tecnológica de Banco Nacional de Evidencia Digital.

Descripción técnica de la propuesta

A nivel lógico, a través de la infraestructura de red de la Policía Nacional que conecta a las distintas unidades de policía, se conectan a las ocho regiones de investigación criminal en las cuales funcionan los laboratorios de informática forense, para que accedan por red al propuesto Banco Nacional de Evidencia Digital que tiene varias funciones, entre las que están:

- Almacenamiento
- Procesamiento
- Análisis
- Correlación

De esta forma, los usuarios que accedan al banco de evidencia digital, podrán cargar al mismo, la imagen forense de la evidencia analizada para cruzarla con las demás evidencias

históricas y actuales existentes.

Para este fin se requiere adquirir una capacidad de almacenamiento mínima de 5 Peta Bytes, dado el volumen de evidencias que se están recolectando. Este almacenamiento será instalado en el nodo de almacenamiento de la solución de hiperconvergencia existente.

Así mismo, con el fin de delimitar el alcance de la propuesta a través de la ampliación de almacenamiento y la adquisición de un correlacionador de evidencia digital, para el uso de 10 usuarios concurrentes, análisis y correlación de hasta 500 evidencias (imágenes forenses y/o extracciones de equipos terminales móviles), desde los 8 laboratorios regionales de Informática Forense, con una capacidad centralizada de almacenamiento de 1 Peta Byte por año, escalable a 5 Peta Byte.

Se debe dotar tecnológicamente (con Hardware y Software) el laboratorio, en donde se fortalecerá con almacenamiento (1 Peta Byte), procesamiento (sistema de Hyperconvergencia) y correlación de alta disponibilidad la centralización de capacidades con el fin de preservar, analizar y realizar minería de datos logrando identificar patrones de cibercrimen asociados a estructuras organizadas.

En este sentido, se verá reflejado el aumento de la capacidad de almacenamiento procesamiento y correlación de evidencia digital en un 100% cada año, dando respuesta a los requerimientos judiciales, atención de casos e investigaciones en todos los campos, y eventos o amenazas de ciberseguridad, con calidad, oportunidad, impacto, confidencialidad y aporte significativo a la administración de justicia, y en consecuencia, el incremento de resultados estratégicos y operacionales que contribuirán en los planes y programas de seguridad ciudadana, minimizando los factores y fenómenos delincuenciales que atentan contra la estabilidad y seguridad digital en el territorio colombiano.

TOTAL GIGABYTE ANALIZADAS				
Regional	**2017**	**2018**	**2019**	
1	29.062	48.161	25.338	
2	3.050	3.350	2.500	
3	78.079	38.640	18.182	
4	14.048	18.132	9.225	
6	114.694	138.894	98.227	
7	12.299	12.069	23.090	
8	11.475	11.953	8.831	
Laboratorio CECIP	129.618	53.261	34.955	
TOTAL	380.850	324.460	220.348	925.659

Tabla 11. Gibabytes analizados

Información recopilada de los años 2017, 2018 y 2019.

Técnicamente se requeriría de los siguientes elementos para realizar la implementación del Banco Nacional de Evidencia Digital, dando continuidad a la infraestructura existente en el laboratorio, así:

- Sistema de almacenamiento de alta disponibilidad
- Software de Correlación

Hardware requerido:

ÍTEM	DESCRIPCIÓN
1	Sistema de almacenamiento alta disponibilidad Dos (2) nodos NX 3155 y trece (13) nodos NX 8155 para ser incorporados al cluster actual, con crecimiento de computo, memoria y almacenamiento con las siguientes configuraciones: • El nodo NX 3155-G6 está compuesto de dos (2) x Intel Skylake Processor 2.1 GHz 12-core, con una capacidad de 192 GB de memoria RAM y cuenta con un sistema de almacenamiento hibrido con dos (2) discos de 3.84TB SSD y dos (4) de 8TB HDD. • El nodo NX 8155-G6 está compuesto de dos (2) x Intel Skylake Processor 1.8 GHz 8-core, con una capacidad de 192 GB de memoria RAM y cuenta con un sistema de almacenamiento hibrido con dos (2) discos de 3.84TB SSD y diez (10) de 8TB HDD. • Capacidad total almacenamiento 500 TB • Capacidad total procesamiento 208 Core • Capacidad total RAM 2.5 TB • GPU Alta disponibilidad • Conectividad a 10 GB

Tabla 12. *Propuesta de hardware a adquirir*

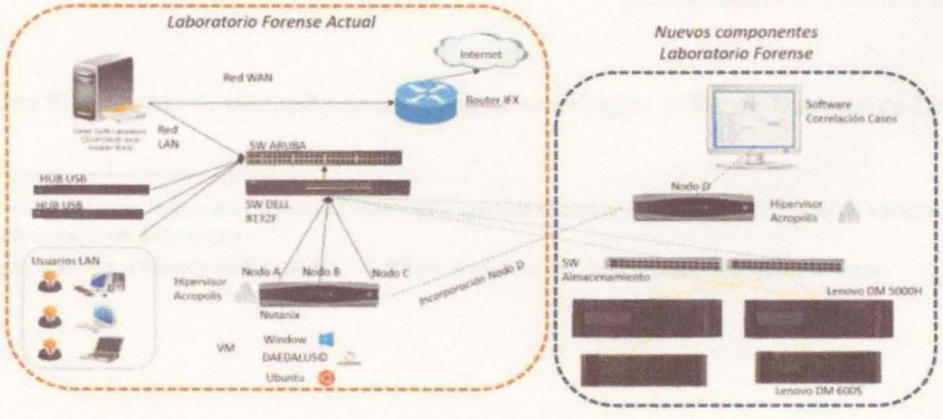
Necesidades de implementación a nivel de almacenamiento, procesamiento y conectividad.

Software requerido:

ITEM	DESCRIPCIÓN	
1.1	Software de correlación	• La detección y combinación inmediata de objetos con imágenes y videos, por ejemplo armas, dinero, desnudez, explotación infantil o documentos. • El enfoque en personas de interés con detección facial automática • El descubrimiento de pistas de manera más rápida con el reconocimiento óptico de caracteres • El análisis de vínculos de las redes relacionadas con el caso para revelar conexiones ocultas, jerarquías de grupo y patrones de comunicación. • La realización de un análisis de casos cruzados por sujeto, tipo de crimen o período de tiempo. Capacidades y beneficios: Trabaja casos más rápidamente, los investigadores pueden tener acceso directo a toda la evidencia forense digital. Con la facilidad de almacenar, indexar y unificar todas las evidencias digitales en una biblioteca de ciencia forense digital centralizada para que no derroche tiempo valioso usando herramientas dispares. Buscando con facilidad entre los datos históricos y los actuales de múltiples casos y fuentes con la seguridad de ver todo el panorama y todas las conexiones críticas que lo definen.

Tabla 13. Propuesta de software a adquirir

Necesidades de implementación a nivel de almacenamiento, procesamiento y



conectividad.

Figura 6. Propuesta tecnológica de Banco Nacional de Evidencia Digital con el discriminado de componentes.

Seguridad:

Para garantizar la seguridad del funcionamiento de esta solución tecnológica se deben considerar soluciones de seguridad perimetral en la infraestructura de red, por lo cual se sugiere la implementación de un firewall2 físico y Sandbox3 que estén conectados a la solución de almacenamiento y correlación de evidencias digitales con el fin de proteger la solución de ciberataques e infecciones de código malicioso.

Fortalecimiento a nivel de infraestructura:

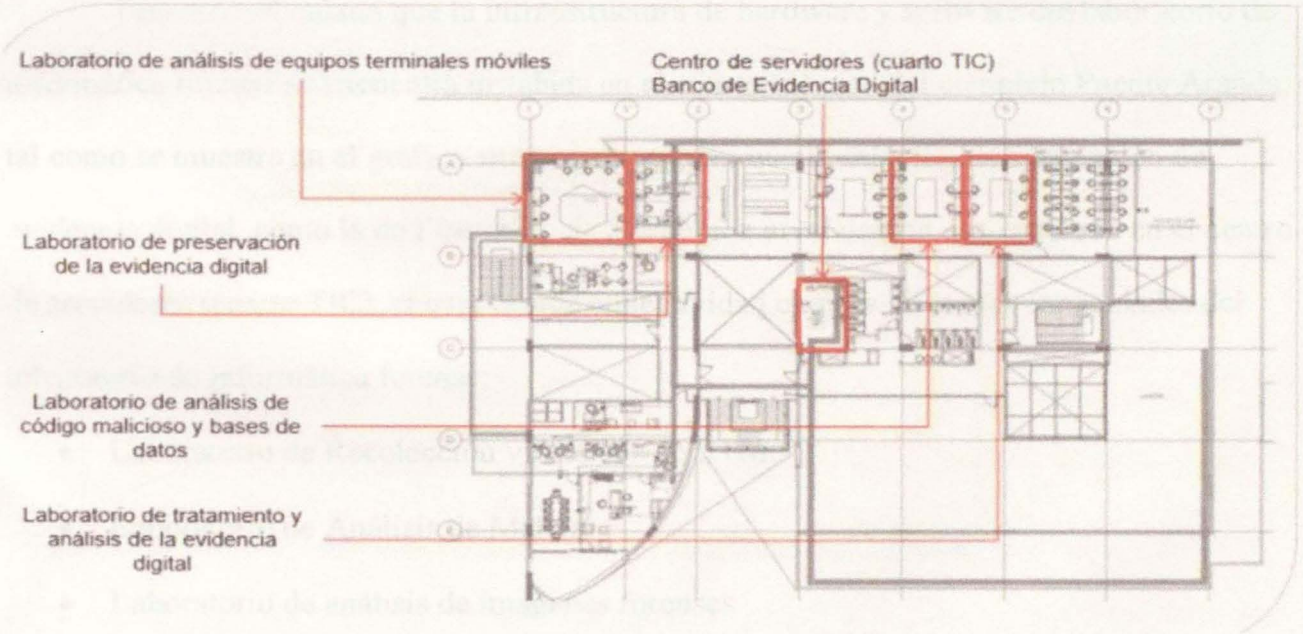


Figura 7. Propuesta de ubicación de componente tecnológico de Banco Nacional de Evidencia Digital.

[2] s es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

[3] A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros

F

Figura 8. Propuesta de ubicación de componente tecnológico de Banco Nacional de Evidencia Digital.

Teniendo en cuenta que la infraestructura de hardware y software del laboratorio de informática forense se encuentra instalada en el cuarto (4) piso del complejo Puente Aranda, tal como se muestra en el gráfico anterior, se sugiere que la solución de correlación de evidencia digital, como la de Firewall y de Sandbox a nivel central sea instalado en el centro de servidores (cuarto TIC), el cual brinda conectividad entre las distintas capacidades del laboratorio de informática forense:

- Laboratorio de Recolección y Análisis de ETM.
- Laboratorio de Análisis de Malware
- Laboratorio de análisis de imágenes forenses

Plan de implementación

Cronograma de actividades	Mes 1 y 2	Mes 3 y 4	Mes 5 y 6	Mes 7 y 8	Mes 9
1. Adquisición de componentes de almacenamiento y procesamiento					
2. Integración de componentes a solución de hiperconvergencia actual					
3. Articulación con laboratorios regionales					
4. Instalación y puesta a punto de software de análisis y correlación de evidencia digital					
4. Capacitación y certificación					

Tabla 14. Plan de trabajo para implementar el Banco Nacional de Evidencia Digital

La implementación de este proyecto corresponde a 10 meses.

Importancia de implementación de propuesta tecnológica

Relación frente a aspectos sustanciales de normatividad nacional e internacional:

Alineándose con los preceptos normativos definidos a través de los tratados sobre derechos humanos y constitución política, esta propuesta representa un reto que permite la persecución penal de conductas criminales que transgredan el código penal colombiano y afectación en el ámbito internacional, más aún cuando Colombia al hacer parte del convenio de Budapest, debe contar con las herramientas necesarias de articulación que permita una respuesta integral contra el cibercrimen en un entorno trasnacional.

Impacto en la administración de justicia:

Ante el exponencial incremento del uso de las tecnologías de la información y las comunicaciones como medio o fin del cibercrimen en el mundo, producto de la migración social de lo analógico a lo digital, ya que la cotidianidad de los aspectos económicos, sociales y culturales de las naciones se desarrollan hoy en día en el ciberespacio (educación, finanzas, comunicaciones, redes sociales, móviles, trabajo, entre otros), sumado a los altos índices de impunidad y poca efectividad en la aplicación de la Ley y sanción penal, motivada, no solo por la escasa cultura de denuncia ciudadana por múltiples factores, sino también, y más importante aún, el desconocimiento, la debilidad argumentativa y técnica frente al debate en estrados judiciales de los elementos materiales probatorios, poner en funcionamiento esta iniciativa permitirá a la policía judicial, a Jueces y Fiscales contar con acervo probatorio de evidencia digital correlacionado, que demuestre más allá de toda duda razonable la responsabilidad individual o colectiva de los hechos investigados, para de esta manera aplicar las sanciones penales correspondientes.

Impacto institucional:

Desembocará en el fortalecimiento de las capacidades de informática forense de la Policía Nacional, para enfrentar los nuevos y exigentes retos de la lucha contra el cibercrimen, posicionando al Centro Cibernético Policial como la unidad líder y pionera en la región frente a la implementación de soluciones de correlación y análisis de evidencia digital, especialmente relacionada a temas de malware, toda vez que esto ayudaría a automatizar el trabajo de identificación de patrones característicos frente al tipo de Malware, familia, autor, fecha de creación, versión, funcionalidad y capacidad a través de una búsqueda especifica de su estructura mediante una validación hash, aportando con esto menor tiempo de respuesta

ante las diferentes solicitudes judiciales.

Así mismo, a nivel estratégico la implementación de esta propuesta se alinea a lo contemplado en el documento CONPES 3995 de 2020 de "Política Nacional de Confianza y Seguridad Digital", concretamente relacionado a su objetivo de establecer medidas para mejorar la confianza y seguridad digital, de manera que la institución mediante el fortalecimiento de las capacidades del Centro Cibernético, aumentando las condiciones técnicas actuales a nivel de análisis y correlación de evidencias digitales incluidas las de software malicioso, aportaría de manera importante al logro de esta política nacional.

Impacto ciudadano:

A través de la operacionalización de la presente propuesta se contribuirá a la generación de confianza ciudadana en los entornos digitales, que constituye un principio vital frente al crecimiento económico y social de los colombianos, impulsando la competitividad y productividad de todos los sectores de la economía nacional, coadyuvando no solo a ampliar esa confianza y seguridad digital, sino al fortalecimiento de las capacidades respecto del actuar profesional del cuerpo policial, combinando herramientas, conocimiento y talento humano, de forma tal, que contribuya significativamente a la misión de la Policía Nacional con enfoque en la prevención, convivencia y seguridad ciudadana.

Por otra parte, es de anotar que el aporte que se pretende hacer con este documento consiste en mostrar la necesidad de implementar un modelo y una solución tecnológica que permitiría apoyar las actividades científicas de los laboratorios de informática forense de los cuales dispone la Policía Nacional en su actuar investigativo. Acompañado de una justificación cuantitativa y una propuesta tecnológica que daría respuesta a los requerimientos técnicos de la infraestructura necesaria.

Funcionalidades de Banco de Evidencia Digital

En este ítem se busca establecer las capacidades del Banco de Evidencia Digital entre los cuales se encuentran:

Almacenamiento: A través del incremento de un 100% en el almacenamiento actual de evidencias digitales correspondiente a 01 PETA BYTE por año para llegar a 05 PB, se aumentará el tiempo de persistencia de los datos para su futura correlación. Este se realizará de manera centralizada, es decir que cada laboratorio a nivel nacional tenga la posibilidad de almacenar su información en un único repositorio nacional.

Control de evidencias digitales: A través de un sistema único, centralizado que haga un inventario a nivel nacional de evidencias digitales gestionadas por los distintos laboratorios regionales, permitiendo su administración y evitando duplicidad de esfuerzos, además con la posibilidad de asignar ordenes de trabajo de acuerdo a la carga laboral de cada laboratorio de informática forense del Centro Cibernético.

Articulación: Mediante la integración de los laboratorios de informática forense por topología de red de Policía Nacional.

Correlación: Cross Match realizado con evidencias analizadas por el sistema de los distintos laboratorios de informática forense.

Generación de productos especializados que permitan la toma de decisiones: Mediante la estructuración de reportes de hallazgos donde el banco de evidencia digital muestre aspectos importantes de un análisis especifico, en la medida que sean correlacionadas las distintas evidencias históricas y actuales a nivel nacional.

NO.	ETAPA	DESCRIPCIÓN (QUÉ PUEDE PASAR Y CÓMO PUEDE OCURRIR)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	¿A QUIEN SE LE ASIGNA?	TRATAMIENTO / CONTROLES A SER IMPLEMENTADOS	PERSONA RESPONSABLE POR IMPLEMENTAR EL TRATAMIENTO	FECHA ESTIMADA QUE SE INICIA EL TRATAMIENTO	FECHA ESTIMADA QUE SE COMPLETA EL TRATAMIENTO	MONITOREO Y REVISIÓN	
									¿CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD ¿CUÁNDO?
1	IMPLEMENTACIÓN	Desarrollo de nuevas tecnologías de recolección de información	Obsolescencias tecnológicas frente a nuevas tecnologías	CONTRATISTA	Solicitud de actualización por 3 años	CONTRATISTA	DE ACUERDO SOPORTE Y GARANTÍA	Al finalizar el contrato de soporte y garantía	Número de usuarios de nuevas herramientas	DE ACUERDO CON EL CRONOGRAMA DEL PROCESO
2	IMPLEMENTACIÓN	Los laboratorios regionales no utilicen la solución	No se logre la correlación de evidencias digitales	PONAL	Cada uno de los jefes de laboratorio deberán informar periódicamente las actividades de uso	Jefes de Laboratorio de informática forense	Con el inicio de implementación del proyecto	Cada vigencia	Muestras correlacionadas por la plataforma para análisis y revisión de logs de acceso	Bimensual
3	IMPLEMENTACIÓN	Los laboratorios no suban las evidencias para análisis	La plataforma no tendrá insumos para correlacionar evidencias	PONAL	Cada uno de los jefes de laboratorio deberán informar periódicamente las actividades de uso	Jefes de Laboratorio de informática forense	Con el inicio de implementación del proyecto	Cada vigencia	Muestras cargadas a la plataforma	Bimensual
4	MENT	Que la solución en red para el análisis y	Indisponibilidad de uso de la plataforma	PONAL OFITE	Solicitud a la Oficina de Telemática para que brinde	JEFE OFICINA DE TELEMATICA	Con el inicio contractual del proyecto	Cada vigencia	Diagnóstico mensual de ancho de	Mensual

		correlación colapse o no esté disponible			disponibilidad en ancho de banda y continuidad en el servicio				banda, nro. de peticiones concurrentes hechas a la plataforma	
5	IMPLEMENTACIÓN	Que no se obtengan resultados del Banco de Evidencia Digital	Se genere un concepto negativo de la operación del banco de evidencia digital	PONAL	Cada uno de los jefes de laboratorio deberán informar periódicamente las actividades de uso	Jefe del Laboratorio Central de Informática Forense	Con el inicio contractual del proyecto	Cada vigencia	Seguimiento a muestras analizadas, correlaciones exitosas	Mensual
6	IMPLEMENTACIÓN	Al ser una tecnología nueva puede generar problemas por falta de capacitación	Resultados negativos por falta de capacitación	CONTRATISTA	Incluir en especificaciones capacitación y acompañamiento	CONTRATISTA	DE ACUERDO CON EL CRONOGRAMA DE IMPLEMENTACIÓN	Durante la ejecución del proyecto	Medición del desempeño de analistas y de uso de herramienta	DE ACUERDO CON EL CRONOGRAMA DEL PROCESO

Matriz de Riesgos del Proyecto

Tabla 15. Definición de riesgos producto de la implementación del Banco Nacional de Evidencia Digital

Identificación de Stakeholders:

El equipo de proyecto del Centro Cibernético Policial de la Policía Nacional identifica los Stakeholders para el proyecto a través de una sesión de lluvia de ideas. En esta sesión participa el equipo primario de proyecto, el Sponsor del proyecto y está dividida en dos partes: la primera parte se enfocará en los stakeholders internos de la Policía Nacional como y la segunda parte se enfocará en los stakeholders externos, Los siguientes criterios son utilizados para determinar la inclusión de un stakeholder:

¿La persona o la organización esta directa o indirectamente afectada por este proyecto?

¿La persona o su organización mantienen una posición desde la cual pueden influenciar al proyecto?

¿La persona tiene un impacto en los recursos del proyecto (materiales, personal, fondos)?

¿La persona o su organización tienen habilidades especiales o las capacidades que el proyecto requerirá?

¿La persona es potencialmente beneficiada por el proyecto o están en una posición para resistir el cambio?

Cualquier individuo que cuente con una o más de los criterios mencionados anteriormente, son identificados como stakeholder. Stakeholders de la misma organización serán agrupados con el fin de simplificar la comunicación y la administración de los mismos, a continuación se listan los interesados identificados por categorías:

Equipo primario del proyecto:

- Liderado por el Jefe del Centro Cibernético Policial como gerente del proyecto.
- Profesional en tecnología.
- Profesional de comunicaciones.
- Profesional perito en informática forense.

Apoyo al equipo del proyecto

- Contratista de implementación.
- Proveedores de tecnología.
- OFITE - Director de la oficina de telemática.

Usuarios del Banco de Evidencia Digital

- Peritos de informática forense laboratorio Central.
- Peritos de informática forense laboratorio.
- Jefes de laboratorios regionales de informática forense.
- Gobierno Nacional.
- Fiscalía General de la Nación.
- Otras especialidades de la Policía Nacional (DIPRO, DIASE, DISEC).

Patrocinadores

- Ministerio de Defensa Nacional.
- INL.

Afectados por la ejecución del proyecto:

- Organizaciones del cibercrimen.

Otros intervinientes que pueden colaborar con la ejecución del proyecto

- Entes internacionales contra el cibercrimen.
- Unidades internacionales de cibercrimen.
- FBI.
- EC3 – European Cibercrime Centre.
- Grupo 24/7 del G8

Stakeholders clave:

El equipo del proyecto C4 de la Policía Nacional identifica los stakeholders clave quienes tienen la mayor influencia en el proyecto o quienes pueden llegar a verse más impactados por el mismo. Estos stakeholders clave son aquellos que también requieren la mayor gestión y comunicación las cuales serán determinadas como los stakeholders a analizar.

Una vez identificados, el Administrador del proyecto desarrollará un plan para obtener su retroalimentación en el nivel de participación que decidan, la frecuencia y el tipo de comunicación y cualquier asunto o conflicto de intereses que se presente.

Modelo de stakeholders

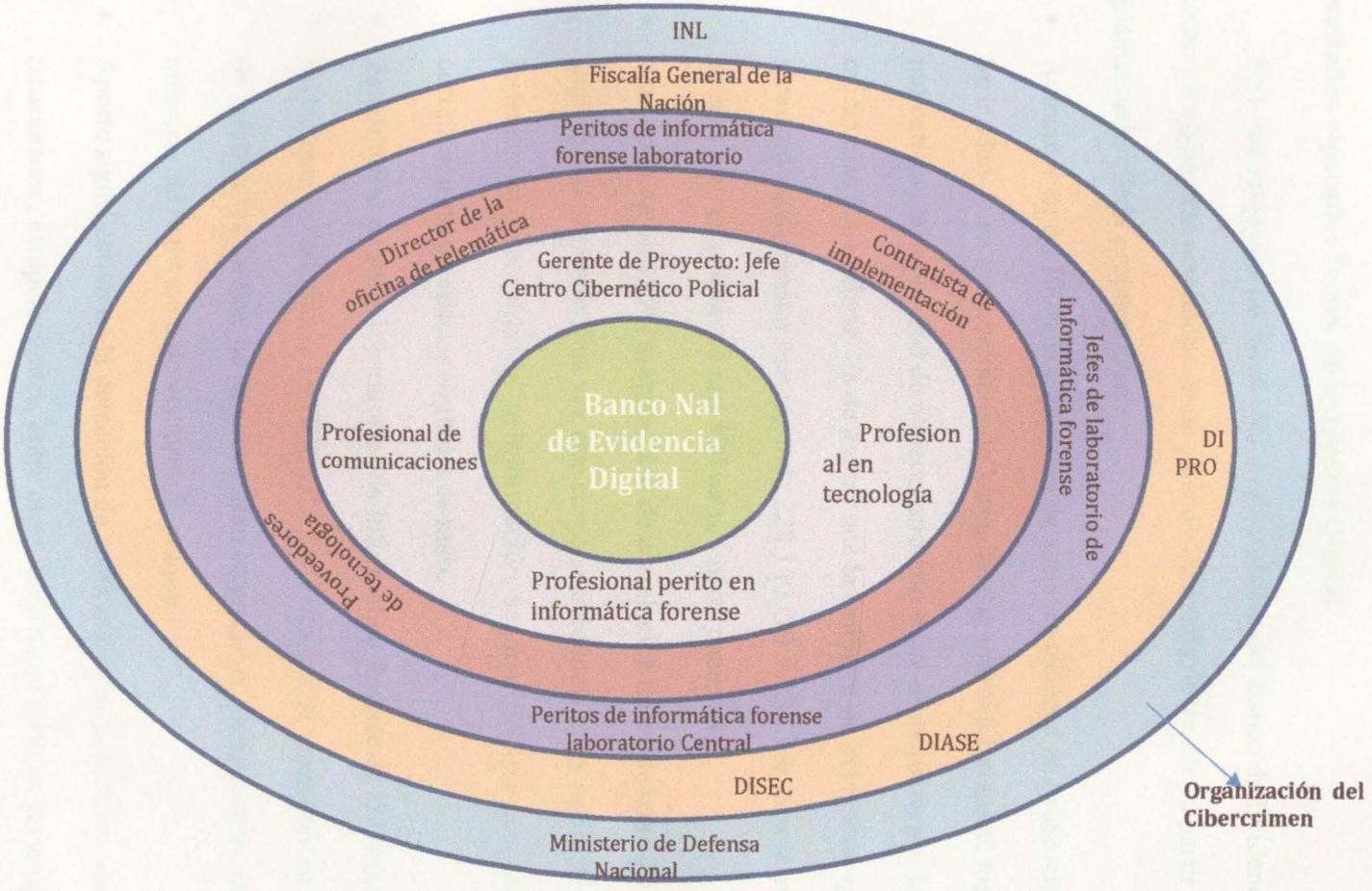


Figura 9. Definición de interesados del proyecto

Resultados esperados Banco de Evidencia Digital

Una vez revisadas las funciones y capacidades del Banco de Evidencia Digital, se esperan los siguientes resultados en un periodo estimado de un año, a partir de la implementación de la propuesta, así:

- Aumentar en un 100% la capacidad de almacenamiento de evidencias digitales. Se evidencia en los resultados de las encuestas practicadas donde los peritos indican que la capacidad de almacenamiento se ve desbordada por la cantidad de evidencias por analizar. Es de anotar que la cantidad de evidencias que se ha alcanzado a almacenar corresponde 228.140 GB = 228 Teras, solo en lo corrido de este año, en promedio son 500 teras a nivel nacional.
- Aumentar en un 100% la capacidad de correlación de evidencias digitales. Se sugiere este aumento toda vez que como se evidencia en la aplicación del instrumento de recolección de información, se identifica que la capacidad de correlación de evidencias digitales es nulo.
- Articulación de los 8 laboratorios de informática forense de la Dirección de Investigación Criminal e INTERPOL. Toda vez que al momento los laboratorios de informática forense no se encuentran conectados. Dificultando compartir muestras de malware ó de vectores de ataque.
- Aporte significativo en la detección de cross match de evidencias por casos de ransomware, estupefacientes, entre otros delitos que utilizan las tecnologías de la información como medio. Lo anterior, toda vez que actualmente no se cuenta con herramientas que realicen este tipo de función en la Policía Nacional.

Conclusiones

Una vez revisados los resultados del modelo para la implementación de un Banco de Evidencia Digital, se puede concluir:

- La implementación de este tipo de soluciones tecnológicas puede contribuir a la Policía Nacional en la generación de nuevas capacidades para combatir el cibercrimen a través de la correlación de evidencias digitales asociadas al cibercrimen y generar valor frente el apoyo a la administración de justicia.
- La Policía Nacional no cuenta con una solución tecnológica que permita el almacenamiento centralizado de evidencia digital y su análisis bajo los conceptos de correlación e hiperconvergencia.
- Teniendo en cuenta el incremento del uso de las tecnologías de la información y las comunicaciones como medio o fin del cibercrimen, se hace necesario contar con una plataforma hiperconvergente que permita el almacenamiento, procesamiento, correlación y análisis centralizado de la evidencia digital de los laboratorios de informática forense del Centro Cibernético.
- Con la implementación de esta propuesta se espera que se incrementen los resultados estratégicos y operacionales que contribuyan en los programas de seguridad ciudadana e investigación criminal, logrando minimizar los factores y fenómenos delincuenciales que atentan contra la ciberseguirdad de los ciudadanos.

Glosario

Adquisición: se refiere al procedimiento técnico-forense de la realización de una copia exacta a partir de un dispositivo de almacenamiento de datos digitales.

AES: Algorithm Encription Standard – Algoritmo Estándar de Encripción.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Análisis de evidencia digital: Etapa en la cual a través de scripts y de herramientas de software forense, se logra recuperar, indexar, correlacionar, reconstruir información y archivos del sistema, dando cumplimiento a lo ordenado por la autoridad judicial competente.

Análisis de Grandes Volúmenes de Información en Sistemas Informáticos forense: Examen o revisión de carácter pericial que debe ser objetivo, crítico, sistemático y selectivo. Se puede resumir en un procedimiento técnico legal que combina diferentes áreas entre ellas; investigación, análisis de información, recopilación de pruebas, evidencias legales, declaración, testimonio certificado, preparación y habilitación de pruebas.

Antivirus: Categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

API: Interfaz de programación de aplicaciones, abreviada como API (del inglés: Application Programming Interface), es el conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Cadena de custodia: Herramienta que permite garantizar la autenticidad, preservación e integridad de los elementos materia de prueba (evidencias), recolectados en virtud de una investigación.

Cifrado: En criptografía el cifrado, es el procedimiento gracias al cual se escribe un mensaje utilizando un código secreto o cifra de forma que la comprensión del mensaje sea imposible o, al menos, difícil a toda persona que no tenga la clave secreta para descifrarlo.

CMD: Símbolo del Sistema aplicado a Windows y otros asociados a las versiones de Microsoft.

Contención de la Amenaza: Este parámetro indica que capacidad tiene la tecnología antivirus actual para impedir que la amenaza se propague. Como norma general, las técnicas de virus antiguas suelen detectarse con facilidad. Los nuevos tipos de amenazas o los virus muy complejos son mucho más difíciles de detectarse y, por lo tanto, son algo más que una amenaza para la comunidad de usuarios. Los valores posibles son fáciles (la amenaza se detecta con facilidad).

CPU: Parte interna del Equipo de cómputo descrito como Unidad Central de Procesamiento.

Crimeware: Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Cuarentena: Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar.

Datos volátiles: Se refiere a los datos que se encuentra en memoria RAM, correspondiente a procesos, aplicaciones y servicios. Que son fundamentales cuando se hace

la preservación de información en el lugar de los hechos, siempre y cuando el o los dispositivos se encuentren activos (encendidos).

Dispositivo de almacenamiento digital: Son componentes que leen o escriben datos en medios o soportes de almacenamiento, y juntos conforman la memoria o almacenamiento secundario de la computadora.

Dispositivo móvil: Corresponde a un equipo electrónico, con capacidad de almacenamiento y procesamiento, diferentes funciones multimedia, hasta de comunicación y navegación en internet entre otras características.

Disponibilidad: Que la información se encuentre disponible para quien está autorizado disponer de ella.

Display (visualizador): ciertos aparatos electrónicos que permite mostrar información al usuario de manera visual.

Dll: Librerías de Windows NT en adelante.

EMP y EF: Corresponde a los elementos materiales probatorios y/o evidencia física, en el caso de la informática forense a dispositivos tecnológicos o electrónicos que son recolectados y sometidos a cadena de custodia, para que obre dentro de un proceso investigativo.

Equipo Terminal Móvil (ETM): Equipo electrónico que posea un identificador internacional único por medio del cual el usuario accede a las redes de telecomunicaciones móviles

ESN: (Número de Serie Electrónico) más conocido como IMEI, es un número de identificación permanente que se utiliza para identificar los dispositivos móviles

Evidencia Digital: Cualquier información que sujeta a una intervención humana u

otra semejante, ha sido extraída de un medio informático. Tomado de Cano, J. (2009) Computación forense. Descubriendo los rastros informáticos Pág. 3.

FAT: File Alocated Table – Tabla de asignación de archivos, comúnmente conocido como FAT (del inglés file allocation table), es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me.

Firma antivirus: Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes.

Forense: es el que ejerce su función por delegación judicial o legal.

Función Hash: Algoritmo matemático que, a partir de un archivo, puede generar un valor único e irrepetible, que permite preservar la integridad de este. Los más comunes MD5, SHA1 y SHA2.

GUI System: Interfaz gráfica del usuario del sistema.

Hardware forense: Definido como los equipos tecnológicos que participan en el desarrollo de la informática forense, los cuales permiten ejecutar el software forense para realizar las actividades propias de la materia.

Hexadecimal: Se trata de la observación y análisis mediante números y letras donde se determinan los aspectos de importancia de la memoria volátil.

Hook: Enganche hacia procesos y aplicaciones.

ICCID: Identificador Internacional de la Tarjeta de Circuitos.

Identificación Temporal del Abonado Móvil (TMSI): identificación del teléfono

móvil en determinada zona que es asignada al azar por el Visitor Location Register VLR (Registro de Localización de Visitante) y cambia cada vez que se mueva de área geográfica o zona.

IEA: Información Electrónicamente Almacenada, corresponde a cualquier elemento del activo de la información y los datos dentro de cualquier dispositivo de almacenamiento.

Imagen forense: Es una copia exacta bit a bit, que se realiza a un dispositivo de almacenamiento digital, se puede realizar la adquisición con varias herramientas forenses.

Imagen física: Copia exacta que se realiza desde el primer bit al último bit de un dispositivo con capacidad de almacenamiento.

Imagen lógica: Extracción de parte o total de archivos lógicos que se encuentran almacenados dentro de un dispositivo con capacidad de almacenamiento.

IMEI (Sistema Internacional para la Identidad de Equipos Móviles): es un código que identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta.

IMSI: Identidad Internacional del Suscriptor u operador Móvil.

Informática Forense: Disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios Informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. Entendiendo los elementos propios de la tecnología de los equipos de computación ofrece un análisis de la información residente en dichos equipos. Tomado de: Computación Forense: Descubriendo los rastros informáticos"PH.D CFE Jeimy José Cano Martínez.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias

negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Integridad: Garantizar que la información se encuentre completa, que sea la información original, para esta tarea se usan los algoritmos matemáticos MD5, SHA1 y SHA2.

Inyección de Código malicioso: Algunos factores y ataques realizados por ciberdelincuentes pueden estar ejecutados en memoria, esta actividad puede ser analizada entendiendo las diferentes actividades de origen malicioso que pueden convertirse en no nativas para un sistema operativo, por esta razón es vital determinar y enumerar cada uno de los pasos en la identificación, verificación y cuantificación de procesos ejecutados en el sistema.

Malware: También conocido como código malicioso y software malicioso, se refiere a un programa que se inserta en un sistema, por lo general de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos de la (s) víctima (s), aplicaciones o del sistema operativo o de lo contrario es molesto y puede interrumpir el acceso a la información de la víctima.

MEID: Número único global que identifica un teléfono móvil, se puede ver como un IMEI, pero con dígitos hexadecimales

Modos de visualización y parseo: Se detallan de acuerdo a su estructura y composición de lenguaje de observación y análisis.

MSISDN (Mobile Station Integrated Services Digital Network): estación móvil de la Red Digital de Servicios Integrados hace referencia al Número Abonado del Suscripción RDSI del Móvil.

NID: Number Identification Data – Número de identificación de datos.

No repudio: Quien participa en una actividad con información no podrá desconocer su intervención.

Parsing: Verificación de información por medio de herramientas para recuperación de información.

Perito: Persona que posee conocimientos, técnicos, científicos, artísticos o prácticos y al cual se acude en busca de un dictamen, para que como asesor facilite al juzgador, los conocimientos que sean necesarios o convenientes para una mejor apreciación de los hechos controvertidos.

Pharming: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea.

Phishing: Métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Protocolo: En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos

RAM: Memoria volátil del equipo de cómputo (Random Access Memory).

Software forense: Herramientas especializadas diseñadas para la adquisición, procesamiento, análisis y presentación de resultados, a partir del tratamiento realizado a la evidencia digital.

Suma de verificación: Corresponde a la actividad de calcular la integridad de una información, a través de un algoritmo matemático.

Tarjera mini SIM: es una tarjeta inteligente desmontable usada en teléfonos móviles y módems HSPA o LTE, mide 25 × 15 × 0,76 mm.

Tarjera micro SIM: es una tarjeta inteligente desmontable usada en teléfonos móviles y módems HSPA o LTE, tiene unas dimensiones de 15 × 12 × 0,76 mm.

Tarjera nano SIM: es una tarjeta inteligente desmontable usada en teléfonos móviles y módems HSPA o LTE, sus medidas son de 12.3 × 8.8 × 0.7 mm.

Tratamiento de evidencia digital: Comprende varias etapas por las que pasa la evidencia digital, surge luego de la adquisición de una imagen forense, o de la preservación de información, pasando por una etapa de procesamiento y análisis, finalizando con un reporte de las actividades realizadas.

Variantes de Malware: Las variantes son nuevas cepas de malware que piden prestados códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus: Programa informático escrito para alterar la forma como funciona una

computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

Volcado (Dump) o toma de sub- muestras: Se trata de la detección y la identificación de procesos anómalos o sospechosos para su posterior análisis por medio de sus cadenas de lenguaje o texto.

Código malicioso: es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

C.C.P: Centro Cibernético Policial

Ciberterrorismo: Uso de las Tecnologías de la información y las comunicaciones e Internet caracterizado en provocar y mantener en estado de zozobra o terror a la población o a un sector de ella, afectando el normal desarrollo de las actividades en el ciberespacio, mediante actos que ponen en peligro, la integridad física, soberanía nacional, las infraestructuras críticas de la nación y los medios de comunicación, sistemas informáticos Estatales u oficiales o del sector financiero, nacionales, públicos , privados o extranjeros, así mismo el desarrollo actividades de apoyo, como el reclutamiento, adiestramiento, intercambio de información, difusión de propaganda y la incitación a la comisión de actos de terrorismo a través de las Tics. (DEFINIDO POR EL CCP).

Ciberresiliencia: Reconocida como la capacidad institucional de garantizar la continuidad de los servicios policiales en materia de ciberseguridad y adecuarlos

oportunamente a los cambios vertiginosos que la informática a nivel global nos impone. (DEFINIDO POR EL CCP).

Kaspersky Lab: Es un grupo internacional que opera en más de doscientos países. La sede de la compañía se encuentra en Moscú, Rusia, desde donde supervisa las operaciones internacionales y el desarrollo empresarial.

En la actualidad, emplea a más de tres mil especialistas altamente calificados. Cuenta con oficinas regionales en veintinueve países, y sus productos y tecnología brindan protección a más de trescientos millones de usuarios de todo el mundo. (http://latam.kaspersky.com/sobre-kaspersky/sobre-la-compania)

Entidades del Gobierno de seguridad.

CCP -Centro Cibernético Policial de la Policía Nacional de Colombia es el centro especializado en la ciberseguridad Nacional.

colCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia: es el organismo coordinador a nivel Nacional en aspectos de ciberseguridad y ciberdefensa, el cual presta su apoyo y colaboración a las instancias nacionales tales como el CCP y el CCOC.

Te Protejo: es la primera línea virtual de denuncias en Colombia y Latinoamérica en convertirse miembro de la Fundación INHOPE, con apoyo de la Policía Nacional de Colombia.

Ciberdefensa: capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Tipos de incidentes digitales

Defacement: Consiste en la modificación de la página de bienvenida de un sitio web por otra cuyo contenido (pornografía, política, etc.) depende de la motivación de los atacantes.

Infiltración lógica externa: Actividad de un intruso que accede de manera abusiva a un sistema informático aprovechándose de una vulnerabilidad y eligiendo un vector de ataque de la organización logrando con ello afecta la disponibilidad, confidencialidad o la integridad de los datos.

Infiltración lógica interna: Actividad que se deriva de la participación y responsabilidad de un empleado con conocimientos para acceder a un sistema informático de la organización aprovechando de las potenciales vulnerabilidades o carentes en materia de políticas de seguridad de la información.

Phishing: Técnica utilizada para obtener información confidencial (nombres de usuario, contraseñas, etc.) mediante el envío de comunicaciones electrónicas aparentemente confiables.

Smishing: Variante del phishing enfocada en usuarios de telefonía móvil, mediante el empleo de mensajes de texto (SMS).

Referencias bibliográficas

Centro_Cibernético_Policial. (29 de 02 de 2020). https://caivirtual.policia.gov.co/. Recuperado de https://caivirtual.policia.gov.co/: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Ceballos, A., Bautista, F., Mesa, L., y Argáez, C. (2019). *Tendencias cibercrimen Colombia 2019-2020*. Recuperado de https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Congreso de la República. (24 de julio de 2000). Código penal. [Ley 599 de 2000]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de la República. (03 de agosto de 2001). Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. [Ley 679 de 2001]. Recuperado de https://www.unidadvictimas.gov.co/sites/default/files/documentosbiblioteca/ley-679-de-2001.pdf

Congreso de la República. (31 de agosto de 2004). Código de Procedimiento Penal. [Ley 906 de 2004]. Recuperado de https://www.unodc.org/res/cld/document/col/2000/codigo_de_procedimiento_penal_html/Codigo_de_Procedimiento_Penal.pdf

Congreso de la República. (16 de julio de 2006). Se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. [Ley 1150 de 2007]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

Congreso de la República. (05 de enero de 2009). De la protección de la información y de los datos. [Ley 1273 de 2009]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República. (21 de julio de 2009). Se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. [Ley 1336 de 2009]. Recuperado de https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

Congreso de la República. (24 de junio de 2011). Por medio de la cual se reforma el código Penal, El código de Procedimiento Penal, El código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. [Ley 1453 de 2011]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1453_2011.html

Congreso de la República. (17 de abril de 2013). Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. [Ley 1621 de 2013]. Recuperado de http://www.dni.gov.co/wp-content/uploads/2018/10/Ley-1621-del-17-de-Abril-de-2013.-Ley-de-Inteligencia-y-Contrainteligencia.pdf

Congreso de la República. (24 de abril de 2018). Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. [Ley 1928 de 2019]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Constitución Política de Colombia [Const.]. (1991). 2da Ed. Legis.

CONPES. (2020). Política Nacional de Confianza y Seguridad Digital. Bogotá DC.

Cyber Defense (2019). Cyber Security Statistics for 2019. Recuperado de https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

Departamento Administrativo de la Función Pública. (10 de enero de 2012). Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. [Decreto Ley 019 de 2012]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/decreto_0019_2012.html

Enjoy Safer Technology (2018). ESET SECURITY REPORT Latinoamérica 2019. Recuperado de https://empresas.eset-la.com/archivos/novedades/78/ESET-security-report-LATAM2019-final.pdf

Lewis, J. (2018). *Economic Impact of Cybercrime -No Slowing Down*. Recuperado de https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Ministerio de Defensa Nacional. Policía Nacional. (31 de diciembre de 2015). Por la cual se define la estructura orgánica interna de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias y se dictan unas disposiciones. [Resolución 05839 de 2015].

Ministerio de Tecnologías de la Información y las Comunicaciones -MinTic-. (12 de diciembre de 2014). Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. [Decreto 2573 de 2014]. Recuperado de https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones -MinTic-. (2016). Lo que usted debe saber del Conpes de Seguridad Digital. Recuperado de https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital

Organización de Estados Americanos (2020). Programa de Ciberseguridad. Recuperado de http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

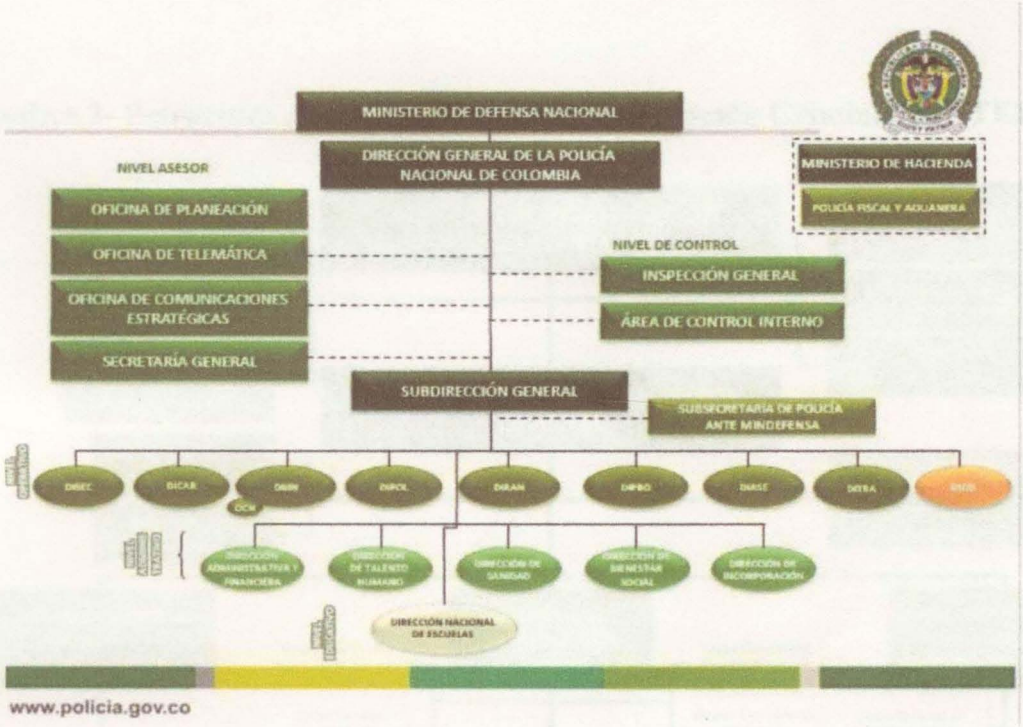
Planeación_DIJIN. (2020). SUITE VISION EMPRESARIAL. Recuperado de SUITE VISION EMPRESARIAL.

Robles, M. (2015). El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico. *Boletín Electrónico del Instituto español de Estudios Estratégicos*, 1-18. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

United Nation (2020). Cybercrime. Recuperado de https://www.unodc.org/unodc/en/cybercrime/index.html

Valencia, F. (2018). *Ciberseguridad.* Universidad Nacional de Colombia. Recuperado de http://pensamiento.unal.edu.co/fileadmin/recursos/focos/desarrollo-sostenible/Simposio_4a_Revolucion/8_Francisco_javier_valencia/9_Francisco_Javier_Valencia.pdf

Anexos



Apéndice 1- Estructura actual Policía Nacional

Imagen 10. Muestra la estructura jerárquica de la Policía Nacional.

Apéndice 2- Estructura actual Dirección de Investigación Criminal e INTERPOL

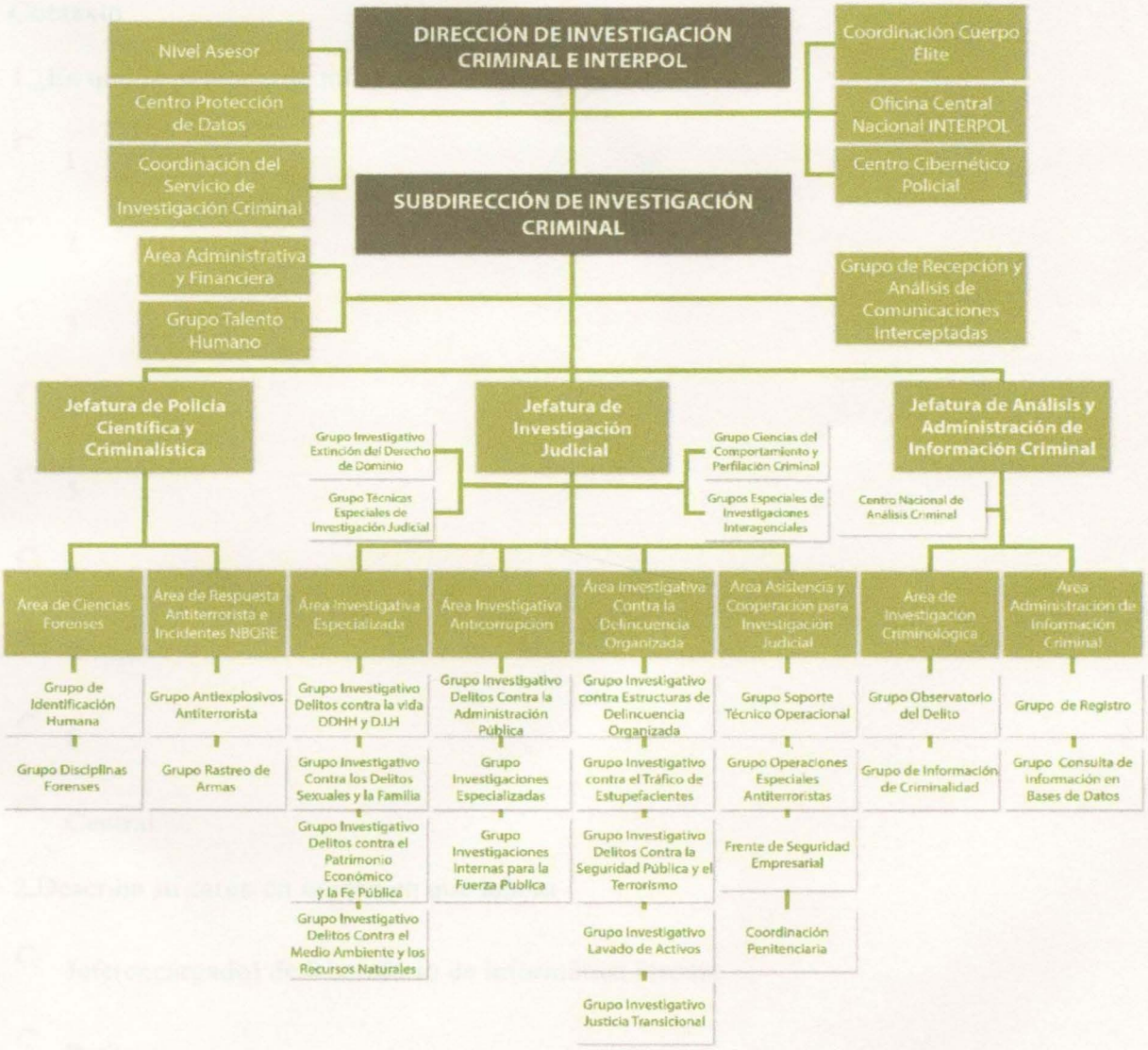


Imagen 10. Muestra la estructura interna DIJIN.

Apéndice 3 – Formato de Encuesta practicada

Proyecto Banco Nacional de Evidencia Digital

Este análisis permite identificar análisis del laboratorio de informática forense

Sección 1

Contexto

1.¿En qué laboratorio de informática Forense labora?

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- Central

2.Describa su cargo en unidad en que labora

- Jefe(encargado) de laboratorio de informática forense
- Perito

3.¿En qué tipo de investigaciones participa?

- [ ] Abuso sexual de menores
- [ ] Lucha contra el terrorismo
- [ ] Ciberdelincuencia
- [ ] Tráfico de drogas
- [ ] Delitos contra el medio ambiente
- [ ] Extorsión
- [ ] Otra

4.¿Qué tipo de actividad realiza en el Laboratorio de Informática Forense?

- ( ) Recolección de Evidencia Digital
- ( ) Análisis de Evidencia Digital
- ( ) Análisis de ETM

5.¿Qué plataformas de análisis de datos usa actualmente su laboratorio o usará en un futuro cercano?

- [ ] BriefCam
- [ ] Cellebrite
- [ ] Forensic Toolkit (FTK)
- [ ] Hansken
- [ ] No usa ninguna plataforma

6.¿Cuáles son las fuentes de información recolectada y analizada como parte de su

peritaje?

- Audio
- Texto
- Imágenes
- Video
- Localización geográfica

7.¿Cuáles son los tipos de datos que recoge como parte de su peritaje?

- Correo electrónico y chats
- Datos de red(interceptados)
- Llamadas telefónicas (interceptadas)
- Dispositivos de grabación
- Teléfonos inteligentes y tabletas
- Proveedores de telecomunicaciones
- Bancos y otros proveedores de servicios financieros
- Cámaras para la lectura de matrículas
- La web y los medios sociales
- Otros

8.¿Qué tipo de información está disponible pero no se usa plenamente? (seleccione todas las opciones que corresponda)

- [ ] Correo electrónico y chats
- [ ] Datos de red
- [ ] Llámadas telefónicas
- [ ] Teléfonos inteligentes
- [ ] Información estructurada
- [ ] Información no estructurada

9.¿Por qué este tipo de información no se usa plenamente? (seleccione todas las opciones que corresponda)

- [ ] No se dispone de datos
- [ ] Los datos no están en el formato adecuado
- [ ] No se dispone de herramientas adecuadas de análisis
- [ ] Otra

10.¿Cuál es el motivo de que estas actividades sean tan laboriosas ? (seleccione tres como máximo)

- ( ) La cantidad de datos
- ( ) La complejidad de los análisis
- ( ) La complejidad de los datos
- ( ) La dependencia de terceros
- ( ) La falta de conocimientos especializados

- La escasa calidad de los datos
- La integración de resultados provenientes de diferentes herramientas y fuentes
- Otro

Sección 2

Tecnología existente y experiencia de usuario

11.¿Actualmente existe alguna plataforma que permita correlacionar distintas evidencias digitales de distintos laboratorios de informática forense?

- Si
- No

12.¿Considera que los laboratorios de informática forense cuentan con una capacidad suficiente de almacenamiento digital respecto de la evidencia digital?

- Si
- No

13.¿Dada la capacidad de almacenamiento actual, por cuánto tiempo se puede almacenar en su laboratorio de informática forense evidencia?

- Menos de un año
- De uno a tres años
- De tres a cinco años
- Más de cinco años

14.En TB cuantas evidencias recolectan y analiza por año su laboratorio

- Menos de 1TB
- Entre 1TB y 3TB
- Entre 3TB y 5 TB
- Más de 5 TB

Sección 3

Oportunidades para nuevas herramientas y tecnologías

15.En un futuro cercano, desde el punto de vista de forense digital ¿a cuáles de las siguientes actividades cree que la tecnología aportará mayores ventajas? (seleccione 2)

- La correlación de evidencia digital a nivel de malware
- El análisis de grandes volúmenes de información
- Análisis de Kernel de sistemas operativos
- Correlación de de evidencia generada por ETM

16.A su parecer, ¿cuáles de las siguientes características son las más importantes para una herramienta de análisis o búsqueda simultánea en distintas fuentes de información para orientar la investigación? (Seleccione dos como máximo)

- Gran capacidad de almacenamiento
- Capacidad de correlación de evidencia digital
- Capacidad de visualización de los datos
- Automatización de procesos

17.Seleccione dos propiedades deseables en una herramienta de correlación y análisis de evidencia digital

- ☐ Tiempos de respuesta mínimos
- ☐ Alta capacidad de correlación de información
- ☐ Gran capacidad de almacenamiento de información
- ☐ Visualización de los resultados