



REPÚBLICA DEL ECUADOR
FUNCIÓN JUDICIAL
www.funcionjudicial.gob.ec

Juicio No: 17282201901265

Casillero Judicial No: 0

Casillero Judicial Electrónico No: 1720369634

afernandezsalvador@odiec.org, derechos@inredh.org, litigio@inredh.org,
pamelayalexandra@hotmail.com, rodrigo.adriel@live.com.ar

Fecha: miércoles 26 de abril del 2023

A: PAMELA CHIRIBOGA ARROYO

Dr/Ab.: PAMELA ALEXANDRA CHIRIBOGA ARROYO

**TRIBUNAL DE GARANTIAS PENALES CON SEDE EN LA PARROQUIA
IÑAQUITO DEL DISTRITO METROPOLITANO DE QUITO, PROVINCIA DE
PICHINCHA**

En el Juicio Especial No. 17282201901265 , hay lo siguiente:

VISTOS: Por sorteo de ley efectuado el viernes 16 de julio del 2021, a las 14:15 (fs. 28), ha correspondido a este Tribunal de Garantías Penales de Pichincha el conocimiento de la presente causa, signada bajo el número 17282-2019-01265, que tiene como antecedente la resolución de llamamiento a juicio en contra de OLA METODIOS MARTÍN BINI, por parte de la doctora Yadira Marisol Proaño Obando, Jueza de la Unidad de Garantías Penales con sede en la parroquia Iñaquito, del Distrito Metropolitano de Quito, de fecha 29 de junio del 2021, resolución emitida de conformidad a lo establecido en el artículo 608 del Código Orgánico Integral Penal, por presumirlo autor directo del delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, tipificado y sancionado en el artículo 234 del referido cuerpo legal. Ejecutoriada dicha resolución y luego de la sustanciación realizada por el Tribunal integrado por la doctora Fanny Isabel Altamirano Cárdenas, Jueza; doctor Milton Maroto Iván Sánchez, Juez; y, doctor Pablo Coello Serrano, Juez Ponente, se constituyen en Audiencia Oral de Juzgamiento para conocer y resolver la situación jurídica del prenombrado procesado Ola Methodius Martín Bini y, llevada a cabo la audiencia respectiva, el Tribunal procedió a deliberar, dando luego a conocer oralmente a los sujetos procesales su decisión y en cumplimiento a lo dispuesto en el artículo 621 del Código Orgánico Integral Penal, en concordancia con el artículo 76 numeral 7, letra l) de la Constitución de la República; y, artículo 130 numeral 4 del Código Orgánico de la Función Judicial, reduce a escrito su resolución, para lo cual realiza las siguientes consideraciones:

I JURISDICCIÓN Y COMPETENCIA: Este Tribunal de Garantías Penales de Pichincha es competente en el tiempo, personas, territorio y materia, para conocer,

sustanciar y resolver la presente causa, conforme lo previsto en el Art. 167 de la Constitución de la República; los artículos 220, 221 número 1 y 222 del Código Orgánico de la Función Judicial, modificados por la disposición reformativa segunda, numerales 14, 15 y 16 del Código Orgánico Integral Penal y acorde a lo establecido en los artículos 399, 402 y 404 número 1 del citado cuerpo legal.

II VALIDEZ PROCESAL: De conformidad con lo dispuesto en los artículos 76, 77, 168.6 y 169 de la Constitución de la República del Ecuador en la tramitación de esta causa, se han observado las garantías de debido proceso constitucional, por lo que verificado su cumplimiento se declara la validez de la misma.

III IDENTIDAD DEL PROCESADO: OLA METODIOS MARTÍN BINI, de nacionalidad sueca, con pasaporte No. 92344157, de 40 años de edad, de estado civil divorciado, de instrucción secundaria, de ocupación director técnico de una organización sin fines de lucro y con domicilio en la calle Juan Dibuja No. Oe2-30 y Voz Andes de Quito.

IV EL JUICIO PROPIAMENTE DICHO: El Juez Ponente del Tribunal de Garantías Penales procedió a informar al procesado Ola Metodios Martín Bini , sobre los derechos y garantías que le asiste la Constitución de la República del Ecuador, el derecho a un juicio imparcial ante su juez natural; a ser informado sobre los cargos propuestos en su contra por parte del Estado; derecho a ser asistido por un abogado defensor; que no pueden ser forzado a declarar contra su voluntad y puede acogerse al silencio; que su testimonio es un medio de defensa y prueba a su favor. **4.1**

ALEGATOS DE APERTURA 4.1.1. FISCALÍA: Por intermedio del doctor Fabián Chávez Zambrano, dijo que Fiscalía dará a conocer un caso que transgrede el bien jurídico tutelado por el Estado Ecuatoriano, como lo es la seguridad de los activos de los sistemas de información y comunicación, hecho suscitado en este Distrito Metropolitano de Quito, el 6 de octubre del 2015, lugar en que el acusado Ola Metodios Martín Bini, de nacionalidad sueca, quien se identifica ante la opinión pública y a través de su defensa como un supuesto desarrollador de software, aseveración que no se ha probado hasta el momento, conforme a derecho; dice que en esta audiencia demostrará que el procesado Ola Bini accedió sin autorización a los sistemas de telecomunicaciones de la Corporación Nacional de Telecomunicaciones (CNT), en contra de la voluntad, sin su consentimiento, con el objeto de explotar ilegítimamente el acceso logrado y así intentar obtener información del contenido digital otorgado, nada más y nada menos que a la Presidencia de la República del Ecuador para su sitio alerno de contingencia que se encontraba para alojar ahí, sus aplicaciones, sistemas, información crítica y confidencial; señala que en este sitio alerno de contingencia, se encontraba ubicado físicamente en el edificio La Previsora de la ciudad de Guayaquil, provincia del Guayas, en las instalaciones de Petroecuador, sitio alerno al Data Center principal de la Presidencia de la República, el cual se encuentra alojado en la ex secretaria de inteligencia SENAI, ahora SIES, sitio que le pertenece a la Presidencia de la República, el mismo que habría sido implementado por recomendación de la Contraloría General del Estado; señala que este acceso se lo realizó sin la autorización ni consentimiento de la proveedora de los datos de internet y que para el presente caso es la entidad estatal Corporación Nacional de Telecomunicaciones, acusadora particular en esta causa; así mismo no tuvo conocimiento ni consentimiento de Petroecuador, entidad estatal que brindaba el alojamiento de

hosting a este sitio de contingencia, así mismo no tenía el consentimiento de la Presidencia de la República, propietaria en sí, de los datos que constaban en este Centro de Contingencia; señala que se demostrará que el señor Ola Metodios Bini, como conector del desarrollo informático estuvo en nuestro país para obtener información posiblemente para su agrupación Wikileaks o gobierno de turno, quien además tuvo siempre la negativa de colaborar con la investigación, peor aún la solicitud de aperturar su amplia gama de dispositivos electrónicos que fueron incautados tanto en el aeropuerto de esta ciudad de Quito, así como en su domicilio; dice que para corroborar con lo señalado, el señor Ola Bini el 6 de octubre del 2015, accede sin autorización al Sistema Nacional de Telecomunicaciones y envía un mensaje en este sentido al aplicativo móvil WhatsApp al señor Marco Arguello, también procesado en esta causa; señala que la Fiscalía demostrará el acceso no autorizado a este dispositivo, el cual está prohibido y no estaba autorizado por la entidad proveedora CNT y que en sí comprometía la información de la Presidencia de la República; por tanto el señor Ola Metodios Bini adecuó su conducta, conforme lo indicado en el artículo 234 COIP, esto es el acceso no consentido a un sistema informático, telemático o de telecomunicaciones; trasgredió el bien jurídico protegido la seguridad de los activos de comunicación; lo acusa de autor directo. **4.1.2. LA DEFENSA DE LA ACUSACIÓN PARTICULAR:** Por intermedio del doctor Juan Pablo Alegría señala que comparece como delegado del procurador judicial y apoderado del abogado Ralf Suástegui, gerente general de la Corporación Nacional de Telecomunicaciones, comparecen porque la empresa pública presentó acusación particular, la cual fue calificada conforme a derecho; dice que demostrará, por medio de las pruebas testimoniales, documentales y periciales, el cometimiento del delito tipificado en el artículo 234 del COIP; en cuanto a los hechos manifiesta que el 6 de octubre del 2015, el señor Ola Matodios Martín Bini, le envía un mensaje por medio del aplicativo de WhatsApp al señor Marco Ricardo Arguello Jácome, con número de teléfono 593995404579 en el cual consta una fotografía que trae a colación la evidencia dirección Ip line 18111357169, que denota el usuario de Ola Bini y que establece la descripción de prevención de ingreso no autorizado al equipo de propiedad de la CNT, el cual presentaba el servicio a Petroecuador SENAI internet; con esta imagen se demostrará que el usuario utilizó la red de anonimato TOT, la cual sirve para enmascarar su identidad y su ID; señala que de igual manera, dentro de esta audiencia se demostrará, que por medio de la conversación de WhatsApp planteada por el señor Ola Metodios Bini y el señor Marco Ricardo Arguello Jácome, conforme a lo que se establece en el informe suscrito por el capitán William Castro Acosta, se adjuntan 147 fojas de conversaciones telefónicas obtenidas en el celular I pone 8, constante en cadena de custodia; señala que la red Lan que consta en la fotografía, es una red local, conforme lo determina la página 6 del informe de 16 de agosto del 2019; señala que se ha planteado el acceso no consentido al sistema de telecomunicaciones, se determina que por medio de la red de anonimato TOR, red que permite enmascarar la identidad, se utilizó el protocolo Tel Net con el afán de realizar una conexión de cualquier parte del mundo a la ONT y el router de la Corporación Nacional de Telecomunicaciones, equipos que son de la CNT y que se prestan para el servicio del cliente; señala que conforme al artículo 234 del COIP, en el cual se sanciona el acceso no consentido a los sistemas no informáticos, telemáticos y de telecomunicaciones y como ya lo manifestó el señor Ola Metodios

Bini, cuando ingresó al ruteador, pasando por la ONT, accedió sin consentimiento de la CNT; por lo antes manifestado señala que se atentó contra la seguridad de la Corporación, de sus clientes y en especial del Estado Ecuatoriano, al realizar un acceso no consentido a los sistemas de telecomunicaciones de la CNT. **4.1.3. LA DEFENSA DEL PROCESADO:** Por intermedio del doctor Carlos Soria Ávila dijo que este Juicio y sus connotaciones hasta el momento, han discurrido en los albores de la penumbra, en el camino de la arbitrariedad, en el influjo político en la administración de justicia, que lo único que han pretendido es escandalizar políticamente a la Función Judicial; esta audiencia por lo tanto será inusual para el sistema judicial ecuatoriano; probará el abuso del poder punitivo del Estado, ya que se trató de prejuzgar y se lo hizo, a una persona en el campo mediático, a una persona siendo inocente; se presentará un ejemplo de lo que no se debe hacer en el derecho penal y probarán que no existe acción o actividad alguna que sea penalmente relevante, para que sea el derecho penal quien busque su ejecución; se comprobará que no se trata de lo que supuestamente hizo el señor Ola Bini, sino de lo que hizo el Estado Ecuatoriano en su contra y que ahora de forma irracional e ilógica, intentan posicionar el cometimiento de un delito; dice que en la audiencia se probaran 2 cosas: que no existe, no existió y no puede haber existido acción penalmente relevante cometida por el señor Ola Bini y por lo tanto no existe delito ni responsable y que además todo el proceso penal desde su inicio, vulneró derechos humanos del señor Ola Bini; se probará además que este proceso inicia con una retención fiscal y judicial inmotivada, ilegal, arbitraria e ilegítima, comprobadas por una sentencia de la Corte Nacional de Justicia en apelación, en una acción de habeas corpus; se probará que la motivación para esta detención, fue por la necesidad única de perseguir a una persona y de justificar elementos políticos de un gobierno vulnerador de derechos humanos; se evidenciará claramente que el utilizar el derecho penal, en este caso el derecho penal de autor para satisfacer intereses, no ha sido importante para los representantes de Fiscalía y la acusación particular; probará en base de la prueba, que este proceso inició violando el derecho humano a la presunción de inocencia, expresado ya en sendas sentencias de la Corte Interamericana de Derechos Humanos; mediáticamente trataron de posicionar el cometimiento de un delito a una persona que no había realizado ningún tipo de hecho relevante, a la luz del derecho penal; se probará que Fiscalía y aprobado por una supuesta jueza de garantías, al haber hecho una reformulación de cargos faltando 3 días para que se acabe esta reformulación, lo que vulneró el derecho a la defensa del señor Ola Bini, considerando que efectivamente se tuvo un solo día para preparar la defensa de este nuevo cargo; dijo que se probará además que como producto de esta detención arbitraria, Fiscalía tuvo autorización para conocer, acceder y analizar los dispositivos que llevaba el señor Ola Bini y se probará que dicho análisis, fue realizado de manera ilegal, vulnerando derechos y todos los principios procesales que rigen las actuaciones de Fiscalía para la obtención de evidencia, pruebas que pretenden presentar en este momento; probará que existen irracionales contradicciones esenciales, entre los informes y reportes de la CNT, de Petroecuador y los testimonios de las personas que trabajaron en estas instituciones; se probará la falta de eficacia probatoria de un informe pericial, realizado por un perito, que de manera subjetiva y extralimitándose del cargo realizado, hace precisiones inexactas, anti técnicas y antijurídicas sobre la realidad de hechos que supuestamente habría

acontecido; probará que la acusación pretende probar un delito informático a través de prueba documental, obviando lo que establece el artículo 500 del COIP, pues esta prueba que pretenden hacer pasar como informática, es una prueba documental, al no haberse hecho las pericias necesarias para la comprobación de un supuesto delito informático, que es el establecido en el artículo 234 del COIP, que motiva esta audiencia; se conocerá en esta audiencia un acto repugnante de abuso de poder; no solo pedirá que se ratifique el estado de inocencia de Ola Bini, sino que se inicien las investigaciones en contra de todos aquellos que practicaron, tanto en la violación de sus derechos desde su retención ilegal, hasta la obtención de prueba fraudulenta para tratar de justificar sus acciones; dice que es importante que se conozca además, que al señor Ola Bini le metieron preso 70 días, por supuestamente haber jaqueado sistemas informáticos, que luego de no haber encontrado nada reformularon los cargos; probará además que no solo cambiaron el tipo penal, para adecuar la supuesta conducta que se ha cometido, cuando en el 2019 dijeron que lo habrían encontrado jaqueando, sino 5 años antes, sin que tenga congruencia lo que dijo la Fiscalía en un inicio y por lo cual se le está procesando este momento, sino que también se cambiaron los hechos, que impidieron que la defensa técnica pueda preparar la defensa y le dejaron en la indefensión al señor Ola Bini, sobre la base de una reformulación de cargos el día 117 de la instrucción fiscal; sobre la base de todo esto solicitaran al Tribunal que se ratifique la inocencia del señor Ola Bini y se inicien las investigaciones necesarias para esclarecer este hecho. **4. 2. DE LA PRUEBA.** Conforme al mandato del artículo 615 del COIP, los sujetos procesales presentan e incorporan la prueba previamente anunciada, en el orden que determina la norma antes citada, la misma que se detalla: **4.2.1. FISCALIA. Prueba Testimonial: 1) DAVID ALEXANDER ANDRADE DAZA:** Mayor de Policía quien dice que presta sus servicios en el Distrito Guayaquil, se encuentra en el curso de ascenso; que en el mes de abril del 2019, prestaba sus servicios en la Unidad de Delitos Tecnológicos de la Dirección Nacional de la Policía Judicial; dice que tiene capacitación en delitos cibernéticos, realizadas en Brasil, Chile, República Dominicana y en el Ecuador; en cuanto a su experiencia: en la Unidad de Delitos Tecnológicos trabajó 3 años y medio, en investigaciones de la Policía Nacional ha trabajado 11 años; dice que ha manejado cada año entre 260 a 280 delitos, en los cuales se trabajaba estafas on line, pornografía infantil, redes telemáticas y delitos conexos; en el presente caso el 11 de abril del 2019 aproximadamente a las 13:30, les llegó un documento de parte de 1800DELITO, que es de la Policía Nacional, en el que se ponen las denuncias vía telefónica, ellos les re-direccionaron a ellos como Unidad Investigativa sobre una denuncia telefónica, documento en que se decía que un ciudadano aducía que el señor Ola Bini se estaba trasladando al aeropuerto de Quito y había escuchado noticias que la señora Ministra había hablado sobre tal ciudadano y que tenía vínculos con el señor Julián Assange, es por este motivo que como Unidad investigativa, tenían que articular de manera inmediata, por esto él generó un memorando para los señores agentes sargento Cristian Camacho y cabo William Molina para que hagan el análisis y se haga lo correspondiente en torno a este caso; señala que a su vez se coordinó con el señor cabo Patricio Paredes, agente de capturadores de la PJ, perteneciente a la Unidad de Delitos Tecnológicos, para que esté pendiente con este trabajo, para que realice el trámite correspondiente; dice que también le generaron otro documento a las 14:30 los agentes Cristian Camacho y

William Molina, solicitando tomar versión al ciudadano Ola Bini y pedir la judicialización ante la Fiscalía, es por esto que se dio a conocer al Fiscal doctor Fabián Chávez; se coordinó con el Fiscal Fabián Chávez, y se generó el documento por parte de Fiscalía para la inmovilización del señor Ola Bini; posterior a eso de las 13:30 le dio a conocer el cabo Patricio Paredes, sobre el trámite que daba cumplimiento de parte de la autoridad competente, del doctor Fabián Chávez; entre las 17:58 nuevamente le generan un documento, el sargento Cristian Camacho y el cabo William Molina, manifestando sobre el pedido de allanamiento al domicilio del señor Ola Bini; es por esto que se da a conocer al Fiscal para continuar con el trámite correspondiente; a las 23:00 avanzaron al aeropuerto, tomó contacto con el señor Fiscal y coordinando con sus agentes de la Unidad de Delitos Tecnológicos y a su vez con personal de Interpol, en este caso con el sargento Luis Vásquez, quien le dio a conocer los derechos al señor Ola Bini, en los dos idiomas, inglés y español; a su vez se coordinó con el personal de Criminalística que se encontraba en el punto, para que levante los indicios, las evidencias; posterior avanzaron entre las 02:30 con el señor Fiscal y los funcionarios de la Unidad de Delitos Tecnológicos el subteniente Rodrigo Muñoz y el sargento Claudio Castillo a realizar el allanamiento en el domicilio del señor Ola Bini, lo cual está detallando en el parte por los agentes; desde las 03:00 se realizó el allanamiento conjuntamente con personal de Criminalística y se verificó un sin número de dispositivos electrónicos como pendrive, aparataje tecnológicos, cableado que estaba tendido y otros arrumados en el lugar; a eso de las 04:30 él se retiró del lugar y fue a su Unidad, en la oficina se encontró con sus compañeros quienes realizaban los partes e informes correspondientes, para dar a conocer sobre el procedimiento y a su vez le dieron a conocer que habían dado la notificación correspondiente ante el consulado de Suecia; **al conainterrogatorio realizado en defensa de la persona procesada responde que** si ha sido capacitado respecto a la aplicación del COIP, así como sus capacidades según la citada norma; que si le han informado respecto a lo que es un delito; cual fue trámite que tenía que hacer el cabo Patricio Paredes: cuando tiene estos documentos de 1800, este les llega a las unidades especializadas y como policías nacionales tiene que articularse inmediatamente porque son delitos de conmoción y como hablaban de la Ministra del Interior, uno se activa con mayor razón, señalando que el País hay un sinnúmero de delitos informáticos que la ciudadanía desconoce de este tipo de delitos tecnológicos y es también un trámite en el cual uno tiene que articularse con todos los entes del gobierno, del Estado y con todas las personas que son vulneradas en este tipo de sistemas, porque a ratos, con el debido respeto, hay muchas personas que vienen de otros países a cometer irregularidades en nuestro País; que le solicitó al agente Paredes?, que avance al aeropuerto, porque ellos estaban con el Fiscal el doctor Chávez haciendo el trámite correspondiente porque era un acto urgente y por eso se le pasó al agente Paredes el documento para su detención; recibió el oficio del 1800-DELITO a la 13h20 aproximadamente; la denuncia del 1800-DELITO decía circunstancias: ciudadano que se identifica con el alias Marco, quien indica conocer a señor Bini Ola Motodius de nacionalidad rusa, el mismo que tiene vínculos con el ciudadano de nombres Julián Assange y vive en las calles Juan Dibuja y Voz Andes, quien es una de las persona que la señora Ministra del Interior nombró en los noticieros de la mañana, así como indica que estaba en camino al aeropuerto de Tababela, con el fin de salir del país; que la llamada fue

recibida en la Unidad de Delitos Tecnológicos a las 13:23; a él le pareció una noticia del delito y además la señora Ministra había halado sobre el tema, por eso articula a su personal y da a conocer a la Fiscalía, para empezar un trámite, un procedimiento y por eso se pide la toma de una versión, con fines investigativo; lo dicho por la Ministra en el noticiero de la mañana él no le puso atención, desconociendo si la Ministra mencionó el cometimiento de un delito informático, aclarando el hecho de que él no escucho a la Ministra en el noticiero; señala que el 1800-DELITOS emite documentos a cada una de las Unidades Especializadas y ellos tienen que generar un trámite, y por eso ellos tienen que dar a conocer a la Dirección Nacional de la Policía Judicial y conjuntamente con 1800-DELITOS, para ver que trámite ellos han adoptado, es por eso que ellos actúan inmediatamente; el 1800-DELITO les remitieron el documento a su Unidad, porque son delitos conexos, inherentes a la Unidad de Delitos Tecnológicos; lo que remite el 1800-DELITOP es una noticia de delito y ellos tienen que actuar con el 1800 y articularse; que en el documento remitido no le dicen la calificación o el tipo de delito; por Secretaría se da lectura el documento remitido por el 1800-DELITO, se confronta con el documento que dice: clasificación de delitos “otros”; les pidió a sus hombres Camacho y Molina que recopilen información, hagan su análisis, hagan su trámite para judicializar, esto es para que se dé a conocer al señor Fiscal y con eso ellos se amparan para un procedimiento; afirma que si revisó el informe de los agentes y remitió el informe a la autoridad competente, él le llamó al Fiscal Fabián Chávez por teléfono y sus compañeros avanzaron donde él, porque era un procedimiento de magnitud y prontitud que tenían que realizar, por eso casi toda la Unidad estuvo en ese procedimiento; el doctor Chávez era el Fiscal que estaba de turno; recibió el informe de los agentes Molina y Camacho a las 14:27, solicitando que le tomen una versión y a su vez que se judicialice con fines investigativos para su detención; se contrasta con el documento donde se lee por medio de Secretaría que el asunto es “detención con fines investigativos”; “es así que el personal de la Unidad de Investigaciones de Delitos Tecnológicos, adscritos a la Dirección Nacional de la Policía Judicial e Investigaciones, en sus atribuciones contempladas en el artículo 449, numeral 5 (tomar las medidas adecuadas para impedir el cometimiento p consumación de una infracción que llegue a su conocimiento)”; los agentes en primer lugar identificaron al ciudadano Ola Bini Methodius, en el sistema SIPNE de la Policía; señala que en la noticia del delito no recuerda la nacionalidad del señor Ola Bini; no recuerda el número de documento de identificación del señor Ola Bibni, revisa el documento y dice que el número del documento de Ola Bini era el No. 84086354, de nacionalidad suiza; el informe de los agentes Molina y Camacho lo recibió a las 14:27, hora en que fue entregado al Fiscal, sin recordar que agente le entregó al Fiscal; la orden de inmovilización, el Fiscal le entregó al cabo Alfredo Salazar; él fue al aeropuerto a eso de las 23:00, el sargento Luis Vásquez estaba de turno en Interpol del aeropuerto de Tababela, le dijo a él, como tiene conocimiento de Inglés y como se suponía que el ciudadano Ola Bini sabía inglés, que le lea sus derechos; el agente Paredes tenía controversia entre si era suizo o sueco, por lo que se revisó en el sistema SIPNE y se dio a conocer que era de nacionalidad sueca; notificaron al consulado de Suecia no recuerda la hora; luego se trasladaron al domicilio del señor Ola Bini, el señor Bini estuvo con el señor agente Patricio Paredes y no fueron al departamento; en el allanamiento no recuerda haberle visto al señor Ola Bini; **2) WILLIAM CRISTIAN**

MOLINA VALENZUELA: Cabo de Policía quien dice laborar en la Unidad Nacional del Ciberdelito; que en el mes de abril del año 2019, prestaba sus servicios en la Unidad Nacional de Delitos Tecnológicos; en cuanto a sus capacitación, señala que ha seguido cursos de análisis de inteligencia, análisis de información, analista en fuentes abiertas de información y como policía judicial, tiene una especialización en ciberseguridad y ciberdelitos; dice que en la Unidad de Delitos Tecnológicos lleva 3 años, que la Unidad investiga dentro del área interna que son fraude electrónico, redes telemáticas y pornografía; dice que en el presente caso, el 11 de abril del 2019, mientras estaba cumpliendo funciones en la Unidad, llegó a su conocimiento un memorando suscrito por el mayor de Policía David Andrade, en ese entonces Jefe de la Unidad, en dicho memorando se anexaba un reporte generado por la Unidad 1800-DELITO, en el memorando les disponían que se realice el análisis y la judicialización, ante la disposición escrita, verificó la información en el reporte generado por la Unidad 1800-DELITO, en dicho reporte se indicaba que un ciudadano con alias Marco, indica conocer al señor Ola Bini Methodius, el cual tiene vínculos con el señor Assange y que es una de las personas que la señora Ministra nombró en los medios de comunicación en la mañana y quien estaba a punto de salir del país; en dicho reporte también se menciona una dirección domiciliaria, que describía a la Juan Dibuja y Voz Andes; dice que ingresó al sistema SIPNE donde se digitó el nombre de Ola Bini Methodius, desplegándose un nombre que correspondía a la identificación de Ola Bini Methodius que correspondía a un país extranjero; esa información se elevó mediante parte, al Jefe de la Unidad, posterior a ello continuó con la verificación a fin de verificar si la dirección constante en el reporte, que se describía las calles Juan Dibuja y Voz Andes, por lo que conjuntamente con el sargento Cristian Camacho, a quienes les habían asignado, se trasladaron hasta el lugar y luego de las técnicas especiales de investigación, o sea entrevistas, se contactaron con 2 personas que no quisieron identificarse y dijeron que presuntamente el nombre que se indagaba Ola Bini Methodius vivía en el edificio Bertone, 4to. piso, departamento 12; verificaron la información y pusieron en conocimiento del Jefe de Unidad a fin de que realice las coordinaciones pertinentes; posteriormente, a eso de las 03:00, le fue asignado a que colabore con el doctor Fabián Chávez, para indicarle la ubicación del inmueble, lo cual se le colaboró; **al conainterrogatorio realizado en defensa de la persona procesada responde que** si está capacitado para saber que es un delito informático; que las características generales en el delito informático, a breves rasgos, es realizar investigaciones en el entorno digital; para poder cometer un delito informático en general, se necesita de una persona, un dispositivo móvil, un ordenador y acceso a internet; en el anexo remitido por el 1800-DELITO no había establecidas esas características; señala que en este caso, fue un reporte generado por la Unidad 1800-DELITO, en la cual les dispusieron mediante memorando analizar y judicializar la información; solicitó la detención con fines investigativos, por el reporte televisivo generado por un Ministro, que decía que era una de las personas que había nombrado la Ministra de ese entonces; en ese reporte televisivo les da conocer un nombre y la inmediata salida del País; aclara que no escuchó el reporte televisivo, pero se encuentra registrado en el reporte generado por la Unidad 1800-DELITO, dentro del reporte se indica que un ciudadano alias Marco, decía conocer al señor Ola Bini Methodius, quien tenía vínculos con el señor Julián Assange y que estaba

próximo a salir del País; señala que él realizó un acto urgente, en base al reporte generado por 1800-DELITO, en base al reporte generado por dicha Unidad, en el que alias Marco dice conocer al ciudadano Ola Bini Methodius, quien estaba por salir del País; sobre el acto urgente, señala que se puso en conocimiento del Jefe de Unidad y que lo validen jurídicamente con el señor Fiscal; la verificación la realizó el 11 de abril del 2019, pedido recibido mediante memorando, a eso de las 14:00, en el cual le solicitaban que haga un análisis y judicialización, esto es remitir a Fiscalía la información generada por la Unidad 1800-DELITO; señala que realizaron dos verificaciones, la primera pasado las 14:30, se puso en conocimiento del señor Jefe de la Unidad, solo le puso en conocimiento de él la información encontrada en el SIPNE; luego del análisis y de ser procedente, se dice que Fiscalía vea en lo pertinente si se da paso o no a la petición para que se evita la consumación de delito, esto es la salida del País; señala que es un agente investigador y cumplía con una disposición escrita que pedía que se analice y se judicialice la información; en cuanto a la hora en que la Unidad 1800-DELITO recibió la información de alias Marco, este había llamado a eso de las 13:00, no sabe la hora exacta; en su verificación en el sistema SIPNE el nombre Ola Bini Methodius generó el número de documento emitido por un país extranjero, Suiza; en su informe sí solicitó la detención con fines investigativos, porque dicha persona estaría en medio de una infracción flagrante, esto es la salida del País; señala que a la Unidad Nacional de Cibercrimen llega una noticia del delito y se trabaja bajo delegación fiscal y reportes que se generan por la Unidad 1800-DELITO; luego de entregar el informe al mayor Daza, éste le pidió que le colabore al Fiscal a fin de identificar el inmueble que se había verificado; dice que él fue a verificar el domicilio del señor Ola Bini con el señor Fiscal a las 03:00; la información desplegada por el 1800-DELITO señalaba a las calles Dibuja y Voz Andes; él realizó las entrevistas a personas que vivían en el sector, las cuales no quisieron identificarse, eso se realizó pasadas las 15:00, hicieron un parte de esta verificación; aclara que ellos no realizan investigaciones con vigilancias y seguimiento, sin autorización judicial; realizó además la toma de versiones; si estuvo presente en el allanamiento del domicilio de Ola Bini, estuvo a eso de las 03:00 del día 12 de abril del 2019, no recuerda hasta que hora porque ese día en comisión de servicios a la ciudad de Guayaquil; aclara que no estuvo en todo el allanamiento, no firmó el parte del allanamiento; no firmó un reconocimiento del lugar de los hechos en el domicilio del señor Ola Bini; para estar presente en el allanamiento, le autorizó su Jefe de Unidad; desconoce si su nombre consta en el acta de allanamiento, ese no fue su procedimiento; no estuvo en el inicio del allanamiento, llegó como a las 03:00; **3) ANGEL ESNEDY GUARNIZO ROSILLO:** Sargento primero de Policía quien dice laborar en Interpol de la Policía Nacional; que en el mes de abril del 2019 trabajaba en Interpol; en cuanto a sus capacitaciones en idioma inglés, tiene una licenciatura; que él asiste en detención de personas en delitos internacionales o donde hay ciudadanos de lengua inglesa, además traduce documentos para Interpol; en Interpol ha realizado múltiples capacitaciones en el idioma Inglés y ha participado en la lectura de derechos a ciudadanos de habla inglesa; en el presente caso, por disposición del Jefe subrogante de su Unidad, capitán Vanesa Muñoz, colaboró en un procedimiento con el señor sargento Segundo Luis Vásquez, para leerle los derechos constitucionales en inglés, a una persona extranjera de habla inglesa; es así que al señor Bini, en la Unidad de

Delitos Informáticos se le dio la lectura de los derechos constitucionales en el idioma inglés; que el 11 de abril del 2019, en horas de la tarde, vía telefónica, le fue dispuesto por el Jefe capitán Vanesa Muñoz, para que colabore en un procedimiento policial, mediante llamada telefónica le contactó el sargento Luis Vásquez, le dijo que esté pendiente para avanzar a la Fiscalía de Flagrancia para leer los derechos constitucionales a una persona extranjera de habla inglesa; que el 12 de abril del 2019 a las 05:30 conjuntamente con el sargento Luis Vásquez, avanzó hasta la Unidad de Delitos Informáticos de la Policía, ubicada en la Av. Amazonas y Roca de la ciudad de Quito, en el lugar tomó contacto con el señor Patricio Paredes y el detenido, quien se identificó como Bini Metodiuos, a eso de las 06:00 le leyó sus derechos en el idioma inglés, de acuerdo al artículo 77 de la Constitución de la República del Ecuador; el señor Bini le indicó que había entendido lo que le leyó y que entendía tanto el idioma español como el idioma inglés; posterior a esto, a través de teléfono celular que le proporcionaron, el señor Bini se comunicó con una persona que dijo ser su abogado, luego el señor Bini indicó que no podía firmar ningún documento porque eso le había sugerido su abogado y no firmó la hoja de derechos que le estaba indicando; destaca que durante el procedimiento, sus compañeros le indicaron que al ciudadano ya le habían leído sus derechos en el aeropuerto de Quito, por parte de su compañero Luis Vásquez en Ingles y por parte del cabo Patricio Paredes en el idioma español, pero igual él le volvió a leer sus derechos en inglés, puesto que en esos momentos se estaba realizando el parte policial; luego se retiró de las instalaciones de la oficina de Delitos Informáticos; **al contrainterrogatorio realizado en defensa de la persona procesada responde que** el sargento Luis Vásquez ya le había leído los derechos al señor Bini; que su Jefa de la Interpol no le dijo la nacionalidad del detenido; cuando el sargento Vásquez se comunicó con él, no le dijo de que nacionalidad era, solo que era de habla inglesa; cuando llegó a la Unidad de Delitos Informáticos, él no verificó de que nacionalidad era, le parece que no; que el señor Ola Bini fue detenido en el aeropuerto Mariscal Sucre; que él no revisó los partes, solo le leyó los derechos, el procedimiento estaba a cargo de los agentes de delitos informáticos; al señor Ola Bini le informó que estaba siendo detenido por orden de autoridad competente, de acuerdo a lo indicado por los compañeros que tomaban el procedimiento policial, no recuerda que acción que se le acusaba; sus compañeros le mostraron el parte policial de la Unidad de Delitos informáticos; había una orden de autoridad, no recuerda el número de esa orden; la orden no recuerda si se le facilitó, él se imagina que si la debió ver; no logró ver la nacionalidad del detenido; en el documento consta que el ciudadano es de nacionalidad suiza; a él no le infirmaron que el ciudadano era de Suiza, sino que el indicaron que era de habla Inglesa; a él no le indicaron que tenía nacionalidad Suiza, solo le dijeron que hablaba inglés, él no informó a su superiores que era un ciudadano Suizo; sobre la infracción presuntamente cometida, solo le dijo en inglés que estaba siendo detenido por las personas que firmaban el parte, por orden de autoridad competente, con el número de documento que le indicaron los compañeros; no recuerda si firmó la hoja de la lectura de los derechos, en ella no existe delito, solo la orden de autoridad competente, si consta su firma en la hoja de la lectura de derechos; el abogado del señor Ola Bini se llamaba David Ochoa; le leyó textualmente la hoja de lectura de derechos; **4) RICARDO MARTÍN MUÑOZ NAVARRETE:** Subteniente de Policía con 10 años de servicios, labora en la

Unidad del Ciberdelito; señala que en el mes de abril del 2019 presentaba sus servicios en la Unidad de Investigación de Delitos Tecnológicos; en cuanto a su capacitación dice tener un diplomado en Ciberseguridad y Cibercrímen, así como varios cursos internacionales y nacionales en la materia de Ciberdelito; tiene experiencia de 7 años en esta Unidad de Delitos Tecnológicos; dice que en el presente caso realizó un parte policial en el año 2019, específicamente el 12 de abril, en el cual indico que por disposición de Jefe de Unidad de Delitos Tecnológicos, un equipo de esta Unidad, conformado por el sargento William Frías, el sargento Claudio Castillo y el cabo Luis Aldáz, como su persona, avanzaron hasta la calle Juan Dibuja, a eso de las 03:00 del 12 de abril del 2019, con el Fiscal del caso doctor Fabián Chávez con personal de Criminalística y del grupo GOE, se dirigieron a la puerta del edificio Bartone, el Fiscal tomó contacto con el administrador del edificio, él dijo el motivo de su presencia, esto es dar cumplimiento a una orden de allanamiento dispuesta por la Jueza doctora Gloria Mayorga, en la que autoriza el allanamiento del inmueble ubicado en el 4to. Piso, departamento 12; conjuntamente con el señor Fiscal y los grupos tácticos, avanzaron al 4to. piso, departamento 12 y se dio cumplimiento al allanamiento, ingresaron al domicilio y fijaron varios indicios de carácter electrónicos y otros, el equipo de Criminalística los fijaron, recolectaron y etiquetaron, los que fueron ingresados a la bodega de Unidad de Flagrancia con su respectiva cadena de custodia; señala que en el sitio estuvo a eso de las 03:00; **al conainterrogatorio realizado en defensa de la persona procesada responde que** él fue parte del equipo del allanamiento, en calidad de oficial del allanamiento; colaboró y verificó el procedimiento; la cadena de custodia la levantó el 12 de abril, a eso de las 04:00 cuando se entregaron los indicios a Criminalística, no recuerda el número de indicios, eran más de 300; por disposición del Fiscal levantaron los indicios de carácter electrónicos, computadoras, tablet, celulares, USB, entre otros que se encontraban en el lugar; el Fiscal les dijo que indicios se levantaban; dice que en la orden se indicaba “otros”, así que se levantó además los libros, una caja fuerte no recuerda si la levantó; sobre si levantó un pasaporte, indica que eran más de 300 no recuerda todos, pero están descritos en la cadena de custodia; revisando la cadena de custodia dice que se tiene 15 indicios levantados, con varios elementos en cada indicio; el indicio número 4 es una caja fuerte, no puede indicar el contenido del mismo, la caja fuerte como tal no es un elemento informático; el indicio número 7 corresponde a un pasaporte número 90137675 a nombre de Bini Ola Methodius Martin; un pasaporte número 84086355 a nombre de Bini Ola Methodius Martin; un pasaporte número 84086354 a nombre de Bini Ola Methodius Martin; una tarjeta Visa número 4485591001037526 a nombre de Ola Bini, color azul; una tarjeta Visa número 4918890010537022 a nombre de Bini Ola Methodius Martín, color verde; estos no son elementos informáticos; la orden judicial le fue entregada a las 03:00 por medio del Fiscal, quien le dio a conocer al administrador del edificio; dice que él si leyó la orden de allanamiento; que la cadena de custodia se le entregó al personal de Criminalística y les fue devuelta para la movilización de los mismos; cuando llegaron al departamento del señor Ola Bini estaban presentes ya personal de Criminalística, de Fiscalía y de investigadores; él no había estado antes en ese edificio; cuando llegó al edificio no vio al señor Ola Bini; dentro del procedimiento la puerta la abrió el equipo táctico, luego estuvo el equipo de investigadores, al momento del ingreso, personal policial únicamente abrió la puerta a fin de dar

cumplimiento a la orden judicial; no vio directamente si se violentaron las cerraduras del departamento; a la pregunta de que si conoce al abogado David Artieda, responde que no lo recuerda; el 11 de abril 2019 a las 23:00, se acercó una persona en la gasolinera Primax de la 9 de Octubre y Orellana, ya que cuando estaban en el edificio Bartone, un vehículo no identificado salió en precipitada carrera y su función es la seguridad ciudadana y estando dentro del horario de actividades, lo siguieron y pidieron los datos al propietario del vehículo, el cual se identificó e indicó sus documentos y posterior se le solicitó que continúe su marcha, porque no presentaba ninguna novedad; él estaba con su equipo de trabajo, no registraron el vehículo, únicamente lo visualizaron desde la parte exterior; no recuerda haberle comunicado al Fiscal Chávez de este particular; en su parte policial se dijo que dio cumplimiento a la orden de autoridad competente; que al finalizar la diligencia si realizaron la clausura de la escena, a eso de las 16:00 del 12 de abril; que el inmueble quedó con resguardo policial, ya que habían varios indicios y posterior a retirarse podían existir más indicios; el resguardo lo ordenó el Jefe de la Unidad; **5) DIEGO MAURICIO LÓPEZ TAPIA:** Capitán de Policía y perito del Departamento de Criminalística; dice que el 11 de abril 2019, a eso de las 23:00, realizaron la inspección ocular técnica en las instalaciones de la oficina de Interpol, del aeropuerto Mariscal Sucre; dicha diligencia fue dispuesta por el Fiscal doctor Fabián Chávez, quien dentro del actor urgente se procedió a realizar la inspección ocular técnica de 4 maletas; luego de realizar la inspección técnica de las 4 maletas, se pudo establecer que existían 4 indicios, que a pedido del señor Fiscal doctor Fabián Chávez, solo se realizaba la fijación técnica de elementos electrónicos, informáticos y de telecomunicaciones; en los 4 equipajes, el identificado como indicio 1) es una maleta de color gris, 2) es una maleta negra tipo mochila y 2 maletas de viaje signadas como indicios 3) y 4); en el interior del indico 1), realizó la constatación de documentos tipo tarjeta, a nombre de Ola Bini y 90 dólares americanos y dos tarjetas plásticas con un logo que decía Visa; en el equipaje 2) constató diferentes artículos informáticos, electrónicos y de telecomunicaciones, siendo los principales una computadora portátil, 2 tablet, 2 teléfonos celulares, 2 tarjetas plásticas con chip SIM, USD 1.200,00, 14 nano llaves de seguridad, 29 dispositivos tipo llaves, 23 dispositivos tipo USB y 23 contenedores y alambres tipo USB, una antena de recepción de señal, entre los principales; en el indicio 3), maleta de viaje, se encontraron dispositivos de conexión USB, así como también cables auxiliares tipo USB y artículos electrónicos como cables de conexión; en el indicio 4), en el interior de una de las maletas, un parlante portátil, dos modem de conexión a internet, 14 cables de conexión y dos cables de red; luego de realizada la inspección ocular técnica, embolsó y etiquetó a cada uno de los indicios y fueron entregados al señor agente Chamba, quien se hizo cargo de los indicios levantados; **al interrogatorio realizado por Fiscalía responde que** lleva 15 años en la Policía, 14 como perito Criminalístico; trabaja en la sección de inspección ocular técnica, balística, identidad humana y audio y video; que en el mes abril 2019, era Jefe de inspección ocular técnica del Laboratorio de Criminalística de Quito; en cuanto a su capacitación dice tener cursos de Criminalística nacionales e internacionales, tiene una maestría en escenas del crimen, investigación forense, realizado en España; como experiencia ha trabajado 15 años en dicha áreas; dice que ha elaborado más de 400 informes; en cuanto a la funcionalidad de los indicios levantados, se tiene que establecer por medio de perito en informática forense, ya

que cada uno de estos dispositivos son de carácter informático, electrónico y cumplen ciertas funciones específicas, que con la pericia de inspección ocular técnica no se los puede establecer; **al conainterrogatorio realizado en defensa de la persona procesada responde que** las personas que realizaron la pericia fueron él y 3 peritos más que estaban de tueno, el capitán Ariel Velasco y los sargentos Lincango y Talabera; terminaron la pericia a eso de las 03:00; conoce de que infracción fue el levantamiento de indicios?, responde que fue por disposición del señor Fiscal Fabián Chávez, quien dispuso que dentro de la Inspección Ocular Técnica se recoja elementos de carácter informático, electrónicos y de telecomunicaciones, él desconoce las causas de la investigación que llevaba la Fiscalía; los indicios fueron entregados al agente Chamba, el equipo de inspección levantó los indicios, el capitán Ariel Velasco, los clases y su persona; no recuerda la hora en que los entregaron al agente Chamba, lo hizo el capitán Ariel Velasco; no puede precisar en dónde las entregó, ni tampoco donde estaba el agente Chamba; no había llaves de puerta sino dispositivo electrónicos tipo llaves; no le requisaron al señor Ola Bini; dice que no realizó otra pericia dentro de esta caso; aclara que en otro informe de reconocimiento de objetos en un domicilio en el sector norte de Quito, participó como coordinador con Fiscalía y las otras Unidades de Inteligencia; las conclusiones de ese informe es que existe el lugar, de que los elementos que fueron levantados fueron ingresados bajo cadena de custodia, se aplicó la metodología de inspección ocular técnica, en relación al trabajo realizado en el lugar; el inicio de esta diligencia fue a las 03:37 según consta del informe; en el lugar estaban presentes el señor Fiscal doctor Fabián Chávez, el equipo de Criminalística y los agentes investigadores; esta pericia la realizaron con el capitán Marco Aurelio Pazmiño, el capitán Ariel Velasco y los sargentos Talabera y Lincango; la diligencia la concluyeron el 12 de abril 2019, el informe indica a las 14:00; en este segundo informe se actuó de acuerdo la disposición del Fiscal doctor Fabián Chávez; señala que dentro de las investigaciones que se encontraban realizando, contaron con la presencia del Fiscal doctor Fabián Chávez, quien dirige las investigaciones, aclarando que no puede precisar si recibieron la disposición de levantar como indicios a los libros, ya que él se desempeñaba como coordinador; el capitán Ariel Velasco con su equipo se encargó del levantamiento de indicios y se encargó además de entregar las evidencias, no recuerda a quien las entregó; durante la diligencia, en el inmueble estaba el señor Fiscal, él por sus funciones de coordinación se retiró y se quedó a cargo del procedimiento el capitán Ariel Velasco, no sabe cuánto se quedó el Fiscal; él no conocía en ese momento quien era el señor Ola Bini; no recuerda cuando abrieron la puerta del departamento; **6) ARIEL ALEXIE VELASCO ALBÁN:** Capitán de Policía y perito del Departamento de Criminalística, quien dijo haber realizado el reconocimiento del lugar de los hechos, el reconocimiento de evidencias, según Informe No. 242, por lo cual, mediante orden de allanamiento No. 17282-2019-0086G, suscrito por la doctora Rocío Mayorga; se trasladaron hasta el sector norte de la ciudad de Quito, procediendo a realizar el reconocimiento del lugar de los hechos, el mismo que se encuentra en el sector norte de Quito, en la calle Juan Dibuja E02-30, piso No. 4, departamento No. 12; el mismo que para su ingreso tiene una puerta de madera, luego por un pasillo, al lado izquierdo hay un ascensor, por donde suben al 4to. piso, al departamento 12, dentro del cual se observa los siguientes ambientes: cocina, sala, al costado derecho existe

un dormitorio, seguido de un ambiente destinado para oficina, a continuación hay un baño y al fondo se encuentra un ambiente destinado para el dormitorio No. 2; en este inmueble se procedió a la fijación de varios dispositivos electrónicos, tarjetas, computadoras, modem, dispositivos electrónicos, soporte de papel moneda, cables de poder, USB, tarjetas; dice que se suscribe la respectiva cadena de custodia; en sus conclusiones estableció que el lugar existe y se encuentra descrito en el acápite de operaciones, a su vez realizaron el reconocimiento de los objetos antes detallados; **al interrogatorio realizado por Fiscalía responde que** dice que lleva como miembro de la Policía 12 años, en el Departamento de Criminalística desde hace 9 años; en el mes de abril del año 2019 estuvo en la sección de inspección ocular técnica del Laboratorio de Criminalística; en cuanto a su capacitación: tiene cursos de inspección ocular técnica, de documentología y de reentrenamiento en inspección ocular técnica; ha realizado alrededor de 100 pericias de esta clase; en cuanto a los indicios levantados y fijados: 1) un dispositivo electrónico color negro, marca Delean, sin cable, localizado en el ambiente de sala, sobre el aparador color negro; 2) un modem marca Aris color negro y su cable de poder, localizado en la sala, sobre el piso; 3) un computador portátil marca Toshiba, color plomo, con batería y cargador, con un dispositivo USB marca Scandis, encontrada sobre un aparador de la sala; 4) una caja fuerte metálica color plateada, cerrada, encontrada en el interior del closet del dormitorio; 5) un disco duro externo, marca Hitachi, color plomo, 750 gigas, con un cable; otro disco duro externo marca G Drive, color negro, de tres terabyte; otro disco duro externo marca Toshiba color negro de 500 gigas; un disco duro externo marca Lassie, color negro; otro dispositivo marca Lassie, con estuche plástico color naranja; otro disco duro marca Lassie, color plomo, con estuche plástico color naranja; otro disco duro externo marca Lassie color plomo; otro disco duro externo marca Lassie, color plomo; otro disco duro externo marca Wester Digital, color negro de 160 gigas; otro disco duro marca Wester Digital color negro de 160 gigas; una caja metálica marca Lassie, color plomo con dos puertos, sin serie; una caja metálica marca Adornic, color plomo con dos puertos; un disco duro externo marca G Raigth, color plomo de 4 teras; otro disco duro externo marca WD color negro; una caja metálica marca Acón Data, color plomo con 5 puertos; una tarjeta CD marca Sandic, color negro de 64 gigas; un dispositivo de almacenamiento de datos tipo USB, marca Sandic, color negro y rojo de 8 gigas; 5 dispositivos de almacenamiento de datos tipo USB, marca Kingston color plomo; 4 dispositivos de almacenamiento de datos tipo USB, marca Kingston color plomo de 8 gigas; 2 dispositivos de almacenamiento de datos tipo USB, marca Kingston color plomo de 16 gigas; un dispositivo de almacenamiento de datos tipo USB, color plomo de 32 gigas; un dispositivo de almacenamiento de datos tipo USB marca Sandics, color plomo y negro de 8 gigas; un dispositivo de almacenamiento de datos tipo USB marca Sandic, color negro y plomo de 16 gigas, localizado en un mueble tipo escritorio en estudio; un computador portátil marca Lenovo, color negro; un computador portátil marca Lenovo color negro, sin batería; otro computador portátil marca Lenovo, color negro sin batería; otro computador portátil marca Lenovo color negro, si batería; un computador portátil marca Lenovo color negro con batería; un computador portátil marca Lenovo, color negro sin batería; un I pod marca Apple color plomo; un I pod marca Apple color plomo, con la pantalla rota; un I pod marca Apple color plomo; I

pod marca Apple color plomo; un I pod marca Apple color plomo, sin estuche; un I pod marca Apple, color plomo; un computador portátil marca Lenovo, color negro con batería; una computadora portátil marca Lenovo, color negro, con batería; un computador portátil marca Positivo, color negro, con batería; un computador portátil marca Apple, color plomo con batería; 6) un computador portátil marca Apple, color blanco, con batería bajo un escritorio, localizado bajo un escritorio en el ambiente de estudio; 7) un pasaporte a nombre de O. B.; un pasaporte a nombre de O. B.; un pasaporte a nombre de O. B.; una tarjeta visa a nombre de O. B., color azul; una tarjeta visa a nombre de O. B., color verde; una libreta color negro con manuscritos, encontrada en el escritorio del ambiente de estudio; 8) un libro con la leyenda Haking Secret Chipers, con portada de color blanco y azul; un libro con la leyenda Privace Lod, con portada de color verde; un libro con la leyenda de Panamá Papers, con portada de color negro y blanco; un libro con la leyenda Hackers Play Book, con la portada negro y azul; un libro con la leyenda Hacker Coaccer, con portada de color negro; un libro con la leyenda de The Dark Red, con portada de color blanco; un libro con la leyenda The Black Book, con la portada de color blanco; un libro con la leyenda Cyber Ware, con portada de color rojo; un libro con la leyenda Cyber Ware, con portada de color amarillo; un libro con la leyenda Snowden, con portada de color azul; un libro con la leyenda Snowden, con la portada de color negro y celeste; un libro con la leyenda Wikileaks, con portada de color negro; localizados en un mueble madera tipo librero en sala; 9) un teléfono Snow 870, color negro, encontrado sobre el mueble de aparador en el ambiente de la sala; 10) un computador marca portátil marca Apple, color plomo; un router marca Delín, color blanco, con cargador y antena; un router marca Delin color negro, con cargador y 3 antena; dos equipos electrónicos de color negro, con teclado alfa numérico, con puertos de entrada rotulados Ola1 y Ola2; un disco duro externo marca Toshiba color negro; 20 tarjetas magnéticas de color blanco, rotuladas RFID; 20 tarjetas magnéticas blancas rotuladas RFID; un equipo electrónico marca Lenovo, color negro, con múltiples puertos; un Aple TV color blanco, marca Appel; un componente electrónico negro con varios cables; un equipo electrónico color blanco, con un teclado y con una leyenda CARD; 12 hojas de papel A4, con texto impreso y manuscrito; un soporte de papel tamaño A5, con varios textos impresos; un periódico con la leyenda que se lee El Comercio martes 15 de octubre del 2013, con 6 hojas de texto impreso y fotográfico; un periódico con la leyenda El Telégrafo, de martes 13 de octubre del 2015, que contiene 8 hojas con texto impreso y fotográfico, localizado en el piso del estudio; 10) 5 cargadores de computador color negro, veinte cables de poder de color negro, tres cables UTP blanco y azulo; 12 cables de impresora, 23 cables USB, 5 cables de monitor; 7 cables DNI, localizados en la puerta del estudio; 11) 2 router marca Apple de color blanco; dos I phor extreme, marca Apple, de color blanco; un CPU marca Apple de color plomo, sin su cable; un CD router externo marca Apple, color plomo con cable USB, encontrado en el ambiente destinado a sala; 12) un computador portátil marca Lenovo sin batería ni cable de poder: otro computador portátil marca IBM, sin serie y sin cables ni batería; 4 cables de poder color blanco; un cargador marca Lenovo; un aparato electrónico marca NET GEAR, color azul; un cargador Net Gear; un cargador de link, ubicado en una mesa de la sala 13); un computador marca System 76, color negro; un Apple TV de color blanco; un I phor extreme marca Apple, de color blanco; un cable de poder color blanco; un cargador

marca Appel de color blanco; un teléfono celular marca I pone, modelo A1387, de color negro; un teléfono celular marca Samsun, color negro; otro teléfono celular marca I pone, modelo A1387, de color negro; otro teléfono celular marca I pone, modelo A1574, de color negro; 2 dispositivo de almacenamiento de 16 gigas, marca Sandics; 2 dispositivos de almacenamiento de 32 gigas, marca PNY, color plomos; 2 dispositivos de almacenamiento de 8 gigas, marca Sandics, de color plomo; 2 dispositivos de almacenamiento de 32 gigas, marca Sandics color negro; un dispositivo USB, marca Logiteg, de color negro sin tapa; un dispositivo de almacenamiento de 16 gigas, marca Intenso, de color negro; un dispositivo de almacenamiento de 2 gigas, marca Sandics, de color negro; un dispositivo de almacenamiento marca Tourgus, de color negro; una llave USB, marca Strangelo de color plomo; un dispositivo de almacenamiento de 128 gigas, marca Kingston, de color blanco; un dispositivo de almacenamiento de 8 gigas, marca TDK, de color verde; una tarjeta SD marca Panasonic de 8 gigas de color azul; 154 hojas de papel con texto impresos y manuscritos, encontrados en el piso del ambiente de estudio; 14) 123 soporte de papel moneda, de diferentes nominaciones y países; un documento de identificación a nombre Esveriges Ambasad London; una tarjeta con la leyenda que se lee Visa, a nombre Sandel Mali; una tarjeta con la leyenda que se lee Mastercard, a nombre de Valer Karkole; una tarjeta con la leyenda que se lee Atlantic, a nombre de O.B.; una tarjeta con la leyenda que se lee Asociación for Computing Machineri, a nombre de O.B.; una tarjeta con la leyenda que se lee National Unturance, a nombre de O.B., localizada en el piso destinado a estudio; **al conainterrogatorio realizado en defensa de la persona procesada responde que** en su informe consta el acápite reconocimiento de la escena del delito; cuando llegó ya había Policías en el departamento, él llegó a eso de las 03:30, inició la diligencia a las 03:37; al departamento ingresó porque la puerta estaba abierta, no sabe quién la abrió; los libros que se levantaron como indicios no eran los únicos libros que había en el librero, no recuerda cuantos más había; no tomó fotos del interior de los libros; los agentes investigadores estaban ahí, ellos les indicaron que libros se fijan como evidencias; si había disposición judicial para realizar el allanamiento; no conoce cuál era la disposición judicial en detalle; en su informe si hay un acápite que detalle el reconocimiento de objetos; el no conoce cuál era la infracción que se investigaba; que el teniente Martín Muñoz era el investigador que inició la diligencia, le entregó la cadena de custodia a él a eso de las 14:00; en el departamento de Ola Bini estuvo la persona que estaba al mando, el subteniente Martín Muñoz y el Fiscal doctor Fabián Chávez; no había estado nunca antes en ese edificio; cuando él llegó al departamento Ola Bini no estaba en ese lugar; no sabe si el departamento fue abierto con la llave del señor Ola Bini; señala que según su informe concluyeron el procedimiento a las 14:00; también firmo el Informe No. 241, que se refiere a la fijación de indicio en el aeropuerto, los que ya fueron descritos anteriormente por el Mayor López; llegó al aeropuerto a eso de la media noche, según el informe a las 23:00, del jueves 11 abril del 2019; que en ese reconocimiento se fijaron 142 indicios electrónicos; dentro de dicha pericia si hay un acápite que se denomina reconocimiento de objetos; no sabía a qué infracción se refería la investigación, los agentes investigadores les indicaron que indicios fijar; al mando de la UIEDT estaba el Mayor David Andrade; los indicios fueron entregados al sargento Wilson Chamba Guamán, el día 12 de abril del 2019, a las 09:50, los entregó en el

Laboratorio de Criminalística; dice que desconoce quién incautó las pertenencias del señor Ola Bini; reitera que a él le entregan los agentes investigadores los indicios para fijarlos; **7) HENRY DANIEL YEPEZ ORTIZ:** Cabo de Policía quien dice que por delegación fiscal, realizó la pericia de reconocimiento de los indicios, que se encontraban dentro de la cadena custodia, que tenía relación con la aprehensión del señor Ola Bini, para lo cual se trasladó al Centro de Acopio de indicios y evidencias del Departamento de Criminalística, con el fin de retirar los indicios que se encontraban bajo cadena de custodia No. 177219, mismos que le fueron entregados por el custodio; señala que dentro de los trabajos realizados, se utilizaron la técnica de la observación, descripción y sobre todo la fijación fotográfica; exhibe las fotografías que contienen los indicios encontrados en el aeropuerto, en relación a las cadenas de custodia UDI-DMQ-8844159; los siguientes indicios; 1) 10 tarjetas plásticas a nombre del ciudadano Ola Bini; dos documentos de identificación a nombre de Bini Ola Methodius Martín; dos tarjetas de presentación con texto impreso; dos tarjetas de plástico color blanco y dos fragmentos de papel de color rosado, con textos manuscritos color negro; soportes de papel con similares características a billetes de 20 dólares (3) y de 10 dólares, así como una moneda de 050 euros; una billetera con un logotipo; un fragmento de papel de color blanco que se lee movi plus; 2) un fragmento de papel color negro con el texto de un tríptico impreso; cuatro fragmentos de papel con textos impresos; tres documentos con textos escritos impresos, relacionados con documentos de vacunación; un pasaporte a nombre de Ola Bini Methoduis Martin; dos tarjetas de cartón de color negro, con 33 copias fotostáticas en blanco y negro; 60 soportes de papel con similares características al billete de 20 dólares; una tarjeta plástica con chip; una tarjeta de presentación con textos impresos; una tarjeta plástica color blanca con chip; 4 dispositivos de almacenamiento de datos electrónicos tipo USB, los mismos que estaba sellados; 8 concentradores de poder conocidos como PAV; 3 acumuladores de energía portables y un dispositivo de alimentación de energía; 7 adaptadores de puertos para transmisión de datos; 19 elementos de almacenamiento de datos tipo PAV; un adaptador; 5 lectores de tarjetas inteligentes; 10 dispositivos de autenticación de credenciales; 13 dispositivos de autenticaciones de credenciales; 12 nano dispositivos de identificación de credenciales; otros 2 nano dispositivos de identificación de credenciales; 14 dispositivos de almacenamiento de datos electrónicos tipo USB; 6 lectores de tarjetas inteligentes; un computador portátil marca Lenovo; 2 tabletas tipo I pod marca Apple; un dispositivo de comunicación móvil tipo celular, marca Apple, color negro y un dispositivo color negro de comunicación móvil, marca Samsun; una foja de papel con escritos en el anverso y reverso; una tarjeta plástica blanca con celeste y una tarjeta plástica blanca; 2 soportes de papel con similares características al de papel moneda de 50 Euros; 2 monedas metálicas que se lee 2 Euros; 3 monedas metálicas que se lee un Euro; 3 monedas metálicas que se le 050 Euros; 5 monedas que le lee 010 Euros; 20 monedas metálicas que se lee 020 Euros; otras monedas que lee Euros; 12 cables de datos con diferentes interfaces; un conector de puertos; un acumulador de energía portable; 4 dispositivos de almacenamiento de datos tipo USB; dos cables de datos; un concentrador de puerto, dos enrutadores; 7 cables de datos; un altavoz inalámbrico; un dispositivo de alimentación de energía; 3 regletas de alimentación de energía. Dentro de la cadena de custodia No. 8851922 encontramos los siguientes

indicios: 1) un Swift de 24 puertos; 2) un modem; 3) un computador portátil marca Toshiba, color plomo, con un dispositivo USB de 16 gigas; 4) una caja fuerte metálica, color plateada; 5) un dispositivo de almacenamiento disco duro marca Hitachi, un dispositivo de almacenamiento de datos, un disco duro externo marca G Drive de 3 Teras de capacidad, con cable de datos USB color negro; 4 dispositivos de almacenamiento de datos externos (disco duro), marca Lassie; dos dispositivos de almacenamiento de datos marca Wester Digital de 160 gigas; un dispositivo de almacenamiento de datos marca Lassie; dos unidades de almacenamiento de datos marca Hitachi, de 2 Teras de capacidad; un disco duro marca Digital: otro disco duro externo; una tarjeta de memoria marca Scan Disc de 4 gigas; 15 dispositivos de almacenamiento de datos electrónicos tipo USB; un computador portátil marca Lenovo; un computador portátil marca Lenovo color negro, sin batería; 6) un computador portátil marca Lenovo; un computador portátil marca Lenovo, sin batería de alimentación; un computador portátil marca Lenovo, sin batería; un computador portátil marca Lenovo; un computador portátil marca Lenovo sin batería; un computador portátil marca Lenovo; un computador portátil marca Lenovo; un computador portátil marca Positivo; un computador portátil marca Apple; un computador portátil marca Apple; 6 tabletas tipo I pod, marca Apple; indicio 7) tres pasaportes a nombre de Ola Methodius Bini Martin; una tarjeta Visa a nombre de Ola Bini; otra tarjeta marca Visa a nombre de Ola Bini; una libreta color negro con textos manuscritos color azul; 8) 12 libros con diferentes títulos en su pasta principal; 9) un teléfono fijo color negro; 10) una computadora portátil marca Apple; un router; otro router; otro router inalámbrico marca Apple; un dispositivo electrónico color blanco con teclado; un disco duro externo marca TOSHIBA de 2 Teras; 40 tarjetas color blanco; dos dispositivos electrónicos con teclado alfa numérico con puerto USB, con su respectivo cable de datos USB; 12 soportes de papel con textos impresos y manuscritos; un periódico que se lee El Comercio 13 de octubre del 2015, con 6 hojas; un periódico que se lee El Telégrafo martes 13 de octubre del 2015; 12 papeles tamaño A4 con textos manuscritos; un soporte de papel A5; 11) 51 cables con diferentes interfaces; 5 adaptadores o cargadores marca Lenovo; 7 cables de alimentación; 12) 2 router marca Apple; 2 router marca I pone, con capacidad de 2 Teras; un lector de unidades ópticas con cables USB; 13) 4 cables de alimentación de energía con un adaptador marca Toshiba; un cargador marca Lenovo; un cargador marca Deline; un computador marca Lenovo; un computador portátil marca Lenovo; 14) un computador Sistem 76; un reproductor de archivos multimedia marca I pone; dos teléfonos celulares, un teléfono celular marca Samsun; un router inalámbrico marca Apple; un router marca Apple; un cable de alimentación de energía color blanco; una tarjeta de memoria de 8 gigas; 6 dispositivo de almacenamiento de datos tipo USB; 54 soportes de papel con textos impresos y manuscritos; 15) un soporte de papen con la leyenda 10 pesos argentinos; un soporte de papel con la denominación 10 pesos argentinos; dos soportes de papel con la denominación de 5 pesos argentinos; y, varios soportes de papel con la denominación de varias monedas extranjeras; un documento de identificación a nombre de Strain Ambas Longan; una tarjeta con la leyenda Visa a nombre de Samer Mary; una tarjeta con la leyenda que se lee Mastercard; una tarjeta con la leyenda Atlantic a nombre de Ola Bini; una tarjeta que se lee Asociación Computer Machine a nombre de Ola Bini y una tarjeta con la leyenda que se lee National Usa

Number, a nombre de Ola Bini; se hace referencia además a las prendas de vestir: una mochila de nylon color negra, con 6 libros de diferentes colores, con diferentes textos; un cable de poder y un audífono; una maleta de viaje color negro, en cuyo interior 13 camisetas negras, 13 pares de medias color negro con plomo, 9 interiores tipo bóxer, 6 esferográficos y una chompa de tela color negro; dos pantalones, uno jean y otro de tela color negro; dos gafas marca Ray Ban; una tarjeta electrónica de color blanco; 6 tarjetas de presentación a nombre de Ola Bini; un bolso pequeño de nylon y un sombrero de color negro; un termo metálico color plateado, 4 frascos de plástico color blanco; una maleta de tela color negro, conteniendo 40 paquetes de galletas; un estuche de nylon conteniendo útiles de aseo; un estuche conteniendo pastillas; tres cinturones color negro y uno amarillo; 2 pantalones de tela; dos chaquetas de tela color negro, dos buzos de licra color negro; un par de zapatos deportivos blancos, plomo y anaranjado, marca Adidas; 5 folletos de artes marciales, un cable color negro y un candado pequeño color amarillo; 9 pares de guantes; llega a la conclusión de que los objetos descritos existen y se encuentran en el Centro de Acopio del Laboratorio de Criminalística de la Zona Nueva, los que se encuentran en regular estado de conservación física; **al interrogatorio realizado por Fiscalía responde que** labora como Policía 9 años; que ha trabajado en el servicio urbano, en tránsito y en el Departamento de Criminalística; que en el mes de abril del 2019 laboraba en el Departamento de Criminalística en Quito, en la sección de informática forense; en cuanto su capacitación, dice haber obtenido el título de tecnólogo y dos cursos de sistemas informáticos forenses y de manejo de evidencia digital; que realiza 10 pericias mensuales aproximadamente; en cuanto a la función de los equipos: señala que los concentrador de puerto Haf tiene el fin de prestar una extensión para admitir más conectores con iter-fas USB; el adaptador alfa Wifi, es un adaptador de red que permite tener una tarjeta de red externa para captar señales wifi; los lectores de tarjetas inteligentes permiten la lectura de estas tarjetas, las que poseen mecanismo electrónicos, es decir tarjetas de débito, de crédito; las nano llaves son llaves que cumplen la función de credenciales de acceso, es decir si en una cuenta de g mail, en lugar de digitar nuestra clave, conectamos este dispositivo para autenticar la cuenta; los dispositivos de autenticación de credenciales cumplen la misma función de tomar el pin de credencial de acceso; enrutadores: son dispositivos que se encargan de distribuir la señal de una red a diferentes equipos informáticos; aclara que dentro de los indicios hay 3 dispositivos que desconoce su funcionalidad, no tiene ni marca ni modelo, ni algún tipo de identificación; habían más o menos 12 computadores marca Lenovo; los libros en su mayoría, de acuerdo al tema, ya que no se analizó su contenido, en su mayoría se trataban de Hacking, es el área de informática que se encarga de buscar y explotar ciertas vulnerabilidades de sistemas y redes; **al interrogatorio realizado en defensa de la acusación particular responde que** la antena marca Acros sirve como puerto para captar señales de internet y obtener una red wifi; los nano dispositivo son lo mismo que las nano llaves: **al conainterrogatorio realizado en defensa de la persona procesada** responde ante la pregunta de que si se le solcito analizar la funcionalidad de los equipos,? responde que para hacer el reconocimiento debe conocer la funcionalidad, una vez emitido el informe el Fiscal no le solicitó determinar la funcionalidad de cada dispositivo, así como tampoco lo hace constar en su informe; sobre el lector de tarjetas inteligentes, señala que pueden leer una variedad de

tarjetas, las que tiene chip, sí puede ser un libro; no analizó la operatividad del dispositivo; dice que Fiscalía no le solicitó el análisis de los libros y que él solo definió la palabra Hacking de manera general; que la antena wifi sirve para conexión a la red; a la pregunta de que si en el informe constan los dispositivos denominados: 1) 3 t v g d r i v e m u v i u s b h a r t d r u - v e s i n c d 0 1 6 2 3 4 4 2 3 6 , 2) 2 t v w d c h a i g t d r a i v e h m o d e l w d 2 o e a d s - 0 0 s 2 d v o s i n w d - w c a v y 0 4 2 3 5 1 8 ; 3) 6 0 g b t o s h i v a h a i g t h d r i v e m o d e l m k i 6 3 7 g e c x s y n 9 7 o e s o x u u t , responde que no están dentro del informe realizado señalando que a su parecer son KEYS, que contienen discos duros, los cuales no fueron revisados; dice que los router distribuyen señal a una red de datos o internet; que la diferencia entre red ruteable y una red no ruteable: no sabe; que la red pública es la que asigna a un proveedor de internet; que la red privada se encuentra dentro de la red interna, de la red local; hay números IP identificados como privados; el router asigna un número de IP.

Perito que dice haber realizado otro peritaje, el No. SNNLCF-LCCF-Z9-IF2019-0316-PEE; expone: que el objeto de la pericia fue realizar la fijación, adquisición y preservación del contenido digital, almacenados en los dispositivos electrónicos encontrados en la caja fuerte, los mismos que, a través de la generación de copias espejo e imágenes forenses, fueron exportados a dispositivos de almacenamientos nuevos, ingresados mediante la respectiva cadena de custodia, al Centro de Acopio de Criminalística; señala que retiró los indicios que se encuentran en la cadena de custodia No. 276219, estos dispositivos corresponden a 2 dispositivos de almacenamiento externos, mismos que fueron individualizados como DE01 y DE02; las características técnicas de identificación son: el DE01 es de marca Toshiba serie 76EE7G06DPGC, de 2 Teras de capacidad; y, el dispositivo identificado como DE02, corresponde a un disco duro marca Selgay serie NA8RA821, de 2 Teras de capacidad; dice que además se encontró dentro de la cadena de custodia, 15 dispositivos de almacenamiento de datos tipo flash memory, de los cuales 13 son de marca Kingston y 2 de marca Scan Disc; de estos dispositivos se procedió a la generación de imágenes forense, siendo exportados a un dispositivo de almacenamiento externo, es decir un disco duro; aclara que el dispositivo DE02 no fue identificado a través de instrumental forense por tal razón no se realizó la generación de información, no generaron la imagen forense; el dispositivo que contiene estas imágenes forenses es marca Western Digital, tipo disco externo, ingresado en cadena de custodia No. 2904-19; afirma que en sus conclusiones estableció que las imágenes forenses adquiridas, fueron exportadas a una unidad de almacenamiento externo, que fue ingresado al Centro de Acopio con el código de ingreso 2904-19; ese informe lo presentó el 28 junio del 2019; la fecha de la audiencia privada para analizar esos dispositivos no consta en el informe; que no recuerda si se realizó una audiencia privada.

Realizó otro informe signado con el número CNMLCF-LCCF-Z9-INF-2019-0289-PER; expone: con fecha 18 junio del 2019, recibe un oficio de Fiscalía en el que y en su parte pertinente señala que se realice la fijación, preservación y extracción del contenido digital constante en 6 URL o direcciones electrónicas; señala que a fin de dar cumplimiento, dijo que accedió a través de un navegador: URL: https://www.youtube.com/wapch?ube=blorwlbvxvo*fearqre=youtuve.e; esta dirección es ingresada a la barra del navegador, obteniendo un mensaje dentro del contenido digital, que presenta que el video no está disponible; la siguiente URL:

<https://www.youtube.com/wapch?ube=1210913100hbien>, navegador en cuyo contenido digital tiene un mensaje que dice el video no está disponible; la tercera URL: <https://www.youtube.p/bhkeh4vbz6d>, la cual se digitó en la barra de direcciones, misma que presenta un mensaje en el contenido digital, no se puede acceder a este sitio; la cuarta URL: <https://www.youtube.b/b36f9t4anq0> misma que presenta un mensaje en el contenido digital, no se puede acceder a este sitio; la quinta URL <https://ww.eluniverso.com/noticias/2019/04/16/nota/7289255/lenin-moreno-dice-que-se-sorprendió-ola-bini-hakeando-cuentas>, misma que presenta dentro de su contenido digital, una página web dentro del sitio El Universo, que lleva como título Lenin Moreno dice que se sorprendió a Ola Bini hakeando cuentas del gobierno y personales, señalando que esta publicación data del 16 de abril del 2019, a las 18h32, este contenido digital fue materializado, es decir impreso y se adjuntó al presente informe dentro del anexo 1; la sexta URL: <https://www.facebook.com/watch/?v=821680031522415>, se la digitó en el navegador, la cual presenta en su contenido digital una publicación dentro del sitio web Facebook.com, publicación realizada por el usuario denominado SR radio, información que es de carácter público, es decir se encuentra a disposición de cualquier usuario que tenga acceso a internet, de fecha 11 de abril del 2019, a las 08h56, esta publicación contiene un texto y un archivo multimedia, es decir un video, el cual se procedió a la exportación y preservación a una unidad de almacenamiento óptico, es decir a un CD, el cual se adjunta dentro del presente informe; a las conclusiones a las que llegó, dice que 2 URL presentan dentro de su contenido digital, el mensaje el video no está disponible; 2 URL que no se puede acceder al sitio y que la publicación da facebook tiene un archivo de video; **al interrogatorio realizado en defensa de la persona procesada responde que** en el acápite quinto de su informe tiene como título la página: Lenin Moreno dice que se sorprendió a Ola Bini hakeando cuentas del gobierno y personales; que la fecha de publicación data del 16 de abril del 2019; el texto de la segunda parte del informe dice en su último párrafo: Política, 16 de abril del 2019-18h32, Quito: este martes el presidente Lenin Moreno dijo en Washington, EEUU, que el ciudadano sueco Ola Bini, se le ha sorprendido haciendo hakeo de cuentas del gobierno, personales y hakeando teléfonos, lo dijo en diálogo interamericano, uno de los principales centros de análisis de políticas públicas hemisféricas; en la publicación del 11 de abril del 2019, dentro del texto publicado se lee: rueda de prensa ofrecida esta mañana del Ministro de Relaciones Exteriores José Valencia y la Ministra del Interior María Paula Romo Rodríguez sobre el retiro del asilo diplomático al señor Julián Assange; **se solicita la exhibición del video adjunto al informe pericial:** se establece que el contenido del archivo exhibido ante el Tribunal, no corresponde a lo descrito por el perito, quien afirma que ese CD es el que contiene el mismo número que consta en el informe. Además dice haber realizado otro informe pericial, el No. SNMLCF-LCCG-Z9-INF-2019-0302-PER, de fecha 24 junio del 2019; dentro del objeto de la pericia, está el de la fijación, preservación, extracción y materialización del contenido digital constante en la URL: https://www.youtube.com/wapch?v=0g9xolmoa6g*t=8155S, fue digitada en el navegador y presenta en su contenido digital una publicación con título veráz29mapaularomo, de fecha 9 de junio del 2019, perfil que publica el video es Carlos Vera Rodríguez, este video se exportó y preservó, almacenándole en un dispositivo de almacenamiento óptico CD, el que se adjunta al informe; **al**

interrogatorio realizado en defensa de la persona procesada, esta solicita la reproducción del CD: el Tribunal aprecia una entrevista realizada por Carlos Vera a María Paula Romo, caso Ola Bini; la publicación es de fecha 9 de junio del 2019; el perfil de usuario que publica el video es Carlos Vera Rodríguez; título veráz29mapaularomo;

Finalmente señala que elaboró el informe No. SNMLCF-LCCF-Z9-INF-2019-0433-PER, de fecha 30 agosto del 2019; la pericia tenía como objeto el proceder a materializar las siguientes URL: 1) https://www.amnesty.org/download/document/amr2808712919_spanish.pdf; mostrando dentro de su contenido digital del sitio web amnesty.org, una publicación de título Ecuador: violaciones de derechos humanos en proceso penal contra Ola Bini: 2) <https://www.amnesty.org/es/lamnst/newps/2019/08/ecuador-gobierno-interfiere-en-proceso-penal-contr-Ola-Bini>; presenta dentro de su contenido digital, una publicación que lleva como título Gobierno interfiere en proceso penal contra Ola Bini, Amnistía Internacional, de fecha 26 agosto del 2019 a las 09h53; señala que estas dos publicaciones fueron materializadas, es decir impresas y se adjuntan en el informe; **al interrogatorio realizado en defensa de la persona procesada, esta solicita se de lectura a las dos hojas de la publicación; al conainterrogatorio realizado por Fiscalía responde que en el texto no hay firma de responsabilidad; no hay certificación de ninguna autoridad que sea la autora; no hay autor de los textos; al conainterrogatorio realizado en defensa de la acusación particular responde que** en cuanto a quien solicitó la pericia, fue por delegación fiscal; 8)

JOSE PATRICIO FABIAN PAREDES RUIZ: Sargento segundo de Policía quien dice prestar sus servicios por 16 años en la Policía y laborar actualmente en la Unidad de Cibercriminología; señala que en el mes de abril del 2019, prestaba sus servicios en la Unidad de Investigaciones de Delitos Tecnológicos; en cuanto a su experiencia, dice que ha trabajado en varias unidades, homicidios, Interpol, capturadores y ahora Cibercriminología, más de 500 procedimientos con detenciones de personas nacionales y extranjeras; que en el caso realizó 2 partes; 1) En cumplimiento de una orden de Fiscalía en la indagación previa No. 055-2019, de fecha 11 de abril del 2019, en el oficio suscrito por el doctor Fabián Chávez decía: impídase por un tiempo no mayor de 8 horas, que el ciudadano Ola Bini Metodius, se ausente del lugar donde sea ubicado, que este procedimiento lo realizó con el cabo primero Líder Núñez, también tuvo colaboración del Capitán Carlos Molina; indica que al ciudadano Ola Bini se le leyó todo el documento en español y en inglés por medio del sargento Vásquez Terán, agente investigador de la oficina central de Interpol Quito; durante este período de tiempo el ciudadano Ola Bini permaneció con su teléfono celular, ya que le dio todas las facilidades del caso, inclusive de ir al baño; en cuanto al segundo procedimiento o parte, fue en cumplimiento a la orden de detención con fines de investigación del ciudadano Ola Bini Metodius, este oficio estaba dispuesto por la doctora Gloria Mayorga, Jueza de la Unidad Judicial de Garantías Penales; dice que le leyó los derechos constitucionales de los artículos 3, 4 y 5 de la Constitución, a quien posteriormente se le puso a órdenes de la autoridad, cumpliendo parámetros y procedimientos, le leyó derechos en español y el sargento José Luis Vásquez de Interpol Quito, le leyó en inglés en presencia del Fiscal y varios funcionarios policiales; posterior a esto personal de Criminalística, realizó la fijación de varios indicios, los cuales constan en el respectivo parte policial; aproximadamente a las

02:00, por disposición del señor Fiscal se trasladó con el detenido desde el aeropuerto hasta el exterior del domicilio del señor Ola Bini, en el lugar el señor Fiscal se acercó al vehículo y le preguntó al señor Ola Bini si deseaba acompañarle al interior del inmueble para ver el operativo y dijo que no deseaba, permanecieron en el lugar por un tiempo más y luego a eso de las 04:00 se trasladó a la Unidad de Flagrancia para realizar el procedimiento, parte médico, gestionar los demás documentos y comunicar al consulado, en la Unidad de Flagrancia de la Patria, al no contar con suministros para la elaboración de dichos partes, se trasladó a Unidad de Delitos Tecnológicos para hacer el parte, dándole las facilidades al ciudadano Ola Bini, como llevarlo al baño, facilitarle una chompa térmica, que hablara nuevamente con su abogado, el señor Ochoa, como consta del parte de aprehensión; además en el lugar se hizo el comunicado al Consulado, el cual está anexo al parte policial; indica además que a eso de las 05:00, el sargento Ángel Guarnizo de Interpol, le volvió a leer los derechos en inglés por tercera vez; el ciudadano Ola Bini siempre estuvo en contacto con varias personas vía telefónica y en la Unidad de Flagrancia conversó con el abogado Ochoa; **al conainterrogatorio realizado en defensa de la persona procesada responde que** le dispuso se traslade al aeropuerto el Mayor David Andrade Daza, Jefe de la Unidad de Delitos Tecnológico, le dispuso a eso de medio día, llegó al aeropuerto a eso de las 14:00 o 15:00; tarde; la orden Fiscal le entregó Alfredo Salazar, agente investigador de la Unidad de Delitos Tecnológicos, minutos antes de las 15:00, aclarando que él se encontraba en la ruta viva; dice que cuando él ingresó al aeropuerto, el señor Ola Bini estaba en los filtros de Migración, donde están las oficinas de Migración, el señor Ola Bini estaba sentado, tenía todas sus pertenencias, no recuerda si estaba con su computador; cuando tomó contacto con el señor Bini no recuerda haber verificado de que nacionalidad era; señala que sí verificó los nombres y en el pasaporte decía suizo; para identificar al señor Bini, recibió colaboración del Mayor Carlos Molina para ubicarlo, él ya lo había ubicado, también estaba en el aeropuerto; le dijo que se comunique con el Mayor Molina el Mayor David Andrade Daza, Jefe de la Unidad de Delitos Tecnológicos; en cuanto a su primer parte dijo que se lo retuvo para recibir su versión libre y voluntaria y se le comunicó al Fiscal; no trasladó al señor Ola Bini donde el Fiscal para que rinda su versión; no constaba ningún delito en el oficio de Fiscalía; el documento si narra los hechos por los que se solicitaba sea detenido; el señor Ola Bini estuvo con su celular y en comunicación con varias personas desde las 15:19 hasta antes de las 23:00, que fue su detención; se contactaba mediante varias personas mediante llamadas telefónicas, en la madrugada lo hizo desde su teléfono con el doctor Davis Ochoa; a las 23:00, hora de su detención, los indicios fueron levantados y entregados a Criminalística; a eso de las 05:00 Ola Bini habló con David Ochoa su abogado, hablaron en español y en inglés; señala que recibió varias llamadas a su teléfono, desde el Cónsul y otras personas más; sobre el segundo parte señala que a las 23 horas le dio lectura de sus derechos y su compañero sargento José Vásquez Terán de Interpol, le leyó sus derechos en Inglés; en su parte no consta que José Vásquez le leyó los derechos y tampoco el sargento Vásquez firma el parte; en su parte consta que el agente Ángel Guarnizo le leyó los derechos en inglés, no tiene una constancia documental sobre ello; en el parte de detención consta copia del pasaporte del señor Ola Bini, es de nacionalidad sueca, está en otro idioma pero le dijo que estaba detenido; en el primer parte dice que adjuntó copia del pasaporte

(por secretaría se establece que el parte no contiene anexos); el momento de la detención le explicó (le leyó) al señor Bini el contenido del oficio de la orden de detención; en la orden de juez no constaba el delito, tenía relatado los mismos hechos que en la orden de inmovilización; al Consulado se le comunicó de la detención mediante correo electrónico, a las 06:49, del 12 de abril del 2019; en la tarde, cuando estaba en el aeropuerto, por disposición de su Mayor y del Fiscal, iban a trasladar al señor Ola Bini a Fiscalía, salieron al parqueadero pero regresaron a la oficina de Interpol por disposición superior; del parte consta que él levantó la cadena de custodia y le entregó al Teniente Velasco de Criminalística; al departamento de Ola Bini lo transportó con su equipo, el conductor Edison Yáñez y el cabo Núñez; en el exterior del domicilio estaba el señor Fiscal, no recuerda si estuvo acompañado de alguien más; estuvieron fuera del domicilio del señor Ola Bini unas dos horas; en los partes que realizó no informó que la lengua materna del detenido no era el idioma inglés, en ningún parte; **9) IGOR KROCHIN LAPENTY:** Gerente Regional y apoderado de TELCONET; dice que rindió una versión en Fiscalía, en ella manifestó, ante la pregunta de detalles sobre el contrato con Ola Bini con su Data Center; que en el mes de abril del 2015, firmaron un contrato de Housing y de enlace de datos para el señor Ola Bini, mediante el cual se le dio un espacio en el Data Center y un enlace de datos de 10 MDT, que el contrato se firmó el 2 de abril y el 10 de abril instalaron los equipos, que consistían básicamente en un servidor de datos; que el contrato terminó el 15 de mayo del 2019, sin tener ningún tema especial, todo fue normal; dice que a la Fiscalía remitió copia del contrato con la copia del pasaporte, la dirección de su domicilio y algunos niveles de servicios; que tipo de contrato se firmó con el señor Ola Bini: fue un formato de contrato para enlace de datos, para clientes corporativos; el contrato estaba en idioma español, no se lo realizó con traductor; él supone que el usuario comprendía el idioma español; dice que Housing es una palabra que describe un servicio que se da en Data Center, los cuales son instalaciones donde se almacenan muchos computadores, es un servicio mediante el cual, un cliente lleva su propio computador y éste es alojado en las instalaciones del Data Center de la empresa que presta el servicio; que es un enlace de datos: es una tecnología y procedimientos que permiten de dos o más puntos, se interconecten entre sí, a través de la nube de internet pueden comunicarse con diferentes puntos; señala que el Data Center de TELCONEL tienen toda la normativa que se requiere para un Data Center de teoría DIR 3, es una calificación de los Data Center, pueden ser del uno al cuatro, siendo el 4 el de mejor categoría, en su caso el Data Center es DIR 3, tiene capacidad de enfriamiento de las alas de las computadoras, las que deben mantenerse frías ya que miles de computadoras generan calor, cuenta con todo el equipo de enfriamiento, de disipación, más las instalaciones del edificio, más el personal que atiende; dice que el señor Ola Bini al firmar el contrato entregó copias del pasaporte y los datos de su domicilio; para el registro de un cliente al Data Center de TELCONET, tiene guardias que tiene una bitácora de ingreso, quienes les registran con su cédula o con un documento que se presenta, se registra en la bitácora, aclarando que debe estar autorizado su ingreso; los equipos del señor Ola Bini en el Data Center están ubicados en la calle Los Aceitunos E5-85 y Av. Eloy Alfaro, al norte de Quito, donde tienen un edificio de dos pisos, los equipos del señor Ola Bini se ubican en el piso 2, en la fila 3, en el RAP 6; no conoce el propósito de los equipos en general de los clientes, presume que hacen intercambio de

información por el mundo; TELCONET cobraba a Ola Bini por esos servicios aproximadamente tres mil dólares mensuales; una vez que se le presenta una factura, dice que en la factura no todos los valores son fijos, pero en el factura que se le presenta, por el servicio se cobra USD 2.800,00, pero el total de la factura es de USD 4.360,00 más IVA; que el contrato celebrado con el señor Ola Bini, él lo hizo como persona natural; los pagos realizados eran mensuales; **al conainterrogatorio realizado en defensa de la persona procesada responde que** no recuerda la fecha exacta en la que rindió su versión, estima que fue en mayo del año 2019, en la cual el Fiscal le hizo una serie de preguntas; no recuerda si el Fiscal le dijo previamente lo que investigaban; no le preguntaron si Ola Bini había accedido a un sistema informático; cree que no le preguntaron en la versión cuanto pagaba el señor Ola Bini por el servicio; en cuanto al desglose de los valores que constan en la factura que se le presenta dice que hay 4 cantidades: 1) por consumo eléctrico: USD 280,00; 2) por el servicio de Housing: USD 2.800,00; 3) por manos remotas USD 80,00; 4) por servicio de enlace de internet USD 1.200,00; total USD 4.370,00; que el Housing es el cobro por el alojamiento del servidor, en un espacio especial, el costo de energía es alto al igual que los equipos para enfriar que son complejos, el Data Center no solo es un alquiler de espacio, son además en las condiciones apropiadas para garantizar el funcionamiento de los computadores; para crear el ambiente propicio de los servidores, ellos han construido dos Data Center, uno en Quito y otro en Guayaquil, el de Quito que nos ocupa es construido desde cero, no adaptan ningún área, usando todas las técnicas y recomendaciones, los mejores prácticas que tiene la industria para esto, y por eso TELCONET tiene los mejores Data Center del país, los cuales cuentan con generadores de buenas marcas y mantenidos adecuadamente, cuentan con equipos de enfriamiento muy complejos, con sistemas de UPC y baterías monitoreadas, lo que requiere personal especializado, el cual es difícil de conseguir, por eso los costos de alojamiento en el Data Center son elevados, a cambio el cliente recibe la garantía de que sus equipos estarán bien; tienen muchísimos clientes en TELCONET, gran parte del sistema financiero, sistema corporativo, entidades del gobierno, muchas son corporaciones y menos personas naturales; si tenía otros clientes similares y que pagaban mucho más que Ola Bini; el contrato terminó por una comunicación de una señora que representaba al señor Ola Bini, quien pidió que termine el contrato, las personas trajeron un poder que les habilitaba en representación de Ola Bini; el acta de cancelación de servicio se suscribió con la persona delegada por el señor Ola Bini; una vez revisada el acta, señala que luego recibió una carta de la Fiscalía, donde se le pedía que esos equipos fueran entregados a la Fiscalía, en base a una orden de allanamiento, lo que se cumplió, por esa razón el acta se la suscribió con el doctor Fabián Chávez de Fiscalía, aclarando que los bienes fueron entregados a Fiscalía: dos equipos, un servidor con el nombre de Ola Bini y un Ruteador que estaba en el RAC del señor Ola Bini, cree que de propiedad de TELCONET; ante la nueva información entregada, Fiscalía solicita una aclaración, ante lo cual responde que dos personas se acercaron en nombre del señor Ola Bini, los que fueron atendidos por el abogado de la empresa, ellos presentaron un poder para dar por terminado el contrato; **10) CRITIAN PATRICIO CRUZ MEDINA:** Dice que es funcionario de carrera en el Ministerio de Relaciones Exteriores, asignado en el Consulado de Queens, señala que es agente consular en Queen; en el año 2018, era Coordinador

zonal 9 de MRE en Quito; dice que sí rindió versión en Fiscalía y entregó información requerida; indicó que ejercía sus funciones en el Ministerio de Relaciones Exteriores desde el 1° de diciembre del 2016 y que respecto del señor Ola Bini, se había identificado 3 visados otorgados, el primer visados en el 2015 y otro en el 2016, visas de trabajo y el tercero y último, emitido en mayo del 2018, fue una visa especial de residencia temporal de excepción; en cuanto a esta tercera visa, dice que como prevé La Ley Orgánica de Movilidad Humana, es una visa de competencia privativa de la autoridad de Movilidad Humana del Ministerio, son autorizadas por el Vice Ministro de Movilidad Humana, este tipo de visas de excepción debe apalancarse en la Gestión Operativa de una Unidad de Prestadora de Servicios, en este caso La Coordinación Zonal 9 de Quito; le emitió por la disposición del Vice Ministro de Movilidad Humana, trasladada a través de un funcionario de la Dirección de Visados y Naturalización, sobre la base de esa autorización verbal, La Coordinación Zonal 9 ingresó el expediente, entonces la visa fue emitida bajo un informe del Vice Ministro, quien autorizó el otorgamiento de la visa, emitida bajo el artículo 45.3 del Reglamento de la Ley Orgánica de Movilidad Humana; en el año 2018 recibió una visa temporal de excepción; que las visas de trabajo del 2015 y 2016, se emiten en virtud de un hecho generador, la condición que sustenta la visa es la existencia de un vínculo laboral que permite a los extranjeros, con contrato de trabajo recibir ese visado, previo al registro del contrato ante autoridad competente; estas visas no correspondieron al período de su ejercicio, en el expediente tiene que constar la relación laboral, el contrato con un empleador, debiendo tenerse los documentos de respaldo y justificativos; que la residencia temporal de excepción, se aplica para casos excepcionales y fija la competencia de calificación y autorización exclusivamente en una autoridad, como lo indicó el Vice Ministro de Movilidad Humana, visas que tienen una particularidad, permiten eximir de tiempos mínimos y máximos de permanencia en el País y en el extranjero, ya que en el año 2017, la normativa preveía que todo residente temporal tenía la obligación de permanecer en el País, al menos 9 meses y podía salir del País máximo 90 días; señala que el expediente de visa de excepción del señor Ola Bini ingresó el 24 de abril del 2018, el mismo que contenía la cita obtenida en el portal WEB, la constancia de pago, la copia del pasaporte del solicitante, la justificación de estadía migratoria regular en el Ecuador, el certificado emitido desde el extranjero de no tener antecedentes penales, el movimiento migratorio y dos comunicaciones al auspiciante la compañía Soporte Libre, y una comunicación de Autonomía Digital; la cita fue sacada el 24 de abril del 2018 y fijada para 12 septiembre del 2018; la visa fue otorgada al 8 de mayo del 2018, esto debido a la cantidad de visas solicitadas, especialmente de ciudadanos venezolanos; que el auspiciante Soporte Libre señalaba que había altas expectativas para colaborar a la industria tecnológica del Ecuador, firmaba como auspiciante el Ing. Ricardo Arguello, el documento tuvo que haber sido en castellano, no lo recuerda; que en cuanto al documento del Centro de Autonomía Digital, no puede aseverar sobre lo que decía ese documento, pues no tenía competencia para el otorgamiento de esa visa, no recuerda en que idioma estaba redactado, tuvo que haber sido en castellano, no lo recuerda; **al conainterrogatorio realizado en defensa de la persona procesada responde que** rindió versión en Fiscalía el 2 de mayo del 2019, habló del visado porque la Fiscalía solicitó copias certificadas del expediente y además hubo presencia de Fiscalía en la Coordinación Zonal 9, ahí

entendieron que había un proceso sobre esto; no recuerda quien de Fiscalía llegó a la Coordinación Zonal 9, pero les dijo que necesitaban revisar documentación emitida en los visados del señor Ola Bini; en su versión le preguntaron solo lo relacionado con el visado del señor Bini, así como la información que les solicitaron;

11) MARCO AURELIO PAZMIÑO MONTALUISA; Capitán de Policía y perito del Departamento de Criminalística: 1) La primera pericia está asociada a una audiencia privada de exhibición del contenido digital, la cual estaba señalada para el 24 de abril del 2019, la que tenía como finalidad exhibir las evidencias ingresadas en cadena de custodia con código de ingreso 1772-2019; dentro de esta diligencia pudo validar 68 equipos, dispositivos y elementos informáticos, constituidos por llaves de acceso o amplificación de credenciales marca Yubico, su numérico de 23 llaves y 12 nano llaves, siendo su principio de funcionamiento, que permite la autenticación de credenciales para acceso de usuario a equipó, permite proteger información que está asociada a internet, como correos electrónicos, la navegación WEB y redes sociales; de igual forma se identificó unas llaves de seguridad, con chip de cifrado de datos GNU GP, de acuerdo a las especificaciones técnicas de estos equipos, permiten cifrar los datos de manera simétrica, lo que implica que se utiliza una clave primaria y otra secundaria, es uno de los cifrados de mayor seguridad, porque utiliza alrededor de 2.048 bytes, para generar la clave de acceso; que el cifrado simétrico se utiliza para pequeños volúmenes de información, generalmente los que se generan en el acceso a internet; de los 68 dispositivos analizados, son 19 equipos de cómputo, 13 de almacenamientos de datos externos, 3 de almacenamiento interno, 31 dispositivos de almacenamiento USB y 2 tarjeta de memoria SD; se generaron las respectivas imágenes forenses de estos dispositivos, generando 72 imágenes forenses con una capacidad de 24,47 terabytes de información, las que exportadas e ingresadas a dispositivos de almacenamiento de datos bajo cadena de custodia 2374-19; es importante resaltar que todas esas imágenes forenses fueron presentadas en la audiencia privada, y tenían como característica principal que tenían un sistema de archivos basados en genelinus y que no permitían el acceso a la data de manera directa, por presentar un código de cifrado de los datos, lo cual fue presentado en audiencia privada y se solicitó a las partes que proporcionen estos accesos y poder visualizar la data; el proceso que se hace para poder visualizar, indexar los datos, es decir ordenar las 72 imágenes, fueron validadas las estructuras del archivo e indexadas, sin embargo era recurrente el proceso de cifrado de la información, por lo que no era legible de manera directa para poder ser presentada en la audiencia privada; se solicitó a Fiscalía, considerando el nivel de seguridad de esta información, se haga una asistencia penal internacional, para enviar la data obtenida a un centro criptográfico, porque el cifrado de datos hace referencia a la implementación de un algoritmo matemático para hacer que los datos que sean legibles se transformen en ilegibles, el proceso de ruptura o de des-criptado necesita una infraestructura sólida para poder obtener este tipo de informe; señala que una vez que concluyó la audiencia privada y se solicitó la asistencia penal internacional, lo que se hizo se validar de manera aleatoria ciertos dispositivos, considerando su cantidad, analizaron una flash memory, una USB, un equipo de cómputo y un dispositivo de almacenamiento externo, al analizar estos dispositivos, vieron que todos manejaban sistemas operativos Linus, y tenían algún tipo de distribución como Fedora, estas distribuciones sirven para hacer, por ejemplo de un

estudio bibliográfico, permite hacer navegaciones seguras, anónimas, Teits tiene la característica de no instalarse directamente en el equipo, sino que utiliza un dispositivo ruteable y se instala en el memoria RAM del equipo, para que una vez que finalice la actividad del usuario, no quede ningún registro, es una forma de proteger los datos, no dejar ningún tipo de registro, para no ser rastreable, para ellos es considerado como una técnica anti forense para poder describir la actividad que hizo, un determinado equipo de cómputo; dijo que analizó además, un dispositivo de almacenamiento de datos mediante el montaje directo de la imagen forense, en una unidad física, en ese sentido el resultado fue que todas las carpetas que estaba visualizadas, eran eliminadas y eran carpetas que no estaban localizadas en el espacio asignado al disco, eso hace que no se pueda visualizar ningún tipo de información; en sus conclusiones estableció que se dio cumplimiento a la audiencia privada, se analizaron y adquirieron las imágenes forenses de los 68 equipos informáticos a excepción de 16 USB, porque eran dispositivos estaban configurados bajo un módulo ruteables, configurados no para almacenamiento de datos, y 2 equipos de cómputo que por la estructura misma, no reconocían los discos internos almacenados para poder hacer el proceso de extracción de información; el resto de dispositivos que fueron ingresados bajo cadena de custodia 1772-19, fueron adquiridos y fueron ingresados en cadena de custodia, para que sean, de acuerdo a la disposición de Fiscalía, enviados a asistencia penal internacional; otra de las conclusiones es que todas las imágenes adquiridas de los dispositivo, tenían como características recurrentes, que eran archivo basados en LINOS y un proceso de cifrado de datos, que no permitía que la información sea legible de manera directa.

SEGUNDO INFORME: Informe de Inspección Ocular Técnica, del domicilio del señor Ola Blni, para lo cual se conformó un equipo multidisciplinario para levantamiento de indicios informáticos relacionados a la investigación, en ese contexto él realizó específicamente un diagrama de red, que estaba instalado en la sala del domicilio, esta red es de datos de acceso a internet que tenía 3 subredes; la primera de acceso normal a internet de todos los equipos enlazados; la segunda red estaba asociada o conectada a 4 Nas, estos dispositivos permiten que de una red física, hacer una red inalámbrica, y puede generar un Back Up, copia de seguridad de todas esa información que está asociada a esas computadoras, y la segunda red era donde están interconectados computadoras Lenovo, que trabajaban con un dispositivo USB ruteable, ya que los equipos no tenían disco duro instalado internamente, este modo de trabajo sirve para proteger datos y la actividad que hace el usuario en la red, ya que nada se registra, se aprovecha los recursos del equipo para red, memoria y el procesamiento. **TERCER INFORME:** asociada a una audiencia privada, donde se generó imágenes forenses de un servidor ingresado con cadena de custodia, imagen forense que fue ingresada para su posterior valoración; **al interrogatorio realizado por Fiscalía responde que** trabaja en la Jefatura de Criminalística, en el Departamento de Ingeniería Informática Forense; que en el mes de abril del 2019, trabajaba en la misma área; en cuanto a su capacitación: sus estudios los realizó en la Universidad de las FFAA, obteniendo el título de ingeniero electrónico, estudió en la Universidad Particular Loja, donde obtuvo el título de abogado; estudió además en el Instituto Superior de la Policía Nacional, obteniendo el título de Tecnólogo en Criminalística; que ha realizado cursos en el exterior, en la Universidad de León, en la Guardia Civil, en la Escuela Iberoamericana, sobre tratamiento, recolección y

análisis de evidencia digital; en cuanto a su experiencia en la informática forense, inició en el 2008, ha trabajado 13 años en el análisis de evidencia digital y extracción de información, desarrolló más de 5.000 pericias asociadas a estos temas, desarrolló manuales para el tratamiento de evidencia digital, desarrolló investigaciones de carácter de conmovión social; que las imagen forense es una copia íntegra BID a BID, copia todos los datos de manera exhaustiva y genera un código de verificación Hash, para mantener la integridad de esos datos, es decir la imagen forense es la copia de toda la información del almacenamiento del dispositivo; el trabajo se lo hace a través de la imagen forense, en cumplimiento a la metodología, para no alterar la operatividad del equipo e integridad de los datos; que es la DATA: es toda la información disponible o utilizada en un disco; el Código Hash: es una función algorítmica, matemática, que permite que cualquier archivo sea validado a través de una cadena fija de caracteres y que tiene como funcionalidad el de validar la integridad de esa información; solicitaron el acceso a los dispositivos a las partes procesales, específicamente a la defensa técnica del procesado, pero no tuvo respuesta, el señor Ola Bini decía que se acoge al silencio, que no entiende el idioma y que no proporcionaría ningún tipo de contraseña; que es un sistema TAILS: es un sistema operativo basado en LINUS, sirve para desarrollar actividades de carácter anónimo y proteger información, sistema ruteable que se instala en un dispositivo portable, la característica específica de este software es que se instala en la memoria RAM del equipo y todas las actividades que se ejecutan son volátiles, ya que cuando se apaga el equipo, se pierden todos los datos y las actividades del usuario; SISTEMA LINUS: es un sistema operativo como el sistema operativo Windows, es un sistema open sor de código abierto, los usuarios de este sistema tiene acceso al código fuente del sistema y lo pueden modificar de acuerdo a sus necesidades, no así el Windows, en LINUS tu puedes aplicar desarrollos de acuerdo al nivel técnico que tienes y acoplarlo a tus necesidades; memoria RAM es la memoria temporal, está activa cuando el computador está encendido, cuando se apaga el computador la memoria se elimina; un sistema operativo ruteable implica que no necesita logiarse con un computador, sino a través de una USB, es un arranque distinto al convencional, la finalidad es utilizar los recursos del equipo, pero no deja ningún tipo registro en el computador; en cuanto al sistema de privacidad utilizado, del análisis de los equipos se visualizó dos cosas importantes: la utilización de llaves LLuvico, que son credenciales de autenticación, son como llaves USB, como pen drive, de acuerdo a tu configuración puedes validar el acceso de un usuario al computador, puedes cifrar la información que envías de un correo o de una red social o cifrar tema de la navegación web; también se tiene llaves para cifrar los datos específicamente, a las cuales se incorpora un chips de la herramienta PG, que es para cifrados de datos asimétrico; y además se utiliza sistemas operativos LINUS, dentro de los equipos de cómputo, donde la información estaba cifrada, no son legibles directamente, a pesar de que se utilizó una herramienta de procesamientos de datos, no pudieron acceder a esa información; cifrar información es utilizar un algoritmo matemático, hace que la información que es legible, no puede ser entendida, existiendo dos mecanismos de cifrados, el sistema simétrico y el cifrado asimétrico, el simétrico utiliza una clave pública o privada, el asimétrico se utiliza para volúmenes grandes de información, de lo que recuerda utiliza 256 BIT para generar el cifrado; en cambio el cifrado asimétrico utiliza 258 BIT, se lo utiliza en

volúmenes pequeños, la herramienta que encontró hacía cifrado asimétrico, el más seguro; una autenticación puede estar asociada a logiarse bajo credenciales de usuario a un determinado sistema o un equipo de cómputo, existe un mash entre el usuario y la contraseña, o para autenticar un correo electrónico; validar un acceso está asociados a sistemas informáticos, por ejemplo de acuerdo a las configuraciones, puedo validar el acceso a una VPN, varias ciertas políticas que él las configurase configura, puede validar ese acceso, por ejemplo validándole a través de una dirección IP; un Tera son 1024 giga bites de información; el tiempo que le llevó para obtener las imágenes forenses: de acuerdo la cantidad de indicios y su capacidad de almacenamiento de los dispositivos, le llevó dos semanas; cifrado de datos sirve para proteger información y para hacer que la información sea ilegible, solo la pueden ver los que tienen la clave de acceso; en cuanto al grupo multidisciplinario que actuó en el domicilio del señor Ola Bini: está constituido por varios peritos, con diferentes especializaciones, estaba compuesto por un perito en inspección ocular técnica, un coordinador, un fotógrafo, un recolector de indicios y un perito en informática forense, grupo creado para tener la mayor eficiencia en el levantamiento de indicios; el diagrama de red de la sala tenía como finalidad contar con entornos de trabajo bien dimensionados: tenía 3 subredes internas almacenadas, conexión a internet, otra para generar un back up, y la tercera para ejecutar un acceso a internet a través de un sistema ruteable; **al conainterrogatorio realizado en defensa de la persona procesada responde que** sobre el primer informe, específicamente sobre el reconocimiento y recolección de indicio en el departamento del señor Ola Bini, afirma que él solo hizo la diagramación de red y de acuerdo al tipo de indicios, el perito de inspección ocular es el que realiza el levantamiento del indicio; afirma que estuvo presente en el allanamiento; dice que de lo que recuerda, estuvo en dos audiencias privadas relacionadas con los indicios, no recuerda las fechas; el perito aclara haber dicho que estuvo en la audiencia privada del 24 de abril; **con la finalidad de establecer una contradicción solicita** se de lectura al acta de audiencia privada de 30 de abril del 2019, en la cual consta la comparecencia del perito; de acuerdo a su informe, la audiencia privada se desarrolla el 26 de abril del 2019, aclara que la audiencia tiene dos momentos, en el primero se identifica sobre qué dispositivos se generarán las imágenes forenses, ya que no pueden revisar directamente la información del computador, luego se suspende la diligencia y luego de generar las imágenes forenses, se las presenta, por tanto la extracción se la hizo en la primera audiencia privada y luego en otra se presenta el informe; que un código Hash es uno algorítmico que mantiene la integridad de la información, es decir que la información almacenada no sea modificada, no son los datos como tal; la imagen forense comprende tanto el espacio asignado como no asignado del disco; el código hash está aplicado a la información del equipo, no al dispositivo, estamos hablando de la integridad de datos; sobre el sistema PAILS, una de sus funciones es la desarrollar actividades anónimas y proteger información, pero sirve para propósito diferentes, las cuales no conoce; el cifrar los datos depende del usuario, si Yo quiero proteger un archivo lo hago, si quiero cifrar mi unidad sin datos lo hago, depende de la persona y sus conocimientos técnicos; afirma que él se comunicó con Fiscalía para solicitar las claves; él conoce que el señor Ola Bini no habla español, pero él no pudo conocer porque no quiso dar las claves; le preguntan si estuvo en una audiencia

privada del 13 de mayo del 2019?, responde que no recuerda, se le presenta el acta y dice que sí estuvo; que en esa audiencia él explicó que el tener una restricción de acceso a la información, este necesita un análisis criptográfico elevado, para obtener los datos primero deben romper las claves de acceso y luego determinar qué es lo relevante, primero hay que descifrar ese contenido; que es una metodología la obtención de los códigos Hash; estos códigos están registrados en su informe de fecha 23 de mayo del 2019; determinó que no pudo acceder a los dispositivos sometidos a pericia; hicieron un análisis de 4 dispositivos, un computador, un disco duro, y los dispositivos ruteables USB, señala que se pudo acceder al sistema de archivo y al sistema operativo que estaba asociado a los equipos, más no a la información como tal; los códigos Hash encontrados están detallados en su informe; el algoritmo utilizado para obtener estos códigos es el MD5, que utiliza 128 bits, para generar los códigos y Sha1 utiliza 156 bits, la información se obtuvo en el año 2019, con la tecnología que se tenía a esa fecha; el sistema TEILS es un sistema operativo, sistema ruteable, está basado en LINUS, independiente; diferencia entre red no ruteable y ruteable: no le puede responder; como determinó el método de protección cifrado o de encriptación?: en la exposición del informe detalló los elementos sometidos a pericia, dentro del informe en la foja 6, hace referencia que existen 6 lectores de tarjetas inteligentes, que están en formato tarjetas SIM, estas internamente tiene instalado un gen UTP, se hizo un estudio bibliográfico de esta tarjetas y las características de esta herramienta es que cifra los datos de forma asimétrica; **en cuanto a OTRA PERICIA realizada, señala que esta** consistió en adquirir la información almacenada en un servidor IBM y un Roouter para la generación de copias espejo e imágenes forenses; utilizó la misma metodología antes descrita, se generó la imagen forense, se obtuvieron los código Hash de los dos discos internos que estaban instalados en el servidor, además se obtuvo las dirección IP del Router y su MAC y finalmente las imágenes forense fueron ingresadas con cadena con código de registro 2788-19; aclara que por un lapsus calami, en el detalle del informe se hizo constar una marca distinta, se le puso marca HP, pero con un documento de aclaración se especificó las características del servidor como tal; que la fecha de las copias espejos no la recuerda, pero se las realizaron dentro del plazo para la presentación del informe; que el ingreso de la imagen forense al Centro de Acopia es del 11 de junio del 2019; la pericia que se le pidió es de extracción, no de audiencia privada; señala que el manual de extracción de evidencias es técnico, no jurídico, no hacen referencia a eso; **sobre un OFICIO remitido por el perito el 28 de agosto del 2019**, en respuesta a un requerimiento de Fiscalía, en el que se hace referencia a una validación o especificaciones técnica de unos dispositivos, de los cuales se debía indicar en que página del informe se encuentran los siguientes dispositivos; a) Tres teras GDRIVE móvil USB GDRIVE, CD número CD0162344236; y b) 2 terabytes WDS GDRIVE modelo WD20 EADS-0060 S2VO; dio contestación indicando que de acuerdo a la descripción de esos equipos, no existen coincidencias con esas especificaciones técnicas, de manera textual. **ACLARACIÓN SOLICITADA por el Tribunal:** que la infraestructura que maneja esta persona o usuario, estos equipos, comprueban que tiene un nivel técnico importante, lo que no es común, que la gente cifre a ese nivel, proteja los datos a ese nivel, que si es un delito o no, eso él no lo podría decir, pero al existir ese nivel de seguridad para acceder a esa información, señala que en el País no

existen personas que manejen ese tipo de cifrado de datos, es por eso que pidieron asistencia penal internacional; señala que él solo valida la información que está ingresada bajo cadena de custodia, se encuentran con un cifrado de la información que nunca lo han tenido; es la primera vez que realiza una pericia con una cantidad así de información cifrada, no tenían ni la infraestructura tecnológica para procesar esa cantidad de datos; señala que se gestionó una asistencia penal internacional, un análisis criptográfico de las imágenes forenses, se hizo una petición con siete puntos, pero la respuesta de esa asistencia no la conoce; **12) CARLOS EDUARDO NINACURI MACAS:** Sargento de Policía y perito del Departamento de Criminalística quien refiere haber realizado 2 pericias informáticas: **PRIMERA:** El objeto de la pericia fue realizar la fijación, preservación y materialización de una dirección electrónica a pedido de Fiscalía; a través de un router se buscó la URL (dirección) solicitada por Fiscalía, aclarando que al 14 de agosto del 2019 se encontraba operativa, contenido digital de acceso público, la misma que contenía información multimedia, animaciones, las mismas que fueron fijadas y materializadas; así también aplicó la herramienta web, se procedió a preservar información, obteniéndose 2 archivos con extensión MP4 y otro con extensión PM; señala que los archivos fueron extraídos con un nombre exclusivo: reportes de vigilancia; el segundo archivo también con el nombre de reporte de vigilancias; y, la última como animaciones; señaló que la información fue materializada y adjunta al informe pericial, así como también los 3 archivos antes mencionados, fueron transportados a un dispositivo de almacenamiento óptico, el cual fue validado mediante su código Hash; en sus conclusiones estableció que la fecha de la experticia fue el 14 agosto del 2019; dirección electrónica estaba operativa, de contenido digital activo de carácter público, además materializó el contenido digital, las animaciones. **SEGUNDO INFORME:** En este segundo informe pericial le solicitaron trasladarse a la dirección Amazonas y Japón, con el fin de fijar y extraer la información de un dispositivo de propiedad de la empresa CNT; para dar cumplimiento a lo solicitado, el 22 agosto del 2019, a las 16:00, se trasladó a la dirección antes indicada, al décimo piso, se entrevistó con el señor Carlos Andrés Medina, responsable de las redes IP, quien les dio las facilidades para acceder al dispositivo antes citado, una UPC; el dispositivo era una computadora marca HP, Compac, modelo 8000; mediante la exploración del equipo se ubicó un archivo denominado CMEDINA, el cual fue validado su código Hash, el mismo que fue abierto mediante un software de correo electrónico instalado en el equipo, verificó la configuración básica de la cuenta de CNT, la cual era carlos.medina@cnt.gov.ec, luego verificó la mensajería electrónica solicitada por Fiscalía, constatando 3 mensajes de correo electrónico recibidos: 1) Tenía como asunto TDE Data Center Contingencia SIN SENAI-PETROECUADOR, el remitente era TYépez y el destinatario COMVanesa y también a otro destinatario Test IP MPDF CIE; 2) El segundo correo electrónico tiene como asunto: Instalación dato de internet Presidencia, su remitente TRevelo AVI, para destinatario AQUINA Ana ITY; 3) El tercer correo tenía como asunto Instalación datos internet Presidente, con el remitente Mosquera Verónica, al destinatario Marianela y al señor Quevedo; correos electrónicos que fueron materializados y se adjuntaron al peritaje como anexos 1, 2, y 3; señala que así también los correos electrónicos fueron exportados a un dispositivo de almacenamiento óptico y adjuntos a la pericia, así como también fueron validados mediante su código Hash; en sus conclusiones estableció que se

realizó la apertura y obtuvo respaldos de la cuenta de correo electrónico de carlos.medina@cnt.gob.ec; que dentro de la cuenta se realizó la búsqueda de tres correos solicitados por Fiscalía, constatando la existencia de 3 archivos de correo electrónico, los cuales fueron materializados y anexados al informe pericial y validados mediante su código Hash; **al interrogatorio realizado por Fiscalía responde que** trabaja en Criminalística 4 años, en la sección de Informática Forense, actualmente se desempeña en el Azuay; que en el año 2019, prestó sus servicios en el Laboratorio Criminalística de Pichincha, en la sección de Informática Forense; en cuanto a su capacitación, dice que es tecnólogo informático graduado en la Politécnica del Ejército y que ha realizado cursos de manejo de evidencia digital; que tiene una gran experiencia y que ha realizado como 200 pericias al año; **Fiscalía solicita se exhiba el contenido del CD, que el perito adjuntó a su experticia:** Se aprecian noticias de prensa (CNN) sobre el ciudadano Julián Assange y su asilo político en la Embajada del Ecuador en el Reino Unido; **al conainterrogatorio realizado en defensa de la persona procesada sobre el primer informe, responde que** sobre el URL de CNT, de lo que materializó solo recuerda el nombre del título de la publicación: Exclusivo reporte de vigilancia develen como Assange transformó una embajada en un centro de operaciones para influir en la elecciones de EEUU en el año 2016; en los tres primeros párrafos del texto no consta el nombre de Ola Bini, si consta el apellido Assange; en la segunda hoja del anexo no se encuentra el nombre de Ola Bini, en esta hoja si consta el apellido Assange; en la siguiente hoja del anexo no consta el nombre Ola Bini, el apellido Assange si consta; en la siguiente hoja no consta el nombres Ola Bini, el apellido Assange si consta; en la siguiente hoja si consta el apellido Assange, no consta el nombre Ola Bini; en la siguiente hoja no consta el nombre de Ola Bini; la siguiente hoja no consta el nombre de Ola Bini, en el penúltimo párrafo consta el apellido Assange en dos ocasiones; en la siguientes siguientes dos hojas no consta el nombre de Ola Bini; **al conainterrogatorio realizado en defensa de la persona procesada sobre el segundo informe, responde** que sobre el dispositivo de CNT periciado, no sabe si se realizó audiencia privada; no estaba en cadena de custodia; que la fecha del primer correo electrónico analizado es el 24 de julio del 2015, a las 09:51 remitido por tyepezedy, enviado para comvanesa, además para destinatario: Test IP MPDF CIE; ASUNTO: EP DATA CENTER CONTIGENCIA SENAI PETROECUADOR, categoría 2; el segundo correo de fecha 29 de noviembre del 2016, a las 22:39, remitido por trevelo avi, para destinatario conalquina ana to, con el asunto instalación dato de internet Presidencia; el tercer correo electrónico es remitido por tmosquera verónica, para el destinatario con ruiz Marianela, con el asunto instalación datos internet presidencia, de fecha 1° de diciembre del 2016, a las 10h53; dentro del anexo 3, que contiene una larga cadena de correos, en la foja 3142, hay un correo de correo carreraanabel, remitido a mauratvanesa, de 23 de julio del 2015 a las 18:26, tiene como asunto data center Contingencia Senai Petroecuador y el texto del correo es: estimados, se envía lo solicitado, se aplica el DEMO, por favor confirmar cuando es la instalación del servicio para desbloquear las IP; señala que en el segundo anexo, fojas 3.151 hay una cadena de correos, los cuales terminan con un correo remitido por alquina ana, enviado el 29 de noviembre del 2016 a las 22:24, dirigido a tecoyamipmplsgy; asunto LV Instalación datos de internet presidencia; estimados mplis uico, por favor su ayuda con la siguiente

configuración, luego saltan dos tablas, dentro de las cuales, en uno de los ítem hay uno que dice wan y un número 10.100.220.1-30; en la segunda tabla también se tiene un ítem que dice wan y hay un número que dice 10.100.220.5-30, adicional hay otra fila que dice lan a rutear con un número 10.50.5.0-29; responde además que no conoce que es el estándar RFC1918; **13) KLEVER GIOVANNY SALGUERO SOSA:** Señala que es ingeniero en sistemas, trabaja en la Presidencia de la República, en la Dirección de Gestión Documental y Archivo; que en el año 2015, laboraba en la Dirección de Tecnología de la Presidencia de la República; en cuanto a sus responsabilidades, era líder del área de redes y conectividad, donde tenía a cargo un equipo de 6 técnicos, encargados de garantizar la disponibilidad y continuidad de los servicios tecnológicos de la Presidencia; que el Centro de Datos de Contingencia de la Presidencia de la República, nace por una observación de Contraloría General del Estado que les informan que se necesita tener un sitio alternativo o de contingencia, para ese entonces las autoridades, por falta de recursos económicos, no se pudo implementar un sitio alternativo y se buscó sitios en Instituciones Públicas para poder alojarse en modalidad de hosting, la empresa EP Petroecuador les presta o les da los equipos y la infraestructura tecnológica de ellos, para poder implementar este sitio alternativo de contingencia; el sitio principal está ubicado, con su Data Center, en Lumbisi, en el Data Center de la ex Secretaría de Inteligencia, actual SIES; en cuanto al tipo de información que se registraba, al tratarse de un Data Center de contingencia, es un sitio presto a solucionar una emergencia del Data Center principal, en el posible caso que sufra un siniestro el principal; en el sitio alternativo de contingencia las autoridades de ese entonces vieron la necesidad de alojar, por el reducido espacio que se tenía, sistemas importantes para el accionar de los mandatarios, en este caso había un sistema de decretos presidenciales y compromisos, se replicó el mail bock, que es su servidor de correo electrónico institucional, para que en el posible caso de siniestro, levantarlo de forma manual el sitio contingente y poder tener correo y los sistemas indicados; en este centro de contingencia, se conoce como información crítica o se le catalogó como información de primera mano que se necesitaba tener en el despacho presidencial, un sistema de mensajería que en este caso es el correo institucional, lo catalogaron como crítica solo en caso de tener un siniestro en el Data Center principal, poder seguir con estos servicios disponibles, hasta que haya solución en el Data Center principal; en el sitio alternativo se replicaba la información, una vez que la proveedora, en este caso CNT proveía los datos como el de internet, que unía los dos Data Center, se empezó a replicar o a copiarse la información del lugar principal al alternativo; el sitio alternativo estaba en la ciudad de Guayaquil, porque la normativa técnica nos dice que necesariamente tiene que estar en un lugar geográfico alternativo, porque estaba en Guayaquil no sabe las razones, por temas de presupuesto o por no poder realizar construcciones en el Palacio de Carondelec; señala que el Centro de Contingencia estaba operativo pero no en producción, se cumplió la primera fase de entrelazar y replicar de información mas no en producción, no se hicieron pruebas de contingencia para dar de baja a sitio principal y levantar el sitio alternativo y probar esos servicios; que el proveedor de enlace de datos es CNT; los datos de conexión son de conocimiento reservado, ya que esos datos de configuración para poder interlazar las dos redes, solo la conoce en este caso el cliente Presidencia de la República, que proporciona esa información a CNT, para la configuración de los equipos de

comunicación; que se implementaron dos enlaces, uno de datos y un enlace de internet, el de internet tiene una dirección pública IP, el proveedor da la dirección IP pública que es la 181.113.57.169, esa dirección IP la configura el proveedor en su equipo de comunicación; de ese enlace de datos tenía conocimiento el cliente Presidencia de la República, el proveedor CNT, la institución donde se estaban alojando EP Petroecuador; **al conainterrogatorio realizado en defensa de la persona procesada responde que** para ejecutar este convenio del Data Center, las autoridades firmaron un convenio interinstitucional, desconoce quién lo firmó, las entidades que intervinieron fueron la Presidencia de la República y Petroecuador; no recuerda la fecha en que se suscribió; revisa su versión rendida y dice: que el convenio se firmó entre finales del 2015 e inicio del 2016, estaba vigente hasta el año 2019 que rindió la versión; que el Data Center de Contingencia tiene varios equipos, servidores, equipos de almacenamiento que ellos los denominan Storash, de seguridad perimetral, farwoods y de comunicación que provee CNT; Fiscalía no pidió información de esos equipos, tampoco le solicitaron las IP de esos equipos, no les pidieron remitir los accesos, no les pidieron posible accesos no consentidos a esos equipos del Data Center; que el 28 de agosto del 2019 que rindió su versión, él estaba como líder del área de redes y conectividad de la Presidencia de la República, era líder desde el año 2015 no recuerda la fecha; previo a la suscripción de este convenio interinstitucional se firmó un DEMO, no tiene en mente las fechas, fue a finales del año 2015, puede ser; que el Centro de Contingencia estaba operativo pero no en producción, desde finales del 2015 y comienzo del 2016; la dirección pública IP de internet fue implementada después de la ejecución de los DEMOS, luego se entrega a través de un acta de entrega del servicio, se entregan los enlaces de datos y del internet operativo; señala que se ejecutó un DEMO, entró en funcionamiento 2015-2016; la dirección IP estaba asignada al enlace de internet, configurada en un router del proveedor; la dirección IP es la misma de los equipos de comunicación desde el año 2016, no sabe si había datos estaban en el router, ya que era administrado directamente por CNT ET; que en este DEMO si estaba configurado un corta fuego, desconoce la fecha que fue instalado ya que estos equipos fueron proporcionados, configurados e instalados por Petroecuador; los equipos no fueron cambiados entre el 2015 y 2016; el cortafuegos estaba ubicado en el centro de datos de Petroecuador, él nunca estuvo ahí, lo supo por reuniones técnicas con funcionarios del Petroecuador por medio de video conferencias, a través de informes del proyecto, describieron la arquitectura de seguridad implementada para los servidores instalados en EP Petroecuador; como equipo técnico hicieron pruebas tanto del equipo técnico de Presidencia, como de EP Petroecuador, que el corta fuegos estuvo configurado de acuerdo necesidades de Presidencia y operativo desde el inicio; que el corta fuegos estaba implementado para los dos enlaces, por varias interface, una para el enlace de datos y otra para el enlace a internet; interface quiere decir que el enlace de datos que viene del proveedor ingresa al farword, a un puerto, en donde va a empezar a filtrar todo el tráfico, eso se hizo para el enlace de datos, en el mismo equipo para el enlace a internet, en otro puerto se conectó el enlace de internet para aplicar las políticas y reglas de seguridad; a él no le han solicitado esas pruebas realizadas; el corta fuego estaba implementado entre el equipo, el farword y luego está el equipo de comunicación del proveedor; **14) WILLIAM DANILO CASTRO ACOSTA:** Mayor de

Policía y perito del Departamento de Criminalística, quien dijo que realizó varias pericias: **PRIMER INFORME:** Pericia de audio, video y afines, con informe No. DCP-219-01010: en cuanto a su objeto, este era realizar la extracción de la información contenida en los dispositivos móviles que constan como evidencias; señala que se recibieron los objetos materia de análisis: un dispositivo Tablet, marca Apple, color plomo con negro, modelo A1701, serie DMPDR03GHP83, la cual no tenía tarjeta SIM (Chip), ni dispositivo de memoria externa; un dispositivo Tablet 2, marca Apple, color plomo, modelo A1701, serie DMPBB1GZHP83, sin tarjeta SIM, ni memoria externa; un dispositivo de comunicación móvil teléfono celular 1, marca Apple, color negro, con tarjeta SIM de la operadora Claro, serie 9308955100054920382; un dispositivo de comunicación móvil teléfono celular 2, marca Samsun, color azul, modelo GT-I9300, i mail 352993/05/639690/6, sin tarjeta SIM, ni tarjeta de memoria; un dispositivo de comunicación móvil teléfono celular 3, marca Samsun, color negro con plomo modelo GT-E100W, con i mail 355874/04/900584/5, con tarjeta SIM o chip, de la compañía COMVIQ, serie 89462046110005771752IQ851; un dispositivo de marca Apple, color negro, modelo A1574, serie CCQQ402WGM1C, sin tarjetas; el siguiente dispositivo es un teléfono celular 4, Apple, color negro, modelo A1387, sin i mail, sin tarjetas; el siguiente dispositivo es una Tablet 3, marca Apple, color plomo, modelo A1673, serie DMPRR024H1MM, sin tarjetas; un dispositivo Tablet 4, marca Apple, de color plomo, modelo A1403, serie BLXHD1PVDNQV sin tarjetas; un dispositivo Tablet 5, Apple, color plomo, modelo A1474, serie BMPLM47FK13, sin tarjetas; un dispositivo Tablet 6, marca Apple, color plomo, modelo A1701, serie DMPVM5W7HP83, sin tarjeta; un dispositivo Tablet 7, marca Apple, color plomo, modelo A1673, serie DMPSR0JXH1MM, sin tarjetas; un dispositivo Tablet 8, marca Apple, color plomo, modelo A1566, serie DMPNR2KAG5W1; señala que dentro de los trabajos realizados está la fijación gráfica y descriptiva de cada aparato, una verificación visual de los dispositivos para ver si están en condiciones de ser sometidos a peritaje; que para la extracción de información que contenían, se utilizó el dispositivo de extracción forense el Universal Forensic Extraction Device UFER; señala que el siguiente proceso dentro de su pericia consistió en la extracción de información de cada dispositivo: TABLET 1: no fue posible extraer información, tenía un código de bloqueo; TABLET 2: también tenía código de bloqueo, no se pudo extraer información; el TELÉFONO 1: también poseía código de bloqueo, no se pudo extraer información; tenía un chip (SIM) de la operadora Claro: extrajo la información: siendo números de asistencia, de emergencia y generales; el TELEFONO 2, marca Samsun: extracción de información en 132 fojas en formato PDF, consta como anexo al informe; el TELEFONO 3: no fue posible extraer información; de la tarjeta SIM del teléfono: información números telefónicos y contactos, así como mensajes de textos; extracción del dispositivo Marca Apple 1: no fue posible extraer información por tener un código de bloqueo; el dispositivo Teléfono celular 4: no se extrajo información por tener un código de bloqueo; el dispositivo Teléfono celular 5 no se extrajo información por tener un código de bloqueo; TABLET 3: no se pudo obtener información por código de bloqueo; TABLET 4: no se pudo obtener información, por cuanto estaba restaurado de fábrica; TABLET 5: tampoco extracción presenta código de desbloqueo; TABLET 6: no fue posible extraer información por presentar un código de bloqueo; TABLET 7: tampoco fue posible la extracción presenta código de desbloqueo; TABLET 8: tampoco se pudo realizar extracción de información por que

presenta daño. En sus **CONCLUSIONES** estableció: que la integridad físicas de los dispositivos, en unos casos era optima y por tanto aptos para peritaje y en otros casos no; que dentro de lo dispuesto en las audiencias privadas, se extrajo información de los dispositivos que se podían someter al peritaje, siendo anexadas al informe; como última conclusión indica que hubo dispositivos que no fue posible extraer información por tener contraseñas o estar en malas condiciones; **al interrogatorio realizado por Fiscalía responde:** que labora en el Departamento de Criminalística 14 años; en cuanto a su capacitación, ha realizado curso de perito en Inspección Ocular Técnica, Tecnología en Criminalística, diferentes capacitaciones internacionales y nacionales en procesamiento y extracción de información digital de equipos de comunicación móvil; capacitador en temas de foto digital, pericial y forense; capacitaciones con el Departamento de Estado de EEUU, en investigación de explosivos; en cuanto a su experiencia en pericias de audio y vídeo, señala que ha realizado más de 100 pericias de este tipo; **al contrainterrogatorio realizado en defesan de la persona procesada responde:** sobre si los IPod tiene ranura para el ingresar una tarjeta SIM o chip: responde que no recuerda si tenían, no lo describió en el informe; en cuanto al Teléfono 1: éste tiene la palabra ENTER PASSCODE (introduce un código de acceso); el IPod 1: tiene la palabra ENTER PASSCODE; el Teléfono 4: contiene la palabra ENTER PASSCODE; Teléfono 5: contiene la palabra ENTER PASSCODE; cuando hace la extracción de la información de los equipos, se genera un informe y el equipo forense realiza una extracción de la información, es una copia de esa información, en reporte PDF y Digital; en cuanto a la información que se pudo extraer, no recuerda el número de audiencias privadas en las que estuvo, fueron previas al informe, donde se exhibieron los dispositivos, ahí no se vio el contenido; que la tarjeta SIM del Teléfono 3: mensajes SMS, octava columna: mensajes enviados o recibidos de este teléfono en otro idioma; aclara que la pericia de extracción de la información la hizo el en el Departamento de Criminalística, no estuvieron presentes los sujetos procesales; que en la captura del Teléfono 1, consta la palabra ENTER PASSCODE, Claro 3G, es decir que el teléfono estaba conectado a la red. **SEGUNDO INFORME:** En esta segunda pericia, su objeto fue que se designe, por parte de Criminalística, de la sección de Audio, Video y Afines, peritos para realizar la exhibición y extracción del contenido digital registrado en los dispositivos de almacenamiento y electrónicos, que reposan en el Centro de Acopio, bajo cadena de custodia 3082-2019; para la elaboración de esta pericia existió una audiencia privada, se procedió a retirar los elementos de la cadena de custodia que eran: **1)** Un dispositivo de almacenamiento óptico marca ADATA, tipo USB, serie no legible, de 8GB, estructura plástica color verde, estaba en un estuche de papel color amarillo, presenta textos manuscritos realizados con tinta roja 3082-19, y además un estuche de estructura mixta plástico y papel multicolor, el cual presenta una carpeta de archivos de nombre "grabaciones", con 756 archivos de audio y 756 archivos de texto; **2)** Un almacenamiento óptico marca BERBATIN, tipo DVD R, serie no legible, de 4.7GB, de estructura plástica, color plateado, con estuche de papel amarillo con textos manuscritos rojo que se lee 3082-19, así como texto manuscrito en tinta azul que se lee oficio SN13 JUNIO-2019 CRATEL.CA. un CD; en las características digitales el DVD lleva el nombre de 190612_2120, contiene 2 archivos de audio y video de nombres 0204-19, Bc hacker Sueco MP 11 abr 2019; **3)** Un dispositivo de almacenamiento óptico marca Maxell, tipo DVD R, serie WEH607100350L10, de

capacidad 4.7 GB, de plástico color dorado; en su estuche de papel amarillo con textos manuscritos en tinta roja 3082-19, textos manuscritos en tinta azul en los que se lee Oficio No. 032GG-2019, canal 1; además un sobre de papel donde se aprecian logotipos donde se lee Canal 1 y www.canal1tv.com; también hay textos manuscritos con tinta azul en los que se lee Canal 1 VERAS 9 de junio 2019; el disco poseía un adhesivo rotulado que se lee Canal 1 VERAS 9 de junio 2019; en cuanto al contenido digital, el nombre con el que está grabado el dispositivo es 24 jun 2019; contiene un archivo audio y viendo de nombre VERAS DOMINGO 9 de junio 2019-MA. Paula Romo; **4)** Almacenamiento óptico, un CDR Maxell serie no legible, 700 MB, plástico, con textos en tinta rojo en los que se lee 3082-19, textos manuscritos con tinta azul un CD; rotulado con textos tinta negra: se lee Videos; el disco posee 7 archivos de audio y video; **5)** Almacenamiento óptico marca SEAGATE, es un disco duro de serie NA9QA8H3, con capacidad de 8 TB, color negro, con estuche amarillo con textos de tinta color roja, que se lee 3082-19, tinta escritor azul: Disco Duro SJS1719, Cuerpo 18 EXP55-8019, sin rotulado, el que contiene 2 carpetas de archivos y dos archivos propios del dispositivo; se procedió a realizar la FIJACIÓN de los dispositivos, el martes 6 de agosto del 2019, se dio inicio a la audiencia privada con la participación de las partes procesales; se hizo una revisión de los videos y se dispuso se realice la materialización de los archivos de video obrantes en los dispositivos: señala que debe hacer la siguiente puntualización: parten del fundamento técnico de que un video está constituido por una serie de imágenes fijas, que son capturadas rápidamente, que al ser reproducidas parece o dan sensación del movimiento, por eso se realizan una serie de capturas de pantalla, en las cuales se puede ver el contexto de lo que está sucediendo en ese video, es decir se cambia de una estructura digital a una física que pueda ser percibida por nuestros sentidos; en cuanto a los videos: 1) VIDEO CH05_20190403065610, duración de 45 segundos, se aprecia a una persona de género masculino, la cual se acerca a un ascensor, manipula el tablero de instrumentos del ascensor y realiza con sus manos, la manipulación un dispositivo de comunicación móvil, apreciándose una serie de presionados en el teclado del dispositivo; 2) VIDEO CH05-20190405065818 de duración de 1 minuto y 28 segundos, donde se aprecia a una persona de género masculina que se acerca a una estructura como la de un ascensor, realiza manipulación de los controles y posterior manipula un dispositivo de comunicación móvil; 3) VIDEO CH0520190406094621, donde se aprecia persona de género masculino, se acerca hasta al ascensor, manipula su control y a continuación manipula un equipo de comunicación móvil (teléfono celular), observándose que era una combinación de teclas, luego de lo cual el equipo se desbloquea; 4) VIDEO CH0520190406115301, con duración de 1 minuto con 2 segundos y donde se aprecia a una persona de género femenino, la que se acerca a la estructura del ascensor y manipula sus controles; 5) VIDEO de nombre CH0520190406154623, video donde se aprecia a una persona de género masculina, quien se acerca al ascensor, manipula el tablero, toma un teléfono celular y realiza la manipulación del mismo, parece que digita un código y el teléfono se habilita; 6) VIDEO de nombre CH0520190407103503, se aprecia persona género femenino desciende del ascensor y camina por el pasillo hacia las puertas; 7) VIDEO CH0520190408190405, de duración de 1 minuto y 10 segundos, en el cual se aprecia a una persona con buzo con capucha, quien se acerca estructura como de ascensor, realiza la

manipulación del control y toma un equipo celular y lo manipula, al ser una actividad recurrente y gracias a las condiciones de luz, realizaron una ampliación digital, donde se puede ver el presionado de esta combinación de teclas, que corresponden a los números 5-5-3-7-3-5-7-1, el teléfono cambia la pantalla y aparece habilitado y la persona continua con su actividad, sube al ascensor; 8) VIDEO de nombre CH05_20190409065738, se aprecia nuevamente a la persona de género masculino, quien se acerca al ascensor, manipula los controles del ascensor y digita un combinado de teclas en el teléfono celular y este cambia la pantalla y se activa; 9) VIDEO de nombre CH05_20190409183726, de 34 segundos, se aprecia a una persona de género masculina y de género femenina, salen del ascensor, caminan por el pasillo y se dirigen a una de las puertas; 10) VIDEO es de nombre CH05_20190411083101, se aprecia a una persona de género femenino portando una mochila, sale del ascensor y se dirige a una puerta existente; 11) VIDEO de nombre CH05_20190441109258, se aparecía a una persona de género femenino, se acerca a un ascensor, manipula sus controles y sube al ascensor; 12) VIDEO de nombre CH05_20190411111248, donde se aprecia a una persona de género femenino, la cual sale del ascensor, camina por el pasillo y aparece una persona de género masculino y continua caminando por pasillo; 13) VIDEO de nombre CH05_20190411113833, se aprecia a una persona DE GÉNERO masculino que porta algunas maletas, se acerca al ascensor, manipula sus controles y sube al ascensor; 14) VIDEO de nombre CH05_20190411213410, se aprecia a una persona de género femenino, quien sale del ascensor, camina por el pasillo y se dirige a una de las puertas que se aprecian en la cámara; 15) VIDEO de nombre CH0520190411214200, se aprecia a una persona de género femenino, quien sale de una de las puertas, manipula el ascensor y espera; 16) VIDEO de nombre CH054_20190412025826, se aprecia que del ascensor salen varias personas, caminan por el pasillo y se van a una de las puerta del lugar; 17) VIDEO de nombre CH0520190412030437 se aprecia pasillo varias personas; 18) VIDEO de nombre CH05_20190412030836 se aprecia dos personas que se encuentran en pasillo cercano a una puerta; 19) VIDEO de nombre CH05_20190412030945, en el cual se pude ver a varias personas, algunas llevan el uniforme táctico de policía GOE, y a varias personas en el lugar; 20) VDEO CH05_20190412034015, se aprecia que del asesor baja varias personas de género masculino y femenino, una de las cuales tienen la chompa de la Policía Nacional; 21) VIDEO de nombre CH05_20190412040013 se aprecia a varias personas, salen del asesor otro grupo de personas; 22) VIDEO de nombre CH05_20190412041155 se aprecia a varias personas de género masculino, se hace un zoom de la persona; 23) VIDEO de nombre CH05_20190412045044 se aprecia a varias personas que del asesor sale persona con ropa formal; 24) VIDEO de nombre CH05_20190412051028 se aprecia a varias personas que manipulan el tablero del ascensor y suben al mismo; dice que también se realizó la secuencia de imágenes de los archivos de audio y video obrantes en el dispositivo BERBATIN: VIDEO de nombre 120419MPG, tiene una duración de 17 minutos y 40 segundos, fundamentalmente se aprecia a dos persona una de género masculina y otra de género femenino, los logotipos identificativos de Tele Amazonas, 24 horas; el siguiente VIDEO es de nombre BCHACKERSUECOMP11ABR2019MPG, tiene una duración de 3 minutos y 38 segundos, se aprecia varias secuencias de personas de género masculinas y

femeninas, estructuras como cables, textos que se presentan en el video y otras imágenes proyectadas y finaliza con el enfoque a varias personas masculinas y femeninas; a continuación se tiene las secuencias de imágenes de los archivos de audio y video obrantes en el dispositivo de almacenamiento óptico MAXCELL, el nombre del video es VERAS domingo 9 de junio del 2019 MA Paula Romo, con una duración de 01h26, se aprecia una persona de género masculino y otra de género femenino, desarrollándose un diálogo entre estas personas; a continuación se tiene la materialización del VIDEO del dispositivo de almacenamiento óptico MAXCELL, color plateado y signado con el número 9: el nombre del video es WhatsApp 2019-06-27 AT91937AM, donde fundamentalmente se aprecia a varias personas que inspeccionan la cajuela de un vehículo color rojo, con persona vestida de Policía y personas con ropa formal; en cuanto al VIDEO de nombre WhatsApp 2019-11-06-27-AT9.23.05AM, con una duración de 2 minutos con 2 segundos, aquí pese a la inclinación de la cámara se puede ver a una persona en el interior de un vehículo, otra persona que se encuentra afuera con una chompa refractivo, interaccionan en un diálogo; el siguiente VIDEO de nombre WHATSAPP-0627AT9.23.40AM, en este video se ve a una persona vestida de Policía que realiza una actividad junto a un vehículo; el siguiente VIDEO de nombre WHATSAPP 2019-06-27-AT9.24.21AM, con duración de 9 segundos, en el cual no se aprecia nada; el siguiente VIDEO de nombre WHATSAPP 2019-06-27-AT9.23.AM, aquí se aprecia a una persona con vestimenta de la Policía Nacional, quien realiza actividades junto a un vehículo detenido; VIDEO WHATSAPP 2019-06-27-AT9.28.45AM se puede apreciar el tablero de instrumentos de un vehículo; el siguiente VIDEO de nombre WHATSAPP 2019-06-27-AT9.31.03AM, en el que se aprecia el interior de un vehículo. Señala que a continuación se realizó la secuencia de los archivos de audio y video de un dispositivo de almacenamiento externo, disco duro tipo USB marca Seagate, color negro, de serie NA9QA8H3, en estos videos en el desarrollo de la audiencia privada, la defensa técnica solicitó la materialización, donde se aprecia en el archivo C115CORREDORADUANA_201904-11_11, 59 minutos 55 segundos, 00MSEG64, es un video bastante extenso, su duración es de 15 horas y 30 minutos, se aprecia la estructura de un corredor, unas bandas transportadoras, se trata de un aeropuerto, se observa además a varias personas portando varios objetos, al parecer equipajes; el siguiente video es de nombre C159BANDASEQUIPAJEINT_2019-04-11_12HORASMIN00S000MS64, nuevamente señala que es un video extenso, con una duración de 15 horas y 29 minutos, en el que se observa una estructura, unas bandas de equipaje, un counter y algunas personas; en el siguiente VIDEO es de nombres C160BANDAS EQUIPAJE COUNTERS MIGRACIÓIM_20190411_11H59:55S000MSG64, nuevamente un video largo de 15 horas y 29 minutos, en un momento de la reproducción del video se aprecia a varias personas; otro VIDEO de nombre C201ALPÚBLICOSALIDASNORTE2019-04-11_11h59MIN00S000MSG64, con una duración de 15 horas y 31 minutos, en el que se aprecia a varias personas que pasan por el enfoque de la cámara; otro video de nombre C213FILTROSEGURIDAD2019-04-11_12H00MIN00S000MSG64, un video bastante largo que en el enfoque de la cámara se puede apreciar un sin número de personas; el siguiente video de nombre otro C216HALLMIGRACIÓN2019-04-11_12H00MIN00S000MSG64, en este video fundamentalmente se observa varias personas, algunas de ellas sentadas, otras paradas y caminando; el siguiente video

es de nombre C2017HALLMIGRACIÓN 2019-04-11_12H00MIN00S000MS.G64, de 15 horas y 29 minutos, en el que se observa a varias personas en el enfoque principal de la cámara; el siguiente video es de nombre C2018HAL-LEMIGRACIÓN201904-11_12H00MIN00S000MSG64, video largo de 15 horas y 29 minutos de duración en el cual en el enfoque de la cámara se aprecia a varias personas transitando en el lugar; el siguiente video de nombre C236SALAEMBARQUE-A7-2019-04-11_12H00MIN00S000MS.G64, de 15 horas y 29 minutos, en el que se aprecia a varias personas; el siguiente video es de nombre C237SALAEMBARCAA6201904-11_12H00MIN00S000MS.G64, igual se aprecia a varias personas, video largo de 15 horas y 29 minutos, se ven a personas con chalecos color verde; en el siguiente video de nombre C249EXTERIORESNACIONAL_2019-04-11_1159MIN00S000MSG64, un video largo de 15 horas y 31 minutos, donde se aprecia a personas a bordo de una moto y un vehículo del cual descienden personas de género masculino; el siguiente video de nombre C261CHEQUENACIONAL_2019-04-11_11H59MIN00S000MSG.64, otro video largo de 15 horas y 31 minutos donde se aprecia a varias personas que se encuentran en columnas; el siguiente video es de nombre C404-TERRAZA-09-04-11_12H00MIN00S000MS.G64, se aprecia a varias personas, vehículos de la Policía Nacional y varias personas con chompas color verde, personas de la Policía, abordan uno de los vehículos, también camionetas que son abordados y se movilizan. Señala que en el desarrollo de esta audiencia, como se aprecia de los videos, se puede inferir una contraseña de desbloqueo de un equipo de comunicación móvil, el Fiscal dispone que la contraseña sea ingresada en todos los dispositivos móviles que constan dentro de esta cadena de custodia y se extraiga la información, contando con la autorización judicial para la extracción, logrando el desbloqueo de un teléfono celular marca Appel, color negro, modelo MQ7C2ZD/A, con i mail 352993090817594, con tarjeta SIM de la operadora Claro, de serie 895930100054920382, sin tarjeta de memoria, equipo en buen estado de conservación y funcionamiento, óptimo para ser sometido a peritaje; en cuanto a la extracción de la información, esta se le remitió en otro informe pericial, por la cantidad de información que existía y como anexo a este informe pericial, toda la extracción de la información se remite en un dispositivo USB marca Kingston, de 128 GB, con número 042715-554A00LF, en el cual constaba toda la información extraída y el reporte en PDF que estaba conformado por 42.864 páginas; así mismo por la naturaleza de la información extraída, se deja constancia de que de esta extracción no se almacenó ningún otro tipo de copia, y que la información, luego de que sea exhibida y de acuerdo a los requerimientos, se procederá a materializar únicamente lo solicitado por las partes. En sus CONCLUSIONES determinó que los dispositivos de almacenamiento tanto ópticos como externos tipo USB, están en el Centro de Acopio del Departamento de Criminalística, bajo cadena de custodia 3082-19, de los cuales se determinó su integridad física y que son aptos para ser sometidos a peritaje; así mismo se logró determinar que los archivos de audio y video obrantes en los dispositivos de almacenamientos, fueron reproducidos mediante software BLC y otros software adecuados, no han sido modificados ni alterados, por lo tanto conservan su integridad y autenticidad; se realizó capturas de pantallas de las reproducciones de los videos, las mismas que corresponden a las secuencias de imágenes, con lo que se logra materializar esos videos; luego de observar en varios

de los videos, el presionado de un código número 55373571, se los aplicó a los dispositivos electrónicos de la cadena de custodia, de los cuales se desbloqueó un Apple I phone 8, modelo MQ7C2ZD/A, con i mail 352993090817594, se determinó su integridad física, su funcionamiento era óptimo y apto para ser sometido a peritaje; el dispositivo I Phone 8, se encontraba en buen estado de conservación y funcionamiento y se extrajo la información, la que se remitió mediante informe técnico pericial DSP201901688; **al interrogatorio realizado por Fiscalía responde que** la clave del teléfono 55373571, la persona que aparece en los videos la utilizó en varias ocasiones; los nombres del archivo de estas imágenes, están identificados por el número de la cámara, en este caso CH05, a continuación tiene el año, en el caso 2019, a continuación el mes 04, el día 03, la hora 06.52.10; de fojas 32 y 33 del informe: en la foja 32 del informe el nombre del archivo es CH0520190411214200 y en la página 33, el siguiente video identificado con el nombre CH0520190412025826; **al conainterrogatorio realizado en defensa de la persona procesada responde que** el informe es de fecha 24 de agosto del 2019; dentro de la cadena de custodia No. 3082, al reproducir el dispositivo que consta en el numeral 4.3 de la pericia, de marca Berbatín No. 6, se aprecia la existencia de 2 archivos: son exhibidos ante el Tribunal: 1) Del Noticiero 24 Horas, entrevista al Secretario de la Presidencia de la República Sebastián Roldán, sobre Julián Assange y aprehensión de Ola Bini en el aeropuerto de Quito; 2) Nota de prensa de Canal 4, sobre Julián Assange y Ola Bini; Solicita reproducir el CD No. 9, marca Maxwell, del informe: en el cual se aprecia a varios agentes policiales que revisan un vehículo; solicita además la exhibición del contenido de un disco duro que contiene varios videos del área de migración en el aeropuerto de Tababela: de la cámara No. C-218: hora 13:40; de la cámara No. C-236, de las horas 12:00 y 14:50; cámara C-237, de las 15:18. **TERCER INFORME:** Realizado con el No. DSP201901688, el mismo que tiene como objeto de la pericia: la extracción de la información contenida en el teléfono celular de marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594; el que se lo pudo desbloquear introduciendo la secuencia numérica observada en los videos que se tenía en la pericia anterior; en cuanto a las características del teléfono modelo MQ7C2ZD/A, chip de la operadora Claro; Fiscalía le dispuso que se ingrese el código, se desbloquea este teléfono celular y se extrae la información, por el volumen de información se la almacena en un dispositivo USB marca Kinston No. 04715-554A00LE, donde consta la información; se almacena además un archivo en PDF con 42.864 páginas, que es el reporte de extracción forense; en sus conclusiones estableció que se recibió varios dispositivos bajo cadena de custodia 1772-19, de los cuales se logró el desbloqueo del teléfono celular I Pone 8, el cual está en buen estado de conservación y funcionamiento, se extrae información mediante el dispositivo de extracción forense UFED, información que por el volumen de la misma, debe ser analizada y se solicita materializar lo que Fiscalía disponga y que tenga relación con el caso investigado; el indicio es devuelto luego de practicada a Criminalística; **al interrogatorio realizado por Fiscalía responde que** en el desarrollo de la audiencia privada donde se aprecia los videos, se dispuso que se ingrese las claves en todos los dispositivos para ver si alguno se desbloquea, en la misma audiencia Fiscalía dispone se proceda con la extracción de la información; se extrajo la información y la audiencia continúa y se exhibe todo el contenido extraído, el resumen de extracción es el que señala que contiene 42.864

páginas; en esta exhibición de la información se dio a conocer a las partes el contenido de lo extraído; UFED (dispositivo de extracción forense) es un dispositivo de la empresa CELEBRY, permite extraer información de varios tipos de dispositivos como celulares, USB o Drones, la forma en que trabaja este equipo es que, una vez conectado, existe el emparejamiento entre el dispositivo y el equipo, el operador del equipo hace extracción de información, del todo o parte, según los requerimientos, aclarando que la información extraída es la que se encuentra dentro del dispositivo; **al conainterrogatorio realizado en defensa de la persona procesada responde que** en cuanto a las precauciones tomadas antes de ingresar la clave: utilizan una caja Faraday, la permite que las ondas electromagnéticas no llegue al dispositivo; luego viene la interacción entre el usuario y el equipo, luego le colocan al dispositivo en modo avión y luego se lo saca de la cámara Faraday; se lo traslada al equipo a un computador para conectarle al dispositivo UFED; esto permite que la red de comunicación de la operadora, no se enlace con el teléfono, la trasmisión de datos es otro tema muy aparte; el modo avión también evita la comunicación del dispositivo con la operadora; en este informe no hay todavía capturas de pantalla; en otra audiencia privada se exhibe el contenido, ante las partes, la defensa del procesado además; en esa continuación de la audiencia, él colocó el informe y se exhibe todo y los sujetos procesales revisan lo sustancial de la extracción, ya que en una audiencia es imposible que se revise todas las páginas; Fiscalía, a petición de la defensa del procesado, dijo que para garantizar la privacidad de la información, solicitaría se materialice únicamente lo pertinente con la investigación, luego se ordenó que se extraiga y materialice una cierta información, dando oportunidad a la defensa para que solicite la materialización de la información que considere necesaria para ellos; posteriormente se remiten a Fiscalía oficios con la información materializada que solicitó; en el informe realizado adjuntó el USB con toda la información obtenida, de lo que conoce Fiscalía habría dispuesto nuevamente que el USB sea ingresado nuevamente al Departamento de Criminalística con la respectiva cadena de custodia; el cambio del idioma en el teléfono celular, cuando se dio?: señala que una vez que el teléfono celular fue desbloqueado, para él como perito es imperioso poder interactuar con el dispositivo de comunicación móvil, en un idioma que sea entendible para él, en este caso su idioma natal es el idioma español, sin que esto represente ningún tipo de alteración de la información digital obrante en el teléfono, ya que el idioma es la forme en que el dispositivo se comunica con el operador; aclara que el teléfono se lo conservó con la clave y solo se realizó la maniobra de la extracción. **OFICIOS QUE REQUIEREN MATERIALIZACIÓN DE LA INFORMACIÓN:** Luego de estos peritaje Fiscalía remitió oficios disponiendo que se realice la materialización de determinadas informaciones, las que consideraron de importancia para su investigación, por lo cual él procedió a cumplir con los requerimientos de Fiscalía, entregando un dispositivo como anexo a su informe, un USB, materializando a pedido de Fiscalía 147 fojas que se refieren a chat y mensajes de una red social, además dijo que solicitó se le conceda una prórroga de 5 días para la entrega además, de unas imágenes requeridas; su pericia se trató solo de la materialización de las imágenes requeridas; **al conainterrogatorio realizado en defensa de la persona procesada responde que** en el oficio que se remitió no se señala la cadena de custodia; en el anexo (**página**) uno de su informe, en cuanto a los participantes se lee: Ola (propietario) * Karina origen TINDER archivo de

cuerpo: chat-115txt; en la siguiente línea se lee: hora de inicio 17/04/2017 09:16:09 (utc-5); siguiente línea de texto: actividad más reciente: 21/04/2017 19:49:02 (utc-5); en cuanto a la palabra Tinder, explica que según su conocimiento es una red social, que el perito no la ha utilizado; que el texto entre Ola y Karina está en otro idioma; en el texto no existe las siglas CNT; se encuentran las letras IP: no se encuentran;

Segunda página: en la primera línea un mensaje entrante, de 24 marzo 2018, interviniente VENGT-AKE VERG; segundo mensaje 24 de marzo saliente Ola Bini, esta página es entre los dos intervinientes; **Tercera página:** primer mensaje del 10 de noviembre del 2011, interviniente DANIEL SPIEWAK, el otro interviniente con mensaje saliente Ola Bini, respuesta 10 de noviembre del 2011; último mensaje de 11 de noviembre del 2011; **siguiente página (cuarta)** mensaje entrante STELLA SANDEL, de 10 de noviembre del 2011; la contestación es de 10 de noviembre del 2011, remite Ola Bini; **siguiente página (cinco)** con mensaje saliente de Ola Bini, dirección entrante STELLA SANDEL; el último mensaje de esa página es de fecha 16 de noviembre 2011; **página seis**, consta el cuadro de participantes: apple@olabini.st más 46735804015, en la siguiente línea aparece EMA BERT; existen 3 mensajes, dos del 19 de diciembre del 2104 y otro del 6 de marzo del 2015;

página 8: cuadro de participantes: 34687491770@s.WathsApp.net; en la siguiente línea dice Adoración Guamán, siguiente línea 593968942120@s.WathsApp.net, siguiente línea Ola Bini (propietario); **página 44:** participantes: dirección entrante 593996783839@s.WathsApp.Net (Cristian Cruz), de fecha 15-09-2017; en el mensaje de 22 de septiembre del 2017: lo envía Cristian Cruz; **en la página 47**, otra conversación con STELLA SANDEL, de fecha 20-06-2018, con esa persona la conversación va desde la foja 3209 hasta la 3291; **página 139** de la pericia: el primer mensaje es de 11-04-2019, mensaje saliente 593968942120@s.WathsApp.Net (Ola Bini), el otro interviniente dirección entrante 593995047749@arobas.WathsApp.Net (Sara), esa conversación tiene 3301 hasta 3306 fecha del último mensaje 11-04-2019; 15:49:58, emite el último mensaje entrante 593995047749@s.WathsApp.Net (Sara), esa conversación tiene 3301 hasta 3306; último mensaje 11-04-2019, a las 15:45:58 (UTC5), **página 147 informe:** primer mensaje de 11 abril del 2019; 15:27:47, envía Leslie Jarrín; respuesta 15:33 Ola Bini; el último mensaje es de 11 abril 2019 15:53 enviado por Ola Bini; Se exhiben ante el Tribunal, las fotografías materializadas constan de fs. 3521 a 3654, aproximadamente 260 fotografías; **al conrainterrogatorio de la defensa del ciudadano procesado responde que a fs. 3638** la imagen que comienza con URL, esta imagen la genera la herramienta UFED. **EN RESPUESTA A OTRO OFICIO:** Materializaciones de otras imágenes: a fs. 33.115 y que se materialice una imagen: Imagen extraída contenida en el informe; ruta de donde se encontraba: la imagen almacenada tiene la siguiente ruta: IPONE/APPLICATIONS/GROUP.NET.WHATSAPP.WHATSAPP.SHARE/MESSAGE/MEDIA/599995404579@WHATSAPP.NET/A/9/A95079D384EDBE1B75A21A558A22383C.JPG; el nombre de la imagen A95079D384EDBE1B75A21A558A22383C.JPG; en la hoja hay dos imágenes de la red social WhatsApp, en la ruta de la imagen, termina con punto y THUMV, los teléfonos y aplicación WhatsApp, generan una imagen residual más pequeña almacenada (miniatura); que el contenido de las imágenes son lo mismo; las fotografías no son las mismas, porque la de miniatura contiene otros metadatos; amplió la imagen y esta dice: [/HOME/OLABINI] (1004) existe un símbolo como una y invertida; a continuación TORSOCKS2 TELNET

181.113.57.169; en la siguiente línea se tiene: [OCT0612:51:56] ERROR TORSOCKS [23473]: UNABLE TO RESOLVE. STATUS REP; en la siguiente línea: TRYING 181.113.57.169...; en la siguiente línea de texto dice: CONNECTED TO 181.113.57.169.; en la siguiente línea del texto tenemos la palabra: ESCAPE CHARACTER IS, una V invertida],.; en la siguiente línea de texto la letra C y varios ***** en toda la línea; en la siguiente línea: EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTÁ PROHIBIDO. En la siguiente línea de texto dice: Usted debe tener permiso explícito para acceder/o; siguiente línea de texto: Configurar este dispositivo. Todas las actividades realizadas; en la siguiente línea dice: son almacenadas. UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBIPET. Siguiendo línea de texto: YOU MUST HAVE EXPLICIT PERMISSION TO ACCESS OR; en la siguiente línea de texto: CONFIGURE THIS DEVICE. ALL ACTIVITIES PERFORMED ON THIS DEVICE; en la siguiente línea dice: ARE LOGGED; en las dos siguientes líneas existen *****; en la siguiente línea del texto: CORPORACIÓN NACIONAL DE TELECOMINICACIONES CNT E.P.; a continuación existe un logotipo de CNT; en la siguiente línea de texto: EL ACCESO O USO NO AUTORIZADO SE CONSIDERA UN ACTO CRIMINAL; en la siguiente línea de texto dice: PETROECUADOR SENAIN INTERNET; a continuación un línea de asteriscos *****; en la siguiente línea dice: USER ACCESS VERIFICATION; en la siguiente línea dice: USER NAME: % USER NAME: TIME OUT EXPIRED ; CONECTION CLOSED BY FOREIGN HOST. [/HOME/OLA BINI] (1005) y un símbolo de una Y invertida. En la parte inferior izquierda de esa imagen está la palabra LENOVO. Señala que el tipo de fotografía es digital, es una captura realizada en una cámara oscura de un parte fija de la realidad; existen las fotografías análoga y digitales; señala que esta captura de la imagen digital, esta captura de una imagen fija, se la realiza con un dispositivo de toma, que puede estar en un teléfono celular o puede estar independiente, a diferencia de la fotografía análoga cuyos ases de luz se plasman en una película, en la digital estos haces de luz se convierten en estímulos eléctricos, los cuales son interpretados por el sensor de las cámaras digitales y procesados como un archivo de mapas de VIT, cada color es procesado por el sensor y se convierten en mapas almacenados en pequeñas cuadrículas, que pasan a ser los pixeles de una fotografía y se puede almacenar en una memoria digital; dice que los archivos THUMBNAILS, que traducido quiere decir miniatura; en nuestros teléfonos celulares se crean esta miniaturas para que cuando la interfaz nos proyecta las fotografías para poder revisarlas, se pueden cargar de una manera más rápida, al ser miniaturas; los metadatos son cierta información que todo archivo digital posee, ejemplificando, se dio la ruta en la página 3.115, los metadatos nos da a conocer en pixeles esta fotografía, y la orientación que tenía la cámara en la captura de la imagen, horizontal (normal); **al contrainterrogatorio realizado en defensa del ciudadano procesado responde que** las imágenes que terminan con la palabra JPG, significan como extensión para almacenar fotografías, así como las propiedades que tiene la fotografía, o extensiones de almacenamiento; que si JPG siempre asociado a fotografía, no lo conoce; un dibujo o foto de JPG si se puede capturar de internet; la aplicación Paing, si hace un dibujo, lo pone como nombre Ola Bini se lo puede guardar en JPJ?: sí; MD5 es o significa una forma de Hass que existen, el que es un código alfanumérico, el MD% conformado por 32 caracteres, que permite a cualquier archivo digital de cualquier extensión, darle una extensión

fija, este código le da una identidad a esta imagen de acuerdo a las propiedades y a cómo está conformada, así como la cantidad de píxeles que tiene; Código MD5 es único para un archivo determinado, no ha visto en su experiencia dos archivos MD5 con el mismo código; podría pasar que exista dos archivos diferentes con el mismo código MD5; explica que un código MD5 se lo puede obtener de varias formas o nombres, como Hash, MD5, SHA; según la doctrina se recomienda para obtener un código Hash, de mayor número de caracteres, varía según la utilizada que se le quiera dar; en los cuadros que materializó, específicamente a las fotografías, se establece que está en una ruta determinada, en la ruta se lee WhatsApp, Share, Mensaje, Media y un número telefónico, ya se hace referencia que si existió una conversación de WhatsApp para esto, para poder identificar esta conversación de WhatsApp, tendremos que remitirnos al informe de extracción, a la parte puntual donde están todos los chats de WhatsApp y tratar de identificar en donde se encuentra este nombre de imagen, para saber si fue un mensaje enviado, recibido, si la imagen fue cargada como archivo adjunto y otras circunstancias; señala, sin estar seguro que la palabra “share”, traducida quiere decir compartido, esto es enviado o recibido; el un número interviniente sale, el otro no; en las fotografías hay una imagen que parece una Piza, que tiene respaldo digital; señala que en el oficio que recibió, se le solicitaba que materialice la imagen estaban en una carpeta, que estaba en el teléfono celular, este archivo específico estaba en la ruta de la aplicación WhatsApp; **15) MARÍA SOLEDAD CASCO RUEDA:** Perito traductora; señala que fue designada para realizar dos traducciones, previo al sorteo realizado por el Consejo de la Judicatura; dijo que la primera traducción se relaciona con conversaciones en varias plataformas de mensajería como WhatsApp o Tinder constantes en un dispositivo móvil; la segunda pericia es una traducción del inglés al español, se la realizó de varios audios contenidos en un CD; recibió la documentación de la Fiscalía General del Estado y entregó el informe el 9 de septiembre del 2019; en sus conclusiones estableció que la traducción es textual de los originales que le entregaron; **al interrogatorio realizado por Fiscalía responde que** ella es tripulante de cabina y perito acreditada al Consejo de la Judicatura desde el año 2016, en traducciones del inglés al español; que en el año 2016 estaba acreditada con el No. 1836169; en cuanto a su capacitación señala que es graduada en EEUU, en el Estado en Montana, donde obtuvo su bachillerato en idiomas; además dice que es traductora registrada en la embajada Británica; en cuanto a su experiencia, señala que desde el año 2016 ha trabajado en asuntos internacionales, ha realizado alrededor de 15 informes; que la documentación a ella entregada, fue documentación incorporada mediante oficio 3019-2019, de 29 de agosto del 2019, por parte del perito Capitán de Policía William Castro Acosta, de la sección de Audio Video y Afines del Departamento de Criminalística, esto referente a la materialización de chat y audios que le entregaron en un CD, según el oficio correspondían a la extracción de la información contenida en un dispositivo móvil I Pone 8; que existían a fojas 33: que la conversación de 22 de junio del 2017, desde las 03:50:13 a las 03:51:44 conversación entre Adoración Guamán y Ola Bini: habla Adoración Guamán: buenos días, ahora conoceré a Assange y estoy feliz, tengo mi presentación esta mañana con él y estoy tratando de escribir algo interesante, también conoceré a Garzón; fs. 34 hasta 15:42:42: Ola Bini: Garzón está en Ecuador?, buena suerte con todo; Adoración Guamán: tengo adjuntos

<http://ciespal.org/event/ii-jornada-de-reflexión-assange-5-años-libertad-negada/>;
adjuntos Assange 5 años de libertad negada <http://ciespal.org/event/ii-jornada-de-reflexión-assange-5-años-de-libertad-negada/d4cep9aa4-be18-41f5-abcd-884232c4b604.thumb>; Adoración Guamán: sigo pensando que decir; Adoración Guamán tengo adjuntos también https://mng.whatsapp.net/b/f/am_3ryoxiuskmdwc02jeh-4rmjoy45ideryppfj3i1y.enc28b7ac55-4a85-43b0-aa79-88cc0367fd3a.gtp; Ola Bini: bien; Ola Bini finalmente estoy en la casa de mis padres, Ola Bini: como estas, Ola Bini: te extraño; ... estoy en Ciespal todo el día, ahora en casa a trabajar un rato; Adoración Guamán: si, también te extraño; Adoración Guamán: y Garzón estuvo ayer en Riobamba con el Mashi?; Ola Bini: que bueno escuchar eso; Ola Bini: y a ok; Ola Bini: escucharlo fue bueno?; Ola Bini: adjuntos, la vista de la casa de mis padres a las 9; (texto ilegible); Adoración Guamán: si estuvo realmente bien; Ola Bini: ok, bueno; Adoración Guamán: se lo que ha estado sucediendo con el tratado vinculante, frente a la gente de cancillería, entonces perfecto; Fs. 40, 15:56.56, del 26 de julio del 2017, hasta las 16:06:12: Ola Bini: usualmente tengo para esta semana reuniones políticas, pero esta vez es demasiado; 15:56:56: hasta las 16:06:12:, fojas 40 y 41 del informe: Ola Bini: podría perder mi visa y posibilidad de hogar en Ecuador en 5 semanas: Ola Bini: y hay algunas otras cosas de las que no puedo hablar; Ola Bini: de cualquier manera; Adoración Guamán; hay; Ola Bini: entonces, extraño Ecuador ahorita; Ola Bini: vivo para estas semana para relaciones políticas pero esta vez es demasiado; fojas 43, conversación de 1 de septiembre del 2017 desde las 14:32:13 hasta las 21:55:13; participantes: Katerine Gim con número telefónico 12178198974 y Ola Bini con número de teléfono 593968942120; Katerine Gim: hola me encanta eso, quien es el pájaro afortunado que financia tu trabajo?, si puedes revelarlo; Katerine Gim: ya has encontrado todo tus compañeros de equipo; Ola Bini: los fondos provienen de un fondo político confiable llamado people soporte foundation; Ola Bini: y tengo un montón de gente que viene conmigo, pero espero encontrar gente nueva; que a fojas 43 de su pericia, sobre la conversación del día 29 de septiembre del 2017 a las 13:41:30 hasta las 13:49:07; Katerine Gin: viste la orden de Trump de recopilar información de todos los inmigrantes en las redes sociales, pensé, Ola tenía mucha razón en irse; Ola Bini: si es loco; **fojas 44 y 45 del informe**, conversación del 15 de septiembre del 2017, desde las 18:38:31 hasta la foja 45, de fecha 26 de octubre del 2017, a las 07:00:44; participantes: Cristian Cruz 593996783839 y Ola Bini 593968942120; Cristian Cruz: pero necesito imaginar una justificación muy fuerte; Cristian Cruz: o podrías intentar darle una visa; Cristian Cruz: lo que significa que recibe dinero; Cristian Cruz: precedente de fuentes nacionales o internaciones; Cristian Cruz: en este caso de la Organización; Cristian Cruz: pero necesita pensar correctamente esta acción; Ola Bini: ah, ya veo, entonces la visa de residencia no es posible?; Ola Bini: no sé a cerca de la visa rentista; Cristian Cruz; podría ser posible si me visitas por favor; Cristian Cruz: para una análisis más sólido de su situación; Ola Bini: sí, seguro, estaría bien el jueves?; Ola Bini: buenos días, cuando debería visitarte; Cristian Cruz: podrías visitarme a las 11:00 hoy? en la Av. 10 de Agosto frente al edificio principal del Ministerio; Cristian Cruz: estamos ubicados en un edificio con ventana verde; Ola Bini: lo siento tengo reuniones hasta la 13h00, sería posible después; Cristian Cruz: sí, puede ser a las 15:00?; Ola Bini: perfecto; Ola Bini: cuál es la dirección, tengo tiempo; Cristian Cruz: nuestra oficina es la

Coordinación Zonal 9, frente al edificio principal; Cristian Cruz: es un edificio de 5 pisos con ventana verde; Cristian Cruz: en la Av. 10 de Agosto, estamos en planta baja, por favor informe que tiene reunión conmigo; Ola Bini: gracias, te veo hoy; Cristian Cruz: perfecto; Ola Bini: hola, espero que te encuentres bien, estoy en el procesado de conseguir empleo en una empresa aquí en el Ecuador, pero los abogados nos dicen que es imposible para mí, obtener una visa de residencia permanente, ya que cambié mi empleo; Ola Bin estoy trabajando con algunos abogados diferentes, que se preguntaban sobre la sugerencia que usted me dio, pueden llamarle para aclarar las cosas, gracias; Cristian Cruz: hola, hoy conocí un abogado enviado para mi oficina para el análisis de su caso; Cristian Cruz: una posibilidad podría ser una solicitud de visa de trabajo con un nuevo empleador; Cristian Cruz: mantendrás un estado de visa temporal por 2 o 3 meses y luego solicitarás el estado permanente; Cristian Cruz: de acuerdo con la regla de los 21 meses; Ola Bini: ah, ya veo gracias, vale la pena intentar; Ola Bini: hola, disculpa, tal vez mal entendí, los abogados que hablaron con usted dicen que no hay firma de hacerlo con un nuevo empleador, estoy muy confundido; Ola Bini: señor; Cristian Cruz: bueno la mejor opción sería una relación laboral con el mismo empleador, que le permitiría solicitar una visa permanente, para que tenga una visa continua de 21 meses; Cristian Cruz: si eso no es posible, puede cambiar a una nueva ración laboral, con un nuevo empleador; eso significa que recibirá una nueva visa de trabajo, mientras tanto solicitaremos nuevas instrucciones, si las personas en situaciones como usted, pueden cambiar permanentemente, incluso si la relación de trabajo actual corresponde a una nueva etapa; Cristian Cruz: una nueva opción puede ser quedarse aquí como turista, significa que, desde el día posterior a la expiración de su visa, debe recibir un permiso de turista por 90 días, que puede extender por otros 90 días, con una tarifa de 125 dólares; fojas 64 del informe, la conversación del día 11 agosto del 2018, a las 08:48:59: participantes: **Estela Sandel con número de teléfono 46760214242 y Ola Bini con número de teléfono 593968942120**: me estás escuchando ahora?; si definitivamente; como lo sabes; he estado del otro lado; cómo se siente; muy normal; fojas 81, 82, 83 del informe: conversación del 23 abril del 2018, a las 09:23:17 hasta el 02 de mayo 2018 a las 18:15:40: participantes: Ola Bini con número 593968942120 y Sonia Alcívar con teléfono 593998722627; Ola Bini: buenos días, esta es Ola Bini, el amigo de Iván Orosa, como estás; Sonia Alcívar: hola querido; Ola Bini: voy a tener todos los documentos listos Z11 A.M. hoy, a qué hora es bueno para venir a las cancillería; Sonia Alcívar: podría ser a eso de las 16:00 por fa; Ola Bini: perfecto; veamos; Sonia Alcívar: te espero; Ola Bini: piensas que necesito adjuntar antecedentes también?; Sonia Alcívar: si los tienes, está bien traerlos; Ola Bini: ok, gracias, estamos en camino finalmente, tuvimos unos problemas, ja ja; Sonia Alcívar: al menos ya se resolvió; Ola Bini: sí; Sonia Alcívar: como te fue en el Sur; Ola Bini: fue muy bien; ahora solo necesitamos esperar, pero solo la terminación; Sonia Alcívar: muy bien, ya le hacemos seguimiento; Ola Bini: muchas, muchas gracias; Ola Bini: hola, recibe un correo sobre mi visa, parece que hay un problema, tienes un i mail?; Sonia Alcívar: hola Ola, mi correo sonialacívar@gotmail.com; Ola Bini: gracias lo he enviado; Sonia Alcívar: no te preocupes aquí hay feriado lunes y martes, el miércoles lo resolvemos; Ola Bini: ah, gracias; Sonia Alcívar: hola Ola, estás en Quito, ya tengo resuelto tu tema; Ola Bini: no puedo estar en Quito este viernes, que pasa?; Sonia

Alcívar: ya tengo tu visa aprobada, cuando vienes; Ola Bini: en serio, uohhh, el lunes; Sonia Alcívar: sí, entonces así lo hacemos, está bien; Ola Bini fantástico, gracias; fojas 100 del peritaje, conversación del 19 de febrero del 2015, a las 11:06:41; **participantes Ola Bini con número 593968942120 y Ricardo Arguello** con número 593995494579; Ola Bini: viste que Lenovo envía una cuenta tercera de temporal a los usuarios de Windows? (carita triste); en la foja 120 de la pericia, la conversación de 6 de octubre del 2015, a las 12:53:17, hasta el 6 de octubre del 2015 a las 16:56:26; entre los mismos participantes Ola Bini y Ricardo Arguello: e x i s t e n a d j u n t o s q u e d i c e n : https://mni611.whatsapp.net/b/aqprufre_crezrzftepbcu3uohpfbzopkegpc8rbfbc8.jpjga95079d384edbe1b75a21a558a22383c.jpj; los adjuntos hasta las 16:49:24: <https://www.hipowold.com/atico/2987529/alfa/insaider-recor.lost-interes-java-htpl>; de Ola Bini para Ricardo Arguello: si lo encontré; Ricardo Arguello: eso tiene que ser un enrutador le preguntaré a mi contacto de CNT; **en la foja 134 de su informe, la conversación de 11 de abril del 2019 desde las 05:36:49, hasta la foja 143 del informe, a las 15:34:19: conversación entre Ola Bini con número 593968942120 y Sara** con teléfono 593995047749; Ola Bini: hay un texto ilegible, ha sido arrestado (carita triste), Sara: mierda; Sara: es horrible; Ola Bini (carita triste), plena cooperación de Ecuador; Sara: viendo las noticias en Ecuador, absolutamente esto es muy muy malo; Ola Bini: sí, me siento bastante deprimido; Sara: tengo miedo de lo que pasará ahora, lo entiendo cariño; Sara: los principales medios ecuatorianos lo justifican diciendo que Ecuador es un país soberano; Ola Bini: sí, por supuesto que lo hacen; Ola Bini: a pesar de que rompe todas las convenciones internaciones; Ola Bini: y es una mierda (cara triste); Ola Bini: ya hay confirmación de que hay una orden de extradición de EEUU, muy malo; Sara: oh mierda, he escuchado declaraciones de diplomáticos que dicen mire a Many, sufrió tortura, no, EEUU no lo va a las timar de ningún manera; Sara: esto es una locura; Ola Bini: oh mi dios, muy estúpido (cara triste); Sara: y esa es la opinión general que se muestra en los principales medios de comunicación; Sara: es tan asqueroso; Ola Bini: sí, (cara triste); Sara: puedo hacer algo por ti, quieres almorzar hoy?; Ola Bini: salgo a las 12 para el aeropuerto; Sara: ya veo, si quieres podría visitarte hasta de ir a la oficina; Ola Bini: gracias, estás bien?, tienes mucho que hacer hoy, supongo; Ola Bini: trata de descansar, lo necesitas; Ola Bini: disculpa, quería decir (cara triste), ah; Sara: ok, viste la conferencia de prensa; Ola Bini: no; Sara: estoy preocupada; Ola Bini: porsiacaso, Robin: +13.29539489, Leslie: +593995827803; Estela: +46760214242; Sara: +593995047749; Sofi +593987172534; Dad: +46706007503; Sara: ok cariño; Ola Bini: tengo adjuntos; Sara: adjuntos; Ola Bini: correcto es lo que estaba tratando de preguntarte; Ola Bini: no creo que haya nadie excepto Yo que consiga, pero quien sabe, adjuntos; Sara: sí, también estoy buscando noticias todo el tiempo; Ola Bini: je je, sí, lo siento; Ola Bini: también varios minutos sigo aquí, adjuntos; Sara: adjuntos; Ola Bini: ok, buena suerte; Sara: adjuntos; Ola Bini: por supuesto; Sara: en la oficina ahora; Ola Bini: ten cuidado; Sara: tú también; Sara: (cara feliz); Ola Bini: 30 minutos, sigo aquí; Sara: bien, bien; Ola Bini: las cosas están bien en la oficina?; Sara: adjuntos; Ola Bini: ok, genial, no hablas ni te preocupas por el Julián; Sara; ahorita estoy en twitter; Ola Bini: sí, ya vi; Sara: cuando llegué a la oficina estaban viendo oficinas de RT, la televisión sigue encendida; Ola Bini: ah, ok; Sara: cómo estás; Ola Bini: adjuntos; Sara: adjuntos; Ola Bini: 30 minutos sigo aquí; Sara; bien, bien, en

camino para allá; Ola Bini: adjuntos; Sara: adjuntos; Ola Bini: 30 minutos sigo aquí; Sara: ok; Sara: pregunta rápida a cerca del seguro privado; Ola Bini: no tengo idea honestamente, para mí o para todas las personas; Sara: necesito nombres completos, relación contigo, porcentaje con el que la persona se beneficiaría; necesito esa información de todos; Ola Bini: lo necesitas ahora?; Malín Yohana Catrín Saldel, el 30% amiga; Dad Gusterson, 35% padre; Ángela Cristina Bini Gusterson 35% madre; Sara: muchas gracias; Ola Bini: en el contexto de hoy, esto se siente muy mórbido de hacer; Sara: lo sé, lo siento mucho, lo necesitaba hacer; Ola Bini: sí, lo sé, no te preocupes; me estoy sintiendo muy raro; Sara: (cara triste); Ola Bini: está bien, 30 minutos sigo bien, yendo al aeropuerto; Sara: te iba a preguntar eso, va bien hasta ahora?; Ola Bini: todavía estoy esperando que me dejen entrar en el área de check in, nada fuera de lo común, hasta ahora; Sara: eso es bueno, estoy feliz; Ola Bini: ahora esperando para hacer el check in; Sara: voy a ver las noticias ahora; Ola Bini: 30 minutos todo bajo control; Sara: bien, bien, nada nuevo hasta aquí; Ola Bini: ok, bien, solo estoy en espera de las noticias; Sara: esperemos que no sean malas, al menos para ti; Ola Bini: sí, las noticias ya son malas; Sara: estoy cruzando los dedos por tí; Ola Bini: ok, acabé con el check in, pasando por seguridad ahora, estaremos en contacto después; Sara: ok, buena suerte; Ola Bini: seguridad listo, ahora inmigración; Sara: todo en orden?; Ola Bini: bien, inmigración listo, horario de 30 minutos comienza de nuevo; Sara: ok; Ola Bini: 30 minutos sigo aquí; Sara: bien, bien; Ola Bini: 30 minutos todo bien; Sara: ok; Sara: estoy almorzando ahora; Ola Bini: espero que tengas un buen almuerzo; Ola Bini: voy a mi puerta ahora; Sara: por favor ten cuidado, buena suerte con todo cariño; Ola Bini: por supuesto, te dejo saber cuándo haya abordado; Sara: muchos abrazos; Ola Bini: abrazos, abrazos; 30 minutos todo bien; Sara: (carita feliz) estoy en la oficina otra vez; Ola Bini: chequeo de equipaje, te dejo saber cuándo haya terminado; Sara ok, buena suerte; Ola Bini: adjuntos; Sara: debo hacer algo; Ola Bini: no todavía, gracias, solo estoy esperando que me llame un abogado; Sara: ok, por favor mantenme al tanto; Sara: cariño mantente fuerte; Ola Bini: gracias; Sara: muchos abrazos; cual es la explicación que te dan?; Ola Bini: nada todavía, digo que quiero un abogado una traducción al inglés para estar seguro; Sara: bien, están contigo ahora?; Ola Bini: están afuera, se ha publicado mi nombre?; **de fojas 145 del informe, la conversación desde el 11 abril del 2019 a las 08:11:38, hasta la foja 147 de la pericia a las 15:53:52; participantes: Ola Bini con número 593968942120 y Leslie Jarrín, con número de teléfono 593995827803;** Ola Bini: buenos días, hay noticias acerca de Julián (cara triste), entonces esto; Ola Bini: adjuntos; Ola Bini: no estoy ciento por ciento seguro que estén hablando de mí, algunos detalles no concuerdan, pero no es imposible; Leslie Jarrín: (ilegible) estamos .. no estoy segura de que sea la expresión correcta; Ola Bini: sí, tampoco me gusta, pero quien sabe; Leslie Jarrín: hablaste con Jasón por si acaso; Ola Bini: no, voy a esperar y ver; por si acaso Roy: +13129539489, Leslie: +593995827803, Estela: +46760214242, Sara: +59399547749; Sofi: +593987172534; Dad: +46706007503; Ola Bini: en realidad los llamaremos; Leslie Jarrín: estás en Japón?; Ola Bini: estoy viajando esta tarde; por favor llama cuando tengas un segundo; Ola Bini: pasando inmigración y seguridad ahora, no hay problemas hasta ahora; Leslie Jarrín: disfruta de Japón, espero poder ir algún día; Ola Bini: gracias, gracias; Leslie Jarrín: adjuntos; Pablo Encalada, teléfono +593991805859; Ola Bini: hablé con él, no

estoy seguro si él enviará a alguien o puede venir; Leslie Jarrín: lo sabré en 5 minutos; Ola Bini: gracias, estoy un poco asustado, me quieren quitar el teléfono, necesito ayuda en el aeropuerto; Leslie Jarrín: ilegible; Ola Bini: no sé si él me puede ayudar; Leslie Jarrín: sí, acabo de hablar con David Ochoa, él o su compañero están yendo; te confirmo en un segundo; Ola Bini: no van a permitir más textos, solo pueden llamarme los abogados, mensaje final: **SEGUNDO INFORME:** al igual que en la primera traducción, afirma que no omitió palabra alguna de los audios entregados; le entregaron documentación incorporada al oficio antes mencionado, de fecha 29 de agosto del 2019, suscrito por el Capitán William Castro Acosta, del Laboratorio de Criminalística, referente a la materialización de chat y audios que le entregaron en un CD, el que, según el oficio corresponde a la extracción de la información del dispositivo marca Apple, modelo iPhone 8; contenido total de la traducción de audios: 1) audio: 2f52a366-6577-4083-957e-6eafb5d92f69: ok, es una restricción temporal de movimiento de hasta 8 horas en el aeropuerto, ah el abogado enviará a alguien; 2) audio: 3da6f3f7-55f5-41e1-a1b6-310343429acf: hey, me alegro de que ya lo tengas, eso es algo importante en caso de que ocurra algo y no te preocupes, ya sabes, siempre te he dicho que si puedo hacer algo por ti, házmelo saber, es mi deber como amiga, así que no te preocupes, ah bueno, por supuesto que vamos a estar en contacto, ahora estamos, Yo estoy yendo a la oficina, así que espero que las cosas vayan bien; 3) audio: 5aaf847-7001-40aa-bb23-44946827def4: hey hey, perdón por no decir adiós correctamente, ah, pero Leslie me decía que está obteniendo la información del abogado, así que lo tendré cuando llegue al aeropuerto al menos, así que en caso de que ocurra algo, tengo un abogado al que puedes llamar, de cualquier forma y gracias de nuevo querida, realmente lo aprecio; 4) audio: 8fc75c28-8c27-45d0-86c9-29aa189e4a4: ok, acabo de llamar a Leslie, me están llevando lejos y no se me permitirá viajar, Leslie se pondrá en contacto del abogado, no estoy detenido, pero no tengo permitido salir del aeropuerto, eso es todo lo que sé ahora; 5) audio: 8fc75c28-8c27-45d0-8c69-29aa1894e4a4: ok, acabo de llamar a Leslie, me están llevando lejos y no se me permitirá viajar, Leslie se pondrá en contacto con el abogado de inmediato, no estoy detenido, pero no tengo permitido salir del aeropuerto, eso es todo lo que sé ahora; 6) audio: 10e0f420-2359-44e6-b9bb-37994347fb94: voy de camino a la oficina, solo necesitaba recoger algunas baterías, marcadores y unas facturas, así que en este momento estoy caminando hasta la oficina y por favor, por favor mantenme actualizada; 7) audio: 35afd77d-f7cc-4enter44-9a63-13460c08e7a6: en realidad he estado planeando hacer eso, quiero decir que no necesitamos asustar a nadie ni hacer que esto sea más grande; 8) audio: 57dcp485e-7847-49cd-949c-513c97dea2d: ahora estoy en soporte libre porque Clara me pidió que recogiera algunas cosas que tuviera Gino, así que sí; 9) audio: 92a97dca-9139-4af8-8741-c98f51caa3de: estaba leyendo nuevamente el artículo, habla de 4 personas, los dos rusos, el miembro de Wikileaks y la persona cercana a Julián, así que son cuatro, no tres, así que es algo en tener en cuenta; 10) audio: 981bcc6-d037-4135-8757-17dae5dd949e: hola Ola, así que hay un nuevo artículo en el Universo, aclara eso o tal vez no sé si en la conferencia de prensa, se dijo esto claramente, pero aclara que los hacker rusos estaban viajando con Patiño y de que se trataban estas preocupaciones, las afirmaciones es que los dos hacker rusos estaban trabajando en estrecha colaboración con Patiño, por lo que puedo decir las cosas sobre el miembro de Wikileaks no estaban asociadas con los países o con

Patiño, están separadas de eso, así que tal vez eso explique algo de la confusión sobre las cosas; 11) audio: 4473y0da-4a37-4ed1-ab63-673c71f7f0cd: hablé con Leslie, en este momento aparentemente ella está tratando de encontrar un abogado que pueda ir para ayudarte en este momento, si no puede encontrar a la persona que está buscando, ahora va a hablar con David, así que sí; 12) audio: a094f7b9-aa30-4f10-a3b0-6fb3a28771a1: poco claro?, es demasiado bueno, olvidé algo cuando estuviste aquí, lo siento mucho, me pregunto si puedes venir antes de las doce, me doy cuenta de que si algo sucediera tengo una copia extra de mi llave y la tarjeta de acceso para ingresar al edificio y podría ser una buena idea de que alguien tenga eso, en caso de que ocurra algo, por lo que sería genial si pudieras venir antes de doce y diez, en menos de una hora le recogemos, lo siento pero creo que sería una buena idea, verdad?; 13) audio: a5618677-a0e4-4848-a8a2-95061e5933d0: lo bueno de esto podría ser, que no estaba claro que si la Ministra del Interior transmitiría la información de todas esta gente a la Fiscalía, o si se trataba principalmente de los hacker rusos, es posible que solo se trate de los hackers rusos; 14) audio: ce35cdd0-a69f-4605-93a9-ba659a6daead: se me olvidó pedirte algo, si alguien en la oficina pregunta por mí en relación con el comunicado de prensa o en relación con Julián, por favor niega que tengo conocimiento, haz que alguien más y trata, intenta que la gente entienda que no tengo ninguna conexión, la mayoría de las personas en la oficina no sabe que le visité a Julián, así que es mejor que no lo hagan, no sé si eso está bien, lo siento pero creo que es mejor no preocupar a la gente, solo deberían asumir que soy una persona normal; 15) audio: cea163dd-1ec-4dc6-a187-2fb9d2515374: en este momento estamos planeando como hacer, necesitamos tener estas contestaciones a cerca de contabilidad, con la persona del seguro, también necesitamos una evaluación para el maestro de inglés, así que estábamos planeando todo eso, y en este momento los chicos están planeando cuando hacer, como sabes vamos a comprar las nuevas computadoras mañana, así que están planeando cuando instalar todas las cosas que necesiten instalar, así que están trabajando en eso ahora mismo; 16) audio: ba61ef3d-f4cd-4c7f-88b0-df32c9402eb9: por supuesto, no te preocupes, puedo estar ahí pronto, me alegra que me lo hayas dicho, así que debería estar ahí pronto; 17) audio: ebc06fb-1d7f-4d4e-8c17-abc710526f31: sobre eso entonces sí, cuando vi el comunicado de prensa ella estaba hablando de los rusos, dijo que no permitiremos que este tipo de actividades se cometan en Ecuador y también tenemos la información sobre estas otras dos personas, ella pidió los detalles y dijo que en las próximas horas les darían toda la información que tenía a Fiscalía para que tomaran todas las medidas; **al conainterrogatorio realizado en defensa de la persona procesada responde que** en relación a la segunda pericia, el audio que le entregaron estaba en idioma inglés y ella en su informe tiene inglés y español; que en los antecedente de la pericia, si hace constar el oficio de 29 de agosto del 2019, ese oficio estaba adjunto al informe; en el informe solo está específicamente la traducción, cuando le dispusieron la pericia estaba adjunto el oficio; si vio el oficio del 29 de agosto, ahí no se hace mención a la entrega de un CD con audios, se refiere a la información contenida en las 147 hojas del documento traducido; a parte de las 147 hojas no hace mención a los audios; de los audios no podía ella saber, quienes eran los intervinientes, ella solo tradujo la conversación; en su informe no constan las fechas de esos audios; al entregar el informe le ponen una fecha de entrega y una firma de

respaldo; la pericia la practicó una semana antes de la entrega del informe, ya que el sorteo fue realizado el 30 de agosto del 2019 y lo entregó el 9 de septiembre, en el informe solo consta la fecha de entrega, los días específicos en que realizó la traducción no constan en el informe; en cuanto a la segunda pericia, en la primera hoja de traducción los participantes son Ola Bini y Karina, la conversación comienza el 17-04-2017, la conversación se da en la aplicación Tinder, ella entiende que es una aplicación par conversaciones, pero no sabe más; los primeros 5 mensajes son: hola, encantado de conocerte, no estoy seguro de qué decir en un primer mensaje como este, leer tui perfil me hizo sentir curiosidad, de qué manera eres horrible (carita feliz); Karina; hola, encantada de conocerte también, ja ja ja, tómalo con calma, es una broma; Ola: ja ja ja, entonces no lo eres, bueno saber; Ola: eres de Quito originalmente?; que la primera hoja de la conversación de Ola Bini con Adoración Guamán está en la hoja 8 del informe, de fecha de inicio es el 10 de junio del 2017, la conversación va hasta la foja 41 de su informe; que en la foja 43 de su informe está la conversación con Katerin Gim es de fecha 01-09-2017, hasta el 28-09-2017; que en la foja 44 del informe están las conversaciones con Cristian Cruz de fecha de inicio 15-09-2017; que en la página 100 de la pericia, constan las conversaciones con un señor Ricardo Arguello, de fecha octubre del 2015, en la página 120: del 6 de octubre del 2015, de los mensajes que le hicieron leer la hora es: 12:56:26, otro a las 16:48:21, otro 16:48:49 y otro último a las 16:49:24; luego de esos mensajes hay otro mensaje que dice: es el camino para que Google escape de su desastre dejado; siguiente mensaje dice: no creo, creo que Google lanzará otro idioma bifurcado de ...; el 6 de octubre del 2015 no hay más mensajes; ese día 6 de octubre a las 12:44:33 hay un mensaje que dice: hey, de que falta de jabas hablas; previo a ese mensaje hay otro del 6 de octubre del 2015 que dice: hay un sitio (cara feliz), hay un pequeño panel que sale un ícono en la esquina superior izquierda que dice: queda deshabilitado porque lo odio, realmente no puedo descifrar como se llama; el mensaje de 5 de octubre del 2015, desde las 08:32:22, desde la dirección de Ola Bina para Ricardo Arguello: el mensaje es tuiteado a ti; siguiente mensaje que envía Ola Bini a Ricardo Arguello dice: ¡hey!, eres bueno en no?; siguiente mensaje de Ricardo Arguello: no realmente, que quieres hacer; siguiente mensaje de Ola Bini para Ricardo Arguello: algo simple (cara feliz); en la foja 134-144 de la pericia hay conversaciones con Sara: el último mensaje de la conversación es de fecha 11 abril 2019, a las 15:34:19: el último mensaje de la conversación es del 11 de abril del 2019, a las 15:49:58, envía el mensaje Sara: Leslie está tratando de conseguir al abogado, si ella no puede hablar con él, hablará con David, nuestro abogado; a fojas 147 del informe, el último mensaje (no van a permitir más textos, solo pueden llamarme los abogados, mensaje final), es de 11 de abril del 2019, a las 15:53:52, lo envía Ola Bini; **16) GERER ANOUCHKA:** de nacionalidad suiza, perito traductora; señala que Fiscalía le solicitó para realizar una traducción del inglés al español, le entregaron los documentos por parte de Fiscalía el 20 de agosto del 2019, entregó la pericia el 30 de agosto del 2019, documentos que consistieron en 26 fojas a traducción del inglés al español; señala que eran dos documentos, una apostilla con un certificado laboral, y la segunda parte fueron unos chats que había que traducir del inglés al español; **al interrogatorio realizado por Fiscalía responde que** es traductora jurídica, acreditada desde el año 2015 al Consejo de la Judicatura; recibió un correo de Fiscalía que había sorteada y designada como perito; luego del sorteo

de perito, se pusieron en contacto con ella para entregarle los documentos; en cuanto a la PRIMERA pericia: traducción de una certificación laboral: era una apostilla de los EEUU, a fs. 2245, el texto dice: esto sirve para verificar que el documento anexo es una auténtica carta de verificación de empleo, relativa a las operaciones de Top Words, firma ilegible, nombre Magi Varucci, título administradora legal, Estado de Illinois, este instrumento fue reconocido ante mí, el 19 de junio del 2019, por Magi Varucci, firma ilegible y constan unos sellos; en la fs. 2246 es un certificado de Top Word, con fecha 26 septiembre del 2019, que indica: a quien corresponda: Esta carta sirve para verificar que el señor Ola Bini fue empleado por Top Word, como el desarrollador principal desde el 10 de febrero del 2010 hasta el 30 de septiembre del 2016, el señor Bini fue asignado para trabajar a Ecuador desde el 11 de noviembre del 2013 hasta su último día de empleo hasta el 30 de septiembre del 2017, su sueldo anual fue de USD 220.000,00, durante su empleo su salario pagado por Top Word, con depósito directo a su cuenta bancaria en Estados Unidos, atentamente firma ilegible, Jeremy Gordon, Consejero Asociado General y Vicepresidente de Top Word; señala que en el SEGUNDO paquete de documentos que constan de 23 fojas, desde la fs. 2549, como lo introduce el documento el FBI ha acompañado con éxito un archivo que contiene registros relacionados a chats entre Ola Bini y otras personas a menudo no identificadas, que los chat son de una plataforma conocida como Llave, que permite a los usuarios intercambiar informaciones cifradas similares a los mensajes de texto; que los chats comienzan en el mes de octubre del 2013 y continúan hasta el 17 de julio del 2015; que los errores de ortografía, gramática y puntuación son los que están en los mensajes de texto originales; las fechas e identidad de los comunicantes son evaluaciones hechas por el Departamento de Justicia; que los 4 primeros párrafos dicen: con fecha 11 de oct 2013, una persona con iniciales JZ, quien creen que es Jeremy Sinelman escribió: estaba en la embajada, aparentemente hiciste una buena impresión; Bini respondió: oh me alegro de oír; la conversación continuó de la siguiente manera: la pasaste bien en la embajada?; sí, pero nuevo embajador nuevos reyes, los invitados se van a las 12; que hacker tan antipático; ah eso apesta; 2) es media tarde del hackers, sobre la hora del té; Usmael: exactamente, vimos la primera conferencia de Evan Mouven mientras comimos libanés y bebimos wiski; ah eso suena increíble, iba a traer una cocina de arte, la próxima vez; **traducción de la foja 2**, chat de 6 de noviembre del 2013: Ola Bini: como te va pase muchas horas con abogados de hoy y fundamentalmente lo más importante que descubrí, es que es importante que el contrato sea conmigo como persona y no con Top Word; pero a excepción de eso todo parece estar bien, estoy listo para empezar tan pronto como podamos; buenas noticias, solo tengo que descubrir todo de mi parte, especialmente con la nueva empresa, pero suena genial, fantástico; me avisas si hay algo que pueda hacer algo para acelerar el proceso, y por su puesto mis abogado tendrán que ver el contrato, pero estoy mentalizado y listo cuando sea; también mi mudanza a Ecuador será la próxima semana; así que después de eso las cosas serán mucho más simples; como va todo con la nueva empresa?; todo está avanzando bien, tiene alguna idea del marco de tiempo calculado de las cosas?, con la resolución de contratos etc.; fs 2: chat del 26 de noviembre del 2013: Bini y Mouven se enviaron mensajes: cómo va todo?, hoye cómo estás; estoy bien, estableciéndome en Ecuador, estamos organizando una conferencia interesante la próxima semana aquí en Quito; cómo

estás?; parece una interesante agrupación de personas; sí con suerte; no he visto a Roy en mucho tiempo, así que será una buena oportunidad para ponerse al día; va todo bien con la nueva empresa?; así que desafortunadamente aún no tengo ninguna actualización para ti, todavía estamos tratando de descifrar, con documentos que ya están trabajando para nuestra organización de noticias; esta noche se va a publicar una gran historia explosiva, no puedo esperar, pero aún no hemos resuelto los problemas de trabajar con personas externas, pero estoy tan ansioso, emocionado de hacerlo; ok, espero el nuevo lanzamiento; estoy triste no hay actualizaciones pero entiendo que es difícil, lo siento por molestarte repetidamente al respecto; no hay problema me alegra que estés emocionado; lo lograrás con seguridad, es solo cuestión de tiempo; todo está muy sensible, especialmente para los nuevos abogados que se ocupan de esto por primera vez; va haber una salida que aún no existe; por supuesto, lo entiendo completamente; hay algo que pueda hacer de mi lado para ayudar, o está completamente de tu lado; completamente de mi lado; está definitivamente en la lista, siendo procesado, ok; **traducción Fs. 3, chat de 12 de diciembre del 2013:** envían mensajes OB: alguna noticia?; GG: hola, nada todavía, sé que es lento pero todavía no hemos llegado al punto de la discusión sobre trabajar con personas externas con contratos, pero lo haremos; cómo estás; GG: estoy bien, como está Ecuador; OB: buen trabajo en las reanudaciones de Suecia; Ecuador es muy bueno, es bastante emocionante; GG: así, de gustan las cosas de Suecia?; GG: Ecuador es interesante?, quiero ir ahí; OB: logramos derogar un artículo insidioso en un nuevo Código Penal, que habrían hecho las cosas realmente malas aquí y, realmente es así y estamos recibiendo mucha consideración de los políticos locales; sería fantástico sacarlo lo más pronto, hay una ola de indignación en este momento y el gobierno está tratando de implementar planes para hacer algo al respecto y nos han pedido ayuda; GG: lo intentaré, es difícil, tengo la presión de todos para hacer todos los países, pero puedo intentarlo; **Fs. 4, del 11 de febrero del 2014:** FR: Dios, estoy ansioso que nos veamos, aunque te pueda parecer frustrante, las preguntas que hago; OB: no te preocupes, también tenemos algunos días, no tengo realmente nada planeado para Londres, excepto visitar a ¿??, tengo algunas cosas e ideas, desde Hamburgo, el 21 tomaré el tren de regreso a Berlín con Mitri, y veré a Assange; OB: Ah, genial; estoy en Hamburgo el 21 y tomo el tren a Berlín el 22, pasaré tiempo con Mitri y Sara; FR: oh, bien; **segundo chat del 11 de febrero del 2014:** OB: mientras tanto las cosas se están calentando aquí en Ecuador, algunas cosas están pasando que no puedo decir aquí; FR: y en Brasil, te acabo de mandar una pequeña conversación sobre centros de datos y estados que ejercen soberanía; OB: sí; FR: hoy nos encontramos con un montón de buenos expertos tecnológicos; OB: he estado pensando en eso, es complicado; FR: cené con el chico de la fiesta OB; ah, chévere; FR: tiene muchas ganas de unirse a ¿??; él es un codificador en su trabajo y muy interesado; **traducción de la fs. 5, de 5 de marzo del 2014:** OB: estamos obteniendo cada vez más confianza del gobierno local, por cierto; FR: genial, fantástico; OB: tanto el Senescyt como el departamento de asuntos exteriores; FR: ted cool; OB: no hacer daño que somos amigos de JA, por supuesto; FR: sí; OB: creo que también hemos construido buenas relaciones fuera de eso, tendrás que venir y hablar con ellos en algún momento; FR: y probablemente necesite amigos después de comentar varios pesados sobre el ex embajador; OB: dado tu historial sospecho que tu consejo sería cien veces más

valioso que el nuestro en muchas circunstancias; OB: sí; FR: me encantaría; OB: por cierto, parece que uno de nuestros amigos irá al Ministerio de Asuntos Exteriores, formará parte de la red mundial; **traducción de fs. 5 y 6, de fecha 13 de marzo del 2014:** OB: como te fue en el marco civil; FR: joder; OB: por cierto avísame si Magy o Roy responden; FR: debo tratar, será la próxima semana, así tenemos otra semana, lo que es bueno, porque nuestra carta a los parlamentarios, que escribí el 27 de febrero, estaba lista una hora antes de que se programara el debate; FR: así que definitivamente no fue un desperdicio; OB: ok, bueno; FR: tenemos un comunicado de prensa, una carta y algunos planes; OB: genial; FR: se nos ha pedido que nos centremos en los partidos de derecha con los argumentos del caso del negocio, y trabajaremos en los ¿?? Y los ¿??, aquí están cada vez más comprometidos y Rafael es maravilloso, realmente disfruto trabajar con él; las ONG con las que estamos pasando aceptan, fue muy frustrante para mí, porque nos quedamos por tanto tiempo sin hacer nada y luego ocurrió una presión muy ad hoc, pero estuve envuelto en temas de procedimiento y también en el hecho de que ha habido una crisis dentro de la alianza del gobierno, uno de los partidos ha comenzado a exigir, él ya no tiene los números ¿??, así que esto es realmente una crisis; OB: sí, Ecuador está también un poco fluctuante, el presidente está haciendo cambios en el gabinete y realmente no sabemos qué pasará con eso; FR: me gustaría que cambiara algunos embajadores; OB: con Iván del Ministerio de Asuntos Exteriores tuvimos una conversación, realmente están tratando de arreglar la situación, pero es difícil; **traducción de Fs. 6, del 4 y 16 de abril del 2014:** FR: Julián recibió el mapa que le envié y le encanta tanto que lo está enmarcando, presente exitoso; está confirmado para el último panel, quería que tratara de ponerlo en el grupo de ¿??; Kimi respondió grandes cosas; **16 abril del 2014:** OB: acabo de hablar con el australiano; FR: oh bien; espero que este bien lo extraño; OB: sí, pero aparentemente no hay muchos cambios con el embajador; FR: maldita sea, voy a pedirle al embajador que envíe una carta solicitando un trato especial, para que podamos quedarnos más tarde y beber wiski; OB: genial; **traducción de fs. 7 y 8, de 18 de noviembre 2014** F, Rubí y Bini, se enviaron mensajes: OB: el ex ministro de defensa del Ecuador, que aparentemente es una buena persona, es el nuevo embajador de la ONU en Ginebra; OB: deberían ponerlos a los dos juntos; FR: oh, bien; OB: sí, se lo diré gracias; FR: sí; OB pensé que te gustaría; FR: sí, es una noticia increíblemente buena; permíteme compartir contigo mi último trabajo para los Wikileaks, niños mal humorados con los que todavía no estoy hablando porque estoy en huelga por su nieto; OB: enviaré un correo electrónico a Iván pidiéndole que lo haga; FR: Ecuador y posibilidades; OB: seguro; FR: sí, eso sería genial, me preocupo por el Iván; OB: está mucho mejor, logramos podernos al día; ha podido despegar totalmente el tema de Chevron, por lo que tiene mucho más tiempo para hacer estrategia, el único problema es que el ministro Luano y que está haciendo un trabajo fantástico para él, convirtiéndose en el asesor más confiable de los ministros; FR: es una bendición muy contradictoria, tengo que irme; OB: sí, cuídate; **traducción de fs. 13 y 14: de 13 de marzo del 2014:** SH: entonces la persona que necesitábamos para esa cosa está de vuelta; OB: debe haber sido un mal momento, ok; SH: hablaremos con ellos mañana, el fin de semana y podemos comenzar la próxima semana; OB: fantástico; SH: bueno, en otra nota estoy molestando otra vez, si no te importa que te pregunte algo; OB: no estoy seguro lo que significa molestar, pero sigue adelante y

pregunta; SH: entiendo que estoy en peligro por abusar de tu generosidad, ah es una palabra del rey Niro, similar a mendigar, es decir ir por ahí pidiendo cosas; OB: ajá, ya veo, adelante; SH: entonces eso podría no ser posible, pero nos preguntamos si ustedes podrían participar, supongo que necesitaría verificar esto, así que no espero una respuesta ahora, así que mantenemos muy en secreto a nuestra gente de tecnología, por razones obvias y hacer todo lo posible para hacerlo, y esta solicitud se refiere a una de estas cosas, queremos una nueva persona que hayamos identificado, el problema es siempre el rastro y las cubiertas bancarias, entonces la solicitud es la siguiente: cuales son los intercambios de su organización para conseguir un nuevo empleado, pero para que trabaje para nosotros y obviamente después podemos ver las formas en que pagamos, por ejemplo te contratamos para el diseño de la página o algo así; OB: ok, intentaré investigar y si es posible para nosotros hacerlo, el peligro es que puede parecer lavado de dinero, mientras que en realizada es lavado de información; SH: sí, entiendo; OB: pero preguntaré por ahí y veremos cualquier posibilidad, sería genial; **traducción de la fs. 16, chat del 13 marzo del 2014** Bini envía un mensaje a una persona no identificada con el apodo Crin PBS: OB: este es el correcto; G: ok, aquí estoy; OB: nuestros amigos tienen un problema que es ocultar a sus técnicos, rastros bancarios, etc., entonces han encontrado una nueva persona que quieren, pero nos preguntamos si podríamos contratarlo potencialmente, mientras trabaja para ellos y podemos obtener dineros de forma indirecta, trabajo por contrato o lo que sea para ocultar rastro, ahora no sé a qué tipo de persona preguntar primero, si es Roy o alguien más y lo que me preocupa principalmente es que se parecería a lavado de dinero; G: porque lo sería?, similar a lo que dijiste antes de Smar; **traducción de las fs. 17 y 18, chat de 14 febrero 2014:** Bini envió mensajes a una persona cuyo verdadero nombre parece ser Cris Bor: OB: pero tenemos una escases de personas con experiencia, que pueda formar aquí; TF: aquí el problema parece más de personas con experiencia que guían proyectos; OB: básicamente somos Rebeca Siter y Yo y no puedo hacerlo en más del 10% de mi tiempo; CS: sí, me doy cuenta de que probablemente estés en demás, han conversado los ecuatorianos con otras nuevas personas de oficina?; OB: y es probable que ganemos un proyecto realmente bueno que empezaría en abril o mayo y en ese momento no tenemos idea de cómo dotarlo de personal; parece que la situación aquí podría ser útil; OB sí, estamos bastante en contacto con las oficinas de África y Brasil; CS: bien; OB: también hemos sido un poco desafortunados teniendo gente que viniera por alguna semana, lo cual es muy recomendable, pero terminó no siendo muy útil; CS: tienes una ventaja, Ecuador está más de moda en la presan internacional en este momento; OB: ja ja, cierto; CS, ah, eso apesta; OB: aunque eso cambiaría, hay guerra fría entre EEUU y Ecuador; CS: sí, estás a punto de revolver un poco de nieve; OB: y se calentará pronto, sospecho, j aja no soy buen chico, nunca haría algo así; CS: si tu país retiraría la solicitud de extradición, solicitaría y calmaría las cosas?; OB: no, realmente, aunque en realidad haría al mundo menos complicado; el mayor problema para Ecuador y Estados Unidos es en realidad Chevrón: **traducción de fs. 19 y 20, chat de 10 de octubre del 2013:** Bini envía mensaje a una persona cuya identidad es desconocida, hasta para el Departamento de Justicia; UI: mientras tanto, malas leyes y prácticas en todo lugar, incluso Ecuador a punto de aprobar una disposición de represión de datos, malo, malo, malo; OB: sí, parece que podríamos ayudar al gobierno ecuatoriano con

seguridad, ver cómo se desarrolla y obtuve mi visa ecuatoriana de todos modos, desearía que tuvieras alguna noticia que pudieras animar; UI: bueno Ecuador aprenderá bien o mal que romper la privacidad no es bueno, entre nos, estaban planeando comprar software para ingresar a las computadoras el año pasado, que los detuvo; **traducción de fs. 21, 22, y 23, del chat de 24 octubre del 2013:** Bini envió un mensaje Diane, cuyo verdadero nombre puede ser Diane Bareto y que puede ser un empleado de Sor Word: D: hola, hola, espero que estés bien, me preguntaba cómo va Ecuador, quería que Andy fuera a echar un vistazo, Mitri es muy escéptico, no presione aquí, sobre todo el asunto aquí, tal vez haya un poco de documentación a fines de noviembre cuando llegue Mitri, vayan ahí, con quien debo hablar según su opinión'; OB: hola, Ecuador se acerca, me mudaré a mediados de noviembre; D: genial, que pasa con la reforma del Código Penal en la que uno tiene que registrar la actividad en línea de los vecinos para evadir la responsabilidad, de todos modos odio ser tan audaz, tuviste la amabilidad de mencionar que podrías hablar algo por mí, creo que es una gran historia y en Europa, qué está sucediendo ahí, alguno de los mejores pensadores van a Ecuador para trazar una nueva utopía y nadie se entera de esto?; OB: sí, no estoy contento con la aprobación de parte de la legislación, es bastante mala; **traducción de fs. 22, chat de 28 de febrero del 2014:** Bini envió mensajes a Martin Pauler, de Sor Word: OB: puedes ayudarme con algo?; NF: seguro, 25 ventana equivocada, perdón por los 25; OB: puedes ejecutar ¿???????? en la consola y luego hacer ¿???????? y enviarme esos dos resultados, seguro, dame un segundo, quieres que lo canalice a un archivo y les envíe?; OB: seguro gracias; NF: bien, en eso; OB: gracias; NF: de nada, ¿?? parece inalcanzable, pasa por el primer salto y luego nada, 110.71.23.254 (10.71.23.254) 3.276MS2.745MS3.047MS 234 hasta ahora; OB: interesante; me costó mucho mapear las redes de Ecuador; NF: lo mimos, llego al primer salto que creo es nuestro enrutador y luego nada; OB: mmm, extraño, por lo que nuestra red en la oficina está haciendo cosas estúpidas; NF: puedes bloquear las rutas de rastreo de nuestro enrutador? OB: sí; NF: entonces tal vez eso es lo que hicieron; OB: es solo una simple cuestión de bloquearlos los tipos correctos de paquetes UDP, no sé porque harían eso, pero Ecuador también ha bloqueado a un montón desde afuera; NF: raro; OB: sí; gracias de todos modos; **traducción de fs. 23 acápite: las preocupaciones de BINI por viajar, de 18 noviembre del 2013** Bini le preguntó a Martín Flourer hablaste con Leslie sobre Roy más Korea; Foulter respondió aún no; las preocupaciones de Bini sobre viajar; alrededor del 30 de octubre del 2014 Bini entabló un intercambio con una persona no identificada y declaró que Quito es fantástico, pero extraño mucho Chicago, es una mierda no poder volver, cuando se le preguntó si planeaba regresar a los EE.UU. Bini opinó: no te lo dije, no puedo arriesgarme a pasar la frontera de EE.UU., uno, es un poco demasiado represivo, además afirmó que era algo casi permanente, a menos que el gobierno de EE.UU. cambie de manera significativa, dejando caer muchas acusaciones, lo trato como permanente, lo cual es bastante molesto; alrededor del 19 de marzo del 2015, hizo declaraciones similares sobre Australia con una persona no identificada; OB: decidí hace un tiempo, que ya no puedo arriesgarme a ir a Australia, es solo el segundo país después de EE.UU., por lo cual tomé esa decisión, aunque ayer comencé a pensar lo mismo sobre Canadá; UI; que riesgo ves aquí, incluyendo a los EE.UU. pero no sucede en mucho aquí, el gobierno es una mierda, incompetente y las

personas son demasiado relajadas para implementar gran parte de cono sur; OB: ah, tal vez no te he hablado de esto; UI: no; OB: tengo miedo de algunas cosas diferentes, supongo que no hemos hablado en mucho tiempo, trabajo con amigo donde no podría responder sinceramente preguntas en las fronteras y tengo algunas cosas en mi computadora que no podía dejar caer en las manos equivocadas; **al conainterrogatorio realizado en defensa de la persona procesada responde que** el primero documento que tradujo de Top Words, inicia: a quien corresponda, al final luego del atentamente había una firma ilegible, el autor del documento es Jeremy Gordon; en el segundo documento, este es una apostilla: firmado por Jese Wait, también se dice firma ilegible; el tercer documento dice que el FBI ha descifrado con éxito y sigue un párrafo, al final del documento (fs. 23) no hay firma alguna ni ningún nombre; en la parte inicial del documento no se hace mención de una orden de Juez; había un oficio de la Fiscalía, no había oficio de un Juez; en la página 23 del informe: las preocupaciones de Bini por viajar, no consta quien lo dice; página 23 las siglas OB y UI, no hay algún documento que explique quién es OB no se identifica a persona en concreto; este documento no tenía sellos; la apostilla era parte de los documentos a traducir, al igual que los chats; la apostilla en su antepenúltima línea: certifica la firma y sello, no el contenido del documento, no es válida dentro de los EEUU; el documento está firmando por Wagner, Notario Público de Queens, con sello de ILLINOIS; el documento del FBI no tenía el sello de Notario Público; **17) GALO DAVID CÁRDENAS CALDERÓN:** Ingeniero en electrónica y telecomunicaciones y perito acreditado al Consejo de la Judicatura; señala que el objeto de la pericia era un análisis integral y conclusiones técnicas del informe presentado por la CNT; las conclusiones fueron: primera: que existe un enlace de internet con nombre Petroecuador-SANAI con fecha julio 2015; segunda: los elementos técnicos no son los suficientes para determinar la creación de usuarios en el equipo de CNT; tercera: el equipo realiza la custodia la CNT; **al interrogatorio realizado por Fiscalía responde** que es master en tecnología de la información, con mención en información informática; certificado en LINUS, telefonía IP, actualmente docente de la carrera de maestría en la Universidad SEC; da también clases en la universidad Israel, de hacking, en maestría; experiencias: más de 25 pericias realizadas; que en el año 2019 estaba acreditado en el Consejo de la Judicatura con acreditación 1838027; señala que un sistema de telecomunicaciones es un conjunto de dispositivos que permite brindar servicios digitales a empresas públicas y privadas, compuesto por elementos activos y pasivos, eso es: routeadores, firewalls, ONTS, fibra óptica y todos los cables de última milla; dice que un sistema informático está compuesto por servidores y aplicaciones que permiten brindar el servicio digital, mientras que la infraestructura, permite el camino para conectar a estos servicios o medios digitales; que los anexos a su informe pericial fueron: 1) Custodia de la ONT; 2) Enlaces de internet 8 megas Petroecuador SENAI; 3) Petición del routeador Telnet; este último anexo es en base a un oficio de la Policía Nacional del Ecuador, Laboratorio de Criminalística y Ciencias Forenses: “en atención a su oficio 707-55-2019-FGE-UIPLL...” dirigido al Fiscal doctor Fabián Chávez, de fecha Quito 14 de agosto del 2019, dentro de la instrucción fiscal No. 55-2019, mediante la cual dispone identifique y materialice la imagen No. A95079D384EDBE1B75A21A558A2283C, “Me permito poner a su conocimiento lo siguiente, se ha procedido a identificar, en el informe de extracción generado por el

software UFED, la imagen solicitada, la cual se encuentra en la página 33115, la misma que se remite impresa, en este reporte se puede verificar todas las propiedades de la imagen, se ha procedido a verificar el archivo fotográfico y se imprime la imagen solicitada, la misma que se adjunta al presente oficio"; afirma que se encuentra adjunta la imagen en este anexo; la imagen contiene un command pro, o sea una ventana para ingresar comandos, el protocolo TELNET, una computadora marca Lenovo, y es ejecutada en lenguaje de bajo nivel THOR; consta en la imagen una dirección IP: 181.113.57.169, esta dirección, según el informe presentado por CNT, con fecha de julio 2015, la empresa Petroecuador EP **realiza una solicitud de servicio, en al cual esta dirección IP es configurada en este ruteador; actualmente** existen muchísimas direcciones IP públicas, estáticas y dinámicas, para identificar una IP pública se requiere utilizar cualquier programa de escaneo, sin embargo se obtiene el nombre del ISP, que es el proveedor de internet, más no el del cliente final; el acceso a una IP de un cliente en específico, se debería hacer un análisis de ingeniería social o estar dentro de la RED LAN y consular la IP pública asignada al cliente; un acceso a un sistema de comunicaciones, según las buenas prácticas y según la norma ISO27.001 se da tres formas: 1) Acceso totalmente restringido, bloqueado, quiere decir que todas las conexiones son rechazadas; 2) Acceso libre: quiere decir que no tiene configurado ningún tipo de seguridad o credencial, se accede sin contraseñas; y, 3) Acceso con privilegios: es el acceso que requiere un usuario y una contraseña y demás factores de seguridad que tenga implementado el sistema; en la imagen motivo de análisis se puede concluir que existe una petición de conectividad hacia el ruteador, que existe conectividad en el ruteador y que devuelve una solicitud de ingreso de usuario y contraseña; mediante la imagen del anexo 3, se puede garantizar que hubo conectividad al equipo routeador; según su experiencia el comando TECNEL por defectos, viene bloqueado en todas las máquinas Windows, por lo que para una persona común, es difícil que pueda ubicar este comando, el lenguaje TOR es un lenguaje no conocido por la mayoría de las personas ya que se utilizan para navegar saltando seguridades y no dejar huellas ni rastros, dentro de los blocks del sistema; como ejemplo dice que se supone que tenemos una propiedad y voy a ingresar para ver si la puerta está abierta o cerrada, sin embargo para hacer esta prueba, he tenido que atravesar el patio de la propiedad primero, por lo tanto cuando abro o cierro la puerta, quiere decir que ya entré al patio, es una analogía de la conectividad al ruteador; **al conainterrogatorio realizado en defensa de la persona procesada responde que el** informe de la CNT fue únicamente documental; que no tuvo acceso a la máquina Lenovo para realizar la pericia; tampoco tuvo acceso al routeador, para verificar su configuración, él lo que hizo es un análisis del informe de la CNT; la fotografía analizada dice que se encontraba dentro del informe de la CNT, O&M-REDES-IP-2019-08-016; revisa el informe y aclara que dentro de ese informe, no está esa fotografía; para realizar la pericia no revisó ningún equipo informático; en el marco teórico del informe define a: IP: es una identificación a nivel de capa de red, de un dispositivo, el cual permite la conectividad dentro de una red; aclara que un dispositivo, si no tiene IP no puede conectarse a una red; IP pública: es aquella que es alcanzable mediante el internet; IP es sinónimo de WAN (red de área extendida; la IP privada se identifican en tres clases: a, b, c dependiendo el número HOST que se requiere en la red LAN; para las IP privadas tiene: 10 para la clase a), la 172/16

para la clase b, y la c 192 con máscara grado 24; generalmente esas IP son las utilizadas, las que dice la norma, sin embargo se puede utilizar a criterio del administrador de la red; que el protocolo IP es un estándar general, el cual garantiza a la conexión en IPV4, para esta conectividad; señala que no conoce al grupo de trabajo de ingeniera de internet; que el estándar que tomó en consideración el protocolo de internet IPV4, que permite la conectividad en el modelo OSI, a modelo de red, la conectividad con direccionamiento IP; el protocolo IPVA define a la red 181 como una red pública; cualquier dirección IP pública no puede ser alcanzada a través de internet; que en el informe CNT explicó si se estableció una configuración de seguridades para acceder IP: 181.113.57.169?, responde que no se puede evidenciar ninguna respuesta de ese tipo, en el informe; ante la pregunta de que si la IP 181.113.57.169 estaba protegida, responde que eso no fue parte de la pericia, ese análisis; le pidieron determinar si el router de CNT tenía algún tipo de seguridad de la red?, responde que no fue parte de la pericia, así como ningún análisis de seguridad de ningún router; reitera que le IP 181.113.57.169 es pública; que si accedió al sitio IP/adress.com, ya que para descubrir una IP pública, existen varios métodos, se puede poner en el internet, como él lo hizo en este caso, entró a la dirección adres, puso la IP para averiguar de qué proveedor o de que ISP pertenece esta IP pública; señala que utilizó una página web para averiguar el proveedor de internet, asociada a esa IP; que si consta en su informe la URL de ese sitio web, así como una fotografía del mismo IP/adress.com; que esa página no contiene esa información; la IP 181.113.57.169 reporta en la página que no privada; al ser pública la dirección 181.113.57.169 no es necesariamente alcanzable por Internet, no tiene los elementos de convicción para decir sí o no; dentro del informe de la CNT había la identificación del equipo asociado a esa IP 181.113.57.169, estaba asociado a los equipos instalados router Sisco 881; el primer pedido según el anexo dos de su informe, era servicio de internet IPON centro de internet de 8 megas, se hace prueba de velocidad a 8 megas, ese pedido era para un DEMO, en la figura 10 dice por favor su ayuda integrando el DEMO configurado en el correo que precede, al equipo y puerto GYECNTE02#SH RUN INTER GI 0/7/0/2; este demo era para la presentación de un servicio de traslado de un servicio; tiene además la solicitud para un enlace de internet de 8 megas; en su informe hay unas gráficas con el título tipologías supuestas de conexión, el anexo uno del informe de la CNT no tiene esas gráficas; afirma que según su experiencia y según el acta de entrega recepción del equipo y según la configuración de los equipos, esa es la topología de la red, no es supuesta, se encuentran en las observaciones del servicio, dice la Red ONE, por tanto está configurada la Red ONE como está en la gráfica y se puede ir al anexo dos en el acta de entrega recepción del servicio, ahí está la configuración ONE MPLS, y la LAN, son las palabras que lo mismo está en la foto; dice en el informe tipología supuesta, porque está transformando lo que dice el papel al gráfico, pero puede ser que varíen las conexiones dependiendo del equipo; no pudo verificar él si así se configuraron los equipos; en las gráficas se identifica los supuestos dispositivos asociados a cada uno de los números IP de la red; ante la pregunta de que si puede identificar con certeza, si una conexión efectivamente sucedió, teniendo solo el dato del número de la IP, responde que la pregunta no está técnicamente bien hecha, no la entiende, aclarando que él puede conectarse a cualquier IP con cualquier equipo, necesitando sólo el número de la IP; se puede determinar con certeza si un acceso a

un sistema informático sucedió teniendo solo el dato de la IP?, responde que no; dice que en el informe de la CNT se responde a un pedido Fiscal, que quería conocer si en la consola de administración existe algún usuario de nombre Ola Bini, en el informe de la CNT se limita a realizar la conexión de internet, respondiendo además que equipos que se pueden conectar a la red de instalación depende del cliente, es decir que solo el cliente puede establecer si alguien se conectó o desconectó a esa red, en este caso el cliente era Petroecuador EP; de la documentación que analizó no se pudo determinar la creación de usuarios, esto debido a que los elementos técnicos no son suficientes para determinar la creación de usuarios en el equipo roteador de la CNT; en su informe no pudo determinar si había asignada en la dirección IP 181.113.57.169, la creación de usuarios, por falta de elementos técnicos y si se habrían creado, teniendo la IP y el acceso, si podría crear usuarios son ningún problema, lo que sería verificable en el LOOCK del sistema que quedan todos los usuarios creados para la posterior revisión de los LOOCKS; si una persona accede a un dispositivo asignado a un IP, si quedaría grabado en el LOOCK del dispositivo; en el informe de la CNT, Fiscalía le solicitó responder que, si acceder a un dispositivo sin autorización por parte del usuario /Ola Bini, constituye un acceso no consentido a un sistema informático, en el informe de la CNT se contestó que “si en el caso de que un usuario no autorizado ingrese y cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático”; en el Informe de la CNT no consta que se hayan creado esos usuarios; en el informe pericial que realizó, también analiza el pedido Fiscal para conocer si al acceder a un dispositivo sin autorización para parte del usuario /Ola Bini, constituye un acceso no consentido a un sistema informático, en su informe no concluye que haya existido un acceso no consentido al sistema informático; no pudo verificar la existencia del usuario /Ola Bini, pues los elementos técnicos no son los suficientes para determinar si se pudo o no crear un usuario /Ola Bini; sin conocer el equipo, no se puede saber la configuración que se le haya dado al mismo; en su informe no consta detallada la configuración del equipo que estaba asociada a la IP 181.113.57.169; en su informe concluye que la conexión a la IP debió haber sido rechazada, llega a esa conclusión en base a la configuración de todos los equipos y a su experiencia, ya que es imposible que un equipo esté abierto al mundo, es un error de seguridad gravísimo, sin saber la configuración del equipo asignado a esa IP; que en su informe técnico no incluye las razones técnicas por las cuales la conexión debió ser rechazada; que no puede identificar al dispositivo ni su configuración; el comando TELNET es un protocolo utilizado para acceso para equipos de manera distantes, puede considerarse como una conexión remota; para poder conectarse con otro dispositivo, los dos deben tener el protocolo TELNET; TELNET permite la conexión con redes públicas como privadas; la redes públicas para evitar conexiones deben tener un firewall que permita el acceso a redes permitidas solo permitidas o bloqueado el puerto por el cual sale TELNET, depende de los sistemas de seguridad; en su informe hay un ejercicio de validación, utilizando el comando TELNET; en la fotografía analizada se ve el comando TELNET 186.43.174.225, él no agregó el comando TOR SOR que sí existe en la fotografía, por tanto el ejemplo no es igual al que consta en la fotografía, pero el protocolo es el mismo; de acuerdo a su experiencia si se puede acceder a conexiones aplicando TOR y el comando TELNET a redes privadas, TOR solo, no se puede conectar a nada; aclara que TOR es un sistema operativo, puedo hacer pin

desde una máquina TOR y puede llegar a pin de una máquina en RED LAN; en el anexo 3 de su informe (en la fotografía analizada) no validó informáticamente, si lo que se muestra sucedió en la realidad, ya que no era parte de la pericia, para comprobar si sucedió, necesitaría que el router esté en línea y la misma configuración esté en línea en el mismo tiempo, es insuficiente solo la fotografía; de la foto no se puede verificar si los comandos fueron ingresados, en ningún momento se le solicitó que haga una pericia de equipo alguno; tampoco le pidieron verificar la existencia de las direcciones IP de propiedad de la CNT, ni las manejadas por la CNT; no le pidieron identificar si la red a la que pertenece la IP 181.113.57.169 de CNT tenía más de un router conectado; una dirección IP es una LAN, no puede ser parte de una red ONE, ya que es privada; volviendo al gráfico, aclara que hay dos escenarios, el escenario de CNT y el escenario del cliente, para el cliente la IP 181.113.57.169 es la IP pública; en la imagen que adjunta consta algún pedido de verificación de usuario para dar acceso al router?, contesta que sí, pero no hay constancia del ingreso de algún usuario, luego consta que el tiempo terminó (no se ingresa usuario y contraseña) y cierra la sesión automáticamente. **PRUEBA DOCUMENTAL:** Incorpora: 1) Oficio No. MDI-BDI-CDM-DCM-2019-1377-O, de 15-IV-2019, suscrito por Anita Chávez, responsable del servicio de Apoyo Migratorio del Ministerio del Interior, al cual se adjuntan los movimientos migratorios del procesado del período 2013-2019; 2) Oficio No. 50DNGR-ABR-2019, de 18 de abril del 2019, suscrito por Francisco Carrión, procurador judicial de TELCONT, en el cual se remite el contrato de servicios, suscrito por el Ing. Iván Croshi y el procesado Ola Bini, de 2 de abril del 2015 y las facturas, pagando las sumas de USD 4.883,00 cada mes; 3) Oficio No. MRENH-DREIDCI-2019-0098-O de 30 abril del 2019, suscrito por el Viceministro de Relaciones Exteriores, en el cual se certifica las visitas del ciudadano procesado, al entonces asilado Julián Assange en el período 2015-2019; 4) Oficio No. MRENH-TRITCI-2019-0103-O, de 10 de mayo del 2019, suscrito por la Vice Ministra de RR.EE., en el cual se remiten copias certificadas de la emisión de visas a nombre del procesado Ola Bini; 5) Oficio No. MRENH-BREIPCI-2019-0097-O de fecha 30 de abril del 2019, suscrito por el Viceministro de RR.EE., en el cual se remite copias certificadas del expediente de la visa de 26 nov del 2015 y del 27 de noviembre del 2016, así como el expediente de la visa de excepción, de 8 mayo del 2018; a favor de Ola Bini; 6) Oficio No. SCDS-DNTLA-19-1264-RESERVADO-EOF de 2 de mayo del 2019, firmado por el Eco. Alan Sierra, de la Dirección de Prevención de Lavado de Activos, de la Superintendencia de Compañías, certifica que procesado no socio, accionista o representante legal de compañía alguna; 7) Oficio No. SCDS-IRQ-SG-SRS-2019-00027746-0, de 2 de mayo del 2019, suscrito por la doctora Gladys Yugcha, Secretaria General de la Intendencia Regional de Quito de la Superintendencia de Compañías, en la que se certifica que Ola Bini no figura como socio o administrador en ninguna sociedad de comercio; 8) Oficio No. SENA-UBAQ-2019-0043-OF, de fecha 2 de mayo del 2019, suscrito por la Inspección de Vigilancia Aduanera, en el que se certifica que Ola Bini no registra declaraciones de dinero en el período 2011-2019; 9) Memorando MINTEL-SEGE-2019-0062-M de 14 de mayo del 2019, suscrito por el magister Raúl Jara, Subsecretario del Ministerio de Telecomunicaciones; mediante el cual se adjunta un reporte de tipos de ataque cibernéticos del 11 al 15 de abril del 2019; 10) Oficio IESS-SPSACT-2019-6179-O, de 22 de mayo del 2019, en el cual se adjunta un

certificado de historial laboral de Centro de Economía Digital en el cual no aparece Ola Bini; 11) Oficio No. 73-NTNGR-NAY-2019 de fecha 31 mayo del 2019, suscrito por el Ing. Igor Croshin de la Cía. TELCONET, mediante el cual se remiten copias del poder especial otorgado por Ola Bini a favor de CDR Loyers, consultores legales, de 10 abril del 2019; en la letra a) del segundo acápite, autoriza para realizar trámite en entidades públicas y privadas; 12) Oficio 014-CC-SPI-DANR-2019, de fecha 5 junio del 2019, suscrito por la doctora Ibeth Charvet, Directora de Asesoría Legal de la Corte Constitucional, al cual se adjunta el Informe Técnico NO. 044-DTI, título ataque informático de 22 de mayo del 2019, describe la caída del portal Institucional, donde se puede observar el mensaje OUT Net Julián Assange; 13) Oficio No. MINTEL-2019-0040-O de 6 de junio del 2019, suscrito por la doctora Mónica Merino, Coordinadora Jurídica del Ministerio de Telecomunicaciones, al cual se adjuntan copias certificadas del expediente de la Asociación Centro de Autonomía Digital, en cuya Directiva se nombra como vicepresidente al señor Ola Bini, representado por la señora Miriam Villacís; 14) Oficio reservado UAFE-CTO-2019-0403, de 13 de junio del 2019, de la Coordinadora de Prevención de la UAFE, al cual se adjunta un informe de TOUR WORDS S.A., DEL 2010 AL 2019 registra ingresos por USD 22.426.738,00, registra 72 depósitos por USD 1.177.899,00; transferencias recibidas por USD 21.248.839,00, transferencias enviadas por USD 19.957.000,00; Ola Bini no tenía relación de dependencia con dicha empresa; 15) Oficio S/N de 14 junio del 2019, suscrito por el señor José Luis Cuesta Rivadeneira Gerente de TOUR WORD Ecuador, mediante el cual se remiten información sobre los ingresos del señor Ola Bini, en los años 2013-2017 fue empleado de la empresa registrada en EEUU; 16) Oficio IESS-CTSAP-2019-7547-O, de 18 junio del 2019, mediante el cual se adjunta información del historial laboral de la empresa Tours Word, el señor Ola Bini no consta en la nómina adjunta; 17) Oficio No. 117012019-OSTR-013538 de 20 de junio del 2019, de la Dirección Zonal 9 del SRI, al cual se adjuntan informes ejecutivos ampliados de la empresa Tour Word y Soporte Libre, donde no consta como clientes o proveedor el señor Ola Bini; 18) Escrito presentado por la Gerente de CNT, al cual se adjunta el oficio No. CNT-ROMGOM-FOM-2019-0966, de fecha 16 agosto del 2019, suscrito por el gerente de OIM encargado, mimos que contiene el informe No. OIM-REDES-IP2019-08-016 de 16 agosto del 2019, suscrito por el Ing. Carlos Medina quien certifica: se evidencia en la herramienta transaccional, que la fecha de solicitud de la petición asignada al cliente de Hidrocarburos EP, fue generada en el año 2015, bajo un DEMO con petición de 28 de julio del 2015 y fecha de retiro 30 de octubre del 2015; el área comercial solicita el traslado del Demo, en ese sentido la configuración fue creada en base a los datos solicitado por el área comercial; dirección IP privada, red ONE 172.16.140.169-30, IP pública, red LAN, cliente 181.113.57.168/29, asignando las siguientes IP públicas asignadas al cliente: red LAN 181.113.57.168/29; 181.113.57.169; 181.113.57.170; 181.113.57.171; 181.113.57.172; 181.113.57.173; 181.113.57.174 y 181.113.57.175.; 19) Memorando FGE-EAI-2019-01093-M de fecha 14 de junio del 2019, suscrito por la doctora Patricia Carranco, Directora de Asuntos Internacionales de la Fiscalía General del Estado, al cual se adjunta la comunicación con la traducción oficial remitida por correo electrónico de la abogada Ángela George, Fiscal de asuntos Internacionales del Departamento de Justicia de los EE.UU., del que se desprende respuesta parcial de requerimientos de la Asistencia Penal Internacional; 20) La Asistencia Penal

Internacional que contenía conversaciones de chats entre el señor Ola Bini y otras personas de una plataforma conocida como Llave, desde el 8 de octubre del 2013 hasta el año 2015; traducida por la interprete; 21) MEMORANDO No. FGE-EAI-2019-0133-M, de 26 julio del 2019, suscrito por la doctora Patricia Carranco, Directora de Asuntos Internacionales de la Fiscalía General del Estado, al cual se adjunta la comunicación de fecha 25 de julio del 2019, recibida mediante correo electrónico de un funcionario del Departamento de Justicia de los EE.UU., en el que se remite respuesta parcial de la API de los dispositivos electrónicos no encriptados; 22) Un escrito presentado por la señora Martha Moncayo, Gerente General de la CNT, al cual se adjunta el oficio CNT-ML-2019-0285, de 27 agosto del 2019, suscrito por el Ing. Miguel Ludeña Gerente Nacional Técnico de la CNT en el que se certifica que la dirección IP LAN, la que maneja a la interna el cliente, es la 181.113.57.168/29, misma que constituye un rango de enrutamiento que se detalla: 181.113.57.168 no utilizada; 181.113.57.169 un nodo de la red local; 181.113.57.170 un nodo de red local; 181.113.57.171 un nodo de la red local; 181.113.57.172 un nodo de la red local; 181.113.57.173 un nodo de red local; 181.113.57.174 un nodo de la red local; y, 181.113.57.175 "Brod Cast" no utilizable; 23) Un escrito presentado por el abogado Juan Chiriboga, procurador judicial de EP Petroecuador, de 30 de agosto del 2019, al cual se adjunta el memorando No. 00176-GIM-OIM-ZSU-2019, suscrito por el Jefe Zonal del servicio sur: señala que el comando TELNET a la IP 181.113.57.169, no se realizó desde la IP Petroecuador; 24) Oficio No. 2019-009-0026037-RST, de 11 de septiembre del 2019, remitido por la Unidad Especializada en Telefonía Móvil Avanzada para la investigación del delito al cual se adjuntan datos generales y de registro de llamadas entrantes y salientes de los abonados 0996299557, del señor David Ochoa abogado del acusado, del número 0968942120 del señor Ola Bini y 0096727647 del señor José Paredes, agente que le lee los derechos al procesado; detallando las llamadas entrantes y salientes del 11 y 12 de abril del 2019; 25) El oficio 2019-0730-F, de 24 de septiembre del 2019, firmado electrónicamente por el Ministro de RR.EE., al cual acompaña un detalle de visitas del señor Andry Meuller al señor Julián Assange en los años 2015 y 2019, en la embajada de Ecuador en Londres, entre los cuales consta el señor Ola Bini y funcionarios de TOP WORDS. El Tribunal por voto de mayoría, dispone incorporar al expediente judicial la prueba antes detallada, con el voto salvado de la Dra. Fanny Altamirano Cárdenas, quien se aparta del criterio de mayoría, remitiéndose al artículo 454 del COIP, el que contiene principios procesales referente a que los Jueces estamos obligados a cumplir, recalcando que debe observarse el principio de libertad probatoria, que no es una libertad probatoria sin alcance ni ilimitado, para lo cual se debe considerar la pertinencia, esto es que las pruebas deben referirse directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción, así como a la responsabilidad penal de la persona procesada, afirmando que hay prueba documental que no tiene esa pertinencia y esa relación con la infracción y la persona procesada.

4.2.2. PRUEBA DE LA ACUSACIÓN PARTICULAR: Prueba Testimonial: Testimonio de: 1) CARLOS ANDRÉS MEDINA MONTALVO: Ingeniero en electrónica y Telecomunicaciones, dice que ejerce su profesión desde el año 2005; en cuanto a su capacitación, dice tener varias capacitaciones complementarias a fin a su profesión, una en la marca Cisco en el nivel profesional CCNP y tres a nivel de especialista en la misma marca; la certificación CCNP

significa tener un conocimiento avanzado en redes de telecomunicaciones en equipos marca Cisco; que labora desde el año 2009 en CNT, trabaja en el área de redes IP, su cargo actual es el responsable de las redes IP; agosto del 2019 su cargo era responsable Operación y Mantenimiento de Redes IP encargado; en cuanto a sus funciones, dice que tiene más de 21 atribuciones, dentro de las principales operar y mantener el equipamiento de la red de CBNT, coordinar la atención de eventos que se presenten y otras es el apoyo a proyectos de nuevas implementaciones de redes de telecomunicaciones; la empresa pública CNT EP si cuenta con certificaciones de seguridades desde el año 2013, con la certificación ISO2701-2013, la misma que se la renueva cada tres años, en febrero del 2022, se la renovó por última vez; tener esta certificación significa que la empresa CNT alcanzó la certificación de seguridad para el proceso de venta e instalación de productos y servicios de datos de internet para clientes corporativos; remitió información a la Gerencia de Operación y Mantenimiento por disposición verbal dada por el Gerente de Operaciones en el año 2019, en atención a un requerimiento de Fiscalía General del Estado, aclarando que elaboró el informe de análisis de Ejecución, Peticiones Open OIM Redes IP de 16 de agosto del 2019; básicamente en atención al requerimiento de la Fiscalía, este informe contiene: 1) la petición 92385433875, que corresponde a una petición de servicio de internet, que se ejecutó en base a la solicitud del área comercial de CNT y se le asignó la IP pública 181.113.57.169, la que permaneció activa desde el 28 de julio del 2015 hasta el 30 de octubre del 2015; 2) la petición 17.38246290, que corresponde a una petición de datos de dos puntas, punta A Quito, punta B Guayaquil, que se atendió en base al requerimiento del área comercial de CNT la misma que a la fecha del informe estaba activa; el aprovisionamiento en las plataformas en redes IP o de OyM se realiza en base a procedimientos internos en base del sistema transaccional OPEN, la CNT EP procedió con el cambio de la UNP de número de serie B815 al cliente que estaba haciendo uso de la misma, para proceder posterior con su retención y custodia, en una orden de instalación de fibra NIPON, la CNT EP realiza la instalación de la última milla y configuración de la ONT asignada al cliente, bajo los estándares de seguridad de la información, además cabe señalar que los equipos que el cliente conecte a esta ONT, así como su direccionamiento son de potestad y responsabilidad del cliente, además sus usuarios y contraseñas; IP pública: no significa que cualquier persona pueda acceder libremente a ella, significa que un direccionamiento IP puede tener una conexión hacia el Internet, es decir desde esa IP yo me voy a poder conectar a los servicios d internet; existe otro tipo de IP, citando los estándares internacionales como el RFC 19-18, por ejemplo que es el que determina cuales son los rangos de direcciones que se pueden utilizar con IP privadas, en ese sentido podemos definir dos tipos de direcciones IP, unas que son privadas y otras públicas; la diferencia entre IP pública y privada, básicamente es que la IP pública tiene acceso a internet y la IP privada no lo tiene, este incumplimiento de los procedimiento internos y del RFC 19-18, el cual, vuelve y repite define cuales son los rangos que se pueden usar en las direcciones IP privadas y por consiguiente las públicas, estas IP privadas se pueden utilizar en diferentes tipos de redes, las que por su tamaño o cobertura se dividen en varios, de los cuales son, ejemplo: LAN, MAN y WAN: las redes tipo WAN, son redes de área extendida, son las que interconectan redes (del cliente con el proveedor del servicio); y, las redes LAN son

redes de área local e interconectan equipos en una misma RED; que la IP pública 181.113.57.169, se la asignó en base a una solicitud del área comercial de CNT, mediante correo electrónico de 23 julio del 2015, se le configuró el servicio a Petroecuador Sanai Internet, el cual se configuró en el equipo de la CNT, en las instalaciones denominadas Boyacá en Guayaquil, para posteriormente atender en base de un requerimiento del área comercial, un traslado de esta configuración, el 24 de julio del 2015 hacia las instalaciones de CNT en el edificio Correos de Guayaquil, traslado que significa que la interconexión del cliente en la Red de CNT pasó del equipo ubicado en Boyacá al equipo ubicado en Correos; esta red de IP 181.113.57.169 no es de conocimiento público, esa asignación está en conocimiento de personal de CNT y el cliente; un particular requería un conocimiento técnico avanzado, es posible conocer el direccionamiento, pero el trabajo que requeriría para que una persona logre conocer el direccionamiento, requeriría de un conocimiento técnico avanzado, sin menoscabo de la cantidad de horas que utilice para conseguir ese objetivo, aclarando que en el mundo existen millones de direcciones IP públicas, de las cuales la CNT tiene aproximadamente 300.000 IP; señala que esa IP 181.113.57.169, corresponde a un sistema de telecomunicaciones que difiere de un sistema informático; la diferencia entre un sistema de telecomunicaciones y un informático, básicamente dice que el sistema informático es el que permite almacenar o procesar información, como una o varias computadoras, servidores, los usuarios del sistema, mientras que un sistema de telecomunicaciones, es el medio físico que se usa para transportar información desde un origen a un destino; el servicio que se entregó al cliente Petroecuador Senai, según los procedimientos internos y el sistema transaccional OPEN, para dotar del servicio de internet al cliente, se utilizó 2 equipos y un cable de interconexión, principalmente; que el primer equipo es la UNT, es el equipo que ayuda a la interconexión del enlace físico desde las instalaciones del cliente, hasta las instalaciones de CNT, el segundo es el ROUTER, es el equipo que ayuda a la toma de decisión desde envío de la información, desde una fuente hacia un destino; y, el tercero es el cable de interconexión, que es el medio físico que une la UNT con el ROUTER; básicamente la CNT realiza sus instalaciones en cumplimiento de las normas, como protocolo de seguridad utilizado para cumplir con la norma antes citada, ellos implementan varias, como bloquear el puerto ASL entre otras; quienes tienen autorización para acceder a la ONT son 2 personas, uno es el cliente y otro el personal autorizado de CNT, esto de manera física, el otro es de manera remota, en ese caso únicamente el personal de CNT tiene la autorización para realizar esa conexión; la conexión de un tercero a la UNT, es hacer uso como medio de paso para ingresar al ROUTER, implicaría un acceso no consentido a un sistema de telecomunicaciones, tal como lo indica en el informe remitido a Fiscalía; **al conainterrogatorio realizado en defensa de la persona procesada responde que** en su informe da contestación a varios pedidos realizado por Fiscalía, el primero en cuanto a la identificación del equipo con dirección 181.113.57.168/29, detallándose dos peticiones, la primera que corresponde a un servicio de internet, la que fue atendida en base de un requerimiento por parte del área comercial, mediante correo de 23 de junio del 2015, mediante la cual se pide la configuración del equipo en la calle Boyacá; el 24 de julio personal de área comercial solicita el traslado de configuración a otro equipo; el día 28 de julio, como consta del informe, se ingresa la petición en el sistema

transaccional OPEN, y tiene vigencia hasta el 30 de octubre del 2015 para proceder a su retiro; en cuanto al segundo pedido, que se encuentra vigente hasta la fecha de elaboración del informe, realizada la petición en el año 2016, la que se refiere a la misma dirección 181.113.57.168/29; aclara que el /29 se refiere básicamente a la cantidad (o máscara) de IP públicas que la CNT le asignó al cliente para que haga uso; esta tenía 8 IP disponibles, en su informe las especifica 181.113.57.168, hasta 181.113.57.175, los equipos instalados por CNT a esas IP son la UNT (un router), conectada a la primera IP 181.113.57.168, los demás equipos conectados fuera de los dispuestos por CNT, son responsabilidad del cliente; aclara que una dirección IP está determinada básicamente por el RF791, el cual indica que una dirección IP está compuesta por 32 bits, unos y ceros, que es lo que se entiende en términos técnicos, divididos en cuatro octetos, cada octeto separado por un punto; una dirección IP puede estar asociado a un computador o a un equipo de telecomunicaciones; una dirección IP puede estar vinculada a un dispositivo; la IP pública nunca va cambiar desde el equipo que la origina; el informe básicamente es un análisis de ejecución de funciones OPEN, ahí solo se detalla el equipamiento instalado y como fue el flujo en el sistema transaccional OPEN, no se detallan configuraciones, en los anexos se detalla las configuraciones que permitieron el enrutamiento del direccionamiento público; en el informe no consta la configuración de ninguno de los dos equipos; una IP pública es aquella que permite la conexión a internet, si Yo tengo internet puedo conectarme a esa IP en el caso de que se lo admita, para que no se damita a esa conexión IP puede haber una restricción en su configuración, depende de los niveles de seguridad que tenga el servicio, también es posible poner un fire word, también se puede pedir un usuario y una contraseña, lo que forma parte de los elementos básicos de seguridad de un equipo; aclara que en su informe no está la configuración del equipo; señala que una IP privada por concepto, no se publica en internet, pero según la red interna del cliente a la cual se le asigne una IP pública, y de esa IP pública y mediante varios protocolos, se puede hacer que d esa IP pública se puedan asignar IP privadas, como en nuestras casas, ya que los proveedores de servicios da un protocolo de asignación de direccionamiento IP dinámico, esa dirección es básicamente una IP privada que sale de la pública; en cuanto al segundo pedido de Fiscalía, le solicitaron remita documentación de soporte, de la que se pueda determinar si en la consola de administración existe algún usuario de nombre /Ola Bini, en su respuesta dice que la CNT se limita a realizar la instalación de internet, de la última milla y la configuración de equipo UNP; dice además que los equipos que puedan conectarse a esta ONT, así como a la distribución y asignación interna del direccionamiento público son de responsabilidad del cliente; que en el pedido 4, Fiscalía le piden a la CNT determinar si al acceder de este dispositivo sin la autorización correspondiente, por parte de un usuario de nombre Ola Bini, constituye un acceso no consentido a un sistema informático, telemático o de telecomunicación, dando como respuesta; si en el caso de que un usurario no autorizado, ingrese, cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático, telemático o de telecomunicaciones; responde que en el informe no se verificó la creación de usuarios; las direcciones IP como se diferencias físicamente?; responde que básicamente dentro del RPC 1918 que es el que define cuales son los rangos que se puede usar las direcciones IP privadas y públicas, recalcando que una dirección IP está basada en 32 bits, cada uno dividido en 4 octetos, entonces los

números o los rasgos que se pueden usar entre IP pública o privada son las que indicó de RPC, como ejemplo, solo viendo las IP uno tendría que determinar si corresponde o no a uno de estos rangos que acaba de indicar, que básicamente son 3 rangos, dependiente la clase a la cual pertenece cada dirección IP y si está dentro de esos rangos sería una IP privada y si no están sería una IP pública: los rangos inician: la clase a) inicia con 10000 hasta la 100255; la clase b) inicia con 172 16 hasta la 172 32; y, la clase c) inicia desde 192 168; estas son las IP privadas; una IP privada puede ser parte de una red de área local o red LAN?, responde que sí; una IP pública puede ser parte de esta red de área local LAN?, responde que depende, pero si podría; una IP pública puede ser parte de una red ONE?, depende del diseño, como ya lo indicó no hay que confundir direccionamiento IP con el tipo de redes, existen dos tipos de direccionamiento IP, públicas y privadas y existen 3 tipos de redes por su tamaño: LAN, MAN y ONE, entonces cuando uno es técnico puede definir si ocupo una o las dos para cada una de estas redes, entonces público o privado pueden entrar en ONE o en LAN; reitera que existen millones de direcciones IP, si a usted se le da un dato de dirección IP 181.54.112.165, y se le pregunta si puede establecer quien se conectó, con el número le basta?; depende, pero no podría determinar solo con el número, si alguien se conectó, hay demasiadas circunstancias con las cuales se podría, se debería tener un conocimiento muy avanzado para saber si se conectó o no se conectó, realizar un análisis, no sabe.

4.2.3 PRUEBA EN DEFENSA DEL PROCESADO; Prueba testimonial:

Testimonio de: 1) DAVID RICARDO ARTIEDA ESTRELLA: De profesión abogado, sobre que conoce sobre el caso, dijo que el día 11 de abril del 2019 a eso de las 16:00 le contactó el doctor David Ochoa a contarle si le podía acompañar al aeropuerto Mariscal Sucre por un potencial cliente porque estaba una persona detenida, estaba ocupado, se desocupé a las 17:00, se encontraron con Ochoa en Tababela a eso de las 17:30 y acudieron al segundo piso, al counter de información, averiguaron si conocía a una persona de nacionalidad sueca que estaba ahí, un tal señor Ola Bini, inmediatamente se comunicaron y le pasaron con el Capitán Carlos Molina, le dijo que necesitaba verle al señor Ola Bini, le preguntó si estaba con la prensa, le dijo que no lo entendía, que quería conocerlo a Ola Bini y conversar con él, le dijo que no le podía ver porque había pasado migración, le dijo que si existía una orden de detención dada por la Fiscal Diana Salazar y firmada por el Fiscal Fabián Chávez, le dijo además que no podían sacarle de la zona de seguridad y que vaya a una UPC a 500 metros, luego de media hora fueron a la UPC cerca del aeropuerto, no había nadie que de razón, regresaron al aeropuerto nadie daba ninguna razón, le pidió a Daniela que trabaja con él, que acuda a la Fiscalía General y ella le dijo que el Fiscal Fabián Chávez estaba a la espera que llegue Ola Bini para dar una versión, que por eso había sido detenido; a las 19:00 vieron que no había movimiento en el aeropuerto, se trasladaron a la Fiscalía General, a eso de las 19:45 llegaron a Fiscalía, les atendió un Policía de apellidos Chicaiza Quinatoa y les dijo que este procedimiento lo llevaba el Fiscal Fabián Chávez, quien salió y les dijo que había una orden y que lo estaban trasladando del aeropuerto a la Fiscalía, esperaron, no había forma de contactarse con Ola Bini, hasta que las 21:00 procedieron a dirigirse a buscar arraigos de esta persona, el abogado Ochoa se contactaba con la persona que lo llamó, se dirigieron al domicilio del señor Ola Bini en la calle Juan Dibuja, edificio Bertone, en eso salieron de Fiscalía y al llegar al

Hotel Marriot en la Orellana y Juan León Mera, los detiene un agente de la AMT, le hace parar y le dice que casi le golpea a una persona transeúnte, le entrega los documentos y le dice siga, avanzaron hasta el edificio de Ola Bini, llegaron al Hospital Voz Andes ya estaban dos patrullas, se bajan policías vestidos de civil y les dicen que hacen ahí, les dicen que venían para conseguir documentación de arraigo, inmediatamente les dijeron que era peligroso y les preguntaron qué estaba haciendo, y les dijo que tenían que llegar miembros de la policías judiciales y que hacían rondas, en ese momento le dicen que se vaya y se quede el carro, les pregunto que hizo, estaba intimidadores, llamó a varias personas para saber que pasaba, no tuvo respuestas, les dijo que se retiraba, en ese momento se retira y cando estaba en la 10 de agosto, le persiguen vehículos sin placas, fue a poner gasolina y paró en Orellana y 9 de Octubre, para y dos vehículos se pusieron junto, se bajan personal sin identificaciones y con chalecos fosforescentes, carro sin placas, le dicen que necesitan registrar su vehículo, les dijo que venía de la casa de un potencial cliente y que quería documentos para el arraigo, le dicen que tiene que colaborar, que ese procedimiento lo estaba llevando el Fiscal Fabián Chávez, les pidió los nombres y en ese momento le dijo Subteniente Ricardo Muños, Mauricio Frías y Claudio Castillo y otros, el subteniente le dijo que tenía que colaborar y ese momento hacen una llamada y se escucha la voz del Fiscal Chávez, le dice que se ha fugado del lugar, le dijo que porqué revisan su vehículo, grabó lo que pasó, filmó lo que registraron el vehículo, no sabía que pasaba, luego vio las noticias y le vio a la ministra de gobierno dando la noticia; no encontraron nada en su vehículo y se fueron; regresó a la Fiscalía y nadie les atendió, estuvo hasta la 01:00 del 12 de abril del 2019 y se retiró y afuera de su casa había patrulleros al igual que en el domicilio de su compañera, esa noche no pudieron dormir; luego supieron que a varios abogados les habían dicho que no tomen este caso, que se meterían en problemas con la Fiscalía; al siguiente día a eso de las 09:00 acudió a la Unidad de Flagrancia para averiguar si llegó el señor Ola Bini y se contactó a las 10:00 con él, entró con el Cónsul y conversó con él, él le contó que le había llevado a las 04:00 a la Av. Amazonas y Roca donde la Policía Judicial, después dio la versión, recién del aeropuerto salió a la 01:00 y lo había llevado a su casa; y después ya tomaron procedimiento otros abogados; que el hecho se dio en el edificio Bertone, fue a conseguir documentos pero aún al siguiente día no lograron conseguir ningún documento; a las 21:00 le parece que ya estaba una patrulla ahí y la otra se acercó con las luces prendidas; en la gasolinera se le acercaron a eso de las 09:45 o 10:00 de la noche; no supo cuál era la razón de la detención del señor Ola Bini, solo le dijeron que lo trasladarían a Fiscalía a rendir una versión; la Ministra no se acuerda bien lo que dijo, que había una detención de un ciudadano ruso; entró con el Cónsul de Suecia a la zona de aseguramiento de la Unidad de Flagrancia, cree que alguien había llamado al consulado; sinceramente nunca vio una orden de detención; **2) SANTIAGO DAVID OCHOA BELTRÁN:** De profesión abogado, sobre que conoce sobre el caso, dice que hubo una detención arbitraria en contra de Ola Bini, el jueves 11 de abril 2019, supo esto porque recibió a eso de las 15:30 una llamada de una amiga de nombre Leslie Jarrín, le dijo que Ola tenía problema para embarcar y el preguntó si le podía dar su teléfono para que él le llame, buscó en la página Web del ministerio del Interior si había prohibición de salida del País, no tenia, recibió la llamada de Ola, le dijo que no tenía prohibición de salida, él le dijo que estaba en el aeropuerto de

Tababela y él se ofreció a ir para ver lo que ocurría y solucionar el problema de que no lo dejaban viajar, pero lo que él nunca había visto es que a eso 16:00 con su colega Arteaga viajaron a Tababela, intentaron hablar con el detenido y no les dejaron, le buscaron y no estaba en el aeropuerto; en la Dirección de Aviación Civil le pusieron al teléfono a Ola y un policía le dijo a su colega Artieda que es mejor trasladarse a Quito, por eso se trasladaron, a él le advirtieron de no hacer público este tema y ellos avanzaron a los medios para que todo el mundo se entere, en Quito se quedó en la matriz de Fiscalía ubicada en la 12 de Octubre y Patria y David fue a Flagrancia, esperaban que trasladen a Ola pero se quedó hasta las 20:00 y no llegaba, fue a flagrancia y nunca lo trajeron; tuvo un par de comunicaciones con Ola pero no tenía la confianza y le dijo que la Policía tenía un largo historial de detenciones ilegales y desapariciones forzosas, se quedó en Flagrancia hasta que llegue Ola, hasta las 06:00, recibió la llamada de un Policía Patricio Paredes, le dijo que iban a trasladarle a Flagrancia y él le aviso a David Artieda, lo vio cuando llegó en la patrulla a las 07:00, cree que es un procedimiento irregular, que detengan a una persona un jueves y lo ingresen a flagrancia el viernes, él no lo conocía a Ola y lo abrazó, pensaba que no sobreviviría de una noche a otra, lo ingresaron y más adelante llegó el Cónsul de Suecia y recién le permitieron a David Artieda hablar en confidencialidad con Ola; el viernes 12 de abril vio en Tuitter que en la cuenta oficial de la Policía, había publicado fotos en referencia a esta detención, con dispositivos electrónicos grandes que con toda seguridad no eran parte del equipaje de Ola Bini, viajó al domicilio de Ola en el sector del Hospital Voz Andes donde vio que había varios policía que tomaban procedimiento, sin fiscal y sin orden para realizar esa diligencia; los Policías le llamaron al Fiscal Chávez, llegó luego el Fiscal Chávez con la orden judicial y le dijo que se retire; **al constraintinterrogatorio realizado por Fiscalía responde que** trabaja en el Municipio de Quito, en desarrollo productivo local, mejoramiento de las condiciones económico de la ciudad; dice que una detención arbitraria es cuando se incumple uno o más de los literales del artículo 77 de la Constitución; con orden de detención puede ser considerada una detención arbitraria, por incumplimiento de uno o varios numerales del artículo 77; conocía si el señor Ola Bini tenía una orden de inmovilización? no conocía sobre aquello; **3) IVÁN ANDRÉS PAZMIÑO MAZÓN:** Ingeniero en sistemas informáticos y computación, más de 15 años desarrollador de software, ahora es consultor informático de una empresa en EEUU, durante 3 años fue parte del equipo de desarrollo de sistemas y herramientas para la protección de la privacidad; señala que la privacidad es importante para protegernos de varias cosas, para que seamos objetivos con la propaganda como por ejemplo cuando se hace una búsqueda por internet, se quedan con los datos de las búsquedas, luego le presentan propagandas específicas de lo que uno ha estado buscando, entonces se busca protección para los ciudadanos es importante para que no sean sujetos de manipulaciones con fines comerciales; señala que las herramientas desarrolladas para proteger la privacidad, hay un abanico de herramientas, para establecer conversaciones como los chats, se cifran los mensajes para que los puedan ver quien los envía y recibe, otra herramienta es ocultar direcciones de cada computador cuando se conecta al internet, ocultar la dirección IP ya que es la información que necesitan para hacer propaganda para grupos específicos de una región geográfica, medios para cifrar correos, entre otras; es común que haya dirección IP ocultas? Es una práctica común

pero no suficientemente difundida; que es una ONT?, desconoce; dice que un ROUTER es un elemento dentro de una red, que sirve para distribuir, ayuda a que los mensajes lleguen a un destino; es un dispositivo informático; que conoce Ola Bini, cuando entró a la empresa consultora de EEUU ahí lo conoció, eran compañeros de trabajo y en el 2015 fue cuando entró a ese equipo para crear herramientas para la privacidad, trabajo en el equipo de Ola, él es desarrollador de Software abierto, así lo ha conocido por 9 años y más, era miembro del equipo de desarrollo de Software; Hacker es alguien que encuentra una solución para algo, pero comercialmente es alguien que evade el sistema, es una mala interpretación para que los programas de televisión sean más atractivos, pero es una persona que encuentra problemas comunes de la vida diaria; el investigador de seguridad informática es una persona que tiene amplio conocimiento del tema y segundo tiene una habilidad importante de desarrollar, desconfiar, porque para poder modelar un ataque por un lado hay que poder hacer un ataque y eso te enseña que en la seguridad informática hay muchos espacios, no es solamente ponerle antivirus a la computadora, no solo poner un Fire Word en la red, hay cuestiones de comportamiento humano, seguridad operativa en los procesos, en un campo amplio y complicado; no hay mucha gente que se dedica a esto, es como una especialidad, no es como decir el nivel de entrada, es un nivel avanzado; sobre lo que es IANA: no sabe de memoria; Grupo de Trabajo de Ingeniería de Internet: son los que trabajan con las solicitudes para hacer estándares de la WEB, la revisión de los presupuestos abstractos del internet, diseñan como debería ser el estándar, hacen sugerencias, guías para la implementación y estos están relacionados con la entidad que se encarga de hacer los informes de los protocolos para el internet, para que funcione, para que sea operativa; que la dirección IP es la forma de encontrar un computador, es como su número de teléfono, en el internet se mete la dirección y se aplasta entre, sirve para poder ubicar recursos, si uno quiere a g mail, esta tiene una dirección IP asignada, son 4 grupos de 4 números que se les asigna un equivalente que es el nombre como por ejemplo Google.com; tipos de direcciones IP que conozca: hay un grupo que se llama direcciones conocidas, públicas que son utilizadas para servidores que están en el internet abierto; otras direcciones que son privadas, que son para las redes internas de una institución; que las direcciones públicas son como los números de teléfono que están en la guía telefónica y los números privados son como los números que tienen en un hotel por ejemplo, que no sabes, manejados en la central del hotel; sabe que es el estándar EFS1918? No conoce; existe un RFC que limita el rango para las IP privadas, es básicamente como ponerles una marca para decir que son privadas, comienzas con 192, van desde el 168 al 192; cuales los tres rangos de las redes privadas: del 168 al 192 cree que van las redes asignadas para equipos de red privada y los rangos que empiezan con 10, son para las direcciones públicas y la primera dirección IP es para el router; si ve una IP puede determinar si es pública o privada?; sí, si solo ve el número puede seguir la intuición de que es pública o privada; la IP 181.113.57.169 no sabe si es pública o privada; sí se puede conocer todas las direcciones IP, hay una programa para determinarlas, asocia el nombre con la dirección si es pública, es el programa JUIS, que puede determinar que corresponde a un dominio determinado, buscar estas direcciones es algo normal, es como buscar un número telefónico en una guía; para un experto en seguridad es algo normal, es de un

conocimiento básico; la herramienta TOR es un medio que ayuda a proteger la privacidad de la gente, protege la IP de la computadora, la creó la marina de los EEUU, ellos comenzaron el desarrollo hace 15 o 20 años y ahora es una comunidad de código abierto, que le sigue dando mantenimiento a este sistema; como funciona: es una herramienta que protege el destino y el remitente de un mensaje; puede ser para proteger la privacidad; quien puede usar TOR: es de descarga gratuita y su código es abierto, también hay un navegador que tiene incluido un TOR y se puede navegar sin que al IP esté al alcance de otras personas; no puede ser utilizado para vulnerar un sistema, solo sirve para conectarse si identificar un IP; TOR sí se utiliza para conectarse a redes públicas como Google, Hot mail; TOR para conectarse a un IP privada no, porque no se las conoce esas direcciones privadas, no hay medios técnicos para poder hacer el direccionamiento hacia esos números; se utiliza Tor para saltarse medidas de seguridad?: NO, solo sirve para conectarse a una dirección pública; TEILS es un sistema operativo que no tiene memoria para guardar las direcciones IP; se utiliza para no tener memoria de las direcciones accedidas, este sistema operativo es de código libre, abierto; un ejemplo de código no abierto: sistema operativo de Windows, nadie puede ver los archivos y códigos que hace funcionar el código operativo que es reservado; él utiliza sí TAILS, se lo puede cargar en una flash, es un sistema operativo; que él sí ha utilizado TOR, todo el tiempo cuando está navegando, no para ver videos porque es lento; VPN es una red virtual que hace que el tráfico de internet este oculto para su proveedor y el resto de intermediarios; TAILS no tiene códigos ocultos, ni maliciosos; muy normal que un técnico utilice TOR o TAILS; los dispositivo de autenticación físicos o lluvicos, son como una llave que contiene códigos, sirve para desbloquear códigos; es normal en alguien que conoce de seguridad; la criptografía en el ámbito digital: la implementación de primitivos, protocolos que permiten la trasmisión segura de un mensaje, es similar a un cifrado, hacer que un mensaje sea ilegible; existen un montón de tipos de cifrados; los cifrados simétricos son cuando la forma de descifrar el mensaje es con una contraseña; que el cifrado de discos duros es una norma básica de seguridad; no permite saber la cantidad de información que contiene ese disco; no se puede saber si tiene algún dato; los algoritmos hash son de una vía, hace como generar un identificador para un mensaje, no trasmite el mensaje en sí; el algoritmo Sha-1 es un hash viejo en el que la longitud del identificador que se crea es de 128 bits, lo cual causa problemas por colisiones entre los nombres y el correo; el hash MD5 es un algoritmo en desuso, tiene un nivel de seguridad muy bajo; es posible cambiar la información en un disco con este tipo de códigos?, que con el MD5 está casi seguro que la longitud es como de 52 o 56 bits, por tato es posible, con el sha1 también es posible, pero necesitaría más tiempo; la compañía Tops Ware empezó hace 30 años en Chicago, está ahora en 20 países, su objeto es la consultoría en el desarrollo de software; la consultoría consiste en que una empresa les dicen el problema que tienen y ellos estudian y construyen la solución; como conoce el presente caso?: responde que fue a la Fiscalía porque Ola había sido detenido en el aeropuerto, en las redes sociales comenzó a circular la imagen que decían era la prueba de que había ingresado a un servidor de la CNT, en la imagen está como un mensaje de bienvenida al servidor y el apuntador esperando que se ingresen credenciales al servidor y después un mensaje que decía no ingresó credenciales, así que se cierra la conexión, él fue a explicar de que esa no es prueba

del ingreso al sistema; en la fotografía que vio, había una primera línea que era un comando para conectarse a una IP, después de establecida la conexión había como un texto que decía servidor de la CNT, algo así, si no es empleado no entre y después aparecía un apuntador para el ingreso de usuario y se imagina que después pediría contraseña, finalmente había un mensaje de que no se había presentado las credenciales de acceso en el tiempo y decía no hay credenciales y por tanto no se podía entrar y se cerraba la conexión; en esa fotografía esa IP era pública; sí había una herramienta TOR, así como otra herramienta TELNET, que es otra herramienta que permite que se conecte desde una computadora hacia otra para administrarla, eso es lo que antiguamente utilizaban los Web Master de las páginas Web, entonces mi página no está funcionando, mi servidor está en las antenas del Pichincha, entonces Yo desde la piscina me conecto para reiniciar el servidor; hoy en día no es una práctica común, es una herramienta no usada porque es una de las primeras herramientas para acceder remotamente a un servidor, tiene fallas de seguridad; la información que se desplegó de la CNT es lo que un servidor muestra como pantalla de bienvenida, es como cuando uno va a un edificio y el guardia en la garita le dice bienvenido al edificio de la Judicatura, presénteme su credencial para poder pasar, no se muestra ninguna credencial y el guardia se cansa de esperar y cierra la ventana de la garita, se acabó la sesión; en la fotografía se ve que le pidió el usuario, hay un time out y se acaba el tiempo de espera y sale un mensaje que se corta la comunicación, la conexión terminó; en la foto no existe acceso, solo establecimiento de conexión, no se presentan credenciales para acceder y se cierra la conexión; de la fotografía no se aprecia otra acción; **al conrainterrogatorio realizado por Fiscalía responde:** que experiencia tiene en telecomunicaciones?, señala que esa es otra rama; que en los sistemas informático existe el software y el de telecomunicaciones es el hardware para establecer las comunicaciones; esos conceptos los tiene porque él estudió electrónica en el colegio Central Técnico y se graduó como técnico en electrónica; que el sistema de telecomunicaciones de CNT no lo conoce; que ocultar una dirección IP es importante, porque sirve para ocultar la ubicación geográfica de una persona, entonces cuando hay campañas de mercadeo, estas están dirigidas a personas de ciertas regiones, entonces somos objeto de esas campañas de publicidades; como se oculta una dirección IP?: se utilizan sistemas que no establezcan conexiones directas con el servidor destinatario, como por ejemplo TOR; sobre la función de Ola Bini en TOP WORDS, señala que era un programador, estaba en equipos de desarrollo, mientras que él estaba en otros equipos de desarrollo; Ola Bini era un programador súper fuerte, famoso, diseñó un lenguaje de relación, desarrollo uno de los proyectos más famosos para la simulación del comportamiento de cédulas, a la final todo era software comercial; hacía proyectos rimbombantes porque era súper bueno; programas de software que desarrolló Ola Bini, dice que seguramente muchos, el conoce un par: uno el de las células de cáncer, el cliente era un centro de investigación gringo, perdón de los EE.UU., de ahí con él hizo una rutina para Leseen Crip que permitía refrescar certificados de seguridad; señala que con Ola Bini hablaban en Inglés; formación académica de Ola Bini: hasta donde sabe estudió como el colegio hasta la mitad; sobre el hacking ético, dice que es una forma de buscar vulnerabilidad en un sistema X, para poder después reportarlo y que las personas propietarias sepan de la existencia de esas vulnerabilidades; que la herramienta TOR lo utiliza cuando

navega en su casa, cuando trabaja, navega en el internet con TOR, chatea con sus clientes con TOR; lo utiliza para evitar que cuando este navegando su IP sea un dato para mandarle propaganda, es viudo y cuando su esposa estaba enferma de cáncer, él buscaba tratamientos en el internet y le comenzaron a bombardear con vitaminas y más propaganda, era víctima de los ataques de publicidad; la herramienta TOR sirve para ocultar la IP; la identidad de quien la utiliza no, la identidad se la puede conseguir de muchas otras formas, solo hace ocultar la IP de origen y la de destino; dentro de un hacking ético, si le contrato para verificar vulnerabilidades, es necesario utilizar la herramienta TOR? NO, Tor es solo una herramienta; sobre los métodos para descifrar información, dice que se puede descifrar teniendo la clave y la segunda es tratando de adivinar la clave o llamada fuerza bruta; con los hash MD5 si es posible cambiar el contenido de un disco, genera un hash para identificar un mensaje existente en el disco, ese hash lo que hace es entrar al mensaje y saca el número 5, entonces hay la posibilidad de que el mensaje tenga una identificación muy pequeña, es un hash antiguo; para cambiar la palabra hola, se hace el Hash en la palabra HOLA, se separan las letras, se les da una longitud en bits, a todas se les alarga hasta que tengan 8 y se les aplica el hash, entonces se puede en estos espacios que quedan, se mete otros caracteres para que el mensaje sea al mismo; por que se utiliza TOR para conectarse a TELNET, para no dejar la IP en todos los lugares intermedios; sobre la FOTO: dice que NO HAY UN ACCESO a un servidor de la CNT que es un sistema informático; no ha presentado ningún informe técnico en la causa; **al conainterrogatorio realizado en defensa de la acusación particular responde que** cualquier persona tiene acceso a una IP pública, porque se puede establecer conexión; sí se puede identificar quienes es el dueño de la IP, también sale quien registro el nombre de dominio, lo importante es que uno pone la IP y sale el nombre de dominio CNT.com; el cliente final es fácil de identificar, se puede saber quién registró la IP, no necesariamente quien pidió que se la registre; no conoce los componentes de infraestructura que utiliza la CNT, ni las seguridades que utiliza para brindar el servicio de telecomunicaciones, pero en el ARCOTEL están descritas las guías de seguridad informática para las entidades públicas, así está que debe haber un Fier Word, las computadoras tienen que tener anti virus y una serie de elementos para mejor seguridad; en la IMAGEN descrita: que componente le solicitó las credenciales?: en esa imagen la conexión estaba hecha a través de TELNET, eso quiere decir que en el servidor de CNT, donde se establece la conexión, tiene que haber TELNET para que pueda interpretar la solicitud para establecer conexión y luego se le presenta el mensaje de bienvenida, entonces ahí hay instalado un TELNET; el utilizar la herramienta TOR no es un medio de violar las seguridades, es solo un medio de conexión que no expone la IP desde la que te conectas, solo se protege de los proveedores de internet; **4) RAFAEL BENJAMÍN BONIFAZ PALLARES:** Master en seguridad informática e ingeniero en sistemas; trabaja en la organización de derechos digitales y trabaja como administrador de sistemas y otras tareas con otras organizaciones; señala que trabaja en defensa de derechos humanos en el mundo digital, normalmente nosotros nos movemos en el mundo físico, ahora nos movemos en el mundo digital o en el mundo del internet y en este espacio nuestros derechos pueden ser vulnerados, por ejemplo el derecho a la privacidad, que es el derecho a decidir que parte de nuestros datos o de la vida se comparte, en el mundo físico es muy fácil comprender por ejemplo una conversación

que Yo estoy teniendo, pero en el mundo digital es muy complicado, por ejemplo si inicio una conversación por WhatsApp, WhatsApp sabe que estoy conversando con esa persona y depende de la herramienta que utilice se puede ver las conversaciones que mantengo; sobre la seguridad informática dice que trabaja desde el 2012 cuando se empezó a preocupar de la seguridad en las comunicaciones en internet, y quien puede ver lo que Yo hago en internet, luego decidió estudiar y en el año 2016 fue a Buenos Aires y sacó una maestría en seguridad informática, desde ahí empezó a trabajar con organizaciones sobre este tema; cuales son las herramientas para proteger privacidad en el campo digital?: existen varias, algunas se encuentran en el uso del cifrado, que sirve para proteger las comunicaciones, que hace que si Yo mando un correo electrónico, hace que solo sea leído por esa persona, existen además aplicaciones como Signal, el uso de TOR, que es una red que tiene varias aplicaciones que permite que las actividad que realice en internet no sea vigilada constantemente, y que toda la actividad quede registrada, esta herramienta permite transitar en internet con mayor seguridad y mitigar el riesgo de ser vigilada como periodista, abogados; otra herramienta es un gestor de contraseñas, permite que tengamos contraseña distinta para cada cuenta en internet, los expertos recomiendan una contraseña para cada caso, en la práctica es difícil pues recordar varias contraseñas es muy complicado, entonces un gestor de contraseñas guarda las contraseñas y genere unas seguras, con lo cual puedo tener varias y distintas para cada sitio; que es una ONT: señala que no ha trabajado con esto; que es un router?: es un dispositivo que generalmente tenemos en casa y permite conectar dos redes, generalmente un router se lo utiliza para conectarse con otra red, red local internet, puede hacerse de Quito a Guayaquil; conoce a Ola Bini desde el año 2013, él era parte de la Asociación de Software Libre del Ecuador y la empresa Thought Works quería abrir oficinas en el Ecuador, tuvieron reuniones con la gente de esa empresa y ahí estaba el señor Ola Bini; que en los años 2013-2015 coincidieron en eventos con Ola Bini y cuando estudió la maestría en Seguridad Informática en Buenos Aires, en un proyecto de la Universidad el sistema venía con la aplicación COYM, que es una aplicación de chat segura, la aplicación había sido creada por Ola Bini, quien las desarrolló con otras personas de Ecuador; en el año 2018 la organización CAD buscaban gentes y él trabajó desde marzo del 2019 hasta junio del 2021, donde trabajó con el señor Bini, trabajaron principalmente en dos proyectos principales, uno que es un sistema de conferencias de audio por internet y el otro es el que ya comenté; señala que Ola Bini es un programador reconocido a nivel internacional, especializado en seguridad informática y actualmente trabaja en el Centro de Autonomía Digital, el que lidera en su parte técnica, en el desarrollo de estas aplicaciones y enseñando como programar en forma segura; reitera que Ola Bini es experto en seguridad informática; señala que la palabra hacker tiene dos connotaciones, originalmente es un curioso de la tecnología, que le gusta conocer cómo funcionan los sistemas y los estudia; otra mediática relacionada como que alguien que ataca sistemas informáticos; que un investigador de seguridad es alguien que quiere entender cómo funcionan los sistemas, que fallas de seguridad podrían tener, para poder mejorarlos; que es la IANA?: es la organización que se encarga de distribución de las direcciones IP públicas en internet; que es la ITF?: es una organización que trabaja en el desarrollo de los estándares que hacen que funcione el internet; una dirección IP es, dentro de

una red de computadoras, cada una se identifica con un número único, conectado a una red, existen privadas o públicas, esenciales para que funcione una red; IP versión 4 son direcciones que se utilizan ahora, que tienen un número finito y que se está migrando a la versión 6 por la cantidad que existen; el tamaño de la V6 es mucho más grande, existe un número mayor de direcciones IP, con números más grandes; RFS 1918; es el estándar que trabaja en asignación de las direcciones IP; en ese estándar se establece direcciones IP privadas y las no establecidas como privadas son IP públicas; que las IP privadas son como de tres rangos, el uno empieza en 10.000, la segunda empieza con 192.168, y la tercera empieza con 172, sin recordar más el rango; existe otro rango 127.00 que es para asignarlos dentro de una computadora; una IP representada por 181.113.57.169 es una dirección pública porque no está incluida en rangos de las IP privados; la IP es pública porque es accesible en internet; todas las direcciones IP están registradas en la IANA, pero existen sistemas como SHODAN que permiten hacer escaneos y ver qué servicios se presentan, permite ver por ejemplo todos los servidores que funcionen con el sistema SCH, distribuidos en el Ecuador; la red ONE: es una red grande de alcance nacional, no es privada, por tanto es pública; un corta fuegos o Faure Word es un dispositivo o software que se pone donde mi red se conecta para proteger la red, o permite bloquear el acceso de forma selectiva; para el escaneo generalmente existen servicios que lo hacen como SHODAN, la utilización de esos servicios es normal para saber si sus IP han sido vulneradas, los investigadores lo usan para saber qué tan seguro es el sistema; que la herramienta TOR se desarrolló en EEUU, con fondos del Estado y otras organizaciones a nivel global; la red TOR sirve para proteger mi actividad en internet, mejora mi seguridad, porque el internet es un espacio muy inseguro; la herramienta TOR, para conectarse a una red privada no es normal, TOR no es un sistema operativo, es una red de anonimato en internet, anonimato es como poder ser utilizado para actividades no identificables; no es una herramienta para vulnerar sistemas informáticos; el sistema operativo TEILS: es una versión del sistema operativo LINUS, que no se instala en el disco duro de la computadora sino que funciona en una memoria flash, básicamente sirve para la protección digital de las personas; funciona a través de la herramienta TOR, es además un software libre ya que se puede saber cómo está hecho, se le pueden hacer auditorías, no contiene códigos maliciosos; sobre la criptografía; se utiliza las matemáticas para proteger información; que en el cifrado simétrico se utiliza la misma clave para cifrar y descifrar los mensajes; que el cifrado asimétrico se utiliza un par de llaves públicas y otra privada, la pública para cifrar el mensaje y la privada para descifrarlo; que para el cifrado de disco duro, lo que se hace es poner una contraseña a la computadora para que nadie acceda a su computador, no se puede acceder a su información sin poner la contraseña; ha visto en internet la imagen que por la que se le acusa a Ola Bini, imagen en la cual se ve que se quiere acceder a través del sistema o servicio TELNET, a un dispositivo remoto a través de un control remoto, se presenta una imagen que dice: si usted no está autorizado para ingresar o en otras palabras el ingreso no es permitido, y se espera que se ponga un nombre de usuario para autenticarse y una contraseña, pero nunca se ingresa el nombre de usuario, por lo cual el sistema aparentemente responde con un time out, cómo que el tiempo de espera terminó y se corta la conexión; en esa fotografía está una terminal de línea de comandos, aparentemente está dentro de una computadora con un

sistema Linux, se utiliza un comando TOR SORS, que le da a entender que se está utilizando TOR, el siguiente comando es TELNET, que se utiliza para acceder de forma remota, con una dirección IP, aparentemente responde y por eso se lee el texto de CNT diciendo que no ingrese si no es autorizado; que la dirección IP de la fotografía corresponde a una dirección pública, porque no pertenece a ninguno de los rangos de las IP privados y adicionalmente se está utilizando el comando TOR, que funciona solo con direcciones IP públicas, es como en la calle hay edificios, se toca la puerta de afuera del edificio y nunca ingresa a una red privada; no sabe puede saber si la imagen es real, se debería contrastar con el sistema al que se quiso ingresar; que el sistema debería guardar esos registros, que establezcan que alguien quiere ingresar al sistema en esa fecha; en la foto no hay cortafuego porque se ve lo que dice CNT, no hay suficiente información de la foto de que se quiso acceder al sistema; **al conrainterrogatorio realizado por Fiscalía responde en cuanto a la diferencia entre** el sistema de comunicaciones sirve justamente para manejar comunicaciones y los sistemas informáticos manejan telecomunicaciones; no conoce el sistema de telecomunicaciones de CNT; que conociendo la dirección IP publica se puede conocer el nombre de a quien está asignada, normalmente se llega hasta el nombre del proveedor de internet y esta empresa puede dar la IP a sus clientes, pero no se puede saber el nombre del cliente final; **5) MARCO RICARDO ARGUELLO JÁCOME:** Ingeniero de sistemas; tiene una empresa que trabaja en infraestructura y software libre, tiene contratos con empresas para hacer mantenimiento de servidores sobre todo LINUX y despliegue de aplicaciones; sobre la privacidad: dice que el hecho de que una persona no tenga que exponer sus conocimiento, pensamientos, criterios, que se pueda reservar alguno de ellos; digitalmente se garantiza esta privacidad por medio de varios mecanismos, claves para tener privacidad, a veces es complicado emitir criterios, es complicado mantener el voto secreto cuando se lo hace telemáticamente; herramientas para proteger la intimidad: cuando se hacen comunicaciones utilizando mensajería o correo electrónicos, estos pueden ser interceptados, la comunicación personal, entonces hay varios mecanismos, hay programas como chats para permitir comunicación segura, encriptándola entre emisor y receptor; que el software libre permite ciertas libertades, es para compartir con otros, para que alguien lo mejore y hacer que el software mejore, los usuarios son libres de compartir copias con un tercero sin violar nada y es una forma de desarrollar el producto o aplicación, muy en el trasfondo de las implementaciones de infraestructura; existen desarrolladores individuales de este software, él ha trabajado en algunos proyectos, hay empresas que contratan a persona para que trabajen en software libre; en la carrera de sistemas se ven informáticos y comunicacionales, la diferencia sustancial es que las comunicaciones tienen el acceso físico a transferencia de datos, sobre la cual se puede implementar un tema de software, que es una capa superior, pero son complementarios; ONT; es un dispositivo que se utiliza en comunicaciones para transformar la señal que llega de fibra óptica de un proveedor de internet, a una red interna, suelen llamarse modem, hacia un router interno; hay aparatos que son ONT y router al mismo tiempo, pero **él** no conoce los dos dispositivos en uno solo equipo; sirve de capa de transporte OSI, que divide en varias capas según la comunicación y un dispositivo ONT, el que hace una transformación a un cable de fibra óptica que se conecta del lado del proveedor de internet a múltiples hogares,

digamos, esa transformación se la conoce como la capa 1, la capa física de comunicaciones; un router es un dispositivo de red que permite el direccionamiento de una dirección IP interna, dentro de una red local, hacia una red externa, generalmente se utiliza para transportar una dirección IP interna hacia una dirección externa en internet; que el protocolo PSTP de capa 4, es el que identifica a cada computadora con la dirección IP y permite el envío de paquetes entre computadoras de una red local, utilizando un protocolo llamado PSTP; IANA: es la autoridad mundial que tiene que ver con estándares de internet, estandarización, se dedica para la asignación de direcciones IP, protocolos etc.; IETF, es un grupo de encargado de emitir estándares para normar procesos de estandarización, ya que en las redes hay varios vendedores y hay que implementar un proceso de comunicación, quedan todos de acuerdo en un estándar; una dirección IP es la forma de identificar un dispositivo o un computador, ya sea en una red local o en internet, de forma única; en cuanto al tipos de IP: hay lo que se conoce como un RFC que es un tipo de estándares, 1918 que define dos grandes tipos: IP privadas, utilizadas en redes local y hay tres segmentos de todo el rango, reservados para las redes local, todos los otros segmentos de direcciones IP son públicas, las que se puede usar en internet, permitido a nivel público; las IP privadas solo se utilizan en redes privadas, no pueden ser accedidas públicamente; las públicas pueden ser utilizadas en internet; las direcciones IP privadas se forman por octetos, tiene 4 octetos: la clase a empiezan con 10.0.0.0; el segundo rango 172.16.0.0; y, el tercer rango 192.168.0.0/, se puede utilizar en cualquiera de estos rangos las IP posibles; las IP pública: es posible rutear a esa dirección IP y se necesita además de la dirección un puerto al que conectarse; la dirección 181.113.57.169 es una IP pública por no estar dentro de los otros rangos de las privadas; el protocolo TELNET: unos de los primeros de internet, permite la conexión interactiva, con usuario y un password se tiene acceso a una conexión mediante un remoto, es un protocolo inseguro porque no encripta la información, el ruteador podrían ver el usuario y password y cualquier comando que escriba, es por eso que es obsoleto e inseguro; TOR: es un mecanismo de conectividad, rutea por internet para conectarse a un servicio a través de una red de capas de cebolla; no se vulnera ningún tipo de seguridad porque los proveedores ponen a disposición del público estos nodos que permiten hacer estos saltos hasta llegar al dispositivo al cual se quiere acceder: se usa esa herramienta para que en el camino realizado de la comunicación, no se pueda averiguar sus datos y sus claves; TOR solamente permite el acceso a redes públicas que están en Internet, no es posible conectarse a una red privada; la ONT lo que hace es transportar las pulsaciones de luz de un cable de fibra óptica, que lo conecta a un proveedor de internet, hacia un mecanismo de capa dos que le permite mediante un ruteador, llegar a una red generalmente privada; señala que existe un servicio que se llama SHODOW, que hace el escaneo de direcciones IP públicas buscando puertos; TAELS es un sistema operativo seguro, basado en LINUS, para utilizar TOR, lo usan los profesionales de seguridad informática, ellos lo usan; tiene incorporado por dentro a TOR, es un software libre, es muy difícil que se utilice como puerta trasera o troyano; TROYANO es un software que se lo instala para una función pero que realiza otra función; cifrado o criptografía es un mecanismo utilizado para hacer que una información en texto plano se ofusque para que no se conozca su contenido, sirve para tener confianza en las transacciones, por seguridad, para que no sean

interceptado; el cifrado de disco duro, sirve para no permitir saber que datos tiene el disco; LLUVICO es un segundo factor de identificación, para no usar solo mi usuario y mi password, se agrega un segundo factor adicional de identificación, como una llave física que se pone una autenticación adicional, llamados Token de autenticación; la red WAN: son áreas grandes de conectividad entre dispositivos distantes, que están a miles de metros entre sí; la red LAN, red local, se conectan servidores que están cercanos a decenas de metros o pisos de un edificio; FIREWALL es un dispositivo que se usa para evitar que alguien acceda a una dirección IP y acceda a un servicio o un dispositivo; un algoritmo hash es uno que se refiere a un resumen de un mensaje, que permite que a cualquier tipo de datos, le saca una cantidad de caracteres fijos, generada a partir de esa información, no hay como regresar del hash al archivo original; el algoritmo hash MD5 es más inseguro, por la cantidad de caracteres que genera, no es recomendable por su inseguridad; señala que conoce a Ola Bini desde el año 2013, lo conoció porque él trabajaba en THOUGHT WORKS y ahí trabajaba su esposa como gerente, profesionalmente no ha trabajado con él; él es parte del Centro de Autonomía Digital, sí ha sido proveedor del señor Ola Bini; que un servidor es un dispositivo pensado para empotrarse en algún dispositivo que se conoce como RAC, sirve para introducir en él varios servidores; conoce que Ola Bini es un profesional de seguridad, trabaja en criptografía, desarrollador de software; fue vinculado a esta instrucción, la acusación inicial fue por ataque informático a sistemas y después fue cambiado a acceso no consentido; lo único que tenía es que le había vendido un servidor a Ola Bini, que eran amigos, al final no se le acusó y salió del juicio; conoce de una fotografía, la vio en la prensa, la vio en el periódico cree que en El Comercio; en esa imagen se ve que se hace una conexión hacia una dirección IP no recuerda cual, y aparece un texto de advertencia de que es un dispositivo de CNT y luego un texto que solicita usuario y luego se ve que se dice que la conexión expiró; en la imagen se identifica al cliente final?: se ve en el texto que dice CNT prohibido el acceso, se puede inferir que era de CNT; decía además algo de Petroecuador, Senai en el texto de advertencia; el dispositivo que despliega esa información es la IP quien emite ese texto; ese texto es configurable por un técnico; identificó algún dispositivo a software cortafuego: no, si hubiera habido un firewall no se habría permitido la conexión, porque el cortafuego lo habría impedido; de la foto no se aprecia si existía un firewall, al final es solo una fotografía; el servicio TELNET tiene que haber estado habilitado para utilizar el servicio; era proveedor de CNT, de mantenimiento de servidores LINUX; si conocía la infraestructura tecnológica que utilizaba CNT, esto en el año 2014-2016; no recuerda haber recibido algún mensaje del señor Ola Bini con esa imagen; lo que dice en la prensa es que Ola Bini manda una fotografía y que él contactaría a CNT; eso es una práctica común; **al contrainterrogatorio realizado por Fiscalía responde que** trabaja hace 20 años en telecomunicaciones y software; que el sistema de telecomunicaciones tiene que ver con todos los dispositivos ópticos, físicos, que aseguran la comunicación entre dispositivos de red local o red remota, mientras que el sistema informático tiene que ver con el conjunto de aplicaciones, arquitectura, para desplegar un sistema de utilización a nivel empresarial; estos dos sistemas se complementan; no conoce el sistema de telecomunicaciones de CNT, no conoce porque está compuesto; dice que sí es importante ocultar IP dependiendo del uso que le quiera dar, TOR tiene un uso

variado; conoce que Ola Bini era desarrollador de software, parte del equipo de desarrollo; si desarrolló algunos programas, no recuerda cuales; se comunicaba con Ola Bini en inglés; el hacking ético es utilizar las prácticas para vulnerar las barreras para proteger o suplir una falencia de seguridad, un hacker no es el que roba la información, sino que experimenta, conoce y tiene mucha experiencia en la tecnología; dentro de un hacking ético es práctica común y usual utilizar la herramienta TOR; TOR es utilizado para permitir el enrutamiento desde una dirección IP de origen a otra dirección IP, y la IP original no se sabe cuál es; TOR no tiene como objetivo de ocultar identidad, es un protocolo de transporte de datos; que la información encriptada es casi imposible de descifrarla, solo existe el método de fuerza bruta, esto es intentar todas las claves posibles; que la utilización de la herramienta TOR es porque es segura y protege esa comunicación; conociendo una IP pública, no es posible identificar al cliente final; TOR para comunicación remota con protocolo TELNET, vuelve la conexión segura; el escaneo está en la página web en la foto no se puede ver; que si utiliza TEALS debido a que utiliza TOR a través de una red, obviamente no saldrá la dirección IP; en cuanto a la formación académica de Ola Bini, anecdóticamente sabe que no terminó el colegio nada más; el servidor que proveyó a Ola Bini fue ubicado en el data center del TELCONT en un Rac, él lo instaló ahí; su número telefónico es 0995494579, teléfono que no sabe desde que tiempo lo tiene; en el 2015 debe haber sido el mismo número; no recuerda haber recibido la foto del señor Ola Bini, luego afirma si haberla recibida, pero la revisó luego en la prensa; **al contrainterrogatorio realizado en defensa de la acusación particular responde que** su contrato con la CNT era dar mantenimiento a servidores LINUS; no conoce la infraestructura de telecomunicaciones que tiene CNT; no conoce los componentes de su seguridad; sobre la certificación IZO27001-2013, no la conoce por no ser experto en seguridad; el acceso a una banca web correspondería a un sistema de telecomunicaciones para la conectividad e informático para la aplicación; **6) ROGER DINGLELINE LINUS NORDBERG:** Dice ser investigador para el proyecto TOR; en cuanto a sus títulos académicos, señala que tiene tres títulos en Massachusetts, pregrado en ciencias informáticas ingeniero en matemáticas y ciencias informáticas e ingeniera eléctrica; en informática: es fundador de una organización Proyecto TOR y escribe software TOR hablando a favor de esta tecnología por 20 años; ha hechos informes sobre esta área? Si ha escrito muchos artículo de alto perfil, escribió el informe principal sobre el diseño de TOR y ha dado muchas conferencias, el simposio PEP de sistemas de aumento de privacidad conocido a nivel mundial; la privacidad para él es muchas cosas, puede ser control, que saber sobre una persona; en el entorno digital la privacidad se garantiza por medio de brauser TOR, hay una red de voluntarios que son 8.000 y lo que hace el brauser del TOR es descargar la lista de todos los relay y se construye un camino a través de tres diferentes relay, de forma que ningún relay solo sabe dónde está ubicada una persona, la idea de esto es descentralizar la información; un relay es un voluntario en algún lugar del mundo que corre el software configurado para hacer tráfico de relay para otras personas; el software libre: es muchas cosas, un licencia de derecho de autor para asegurar que todo el mundo pueda utilizar el software; quien lo desarrolla en general?: hay personas en todos el mundo y una comunidad que trabaja para que todos lo puedan utilizar de una manera segura, en los EEUU hay confusión porque FREE quiere decir gratis o libre, pero en este caso

es libre; no se requiere un título para poder programar, hay muchos voluntarios que trabajan con TOR que no tienen ningún título; él creó TOR mediante una organización sin fines de lucro, creó la primera versión, son tres fundadores Matisen, Saibersen y él; Nick trabaja para una organización sin fines de lucro y Paul trabaja para un laboratorio de investigación en Estados Unidos, para el gobierno de EEUU, pero trabaja sobre TOR; quien financio el proyecto: varias personas en EEUU, muchos gobiernos el Departamento De Estado y el de Defensa de EEUU, la Organización Nacional de Ciencia de EEUU, el Ministerio de RREE de Suecia y otros países europeos, que son gobiernos que quieren que TOR exista, para que las personas sean más seguras; para que las conexiones sean más seguras: todo lo que hace es un routing a través de la red de relay, para que si alguien que mira tu computador, no sepa cuáles son los sitios web que estás visitando o la ubicación donde estés; mucha gente lo utiliza porque las compañías crean perfiles de los usuarios, esta base de datos creadas por las compañías pueden ser vendidas o robadas, la idea de TOR es dar a los usuarios el control, esta información y sus datos solo a los usuarios; quien utiliza TOR: millones de usuarios, entre 2 y 8 millones diariamente, personas ordinarias, ciudadanos que cuidan su privacidad, también periodista de la BBC y del New Time; las compañías como por ejemplo Facebook lo utiliza, tratan de ayudar a los usuarios de TOR para que sea más seguro; habló hace un tiempo con el Ministerio de RREE de Alemania y ellos hacen una capacitación a su personal para enseñarles cómo funciona; también ha hablado con gente de la policía a nivel mundial, los agentes del FBI usa mucho TOR, parte de los temas que él maneja, es la capacitación para los Policías en diferentes Países, como EEUU, Bélgica, Islandia etc.; TOR SOCS: es otra forma de utilizar TOR, se lo utiliza como un Browser y los expertos usan este TOR SOCS; se puede utilizar TOR para conectarse a una IP privada?, NO, solamente a las direcciones IP que están disponibles públicamente puede conectarse a través de la red de TOR; TOR no es sistema operativo, es un programa que se puede correr en la computadora; TOR es un software que funciona en una computadora; puede TOR saltar medidas de seguridad para entrar en un sistema?: No porque una página web es eso, las medidas que tengan las páginas no son las mismas, TOR lo que permite es llegar a una página web con privacidad, pero no cambia la forma en que se pueda utilizar la página web; TOR vulnera seguridades para conectarse a sistemas o dispositivos? No TOR solamente es otra forma de llegar a un servicio que da más control al usuario, para permitir conocer quienes acceden a los mismos; en qué circunstancias se puede dar que TOR pase por una ONT?: cuando usas internet especificas donde va el tráfico de internet a una dirección IP, luego se enruta a esa dirección de IP, los ruteadores interactúan y tú no sabes cómo funcionan ellos; puede un programa de escaneo masivo, escanear un router desde una ONT?: no puedes glogear, no puedes ingresar y tampoco escanear; conoce el programa SHODAN? si es una página web, recolecta un mapa o una vista de cada servicio que está en internet, se puede saber cómo está el internet ese día; es utilizado por personas de seguridad de la red, y también las personas que manejan página web para ver cómo se ven sus páginas web para el resto del internet; SHODAN puede escanear un router a través de ONT?: señala que al estar al alcance de todos en el internet podría, pero que escanear a través de una ONT no tiene sentido, porque el internet lo que hace es conectar a una dirección de IP y de ahí la infraestructura de rearing, ya sea a

través de un rutador, o de fibra óptica no importa; que muchos gobiernos habla de la importancia de la privacidad y de TOR y en especial un reportero de EEUU sobre la libre expresión, David Kane, escribió un reporte sobre las herramientas de cifrados y su importancia para los derechos humanos y también las herramientas para hacer anónimas a las personas, que es importante para los Derechos Humanos; que el señor David Kane trabaja para las ONU; en este informe, una de las importancia que describe es que las herramientas de cifrado son claves para la libertad de expresión y los derechos humanos, y el otro punto clave es que cuando hay vigilancia de parte del estado, es importante tener herramientas de privacidad como TOR para asegurar la libertad de expresión en este tipo de casos; el reporte concluye indicando que los estados, debería adoptar protecciones y no restricciones para el cifrado y para asegurar la anonimidad de las personas, específicamente habla de los defensores de los derechos humanos y de los periodistas que utilizan TOR; que la palabra de garantizar en el área de informática es fuerte, dentro del informe se menciona que TOR es una de las mejores garantías para los periodistas y los derechos humanos; IANA: es la autoridad de asignación de números de internet, esta organización decide quién puede usar y cuales números y direcciones IP; AITE: es un grupo de ingenieros que se reúnen para llegar a consensos sobre protocolos de internet, para que todos puedan construir herramientas combativas; IP: es como un número telefónico pero para internet, describe a dónde va el tráfico de internet y como es ruteado, le parece que el número de teléfono es una buena analogía; las direcciones IP se usan para realizar conexiones: cuando se quiere conectar a una IP, el computador cree unos como paquetes, el internet sabe cómo rutear para saber a dónde tiene que irse el tráfico; EFC: son documentos escritos por de la organización IETF, que describen los estándares de internet; EL ESTANDAR EFC1918: es un estándar muy conocido, describe cuales son los números IP privados y públicos; se reservan rasgos de direcciones?: si, hay rangos que no pueden ser alcanzados por el internet públicos y otros que si pueden ser alcanzados públicamente; rangos privados: hay algunos bastantes conocidos, por ejemplo el 192.168, que son redes internas que empiezan 10, esa es una red interna; los que empiezan con 127 en un computador local; la red 181.113.57.169 es pública o privada? Es una dirección pública, porque no está incluida en las privadas; que es cable de internet? Se usa para conectar en corto, de rango corto entre computadoras; para conectarse a Google se utilizan estos cables, no el acceso a sitios web, pero se necesita más de un cable, se necesita una conexión de internet, conectados a cables de fibra óptica, los que cruzan a través de Estados, Países y luego se conectan nuevamente a través de Google por su lado; cable de fibra óptica: es una forma de transmitir datos en el internet a largas distancias, usa luz para transmitir información; la luz se convierte en datos, hay adaptadores, que los envían a través del internet, es ingeniería para poder transmitir la información a otro lado; para la conversación a través del zoom, se necesita infraestructura física, se necesita la conexión de internet, y por el otro lado se tendrá su propia conexión de internet como la de la sala, se puede mandar información sin saber cómo es la conexión por su lado, pero entre las dos conexiones deben haber cables de fibra óptica, proveídos por las compañías de telecomunicaciones; él sabe ciertos datos técnicos que pasar por su lado, pero desconoce lo del otro lado; cuando hace una conexión, accede a los cables? no accede a los cables para acceder a una conexión, porque ellos están enviando el

tráfico de un lugar a otro, pero él no accede a los cables; Router: son los más comunes de internet, envían el tráfico de internet de un lado a otro; TELNET: programa para conectarse a los servicio de internet, es como un navegador para visitar sitios web; se puede encontrar todos los puertos TELNET por escaneo, si, con un programa que verifica cada puerto de la dirección IP de destino, para ver quienes escuchan; quienes lo utilizan: muchas personas utilizan el escaneo especialmente, los de seguridad de redes, para saber que parte de su red están expuestas y para poder mantenerlas; que es un experto en seguridad informática: personas empleadas por una compañía, que hacen que el internet sea más seguros, entender las vulnerabilidad y poderlas corregir, son técnicos; no siempre son empleados de compañías, hay voluntarios, hay comunidades para compartir conocimiento etc.; si hay una herramienta que se llama SIMAN para escanear todo el internet en cuestiones de horas y días; red ONE: es una red de área ancha, es un término de marketing, es como una conexión de internet a larga distancia, como los cables de fibra óptica que existen entre varias ciudades; red LAN: es una red de área local, un término de marketing, pero son dos computadores comunicándose, puede ser a través de un cable de internet, están ubicados cerca; las direcciones IP pueden ser asignados a estas redes?: se puede llegar a una dirección de IP a través de internet con red LAN o ONE, dependiendo de su configuración, pero no se asigna IP a una red, lo que se hace es que se asigna una dirección IP a un dispositivo que está conectado a una red; una dirección IP pública o privada puede ser parte de estas redes? Si depende de la configuración, no es normal configurar una IP a través de una red ONE, pero depende cuáles son las definiciones de ONE o LAN que se utilizan; que es un firewall: es un mecanismo de control de exceso, puede ser software o hardware, lo que hace es bloquea las conexiones a ciertos servicios; si se la puede utilizar para evitar que se llegue a una dirección IP; si conoce a Ola Bini, desde el año 2013, en una conferencia de seguridad; era una reunión de expertos en seguridad informática, él para compartir información, él daba información sobre TOR; si ha trabajado en un proyecto con Ola Bini, él fue voluntario y desarrollador de TOR para mejorar su diseño, para que sea más seguro para el usuario; que entiende por Hacker: significa diferentes cosas para diferentes personas, para él es alguien con curiosidad sobre este tema y quiere aprehender, los medios de comunicación lo consideran a una persona mala; que es al Hacking Ético? Existe un movimiento entre los expertos en seguridad informática, que utilizan su conocimiento sobre el internet, para mejorar la seguridad de internet, son los conocidos como los de sombrero blanco; los hacker éticos vulnera servicios de comunicaciones? no, una de las metas de estas personas es la seguridad, es la de no causar daño, es entender lo sistemas y hacerlos más seguros; criptografía en el ámbito digital: es el estudio de las matemáticas para proteger información como el cifrado o la firma digital; da su testimonio por un lado para hablar de TOR y ayudar a explicar cómo funciona y para qué sirve, y de lo que sabe, Ola Bini no ha hecho nada malo, ni ha cometido un crimen; ha visto en la prensa sobre el juicio, señalan a un artículo de la EFF sobre un imagen; dice que la EFF es una organización sin fines de lucro en los EE.UU, que trabajan para las libertades civiles, compuesto por abogados que pretenden que malas leyes no prosperen; sobre la imagen publicada, descríbale: lo que se muestra en la imagen es que alguien está haciendo conexión por internet a la dirección IP mencionada antes, 181, está utilizando TOR, esta dirección sí es alcanzable, se

realiza la conexión y sale un banner que es un aviso, que dice que el acceso es prohibido y en la parte inferior de la imagen hay una opción de ingresar el nombre de usuario para hacer el login, y luego dice que venció el tiempo y que la conexión fue cerrada por un anfitrión ajeno, eso quiere decir que se hizo una conexión pero que no se hizo el login, no se ingresó y luego se desconectó; se puede identificar la persona que realizó este comando?, con seguridad NO porque hay un Pront que está en la parte superior, que describe la computadora local, y ahí sale el nombre de Ola, es posible que haya sido pero no con seguridad; hay otra información en ese banner? Si en la parte superior del banner dice el acceso no autorizado a este dispositivo, es prohibido, y que debe tener permiso explícito para acceder o configurar y que todas las actividades realizadas en este dispositivo son registradas, que la información sale en inglés como en español; hay el texto en inglés y español, en la parte inferior está en español y que no puede traducir, pero parece que dice que el uso no es autorizado y pide el nombre del usuario y un prom que pide el nombre de usuario, esto significa que la oportunidad para que se ingrese al dispositivo, luego dice "time out" que quiere decir que se venció el tiempo y eso quiere decir que no hubo un intento de ingreso; hay solo ejecutado un comando y sale en la parte superior; un ejemplo de un comando ejecutado: TELNET es como un navegador de internet y la dirección IP es el destino al que se conecta la persona, el TOR SOR es el comando, es otra forma de utilizar TOR y TELNET para llegar a la dirección de IP y ver el Banner que salió que dice que no se conectó, el ejemplo sería que si caminas por la calle, llegas a casa y ves un letrero que dice no entrar, tú decides no entrar y sigues tu camino; que las de las acciones de la imagen se puede establecer que pasó? No tiene forma de saber que pasó, pero hay una frase en el banner que dice que todas la actividades realizadas en este dispositivo son registradas, entonces se puede ver esos registros, pero solo viendo la imagen es difícil saber si realmente esto ocurrió en algún momento; **al contrainterrogatorio realizado por Fiscalía responde que** experiencia tiene en telecomunicaciones?: depende lo que quieren decir por telecomunicaciones, como trabaja en seguridad de internet ha trabajado mucho en lo que es comunicaciones de internet, no ha trabajado en una compañía de telefonía; que la diferencia hay entre un sistema informático y uno de telecomunicaciones: estas dos frases dependen del contexto, si se habla del sistema informático se enfoca en datos y tráfico, el sistema de telecomunicaciones habla de infraestructura, cables etc.; conoce la infraestructura de telecomunicaciones de CNT: ha escuchado en contexto, ve en la imagen del Banner algo que dice Corporación Nacional de Telecomunicaciones, supone que eso es CNT; que no conoce que compone el sistema de telecomunicaciones de CNT; que como se aprende a programar?: dice que hay muchas posibilidades, en internet hay mucha información por ejemplo sobre criptografía, etc., y clases de universidad transmitidas por internet, donde se puede aprehender, hay conferencias de seguridad informática donde se comparte información y no se requiere de título universitario; la programación es una ciencia? Si hay una ciencia de programación, pero esto no necesariamente al revés, hay científicos que estudian programación, e ingenieros que la realizan, ambas cosas son útiles; el trabajo lo puede acreditar una persona que no tiene título, sobre esto tiene varias respuesta, revisión de pares, que una técnica común en la ingeniería de software libre, las personas miran el programa de otras personas y opinan, ayudan a mejorar los programas, tengas título o no, hay

compañía que venden certificados y acreditaciones, puede que se coleccionen varios de estos certificados, que no sabe si son buenos o útiles; TOR permite no identificar donde estás ubicado en el mundo, ni la identidad de quien lo utiliza, TOR permite que el usuario elija cual información compartir, se usa Facebook sabe quién es, pero no desde donde está ingresando, es una elección personal; que personas utilizan TOR: todo el mundo en todas partes del mundo, esa es la meta de la organización, para que las personas que no tiene la capacidad de pagar software, lo usan en Rusia donde el gobierno ejerce cierto control de información permitida, en EE.UU, en Europa y de todas partes del mundo; TOR tiene una restricción para determinar que está siendo utilizada para fines ilegales? TOR como cualquier software o cualquier navegador, la forma en que funciona es separado para que lo utilizan las personas; TOR puede navegar en la Dark Web: ese es un término de marketing, no sabe a qué se refiere con Dark Web; TOR puede navegar en la red oscura: es una frase inventada por los periodistas que quieren que las personas lean sus artículos, pero no sabe que significa hoy en día, que hay compañías que tratan de vender protección de la Dark Web, es un tema de ventas, lo hacen por marketing, no sabe a qué se refiere la red oscura, pero no se refiere a TOR; diferencia entre un experto en seguridad informática y un delincuente cibernético: el término de delincuente cibernético no lo ha escuchado, no sabe lo que es; la diferencia con un experto en seguridad informática y delincuente?: en cuanto al segundo término, entiende que es alguien que ha violado alguna ley, eso es un delincuente, realmente no ve la relación entre los dos términos; SHODAN es un programa de escaneo masivo de IP públicas?: entiende que sí es la meta de tener un mapa de ver como se ve el internet, conectarse con todos los computadores para ver si están escuchando y ver sus banners; sabe si Ola Bini ha sido contratado por una empresa ecuatoriana para el escaneo masivo?: desconoce; cual es la diferencia entre hacker y delincuente informático?: depende del significado de las palabras, si para ti un hacker es un delincuente informático, eso es una cosa, para sí para ti un hacker es uno ético, es otra cosa, hay que determinar porque la persona está haciendo lo que hace; que el hacker ético es de sombrero blanco, sabe a qué se dedica el hacker de sombrero negro?: hay personas que usan su entendimiento del internet, para hacer un lugar menos seguro, pero él intenta no interactuar con esas personas; si él se sentiría más seguro con un hacker de sombrero negro?: señala que depende a que se refiere, que él puede asegurar sus propios sistemas, le entristece que haya personas que hacen del internet, un lugar no seguro, es por eso que trabajan con TOR, para hacer del internet un lugar más seguro y por eso enseña sobre la seguridad y capacita a diferentes personas; en la fotografía que detalló, se puede verificar si hay algún usuario?: pregunta si la pregunta se refiere a que existe alguien que intentó ingresar al dispositivo o que se quiso correr el comando de TELNET; si alguien quiso ingresar al dispositivo?: dice que en la parte inferior de la imagen dice usuario, pero no hay ninguno indicado, luego hay una indicación que dice que el tiempo terminó, que la conexión es cerrada por el anfitrión, ese es el comando que da TELNET cuando ha terminado, lo que se demuestra en la imagen es que no hubo ningún intento de acceder; después de la terminación o cierre que se ve en la imagen?: hay un pront, que es algo que viene del computador local, que dice home/ola bini/ y parece decir 1005, en la parte superior de la imagen ese mismo pront también dice home/ola bini/1004, eso viene del computador local, de una laptop, pero son las líneas en el

medio que son del navegador de internet; en la imagen descrita al ocupar TOR se oculta la dirección IP de conexión? Hay lugares en el internet donde se puede aprender o conocer la dirección IP, en otros lugares no, hay una privacidad que se tiene con TOR, pero todavía se está conectando con el destino, aquí por ejemplo se tiene la dirección 181., que te indica que te estás conectando con un lugar correcto; al conectarse en esa imagen, la dirección del usuario desde donde se realiza la conexión es protegido, desde el servidor a dónde va la conexión, es decir que esa dirección de 181., ese dispositivo desconoce desde donde viene la conexión; señala que hay varias razones por las que se utiliza TOR, no es por seguridad o privacidad, es para realizar una conexión de otra parte del mundo, se puede utilizar para proporcionar evidencia de que el dispositivo está públicamente disponible, eso quiere decir que puedo conectarme a través de un relay, que puede estar en EE.UU, Alemania o donde sea, para documentar que el dispositivo esta públicamente disponible, seo lo puedo hacer utilizando TOR; aclara que no rindió versión ni presentó un informe técnico en la Fiscalía; **al conainterrogatorio realizado en defensa de la acusación particular responde que** sabe que son los sitios no indexados en la WEB?: hay compañías como Google y otros motores de búsqueda, que hacen un “crow”, para ayudar a las personas a buscar un sitio web que estén buscando, cuando se utiliza la palabra indexado, estás refiriéndote a eso?, sí; TOR permite navegar por lo sitios no indexados en la WEB?: si, si utilizamos la definición mencionada, si Google lo conoce se puede acceder de esa forma y se puede ingresar la dirección de IP y no importa si Google a indexado o no el sitio; que hay una característica en TOR, permite que el sitio web se configure para que los usuarios de TOR puedan navegar de forma segura, por ejemplo Facebook, Tuitter, y también la CIA, han establecido estas opciones, es una forma para hacer que el servidor de web sea más seguro para los usuarios de TOR y generalmente estas direcciones no se encuentran en Google; que entiende por indexar?: son motores de búsqueda que ubican sitios WEB y se da información sobre estos; la ONT es un equipo de telecomunicaciones?: sí, depende de cómo la red esté configurada, algunas tiene cables de fibra óptica, con adaptadores que convierten la información a internet o WIF; la dirección de IP pública es de acceso para todos? De acuerdo con la RPS 1918, quiere decir que es ruteable de forma pública, cualquier persona puede enviar tráfico a través del internet, ahora, si existe un firework, puede ser que no llegue ese tráfico, pero una dirección IP pública, es algo que es públicamente ruteable; **7) LINUS NORBERG:** de nacionalidad sueca, trabajador independiente en consultas informáticas; viven en Estocolmo; en cuanto a su experiencia en informática: trabaja profesionalmente, estudiando y ejecutando software, sistemas y administración; en cuanto a la privacidad?: dice que es el derecho y capacidad de controlar la información sobre mi persona; en el entorno digital como se garantiza ese derecho? hay dos partes, la primera legal, hay leyes que otorgan el derecho a la privacidad, los derechos universales de la ONU de la Unión Europea; la otra es mediante dispositivos y herramientas que combaten la invasión a la privacidad; ejemplos de estas herramientas? hay varias herramientas que se pueden utilizar, ejemplo en computación se usa teléfono el cifrado para asegurar que se comunica con la persona deseada, y terceros no pueda escuchar las conversaciones ajenas y hacer cambios en la comunicación; SIGNOS son mensaje de textos, TOR sirve para proteger la información de quien habla, con quien y lo que se está conversando; el

software libre, es una forma de licenciar software para que cualquier persona lo pueda utilizar, para comprender como funciona y hacer mejoras; que existe un movimiento de personas que quieren aprender más y compartirlo con sus pares; este software es usado por mucha personas para casi todo lo que hacemos en el internet, se usa el software libre en casi todas las cosas, uno de estas formas es el sistema operativo Linux; que es un investigador de seguridad en internet?, es un caso especial de personas interesados en la informática, de tratar de entender que es lo que está mal en el computador y tratar de arreglarlo; que es un Hacker? existen dos definiciones, alguna vez se conocía como alguien estaba interesado en cómo funcionan los computadores, con el tiempo se la conoce como el que abusa de su conocimiento para hacer cosas malas, aclarando que muchas personas recurren a la primera definición; que es el hacking ético?: este es un término para referirse a personas interesadas en el computador, para realizar cosas éticamente buenas, para asesorar a compañías con mala comunicación en línea, para tener equipos más seguros, ante una internet más insegura, así se beneficia todos; la IANA: es una organización que vigila que todos los números o su mayoría, para que el internet pueda funcionar, se refiere a las direcciones de red que permiten a las máquinas interconectarse, vía internet, básicamente es un registro; que es la IETF?: ha formado parte de esa organización, escribiendo una estándar para que todos los dispositivos puedan inter operar para que el internet sea algo útil; que es una dirección IP: es un número único que identifica cuando se conecta al internet, hace posible que otros dispositivos se comuniquen utilizando un paquete de internet; conoce el estándar RFC 1819: RFC son estándares de la IETF, el número hace definir algunas direcciones que no se utilizan públicamente, sino que están siendo utilizadas para enrutamiento interno y que esas comunicaciones no sean enviadas al internet; cuales son estas IP reservadas para el uso privado?: hay tres dentro del RFC 1818, el uno es 10.0.0.0/8, el otro es 172.16.0.0/12, sin estar ciento por ciento seguro, y el tercero es 192.168.0.0/16; si una red no corresponde a esos rango es dirección pública, ruteable para llegar a dispositivos públicos que están en el Internet; que se necesita para conectar dos dispositivos al internet?: se necesita que los dos tengan direcciones IP públicas, pero no es siempre así, lo que pasa es que la comunicación ocurre de un extremo al otro, uno inicia la comunicación y el otro recibe, este último necesita tener una IP pública, mientras que el que inicia la comunicación no necesita una IP pública; como viaja la comunicación de un extremo al otro?: funciona así: el extremo que inicia va a ingresar la dirección pública del receptor y se pone el destino dentro de un paquete IP y también pone el origen de la dirección IP, lo manda por internet y es ruteado como tipo servicio postal, es decir por cada estación por la que pase, va a ver que el destino del paquete es una IP pública, entonces la va a mandar por su ruta, luego para mandar una respuesta el receptor va a hacer el mismo proceso pero al revés, entonces va a poner como destino la dirección IP del que originalmente mandó el primer mensaje y la IP del destinatario original ca a ser como la primera fuente u origen y lo manda por internet; para que un paquete viaje desde el origen al destino, físicamente se necesita que un dispositivo esté conectado a otro, y ese otro a otro, y así sucesivamente, hasta llegar al destino generalmente por medio router con diferentes vínculos, se requiere además cables de cobre para enviar datos, también hay la posibilidad de utilizar un vínculo radial pero no tan usado en internet, siempre y cuando haya un flujo libre de

comunicación entre el dispositivo de origen y el del destino, puede haber comunicación; en la comunicación que tenemos, como se accede a esos dispositivos? Debe haber una conexión y un flujo al menos desde su computadora hasta la de ustedes, para poder enviar los paquetes y de esa forma tener la conexión, pero eso no es acceder, pero para enviar un paquete a Quito por bus o camión, no es que el paquete va a topar el suelo, no accede a esos lugares, lo mismo sucede en internet; Que es una ONT? Adivina que es algo como red óptica, si es lo que creo, traduce entre las redes ópticas y otros medios como los cables de cobre, como conectar una fibra óptica a una casa; RED ONE: es una red de área ancha, término que se utiliza como opuesto a la LAN que son redes locales; dos tipos de redes que la una es local y otra de área amplia, eso se utiliza para conectar dos ciudades o dos países; puede una red privadas ser parte de una red LAN, sí; que tipos de IP se conecta a esas redes?: lo que se podría decir es que una red de área amplia, tiene direcciones públicas y las de área local tiene direcciones privadas, pero puedes tener una compañía muy grande con oficinas en dos ciudades, y se puede tener red privadas en las dos ciudades: FIREWORK: es un dispositivo para filtrar el tráfico entre lo que ingresa o salga de una red; que es el escaneo íntegro del internet?: es apuntar a cada una de las direcciones IP que están en el internet, para averiguar cuáles son los servicios proporcionados; quien lo hace?: esto es realizado por investigadores de seguridad o servicios como SHODAN, que proporcionan a los motores de búsqueda con las direcciones IP que están en la Internet; que es TOR: es una red sobrepuesta por encima del internet que ayuda a los usuarios para que se mantengan privados y menos vigilados; quienes lo usan? Son personas que han entendido que es tan fácil ser vigilados cuando están en internet y usan TOR porque quieren navegar seguros en internet; se puede usar TOR para conectarse a una red pública?: TOR sirve solo para conectarse con IP públicas; en qué circunstancias una conexión, utilizando TOR, pase por una ONG?: cuando se utiliza el internet el tráfico pasa por ONT, por un switch, por otra conexión o por otra capa, como un paquete que viaja por todo el mundo, no puedes saber en qué parte de tierra, aire o mar, pasa el paquete; IFF es una organización responsable de emitir estándares sobre dispositivos, él trabajó para esa organización como experto en software de computación y redes; que derechos precautelan las herramientas como TOR?: sería el derecho a la privacidad y libertad de expresión, te protege de la vigilancia masiva, otorgando formas de poder expresarse sin tener riesgo, para permitir una discusión abierta sobre tus opiniones; cuan es la Institución que hace respetar los derechos humanos en el mundo?: a nivel local en su país, protege sus derechos el Acta Constitutiva de la Unión Europea, que a su vez se deriva de las resoluciones de la ONU sobre derechos humanos; que el sistema operativo TELPS es un sistema pre-configurado con herramientas como TOR que ayuda a los usuarios a mantenerse seguros en el internet; quienes lo usan?: mucha gente que se ha dado cuenta de que el Internet es un lugar peligroso; que tipo de sistema es?: es una versión de sistema operativo libre y abierto, basado en LINUS, el usuario puede inspeccionar el código fuente para saber si es seguro; tipos de dispositivos hay para autenticarse?: un dispositivo Llubique se utiliza en un puerto en USB, identifica a una fuente para utilizar las misma tecnología; quien lo usa?: lo utiliza toda persona que se preocupan por su seguridad en línea, los usan personas comunes, ha llegado al mercado más amplio, Google lo impulsa para que llegue a más personas; que es la criptografía en

el ámbito digital?; es el uso de las matemáticas para la autenticación; que es la encriptación de discos duros?: técnica para asegura discos duros, para que no sean leídos por alguien que no sepa la clave de seguridad; si hay varios tipos: el cifrado se divide de varias formas: una es la simétrica y otra la asimétrica; la simétrica es una clave compartida por ambas partes para poder leer el cifrado; otra es cuando tienes una clave pública encriptada, esto tiene una clave pública y una parte privada de la clave y la parte que va a leer el material cifrado, tiene la parte privada y tú tienes la parte pública; dice que conoce a Ola Bini, 10 años, lo conoció en Estocolmo en el año 2012, son del mismo país y él es el fundador de una de las organizaciones de derechos digitales, Ola está interesado en este tipo de temas, los dos son desarrolladores de software libre; Ola Bini, cuáles son sus credencial profesionales?: sabía de él, cuando se conocieron era Ola medio famoso en Suecia por haber desarrollado un desarrollador de web en ese entonces; sobre este caso que conoce: conoce que Ola es acusado de acceder a un tipo de sistema informático y lo que conoce es que existe una imagen de una laptop que presuntamente es de Ola, se observa alguien conectándose a un sistema informático, se ve que la conexión cae, quiere decir que el sistema se cierra; como conoció la imagen?: la vio en el sitio web de EFF, que es una fundación de derechos digitales, cuando llegó el caso a ojos del público, esto fue como en el año 2019; de la imagen cuál es su descripción?: de la imagen se ve una conexión a un sistema vía internet y este sistema responde con un banner que dice CNT, que entiende que es la compañía nacional de telecomunicaciones, ese banner dice que el acceso no autorizado es prohibido y sale un prompt que pide usuario y password, en el nombre de usuario no se ingresa nada y el sistema remoto cae luego de un tiempo y la foto muestra que el usuario regresa al prompt; existe en la foto un FIREWORK?: no; existe la ejecución de un comando TELNET si, TELNET es un protocolo de comunicación de 1970, protocolo viejo que ya no es utilizado porque no tiene cifrado, no protege el nombre de usuario y el password para ingresar, es susceptible a que se pueda robar el nombre de usuario y el password, no se utiliza si una persona es interesada en seguridad; que se necesita para conectarse en TELNET?: el comando Telnet, el cliente necesita una dirección IP pública, en un dispositivo conectado al internet; vio en la foto una dirección IP?; sí; que tipo de dirección es: es una dirección IP pública que comienza con 181, eso quiere decir que no está dentro de los tres rangos de la RFC 1918; que es un prompt y que contenía?: en la foto sí había un prompt, que es la forma en que el computador indica que es tu turno para responder, indica que está esperando tu comando, que el prompt le recordó algo de Ola Bini, dice que en la foto hay un [/home/olabini] (un número de 4 dígitos) landa, landa es un signo utilizado para indicar que es el final del prompt; que /home/olabini, eso indica que de que alguien tiene una carpeta de nombre Ola Bini/home, esto es utilizado en los sistemas LINUX para indicar donde se guardan los archivos; si el PRONT puede ser configurado?: sí, es lo que se hace, entonces mi prompt puede indicar cualquier cosa como /home/santaclose/, /home/linus/, etc.; hay un número junto al nombre Ola Bini?: Sí, el número 1005, parece, supone que es la ID del último programa que se corrió en ese computador, se puede configurar el prompt indicando donde uno se encuentra y la identificación del último programa que se corrió; cuando comandos se ejecutaron en la fotografía?: un comando que fue ejecutado por TELNET; se solicita un usuario?: el sistema al que se conecta solicita nombre de usuario, pero no se proporciona

ninguno; que el tiempo concluyó que significa?: cuando se solicita información hay un límite de tiempo, luego deja de intentar y se cierra, caduca después de cierto tiempo, no se sabe cuánto tiempo transcurrió, lo que se ve es que no recibió usuario y contraseña; **al conainterrogatorio realizado por Fiscalía responde que** en cuanto a su experiencia en telecomunicaciones: ha trabajado por 13 años con la red nacional de educación con Suecia, que es una organización paraguas que ayuda a dar internet a los 5 países nórdicos; diferencias entre un sistema informático y uno de telecomunicaciones?: en el sistema de las telecomunicaciones estamos hablando de las líneas de cobre, de las fibras, es decir son las capas inferiores, en cambio cuando hablamos de las redes informática, hablamos de las capas por encima de la capa física, como la capa 3, como los protocolos de internet, que son las IP; conoce el sistema de telecomunicaciones de CNT?: específicamente ese no conoce; la herramienta TOR tiene restricción que detecte que se usa para fines ilegales?: tiene el mismo número de formas de detectar que su uso es ilegal, como todo las cosas en el internet, ese número es cero; el hacking ético debe ser contratado?: realmente depende lo que se entiende por ético, el hacking es la intención de ayudar, si eres contratado o no, si lo haces es ético; la herramienta TOR precautela derechos como el de la privacidad y la libertad de expresión?: Es su opinión o consta en una norma jurídica? Le parece que la herramienta no sale en ninguna norma legal, pero un reportero de derechos humanos de la ONU dijo en 2015, dio que la herramienta TOR como otras, son esenciales para proteger los derechos humanos básicos; rindió versión en el proceso?: No; presentó algún informe técnico a la Fiscalía?: No; **al conainterrogatorio realizado en defensa de la acusación particular responde:** cuál es la función técnica de una ONT: es la que convierte señales ópticas que pasan por un cable óptico, a las señales que están pasando por otro medio como por ejemplo el internet; es utilizado en los sistemas de telecomunicaciones para servir en la comunicación de las redes informáticas, funciona como el asfalto en las vías; en la fotografía el pront es generado por un router?: la pregunta no está calara; **8) DENNIS ROGER:** de nacionalidad Italiana, residente en Ámsterdam, con un grado PHD; dice que es oficial técnico de la organización DINE, en la que maneja y dirige el desarrollo técnico de la parte de software, además es un criptográfico aplicado, desarrolla sistemas de autenticación, en los últimos 6 años se ha enfocado en como los datos de los ciudadanos pueden ser protegidos y procesados por los sistemas digitales, trabaja en dos municipios, uno de ellos es Ámsterdam, también realiza asesoría política sobre temas técnicos; que es la privacidad en el campo digital?: básicamente significa la voluntad de revelar información o no revelarla, es la cuestión y libertad de una persona, privacidad es que no voy a revelar los datos cuando no lo quiero; un ejemplo de esto es como como nosotros elegimos compartir los datos médicos sobre nuestra salud, cuando elegimos compartirlo los datos privados con los médicos, porque ellos nos curan, pero no los compartimos con las aseguradora, porque ellos utilizaran la información para hacer que el seguro sea más caro; que cuando se habla de privacidad la importancia de elegir dentro de que contexto compartir la información, en el campo digita, esto se hace cada vez más difícil, porque cuando compartimos información, luego no la podemos recuperar y es muy fácil duplicar esta información por lo tanto en el ámbito digital el tema de privacidad se torna aún más compleja; que es el Software libre; es un movimiento ético basado en cuatro principios, la libertad de correr aplicaciones, de estudiarlas, verificarlas y distribuir las

modificaciones; es decir que un software libre es uno escrito públicamente para poder leer el código y entender que mismo hace este software y la idea detrás de esto, es que las personas solo debería correr el software que ellos eligen correr, de manera consensuado; cuales son las herramientas que protegen la privacidad?: dice que él trabaja con este tipo de herramientas, que se usan con diferentes técnicas matemáticas, para adquirir esa privacidad, algunos ejemplos, GPG que es un software de privacidad, TOR que es utilizado para cubrir conexiones de red, BPN que es una red privada virtual, que se utiliza también para comunicarse de forma privada a través del internet; no es necesario tener título académico para trabajar en eso, él tiene un PHD en filosofía, cree que las personas que tienen conocimiento sobre programación han tenido acceso a las computadoras y que tienen una pasión, no tanto por su título académico sino basados en su capacidad real de hacer este tipo de trabajos y entiende que otras organizaciones escogen a sus empleados de la misma forma, es además muy difícil para la educación formal tener información actualizada, porque lo que se utilizaba hace 10 años, ahora ya no se lo utiliza porque la información evoluciona y como anécdota señala que él tuvo acceso a computadores porque sus padres tuvieron una tienda de computadores, y fue ahí que empezó a hacer programación, aclarando que este tema va vinculado a lo que es el software libre, para conocer quién es la persona que escribió el software, de esta forma podemos saber quién es bueno en este tipo de temas, es mejor revisar el código para saber programar, que revisar un título; IANA: es una institución de asignación de direcciones IP públicas en el internet; IATE: es una publicación que él le sigue en sus publicaciones, ellos no solo asignan direcciones IP sino que generan estándares y protocolos para el internet; una dirección IP: es la secuencia de varios números que va del 1 al 254, separados por un punto, son las direcciones IP públicas, que son las máquinas que son públicamente alcanzables, es algo que se llama la versión 4; existe además la versión 6, hace 20 años nadie se imaginaba que en el internet habrían tantas máquinas, sin embargo lo más conocido es la versión 4, son 4 números con combinaciones; ciertos número son reservados para redes privadas; señala que el estándar que define a las IP privadas según la RFC es 1918, tiene claro cuáles son los números IP privados, hay tres clases, una es el 10.0, otra el 172.0 y la tercera es 192.168 estas son de redes privadas; en cuanto a la infraestructura de telecomunicaciones: es cualquier infraestructura que permite comunicar uno con uno o uno con varios, hay muchas formas de definirlo, la genérica en ingeniería dice que son las diferentes capas, 7 diferentes capas de infraestructura de telecomunicaciones, es algo muy complejo; menciona además el modelo del ISO, que define como es la ingeniería de telecomunicaciones, que tiene 7 diferentes capas, es algo que tiene muchas diferentes partes para comunicar, abarca tanto los cables físicos, la antena hasta nuestra propia pantalla; que es una ONT: no reconoce porque no lo utiliza dentro de su trabajo; que es un ROUTER: si conoce, sirve para distribuir una red en una configuración de internet, básicamente lo que hace es enruta un paquete entre diferentes máquinas, para conectar más de una maquina sin cables, se podría poner un router en medio de unas máquinas, pero lo que se conecta son los cables al router; que es TELNET: es una forma antigua pero activa de conectarse con una terminal por red en el internet; lo utilizó en 1994 para conectarse con su universidad, se conecta mediante un texto sencillo, se conecta solo con texto, se llama teletexto, ahora es menos utilizado por su falta de

protecciones, el día de hoy se utilizan otras formas con la mismas funciones pero es más protegido, cuando se utiliza Telnet todos es público, se puede escuchar lo que se habla o comparte; que se necesita para que dos terminales se conecten por Telnet: se necesita que una persona tenga un programa de TELNET para escuchar y un cliente que se conecta, es muy común así no se haya instalado TELNET, básicamente es un sistema que uno que escucha y otro que habla; existe posibilidad de encontrar todos los puertos abiertos de Telnet?: si en las direcciones públicas esto es posible porque el puerto 23 es lo que controla el puerto de TELNET, si está abierto se puede conectar, son las dirección IP versión 4, se puede verificar si el puerto 23 está abierto, si está abierto la conexión está abierta, es cuando se va a recibir un banner que describe el sistema, luego se decide que es lo que se quiere hacer; que es utilizado por investigadores de seguridad, revisan las IP públicas para ver cuales están abiertas y las pone en un página, para investigaciones de seguridad, revisa las dirección IP usando se va a recibir un banner, se verifica si está abierto el puerto 23; el banner es para quien describe el sistema: se lo describe para que la persona que se conecta, es como un sitio web, abres el sitio web y el sistema lo muestra, la primera cosa que se recibe en una web, o en este caso el banner, si no ves el banner ni la página web, no sabes a que te estás conectando, básicamente un banner es lo mismo que una página web que utiliza el puerto 80 y contiene imágenes, mientras que el banner que ocupa el puerto 23 y solo contiene texto; SHODAN: esto es utilizado por investigadores de seguridad y hace lo que ya mencionó que es revisar las direcciones IP públicas para ver cuales están abiertas y las enumera en una página, es utilizado básicamente para investigaciones de seguridad, revisa las direcciones de IP; que es FIREWORD: es un sistema que bloquea conexiones desde afuera, van al puerto donde quieren conectar y pueden bloquear esa conexión, para decidir si una conexión puede pasar y conectarse con un computador; es importante entender los criterios de que si puede pasar la conexión o no, no hay ningún logging ni contraseña ni usuario, es para verificar si dos sistema pueden conectarse y esto depende de la dirección IP y el puerto, cualquier logging ocurre posterior a eso; que es TOR: es un sistema lo que permite es una conexión privada a través del internet, cuando habla en privada puede ser que considere la conexión entre los usuarios, el internet de afuera no lo conoce, esto en su trabajo, tienen redes de computadores entre la Comisión Europea, entre las diferentes máquina, entonces estas comunicaciones permiten que sean privadas con respecto al mundo, porque cuando se están creando conexiones que comparten datos privados de los ciudadanos, hay mucha responsabilidad involucrada, en Europa tienen reglas muy estrictas sobre la privacidad de los datos, entonces hay que asegurarse de que toda conexión sea privada; quien usa esa herramienta: él lo utiliza, conoce gente que la utiliza esta herramienta, donde hay censura del Internet: por ejemplo: puedes imaginar conectarse al internet en un proveedor en el que no confías, entonces no sabes si lo que estás viendo en la página web realmente es cierto, entonces utilizando TOR te lo que puedes hacer es conectarte desde otro lugar, para ver si conectándote desde otro sitio estás viendo la misma página que estabas viendo tú, entonces por ejemplo cuando tienes un ataque malévolo, lo que hacen esos atacantes es cambiar lo que tú estás viendo en está en la página, que es lo que se conoce como Fishing, conectarse desde otro lugar sirve para verificar si ves lo mismo desde los dos lugares, esto se utiliza cuando hay mucha vigilancia por

los gobiernos, señala que ha trabajado por algún tiempo como voluntario, en donde los activistas que estaban en Irán e Irak, utilizaban TOR para poder escribir en los block para saber lo que ocurría; se puede utilizar TOR para conectarse a direcciones IP?: si, a cualquier IP pública; a las privadas no, es imposible, salvo que pueda entrar a través de una IP pública; la otra opción es que si estas conectado a una red privada y dentro de esta red privada hay un TOR que te permite entrar; TOR vulnera sistemas de seguridad?: no, la herramienta existe para proteger una conexión; que pasa cuando TOR se conecta a un sistema?: con TOR o sin TOR pasa exactamente lo mismo, pero con TOR la conexión va a través de una red protegida, pero pasa lo mismo que pasa con un navegador de internet, TOR es solo un medio; cuando accede a un dispositivo, hay un registro?; si un dispositivo tiene un registro, la conexión es registrada; que es el cifrado simétrico: es un sistema de cifrado protegido con contraseña, entonces existen datos y para poder leer esos datos se tiene que poner una contraseña, pero esa contraseña puede ser interceptada, por eso se llama cifrado simétrico; hoy se utiliza el cifrado asimétrico por ser más seguro; señala que sí conoce a Ola Bini, desde hace 6 años, lo conoció en el año 2016; en qué área?: lo conoció porque él estaba en el directorio de un proyecto en Europa, de tecnología descentralizada de participación de ciudadanos, proyectos de privacidad ciudadana y datos, financiados por la Comisión Europea, él estaba trabajando en una compañía que era socia de un proyecto en la coordinación técnica, estaba muy feliz de trabajar con él, porque había visto que era un coautor de varios tipo de software importantes, en este proyecto estaban desarrollando algo en el cual él le ayudó para darle asesoría para el desarrollo de un idioma informático, que es su especialidad; Ola Bini se dedica a desarrollar software y es investigador de seguridad, como desarrollar de software, por eso lo extrañamos muchísimo porque fue muy útil el en proyecto que fue un proyecto emblemático para la Comisión Europea, y otro proyecto que tenía que ver con la privacidad de datos, financiado para la tecnología Long Gene, hoy en día la Comisión Europea está invirtiendo mucho más en esta tecnología y ellos fueron los pioneros en este tema, su proyecto; no sabe porque está enjuiciado el señor Ola Bini; ha visto la prensa sobre este caso?; ha visto artículos en el EFF que es una organización dentro de los EEUU, le sorprendió ver que estaba en problemas y no sabe cuál es el crimen que supuestamente cometió; varios artículos hablan que tenía una imagen que mostraba una conexión con un banner y una desconexión, lo que él entendió es que supuestamente se muestra una sesión de Telnet, no recuerda más sobre el tema; señala que en la imagen descrita si hay una dirección IP versión 4, que es una imagen que contiene texto, es una IP pública; que es un comando?: hay un comando telnet a una dirección de IP y luego una desconexión, lo que es muy complejo hacer esta conexión, hay que hacer control corchete, pero la desconexión acontece inmediatamente, pero asumiendo de que esa imagen sea una auténtica, de lo que no hay evidencia en ese sentido; aclara que está hablando de memoria porque no tiene la imagen, lo que recuerda es que hay una conexión de Telnet a través de TOR, hay una IP pública y hay un banner que dice CNT, banner de texto que dice básicamente que el acceso es no autorizado, entonces informa de una conexión y luego una desconexión, se acuerda que decía que la conexión se caducó; que es un PRONT?: es lo que aparece en el terminal cuando es abierto; en la imagen había un PRONT?: Si recuerda decía algo de Ola Bini en el comando, lo que muestra es un directorio

donde está, lo que vemos es un comando que fue tipiado dese una carpeta que dice Ola Bini; el directorio que contenía?: de la imagen solo se ve el nombre del directorio, no sabe lo que tendrá dentro, del pron lo que recuerda es que tenía la letra landa y solo tenemos el nombre de un directorio; **al conrainterrogatorio realizado por Fiscalía responde** que experiencias tiene en sistemas de telecomunicaciones?: ha trabajado con sistemas Unics que son de telecomunicaciones, más de 20 años, hoy lo que trabaja más es en construir sistema seguros de telecomunicaciones, trabaja para gobiernos, en el sector público, tiene una buena experiencia, pero su campo especial es la criptografía y software, conociendo menos de la parte física; en cuanto a la diferencia entre un sistema informático y uno de telecomunicaciones, dice que en un sistema informático se entrega información a un computador, en cambio el sistema de telecomunicaciones entrega información a cualquier otra cosa, podría ser un teléfono; conoce el sistema de telecomunicaciones de CNT del Ecuador?: no conoce mucho del nombre, entiende que es telecomunicaciones nacionales, asume que tiene los estándares mundiales; sobre la herramienta TOR, sirve para ocultar la información de quien lo utiliza?: es posible ocultar la procedencia u origen del conector; si utilizando TOR se puede identificar la IP real de quien quiere conectarse?: no es identificable el origen de la IP, porque la conexión se da a través de otra máquina; rindió versión en Fiscalía en esta causa?: no, ha tomado más de dos horas de su tiempo para contestar en base de su conocimiento; ha presentado algún informe: no; **9) DAVID RAFIC MIRZA AHMAD**; ciudadano de nacionalidad canadiense, bachiller; Presidente de una Compañía de Seguridad Informática; en cuanto a su experiencia dice que es profesional desde 1998, realiza pruebas de penetración, pruebas de seguridad de los sistemas, revisa arquitectura de seguridad, asesora a Gobiernos para seguridad informática; en cuanto al tema de la privacidad: señala que es la capacidad para controlar lo que las personas comparte sobre sí mismo; en cuanto a la privacidad digital señala a las herramientas para protegerla, teniendo principalmente herramientas que no son fuertes, pero hay oras como BPN, TOR, utilizadas con frecuencia para mantener privacidad en línea: en cuanto a que es TOR, señala que esta es una herramienta para mantener la privacidad que tiene componentes de la red, si no deseas mantener el origen, se tiene un navegador, herramientas más conocidas y confiadas desarrolladas por académicas con auspicio del gobierno, incluso la ONU; señala que otro tema es que TOR es gratuito mientras que BPN tiene consto; que es el software libre?: es un movimiento político y social para crear software gratuito, entendido para todos con disponibilidad de la fueete, creado por seguridad, desconoce que contiene, por eso el software abierto genera más confianza; se necesita título para desarrollarlo? No, es una de las ventajas es que cualquier persona lo puede leer y aprehender, él lo aprendió del movimiento del software libre, se puede crear su propio software y programar; dice que a veces utiliza TOR en su trabajo, lo utiliza o prueba redes para ver cómo se ven las herramientas de afuera, lo que le permite hacer TOR, que es uno de sus usos; que es IANA: es la organización que asigna los números de internet, es la autoridad de asignación de números de internet; AITF: es un agrupo de ingenieros que publican las especificaciones técnicas para el internet; que es una dirección IP: es un número único asignado a un computador y a una red como un número de teléfono; sirve para transmitir paquetes de información en el internet, si deseo comunicarme con alguien necesito su dirección de internet, para realizar una dirección y tengo como destino la

dirección IP; afirma que son documentos que contiene las especificaciones del internet, como las leyes del internet, que se tiene que seguir para poder comunicarse entre sí; el estándar 1918 es un documento que define las direcciones de IP internas, en comparación de otras designadas para el espacio públicos; cuales son las IP privadas: tienen tres rangos; para organizaciones comunicacionales privadas, si se intenta comunicarse no se lo puede hacer, no permite que los paquetes sean entregados en redes internas; cuáles son sus rangos: son tres rangos: 192.168, cuatro números separados por puntos; el 172.16 y el último empiezan con 10., que son redes internas; que son infraestructuras de telecomunicaciones?: para él es aquello físico, que está debajo de un número IP, son los cables, puertos, interruptores, ruteadores; es el equipo necesario para conexión: tienes conexión IP, que son como abstracciones, de forma física son cables de cobre, fibra óptica, router, interruptores y diferentes cables; cuantos dispositivos se tiene que pasar para una conexión?: la verdad que es arbitrario, puede que por ninguno, en una red del hogar o por muchos, la infraestructura no es aparente para el usuario, puede cambiar de camino, la persona que está haciendo la conexión no tiene que saber el camino; que es una ONT?: es una interfase física, el computador se conecta con una óptica a través de puerto físico; que es óptica: fibra óptica es una tecnología física de comunicaciones, lo hace por medio de pulsos de luz a través de cables de vidrio, es diferente a los métodos tradicionales como cables de cobre; que se conecta a la fibra óptica? router, switches, estructura de telecomunicaciones de bajo nivel, por debajo de las comunicaciones del internet; da un ejemplo: en una calle pavimentada, debajo está la tierra y por encima se vierte el asfalto, la IP es como ser la parte pavimentada de la vía; TELNET; es un protocolo que se utiliza para conectar un computador con otro, con servidores, ahora TELNET ya no es muy utilizado porque es muy expuesto; es realmente no utilizado porque es algo no cifrado; la norma IZO 27001: es una norma de controles de seguridad, tiene información sobre controles de seguridad; esta norma sobre TELNET está en la sección 13, describe que tener instalaciones de internet es seguro, lo que hacemos creamos una matriz de verificación de pruebas, la norma dice que para las comunicaciones seguras y la información segura, hay un marco de control y guías como se debe bloquear a servicios como TELNET; hay ciertos dispositivos antiguos que no pueden correr protocolos más avanzados en sus redes, y usa TELNET si es absolutamente necesario y si está en un red pública; aclarando que si él lo estuviera investigado, lo reportaría como una inseguridad; hay como saber cuántos puertos Telnet existe en el internet?: señala que hay organizaciones que escanea el internet, como el SHODAW, hay otras como la herramienta de escaneo masivo; para que se utilizan los servicios de escaneo? Es utilizado para reunir estadísticas y medir el internet, tiene varios usos, puede haber el impacto de un ataque, para medir el impacto, hay compañías que toman fotos satélites de todo el planeta y de forma similar permiten ver todo el internet; otro ejemplo sería como los datos de mapa abierto de google, donde salen en un carro donde toman fotos de las tiendas, es muy similar, un análogo físico; que es un FIREWALL?: es como una cerca que se pone en una red que restringe el acceso, puede bloquear las comunicaciones, es esencial para controlar su exposición porque el internet está escaneado; para que se usa TOR: hay muchas razones, nos permite utilizar el internet desde otra IP, para ver una red desde otra perspectiva, para verlo como un extraño; se usa para conectarse a internet? es uno de los uso de TOR, es

una capa de red que mueve el tráfico, también tiene un navegador, también hay un sitio web que solo tiene TOR; que restricciones existen para conectarse por TOR?: señala que TOR es lento y hay muchos nodos de salida que controlan como se puede salir, por ejemplo como ingresas con TOR y regresas al internet se unen a la red de TOR para ir a través de ellos, para llegar y salen del internet por los nodos; a que direcciones IP se puede conectar con TOR?: Solo se puede conectar a las direcciones que están en el internet, no a direcciones privadas, solo públicas; aclara que TOR opera a una capa o nivel que ni tiene visibilidad, la salida de TOR salen en un nivel donde no hay visibilidad; que cuando se utiliza TOR se ingresa y sale con TOR a nivel de IP, no es algo que eliges, es algo que hace TOR por sí solo, es como un túnel de IP a IP, no sabes a dónde vas a salir, no sabes cuál es la dirección de IP por donde vas a salir y diferentes direcciones de IP tienen varios caminos por donde puedes salir y no tienes visibilidad; que es CRIPTOGRAFÍA?: es la ciencia de crear super códigos, ciencia para códigos para que destinatarios no puedan leer mensajes, básicamente son códigos severos; la RED ONE?: es la red de área amplia, generalmente de una misma organización, pero puede estar en internet público; red LAN: es una red área local, generalmente privada, en un edificio, en una oficina, para conectar la impresora, direcciones privadas; que tipo de direcciones IP puede ser asignadas a estas redes? Casi siempre son privadas que salen en el aire; a la RED ONE, que IP se asignan?: en una red ONE público o privado, por eso puede ser cualquiera, hay limitaciones para las IP públicas; responde que conoce a Ola Bini desde el año 2013 y sabía de él antes de esa fecha, porque es un miembro importante de Software Libre y ha contribuido a su desarrollo, software que utilizan muchos de sus clientes, no puede dar los nombres, pero es uno de los bancos más grandes de los EEUU, además que lo utilizan muchas compañías, lo utilizan estos módulos los gobiernos, universidades, es un lenguaje que se llama RUBI; que ahora muchos programadores utilizan este lenguaje; junta estos dos mundos por esto ha sido muy útil, es muy popular; señala que Ola Bini se dedica a trabajar para una compañía de software que desarrolla el software libre; entiendo que estaba trabajando con ecuatorianos en ese ámbito; que significa la palabra Hacker: pude ser una palabra difícil traducción, no hay una definición acordada, la mayoría dice que es el uso capacitado del computador para resolver problemas; Hack es algo muy inteligente o solución a un problema, está lleno de atajos a los problemas; entonces refiere que la palabra hacker hace que un programa funcione más rápido; porque Ola Bini esta enjuiciado? Tiene cierta comprensión, ha leído algunos artículos, también se filtró una foto en el 2019, siendo especialista no evidencia que haya habido una instrucción en la fotografía; describa la fotografía: parece que tiene la foto una pantalla de terminal de un computador y parece que indica una línea de comando, luego sale una advertencia, pero no hay intento ni acceso al sistema informático, hay una captura de pantalla donde se muestra que la conexión caduca; en donde queda el registro del acceso a un dispositivo?: eso realmente depende del dispositivo; que es la IP en internet? Es una dirección de IP que no estén dentro de las direcciones privadas es decir que están en el internet público, ruteables, a las direcciones que no estén dentro de esos rangos privados y restringidos; la imagen dice que es una fotografía, porque lo dice? Lo dijo porque se puede ver un reflejo cuando se toma a la pantalla o hay un reflejo; como se puede verificar de la foto, que esa acción se dio?, no se puede verificar, salvo otra información para que se corrobore como un

archivo de registro; **al conainterrogatorio realizado por Fiscalía responde** que si conoce la diferencia sistema informático y de telecomunicaciones: dice que las telecomunicaciones de cierta forma son informáticos, la diferencia de que telecomunicaciones se relacionan con Hardware, mientras que el sistema informático tiene que ver con Software, pero ambos son sistemas que procesan información; que la mayoría son computadores en algún sentido de la palabra; conoce sistema de telecomunicaciones CNT: si sabe de su existencia, pero no tiene conocimiento profundo; con la herramienta TOR se puede ocultar la dirección de quien la utiliza? Si, pero a veces uno quiere utilizar las otras características de TOR, como analista recibe un correo y tiene una página; lo que uno hace es probar los URL utilizando TOR; que si rindió una versión en el proceso investigativo? NO; no presentó un informe técnico tampoco; **al conainterrogatorio realizado por la acusación particular responde** sobre su conocimiento en redes y telecomunicaciones que él realiza pruebas de seguridad de redes, es programador, escribió un código de red, que él realiza prueba de seguridad de redes; afirma que las telecomunicaciones no es el área de su experticia; que la ONT es una IP, si se utilizó una ONT no es posible saber, pero en este caso es de la parte informático no a nivel óptico, lo que Irrelevante porque no hay forma de conocer si se lo utilizó; es una fuente entre los dos entonces en ambos; tecnología GPON: no la conoce, tiene que ver con la fibra óptica; que no sabe si en la tecnología GPON ES esencial la tecnología, no lo sabe; que las capas del sistema de comunicaciones, de cuantas capas está conformada? No sabe exactamente pero cree que existen 7 capas, pero no siempre existen las 7, puede haber más o menos capas, que tipos de capas? Que puede tratar de enlistar estas capas, pero aclara que no la utiliza a diarios, la capa de enlace física, redes de transporte etc.; que la IP está en la capa de la red, el internet en la de la red por debajo la capa del enlace; **10) Testimonio del procesado OLA METODIOS MARTIN BINI**, de nacionalidad sueca, de 40 años de edad, de estado civil divorciado, de instrucción secundaria, con pasaporte No. 92344157; de ocupación director técnico en una organización sin fines de lucro y con domicilio en la calle Juan Dijuga No. Oe2-30 y Voz Andes en Quito; Gracias por la atención, esta no es una situación fácil para él, hace 4 años a mí se me destrozó mi vida, desde entonces he recibido terapia para tratar el síndrome de post estrés, pero como se puede escuchar por la denominación post, es que ya no sigue, pero como escucharan muchas de la causas del estrés que tiene, siguen en pie en la actualidad; lo está diciendo para que vea que a ratos es difícil, las cosas que tengo que decir con carga emocional; pero a la vez el síndrome de estrés significa que muchos de los eventos del 11 de abril del 2019 se han quedado grabados en su memoria y nunca las podrá olvidar; como mencionó es director técnico, sin embargo el trabajo que realiza es desarrollar software, soy programador, escribo el idioma del programador en áreas diferentes; lleva más de 30 años de programador; lleva 20 años de forma profesional para desarrollar sistemas y programas; con este trabajo ha viajado el mundo entero para dar charlas sobre estos asunto, ya que lo consideran experto; en la actualidad y los últimos 10 años, está trabajando para defender derechos humanos digitales; construyó sistemas para la defensa de la seguridad y derechos humanos para las personas del mundo entero; junto a sus colegas construyen estos sistemas y los regalan a todas las personas del mundo para libre uso y se llama software libre; en su tiempo libre durante muchos años ha practicado artes marciales; por muchos

años dedicado al deporte Buchingan Tayú, que proviene del país Japón, tiene 5to. grado de cinturón negro; el 11 de abril del 2019 estaba dirigiéndose al aeropuerto para ir a Japón, el fin de su viaje fue llegar al centro de entrenamiento de las artes marciales, iba a tener la oportunidad de entrenar con el gran maestro, responsable de ese deporte en todo el mundo, fue la primera oportunidad y él estaba muy ilusionado de poder ir al centro más importante para el deporte que ha dedicado tanto tiempo; en uno de sus bultos llevaba lo que necesitaba para su entrenamiento, especificando por ejemplo unos palos de madera y además ropa de entrenamiento y los cinturones necesarios, llevaba meses con este viaje preparándolo y eso se debe que en el Japón el respeto es importante y no podría ir sin representación del maestro local; entonces es imposible pedir a otro realizar el viaje, se programó desde el mes de febrero; había comprado el pasaje a finales de febrero, reservado el hotel, había subido un tuit de lo emocionado que estaba con el viaje; cuando llegó al aeropuerto llevaba el equipo de deporte y para hacer su trabajo, no es exactamente el que se realiza entre las 9 y 5 de la tarde, sino que trabaja usando su tiempo para las tareas que parecen importantes en el avión, necesita programar, debe tener lo que necesita para aquello; y tanto como se ausentaría varias semanas tampoco era de ir sin contacto a sus colegas, viajo como siempre viaja, con sus computadores, memorias USB, adaptadores, lo que la hace falta para trabajar; igual pude parecer extraño en una lista, porque le hace falta tanto equipo, pero trabaja con la seguridad, la defensa, pero trabaja con esto, un principio básico trabajando seguridad es poder separar diferentes asuntos; la explicación es fácil, si trabaja simultáneamente en dos proyectos y si usaba en la misma computadora y si hay fallo en el proyecto, puede dañar al otro proyecto; al final como sus colegas son responsables de varios no sería responsable si usaren la misma computadora para los diferentes proyectos; quiere decir esto porque en el juicio hemos escuchado por horas, a expertos de Criminalística, han hablado de computadoras y USB, números de series, lo que está intentando explicar que eso es algo muy normal tomando en cuenta su trabajo; como dijo estaba contento cuando fue al aeropuerto para ir a Japón, salió a las 12:00, casi siempre vuela con KLM a Ámsterdam, y es el mismo vuelo que sale el mismo día a la misma hora, lo había tomado más de 100 veces; sigue la misma rutina cada vez, sale a las 16:00 y el cheking a las 13:00, él va a la apertura; todo iba según la rutina, estaba antes de la una en el cheking y paso seguridad a la una y cuarto, ahí sucedió una cosa novedosa que nunca le había pasado, cuando salió del control se le acercó un señor con chaqueta de control contra drogas y recibió mi equipaje de mano por completo, revisó el equipaje de mano pero de forma muy detallada, muy profunda, pero luego siguió, pudo pasar por migración, siguió en el aeropuerto y se sentó a leer; a las 3 fue a la puerta de embarque y estaba leyendo, como a las tres y cuarto, una personal de KLM estaba ya presente en la puerta de embarque, todo como siempre; como a las 3 y 20 escuchó que le llamaban por su nombre, sacado para control aleatorio para equipaje facturado, eso no le extrañaba mucho, cada 5 viajes podía pasar eso, se acercó y dijo soy Yo, pero cuando llegó de repente aparecieron gran número de personas y se pusieron 7 personas tras de él, una de esas personas las reconoció, una era la que realizó el control del equipaje de mano; los otros ignoraba quienes eran, no tenía distintivos, ellos no se presentaron se acercaron y que le pidieron que se identifique con el pasaporte; mostró su pasaporte y una persona revisaba leyendo de un documento que tenía en su mano; Yo en ningún

momento vi ese documento, nadie de estas personas le mostró el documento; pudieron comunicarse con él por personal de KLM porque saben inglés, le comunicaron por una mujer de KLM que tenía que ir con ellos para ayudarlos con algo; al parecer esa fue la intención de lo que se decía, se trataba de poca duración, quería regresar para tomar el vuelo; sin embargo pregunto si podía ir en el vuelo y le dieron que no, que los tenía que acompañar; en ese momento estaba preocupado, él siguió a las personas, estaban unas adelante y otras detrás de él; pasando por el aeropuerto tenía su teléfono y mandó un mensaje diciendo que estaba preso por personas que no conocía y que necesitaba un abogado; en ese momento ignoraba lo que pasaba, no sabía que eran policías, era un situación de secuestro, no se había presentado ni explicaciones; le llevaron a una oficina de Interpol junto a migración; le indicaron que se siente, cuanto más adentro mejor y otro se sentó para bloquear la salida; después hicieron entrar a una persona de migración, se dirigía a él hablando en inglés, oraciones cortas; le dijo que fue necesario que se quede pero que él ignoraba que pasaba; ya en el momento que se acercaron a él, en ese momento pedí un abogado y siguió pidiendo abogado; seguía preguntado por un abogado, pedía explicación, porque le privan de libertad, no le dijeron nada; de su parte lleva en su cuello llaves de identificación, memorias USB, información sensible; de inmediato recibió la instrucción de quitarse lo del cuello, tenía que meter en eso en su equipaje de mano, sin explicaciones; los primeros 10 minutos tenía su teléfono, logró enviar un par de mensajes para comunicar que algo raro ocurría; después de 10 minutos se le comunicó que ya no estaba permitido el acceso a su teléfono; le dijeron que era para proteger su seguridad; después de 20 minutos sonó su teléfono y convenció a la persona que responda esa llamada porque pensó que era su abogado, pudo hablar con el abogado un tiempo corto de 3 minutos, le dijo que no sabían lo que pasaba y que iban al aeropuerto; después no se le permitió el uso de teléfono; ahí estuvo sentado varias horas, más que nada estaba confundido, siguió sin comprender como era posible que se le negaba acceso al abogado, no comprendí como era posible una situación así sin acceso a un intérprete para saber o que pasaba; estuvo ahí varias horas, en ningún momento se le ofreció comida o bebida; estuvo mirando su reloj, comparó hasta cuando tendría que haber llegado el avión; pese a eso dijo que se trataba de un mal entendido y pensó que se solucionaría y podría comprar otro pasaje para viajar a Japón; durante el tiempo continuamente preguntaba por lo mismo, que pasaba, y donde está su abogado; la mayoría de las veces no recibió contestación, pero le hicieron preguntas porque cree que está aquí? Eso fue lo único que le dijeron a más de instrucciones; como a las 6 de la tarde llevaba 2 horas sentado, tenía necesidad de ir al baño, se había aguantado mucho rato, pero la necesidad era importante y pido ir al baño, le hicieron salir, pero explica que por unas mesas y un ambiente alargado; en la parte interior que da al control de seguridad hay puertas, ahí estaban los baños, eso significa que cada persona tiene que pasar por esas dos puertas para llegar a migración; las personas que le habían privado de la libertad y con gestos decía que podía utilizar zona de orinar, por eso fue y orinó, pero las personas mantenía la puerta del baño abierta, todos miraban adentro, no solamente las personas que le privaron de libertad, sin que todos los que pasaban por ahí vieron que orinaba en público; no puede expresar lo vergonzoso y humillante que es hacer eso, sin saber el motivo; después regresan a la oficina; estuvieron ahí como hasta las seis y media de la

tarde, tenía su reloj de pulsera, como a las seis y media le hicieron ir al parqueadero del aeropuerto, le hicieron subir en la parte trasera de un vehículo de Policía; pudo por fin hacer que la persona encargada le facilite su nombre, dijo Patricio no su apellido ni su título; él le dijo que nos vamos a Fiscalía y ahí estaría su abogado; pero 20 minutos antes de salir al parqueadero había sonado su teléfono, era su abogado, fue también una conversación breve, les dijo que había ido personalmente pero no tuvieron permiso para verlo; en ese momento no comprendía porque iban a Fiscalía para reunirse con su abogado si ya estaban en el aeropuerto; se alejaron en el vehículo, luego dijeron en 5 minutos, el conductor recibió una llamada telefónica y no sabe que se dijo pero hicieron vuelta y regresaron al aeropuerto; no entraron, estaban en el vehículo en el parqueadero; el no comprendía porque había vuelto, en ese momento se sentía preocupado, le daba la intención que le querían alejar de su abogado; preguntaba una y otra vez que quería su abogado y no recibió contestación; al final le hicieron entrar de nuevo en el aeropuerto a otra zona, en una oficina junto a las cintas de equipaje, le hicieron sentar sin explicación si n saber lo que sucedía; puede ser que eran siete y media de la tarde, recibía llamadas y contestó, era su abogado, fue la última vez que se comunicó con su abogado por ese día; también fue llamada corta menos de tres minutos, dijeron que se encontraban en Fiscalía y le preguntaba dónde estaba él; Patricio le dijo que le aguarden en Fiscalía que irían en poco tiempo; mi abogado le preguntaba que pasaba, si le mostraron documentos, le dijo que no, le dijo a su abogado para que esté pendiente; en medio de la conversación con su abogado, Patricio levantó un documento, lo tuvo en su mano poco tiempo, no pudo leer el documento, pero se percató que estaba escrito en castellano, tenía un nombre que se parecía a su nombre con faltas de ortografía, y una palabra RUSO, fue obvio que él no quería que él no lo llegue a ver, le mostró cuando estaba distraído, pidió que le muestre de nuevo y se le fue denegado; a continuación se le indicó que tenía que terminar la conversación y tenía que dejar el teléfono; las tres horas siguientes estaban de la misma forma como hasta las 11 de noche, les pedía que le expliquen que pasaba, que quería su abogado, pedía ver los documentos y se le negaba; como a las 11 y 10 aparecieron muchas persona, dirigidas por el Fiscal de esta causa, en ese momento no se dio explicación ni presentación en idioma que comprenda, ignoraba quienes eran; la primera persona en entrar en la oficina es el señor Fiscal, empezó a leer en un documento, en un idioma que no comprendió; le ponen de pies y le sacaron todas sus pertenencias, menos las joyas y el reloj; le quitaron su equipaje de mano donde tiene sus libros y las llaves de su casa y le esposaron, en la espalda las manos; después varias personas se dirigieron a él, leyendo documentos, de sus teléfonos, el no comprendía lo que se le decía; a continuación intentaron explicar con señas que debía firmar un documento que habían leído; parecía que ese documento estaba en español, pero él no sabe hablar español, les dijo que no podía firmar algo que no comprendí; parecía que de verdad quería que firme, insistían, le hablaban y no comprendía y con gestos le decía que debía firmar; a continuación le pone de pie con la cara en dirección a la pared, no se le permitía girar la cabeza, cuando le giró , le regresaron para que mire contra la pared; puede ser que tenía que guardar una postura por 10 o 15 minutos, no se le permitían ver ni su reloj; por fin salieron de la habitación, vio que había llegado su equipaje facturado con su de mano, dos de los bultos señalados por que ya eran pruebas; le sacaron por puertas traseras, por pasillos, llegaron al

parqueadero, le tenía cogido de una forma distinta ahora, todos iban como más endurecidos, querían agarrarle para indicar que era su preso; inicialmente no comprendía el motivo del cambio, pero ahí se encontraban cámaras de video y que le estaba sacando fotos y grabando, le metieron en la parte trasera de una patrulla; estuvo sentado, esposado con los brazos atrás, sin espacio para mover sus piernas; pudo ver la pantalla del vehículo, eran como las 23h30, quedó sentado en ese vehículo durante 3 horas, seguía sin saber que estaba sucediendo, sin explicaciones de que porque estaba preso; en ese momento estaba preocupado, crecía su preocupación con el tiempo, fue obvio que ese tal Patricio le mintió y que le había pedido a él que mintiese a su abogado; en el primer momento de ser capturado pidió permiso para llamar a su abogado o una llamada personal pero se le negaron; esa petición la hizo a las 11h10 en presencia del Fiscal Chávez y se le negó; estaba sentado en el vehículo y vio que muchas personas se alejaban, la zona más vacía y oscura, empezó a sentir miedo, nadie sabía dónde él estaba, estas personas que no se presentaron querían esconderle para que no le encuentre su abogado y nunca se buscó un intérprete; cuando estaba sentado a las 24h0 empezó que como a sentirse desaparecido, no había persona que sepa dónde está; para que quede claro, en ese momento con la conducta de estas personas tenía motivo fundamentado para temer por mi vida; llevaba 10 horas de control de estas personas y sus derechos humanos habían sido violados; como va a comprender lo que sucedía ni siquiera le decía o querían hacerle entender, como saber cómo definir porque le negaban el contacto con un abogado; se trata de los derechos humanos básicos; también llegó a pensar de que habían empezado a violar sus derechos humanos, no sería posible de vernos ante un Juez; porque pensó que estando en un país que se confían en su sistema judicial, como se llega ante un Tribunal, todos los derechos humanos que ya habían violado, como harían uso de sus pruebas; fue irónico porque en ese momento pensó que le iban a matar, porque quería pensar como convertían la situación en un proceso penal, pero estaba equivocado, aquí estamos, han pasado 4 años y seguimos hablando de lo mismo; pero está declarando, seguiré declarando es necesario que comprenda lo que sucedió y sepan cómo se violaron sus derechos una y otra y otra vez, que comprendan la decisión del Habeas Corpus, sus derechos se violaron una y otra y otra vez; como dese poder decir que se terminó todo y que de ahí se respetan sus derechos humanos, no sabía que solo era el inicio, como a las 02h30 del 12 de abril del 2019, nos alejamos del aeropuerto por camino largo se detuvieron en su apartamento, pudo ver varias personas circulando, la puerta del edificio estaba abierta, se le acercó una persona no recuerda si fue el Fiscal o Patricio y a larga distancia mostró un documento, la persona le explicó que tenía decisión legal de entrar a su departamento, eso fue a las 03h00, quería que ayude, que abriese de manera voluntaria, no pudo ver el documento, respondió que debía hablar con su abogado antes de tomar la decisión; no recibió contestación, le cerraron la puerta por 20 minutos permaneció; después salieron y le condujeron a un local en Río Amazonas; en ese momento no sabía pero era la Policía de investigación técnica; le hicieron sentar en un sofá y esposado en la espalda; estuvo sentado aproximadamente desde las 03h30 hasta las 08h00, seguía pidiendo un abogado y explicaciones que le dijeran porque está ahí y no le contestaban; en algún momento apareció su equipaje facturado, sacaron sus pertenencias, le ignoraron, pero la mayoría del tiempo lo ignoraron, no le miraron, esperaba en el sofá y ellos

seguían trabajando en asuntos de oficina; quiere hacer un paréntesis; hace un años pudimos escuchar a un experto que dijo que en ese mismo tiempo ahí había trabajado como interprete para traducirlo al inglés, a mí me sorprendió enormemente escucharlo, nunca se ha comunicado con esa persona en su vida entera; Yo puedo decir que en ese tiempo, en esa oficina hasta llevarle a flagrancia no se intentó que alguien se comunice con él en inglés, ni comunicarle sus derechos; como a las 6h00 se le acercó una mujer en la oficina, prendió una TV en la pared, encendió la TV y se sentó dirigiéndose a él, él pudo ver la televisión, no sabía cuál era su intención, quedó obvio que la observaba detenidamente; luego comprendió porque pocos minutos después empezaron noticias en TC, lo primero que vio fue la noticia del día, la gran noticia y vio fotos tuyas, por supuesto no comprendió lo que se decía ya que era en español, pero pudo ver palabras, en la parte de debajo de la pantalla salen palabras, decía su nombre, pudo ver el nombre de la persona Ministra del Interior, también vio una abreviatura de INA, pudo ver fotos en las que aparecía él, al parecer se había bajado de internet, de charlas que había dado, en mediada he dado más de 100 charlas en el mundo entero sobre temas programación y desarrollo de software, también en Ecuador, por ejemplo en 2013 en Riobamba dio charlas como programar mejor; ese mismo año dio charla aquí en Quito, en el IAEN hablaba como defenderse como ciudadanos y la integridad personal; en estas fotos una de la U de Riobamba se le veía a él y se veía un código de Programar, puede aparecer de acceso no consentido, pero eso es código para programar cualquier cosa; sin embargo vio dos fotos que no provenía del tiempo con el público, una de estas fotos fue del aeropuerto, cuando salía del parqueadero, rodeado por estas personas, a él le dio la impresión de que la foto era para darle una impresión muy mala posible; lo que pudo comprender viendo las noticias, estaban tratando de pintarle como un criminal; la otro foto mostraba su equipo USB, sus otros equipos y computadoras puestas de una forma que parecía prueba; otra palabra que se veía era una que se movía: Hacker, y en eso en él provocó que se sentía bien alterado, la palabra hacker se puede comprender de dos formas: la forma antigua de emplearla es como un signo de respeto que se usa para describir un título honorario, entonces la norma establecida en su grupo de programadores, dice que es imposible auto llamarse hacker, es un título que los otros te tiene que llamar; lo menciona porque hablando de persona conocidas como Bill Gate, Hons, los que construyeron Windos y Setp Wostia, junto con otras personas que son los creadores de la sociedad técnica que es en la que vivimos ahora, cuando otro en esta comunidad se refieren a estas personas pueden decirles Hackers para hablar de estas personas; a mí persona nunca me han dado este título tan respetuoso; tampoco me describiría como un hacker, sin embargo al ver aparecer la palabra hacker, que no se la estaba empleando en su forma respetuosa, se estaba empleando de que se hable en el día a día, donde hacer a una persona de forma ilegal que tiene acceso; o bien se puede usar para describir una persona que hacerse de unos conocimientos para atacar a otras personas, son personas que él detesta; van en contra de todo lo que es importante para nosotros los tecnólogos; Yo he dedicado mi vida a defender a las personas comunes contra el ataque de este tipo de personas, él construye muros y puertas, no construye las necesarias para tirar muros, no herramientas para abrir esas puertas, mi vida de trabajo y organización tiene como fin lo constructivo, la mejora del mundo; cuando vio la palabra hacker experimentó una humillación y se

alteró, absurdo ver esa palabra asociado con él, no lo comprendió; quedó claro que la mujer que estaba observándole sabía que iba a salir en la noticia y quería ver su reacción, y porque? Porque sería interesante ver su reacción; lo único que pensó, al no explicarle porque, quería saber mi reacción para recibir esa información por primera vez; llevaba en ese momento 14 horas bajo el control de esas personas; todavía no sabía lo que pasaba, no se había permitirle habar con su abogado en privado; pero de alguna forma los medios de comunicación sabían más sobre su propia situación; y a sí ha seguido por muchos años, la defensa ha llegado a ser informado de noticias, si no mirando medios de comunicación y no las oficiales; como a las 08h15 fue llevado a Flagrancia, le hicieron entrar en el subsuelo, se encontró con su amiga, la responsable de su defensa y también se encontró con su abogado, sin embargo no conversó en privado con él, no le dieron el tiempo; le dijo bueno la verdad no sabe con seguridad donde fue, pero que le dijo que no debía firmar nada si no estaba presente un abogado, 16 horas de ser privado de su libertad; por primera vez vio a su abogado pero no se le permitía conversar; también cuando pasaron 16 horas fue la primera vez que sabía dónde estaba él, le hicieron entrar en lo que es el local de prisión preventiva de flagrancia, seguía sin explicaciones, le alejaron de su abogado, el ingreso en la prisión preventiva, tiene tres pasos, lo primero es que ahí está la persona encargada de la prisión preventiva, le mostró un documento, ahí estaban escritos sus derechos en inglés; seguía aún problemático, ya sabía sus derecho pero no sabía el motivo de su captura; seguía sin saber su estatus legal, estaba en prisión, acusado, no se lo había dicho; no sabe si en ese documento estaba el derecho a un abogado; pero está consciente que el derecho a un abogado es un derecho humano, tiene derecho a la defensa; la persona encargada de la prisión o de las celdas le intentó convencerle a firma el documento, le dijo que venga su abogado; eso fue un motivo por no querer firmar y porque no estaba de acuerdo de no respetarle sus derechos humanos, 16 horas escondido; esta persona intentaba convencerle repetidamente, él dijo que no y al final le mandó al siguiente paso del ingreso, se trataba de una examen físico, no sabe si fue un médico o una enfermera, tenía que desvestirse, ella examinó su cuerpo para ver si tenía marcas de maltrato, él no tenía esas marcas, pero si experimentaba dolor, le dolían las muñecas, las manos, 9 horas esposado atrás de la espalda; además le fijó a la espalda 3 horas sentado en la parte de atrás de un patrullero; pero comprenderán que en esa situación de entonces eran marcas psicológicas y no se pudieron o intentó detectar; el tercer paso del ingreso fue que se le quitaron de sus pertenencias, cuerdas de zapatos, reloj; ya le hicieron entrar en las celdas, se le quitaron las esposas y le hicieron entrar en la celda con varias personas, estuvo sentado el día 12, desde las 08h30 hasta las 22h00, como a las 10h00 le hicieron subir a una oficina de este edificio, fue una oficina abierta, había personas sentadas y quedó obvio que no se permitía conversación privada, fue la primera vez que me encontré con el señor Ula Ernbrg, él se presentó como el Cónsul Honorario de Suecia en el Ecuador, Suecia no tiene embajada en Ecuador, la más cercana en Colombia; le dijo que había sido informado por su situación ese viernes a las 07h00, y eso 16 horas después del momento en que fue privado de libertad; le informó que el gobierno de Suecia ya estaba informado sobre la situación, que está informado y que notificó al gobierno Ecuatoriano que todo tiene que seguir curso legal; le presentó al señor Carlos Soria, llegó a comprender por lo que le contaron,

que estaba contratado por el grupo de sus amistades para ser el responsable de su defensa, los abogados a los que ha hecho referencia trabajaban contratados por su organización, pero eran abogados de negocios, por ese motivo se contrató a Carlos por temas penales; después de eso se sentía que alejado del Cónsul y con Carlos tuvieron para conversar 15 minutos; fue una sensación extraña conversar con el abogado en presencia de otras personas que trataban de escuchar; pensó que ahora le permiten conversar con abogado pero no le respetaban el derecho a una defensa verdadera; le contó lo que había sucedido enfatizando los peores momentos y lo poco que le habían explicado; Carlos no sabía mucho tampoco, no había recibido material de Fiscalía, le pudo informar de los rumores de los medios de comunicación, también le contó que la Ministra del Interior había hablado el día anterior, como a las 5 y 6 del día 11, la Ministra del Interior había comunicado sobre su arresto por tentativa de desestabilizar el gobierno, entonces rebobinamos; pudo verse con Carlos nuevamente un tiempo corto en la tarde, seguía sin saber mucho de Fiscalía; como a las 22h00 le sacaron de las celdas, le hicieron subir a la sala de audiencias, el tiempo no nos permite que Carlos me explique que era la audiencia, no estaba presente un traductor, la única persona presente que hablaba los dos idiomas era ULA, que había regresado, intentaba ayudarlo, en lo que podía, sin embargo su función era de observador, de llegar a comprender para poderle informar a la embajada; él sobre todos se encontraba en escuchar, de vez en cuando le traducía una frase suelta; mencionó que Carlos no tenía tiempo para conversar, que había recibido material de Fiscalía 5 minutos antes de la audiencia; en ese entonces llevaba día y medio sin dormir, seguía sin saber lo que sucedía, lo único que tenía claro era que cada acción de la Policía y Fiscalía y diferentes personas, todas las acciones formaban parte de violación de derechos humanos; puede que parezca extraño pero al ingresar en la sala de audiencia, él tenía muchas esperanzas, psicológicamente estaba mal, pero en ese momento sabía que por primera vez tendría la oportunidad de estar delante de un Juez y sabía todo lo que pasaba, pero podía acabar mal también, puede ser que había muchas películas americanas de delito, pensó que en el peor de los casos sería que a él le suelten, pero con la obligación de pagar caución, no sabe lo que piensan los demás, el señor ULA tenía buenas esperanzas, Carlos siempre tiene un humor positivo, ya que él también sabe que nosotros estamos en lo cierto; estuvieron en esa sala muchas horas, de la argumentación comprendió poquísimo, el Fiscal hablaba de cosas diferentes, ULA dijo que el Fiscal hablaba de los libros que tenía, de la cantidad de las memorias USB para viajar y cuantos tenía en su vivienda, él hablaba de la rueda de prensa de la Ministra del Interior, y mencionó cual era el capítulo del Código Penal en el que sustentaba para acusarlo, decía que había atacado a la integridad de un sistema informático, nunca dijo que sistema, nunca dijo cuándo, ni donde, ni porque, en el momento cuando le tocó a Carlos no se pretendía defenderle de las acusaciones, quedará bien obvio de lo explicado no fue posible defenderle contra estas acusaciones; porque no fue posible? Su abogado no comprendía cuales eran las acusaciones, 5 minutos antes le entregaron más de 100 documentos; el segundo motivo es que no existían tales acusaciones, como acusar a una persona sin especificar cuál es sistema informático atacado; como ayudar en defensa a un supuesto hecho si no se especifica cuando se dio este hecho; llegó a saber después que circulaban rumores, uno de esos dando a comprender que había intentado

fugarse del país, y que no llevaba ropa de entrenar en sus maletas; su defensa se enfocaba en demostrar que practicaba artes marciales, que llevaba lo necesario para los entrenamientos y que había sido programado; también lo que se dejaba claro que no era un apersona con riesgo de fugarse; vivía en el Ecuador 6 años; aquí tiene sus amigos, su oficina, las semanas antes del arresto con sus colegas hicieron una reunión para planificar lo que harían el año entero; presentando todas esas pruebas, que no había riesgo de fuga, pero no tuvieron efecto; el Juez de entonces escuchó, se ausentó un rato, no llevaba reloj pero su regreso se produjo como a las 03h00, él leyó una decisión corta, no comprendió, el señor ULA se dio la vuelta y le dijo que parece que tú te vas un rato a la cárcel, estaba en shock no comprendía lo que sucedía; ingresó con la esperanza que el Juez declare que todo lo que había sucedido era contra la ley; esperaba que él le llamase la atención a la Policía, estaba esperando que dijese que se abrirían nuevos casos para el Fiscal y la Policía; pero lo que fue sin explicaciones, sin motivos, sin acusación, en cambio la decisión fue de prisión de 90 días, sin saber lo que había hecho él; tenía que hablar con su abogado y como avanzar, pero igual que antes le alejaron de su abogado, jalándole para alejarlo de él; parecía que el derecho a defenderse no era importante; Carlos pudo darme un consejo gritándole, que se aleje del mercado interno de la cárcel, de la economía de la cárcel, que no debí apagar por nada; luego lo jalaron y le regresaron a la celda; el día siguiente un sábado 13 de abril, a las 5 de la tarde fue llevado al centro de detención en el Inca; estuvo en prisión en el Inca desde el 13 de abril hasta el 20 de junio del 2019, podría contar muchas anécdotas pero no lo haré, ya saben las cosas que sucedían en prisión en Ecuador en ese tiempo, saben sobre la violencia, sobre los asesinatos a diario, saben que han sido publicadas investigaciones Internacionales, hechos que se dan una y otra vez; llegó a un pabellón donde habían 20 habitaciones, cada noche ahí dormían 120 personas, cada noche dormían entre 8 y 13 por cada habitación, con un colchón, dormían en el piso; en ese entonces el Inca estaba demasiado poblado, llegó a comprender que eran más de 2.500 personas, sobrevivió, otras personas no, se escuchaba la violencia, solamente entre tres cosas que rompieron la rutina, una vez a la semana recibía visitas de sus bogados, a veces fue llevado a otros edificios, la mayoría era a Criminalística, y una vez cada semana podían recibió visitas, sin embargo se permitía visita de dos personas, el tiempo limitado y todas las visitas a la vez; otra cosa que está documentado es el rato que tiene las personas que vienen a visitar; que tan mal el trato hacia los visitantes que otros presos pidieron a sus seres queridos que no los fueren a visitar porque no querían que pasen por las humillaciones al ingresar; abuso sexuales por parte de guardias se veía a menudo, durante ese tiempo no tenía manera para contactarse con sus abogados, en palabras claras, en su pabellón no había firma legal para llamar al abogado, aguardaba su visita; desgraciadamente seguía lo que había visto, no había conversación en privado; intentamos como lo intentaron pero siempre había supervisión; de nuevo se violaban sus derechos a defensa; los primeros día en la cárcel no sabía lo que sucedería, pensaba en salir en un par de días, sin embargo cuando recibió la primera visita le dijo que no, según si presentarse las acusaciones, apelaron la prisión preventiva, de nuevo cometió el error de tener esperanzas, porque con tres jueces a nivel provincial ellos si podía ver que no fue situación de riesgo; esperaba que al llegar a saber de las violaciones de sus derechos el Juez

tendría que ver que esa situación no podía seguir, el día 2 de mayo le llamaron a otro Tribunal, una sala grande muchos representante de medios de comunicación en masa, mucha atención, estaban sus amigos y colegas, y además los tres jueces Provinciales; el Fiscal empezó y hablo cosas parecidas de la primer audiencia, se hablaba del presidente Lenin Moreno, habló mucho de Wikileaks, se habló de la decisión de echarle a Julián Assange de la Embajada, pero no mencionó como estas cosas tenía que ver con él, lo que dijo que en su casa tenía libros en inglés, de nuevo mencionó el número de memorias y computadoras que tenía, de nuevo seguía sin mencionar cual era el delito, mi defensa estaba constituida en lo de antes, quería dejar clara que no había riesgo de fuga, sus abogados ofrecieron caución y oros mecanismo que no se fugaría, también presentaron gran número de violaciones a su derechos humanos y a la defensa; después sintió esperanza, se retiraron para deliberar, pasaron muchas horas antes de que regresaran, regresaron leyeron un documento que daba información que no se había mencionado nunca con anterioridad, dos de los jueces había votado para que se quedase en prisión preventiva, le regresaron ahí, el tiempo que seguía fue el peor tiempo de su vida, es que el tiempo antes tenía idea que el sistema judicial funcionaba y que había otros jueces ejercido su profesión; sus padres estaban presentes en esa audiencia, se sentía contento que saldría y el día siguiente podrían celebrar; sabía que ellos regresaría el sábado, solo quedaba el viernes, y además el día después de la audiencia era su cumpleaños, después de esa pesadilla quería salir a festejar con sus padres; en cambio le alejaron de ahí jalándole, subieron en vehículo y lo retornaron a la prisión preventiva; el día después fue un día duro, su cumpleaños, no vino nadie, mis abogado no vinieron, ni sus amigos, el sábado y domingo sucedió lo mismo, no sabía si se debía por parte de la cárcel había impedido su visita, no sabía que andaba mal, esos días pasó muy solo; sabía que no le abandonarían pero tenía la vocecita que decía que han tirado la tolla, una semana intentaron nuevamente pero fue negado, ya que el Juez dijo que el Fiscal no había dejado claro quiénes eran las partes ofendidas; en esta audiencia no se permitió su presencia; se le permitió una llamada por video sin interprete traductor; se le explico que posteriormente que había una amenaza de bomba, pero no sabe si se consideraba la presencia de jueces fiscales y abogados pero no la de él; se había n dado sus traslados a Criminalística, la finalidad era mirar sus pertenencias, las supuestas pruebas, se dio en diferentes etapas del procesado, muchas veces en estas audiencia; Lo que ha dicho que varias veces fue llevado a la Unidad de investigaciones de la Policía, se vieron sus pertenencias calificándolas como pruebas, entonces llegó a saber que sus teléfonos, computadoras y USB estaba cerrados, no le sorprendió porque trabaja como experto en seguridad, el señor Fiscal Chávez le pidió muchas veces las contraseñas, no dijo no, no se negó a ayudar, sin embargo su respuesta fue, que con mucho gusto considera colaborar si el Fiscal le explica cual el sistema informático de que se trata, cuando ha sido; nunca recibió contestación del Fiscal, no contestaba esas preguntas, pasaron meses sin que les dieron respuesta a esa pregunta básica, el sistema informático atacado, hablara luego de esto; siendo experto en sistemas de información porque se trataría de una dirección IP o de un ordenador físico que se puede indicar, únicamente pedía que le dijese cual ha atacado supuestamente, y además sigue aquí sentado sin tener bien claro cuál es la computadora o sistema que ha atacado, piensa que uno considera

que comete el delito, cual es lo que se ha atacado?; esas audiencias privadas seguían y no le daban contestación a sus preguntas, en junio se presentaron en la cárcel sus abogados, el Fiscal, el secretario y un traductor, pidiendo que él declare, habían hablado con sus abogados y como no se tenía claro las acusaciones no declaró sobre estos hechos; entonces lo que se pueda ver en el archivo del fiscal, a que se dedica, porque está en el Ecuador y que ha dedicado toda su vida a la defensa de derechos; en el momento de declarar le preguntó al Fiscal Chávez, cuál era el sistema informático atacado, cuando, donde como y porque, esta vez contestó, le dijo que es él quien tiene que responder a estas preguntas, después de haberse negado caución, rechazarse la apelación quedaba una esperanza, sus abogados colaboraron con otros especializados en Derechos Constitucionales para pedir un Habeas Corpus, el día 20 de junio del 2019 fue llevado a un Tribunal, a nivel Provincial con tres jueces escuchado, albergaba pocas esperanzas por lo que había pasado, sus abogados presentaron la petición en este gran número de problemas, violaciones de derechos humanos y derecho a la defensa, entonces se presentaron pruebas, material presentado aquí del 11 y 12 de abril, declararon sus abogados, deliberaron largo rato y 2 de tres jueces declararon que recupere su libertad, esa decisión posteriormente se mandó al Tribunal Nacional, y se ratificó esa decisión, no fue que solamente recupera su libertad, también se dijo que sus derechos habían sido violados, desde el primero día que no había tenido abogado, intérprete, escondido en lugares no aptos para presos; pero igual que antes de inmediato se le alejó de la sala y fue retornado a la prisión, igual que antes no se permitió conversar con sus abogados sobre la decisión tomada, cuando regresó a la prisión no había luz, ahí se encontraba él, estaba contento porque los jueces lo escucharon, no comprendía lo que sucedía, horas después se presentó su abogado y luego de unas horas recuperó sus libertades; en ese momento valoró todo lo que había sucedido, ni sus abogados, ni amigos ni nadie, no tenía esperanza que le dejarían en libertad; ni siquiera había preparado nada, no veían posible la salida; al salir vio que su apartamento seguía bajo control de la Policía, nadie explicó porque, fueron muchas veces y cada vez le detenían un vehículo de policía, cada vez pedían información sobre quien había tomado la decisión de vigilancia de su casa y pidieron ver el documento, nunca pudieron tener acceso a esa información ni una respuesta; por fin sus abogados escribieron al Fiscal para que redacte un documento para pedir que su casa no es un lugar de delito y pueda ingresar, después de tres semanas llegó a tener acceso a su casa; pero aun así, no sabe quién había tomado esa decisión de que había un policía día y noche vigilando su casa; ahora lo menciona, pero es uno de cientos de extraños que siguen sucediendo cuando salió de la cárcel; todavía ignora quien está dando instrucción que pasen estos eventos; dijo que 20 de junio recuperó su libertad, pero en realidad no es libre todavía, cada viernes tiene obligación de presentarse, son casi 200 veces que se ha presentado, sus cuentas bancarias están congeladas, no tiene permiso para salir del País, todos estos factores formaban parte de la decisión de Habeas Corpus; pero una cosa que no formaba parte de la decisión del Tribunal fue el de sufrir persecución, cada vez que sale de su hogar le persiguen, se trata de vehículos sin placas, se trata de personas que circulan a su plena vista y que intentan grabarle, muchas veces a sido perseguido por personas en motos, todas estas vestidas de civil, pero en esta situación a veces estas personas van con armas, él ha organizado una seguridad

personal, y el grupo de seguridad ha identificado a varias de estas personas siendo Policías de diferentes Instancias; a veces ha sucedido que le han perseguido policías en vehículos de policía, lleva tres años y medio, en una ocasión un vehículo aguardaba frente a su casa 30 minutos, con una antena grande que iba dirigida a su vivienda y se salía por la parte trasera de su vehículo, tenemos miles de fotos de esas personas, persiguiendo, hemos intentado dirigirse a las instituciones oficiales para ver quien le persiguen, todas responde que ellos no han dado esta orden; en esta situación que llevan armas quienes le persiguen, teme por su vida, no sabe cuál será el fin de esta audiencia, no sabe la intención de esas personas; entonces se ha preguntado porque no denuncia, para empezar hemos iniciado un proceso para tener respuesta sobre quien ha dado la instrucción de que se lo haga, todos respondieron que no tiene nada que ver, la otra parte de la respuesta es que ya han escuchado como se violaron sus derechos en los primeros días, a él le encantaría confiar en el sistema judicial del Ecuador, pero basándose en la conducta de Policías, Fiscalía y Jueces no tiene esa confianza, ustedes me dan miedo, los agentes de policía, el Fiscal, por lo que él ve estas personas hacen lo que les da la gana; después de los 90 días tendría que ser su fin, pronto en la mañana recibe llamada de abogado y le dice que el Fiscal vincula un amigo suyo al proceso, tal vez un día se celebra la audiencia Arguello como coautor, en el mes de mayo aparece en calidad de testigo, y ya saben que en la preparatoria de juicio el Fiscal no lo enjuició, igual que en otra circunstancias no se llegó a especificar porque era coautor, a Arguello, era su amigo aparte de ello nada; pidieron que se les dé respuestas a las misma preguntas así como estaría involucrado Arguello, pero siguen sin respuestas; no puede adivinar, no hay hipótesis del Fiscal, porque no presentó ninguna explicación, solo observó dos hechos, lo primero es que Arguello no fue procesado, el Fiscal decidió no seguir en su contra, lo segundo que tiene claro, el período para investigar se alargó por 30 días más por la vinculación; estos 30 días fueron en agosto del 2019, en ese tiempo por la mitad de agosto, Criminalística tiene acceso su teléfono, que fue modificado antes de que ellos estén presentes en la audiencia, ustedes tiene acceso a las pruebas, lo que no se está mencionando; aproximadamente una semana después una amistad ve un reportaje, no comprendía de que se trataba, le manda una foto, ella le dijo que esa foto se estaba alegando como prueba de que él había accedido al sistema de CNT, el mismo día o siguiente, en la página digital 4 pelagatos aparece una noticia, aparecía esa foto, se decía que esa fue la prueba de la comisión del delito; es la misma foto la que se les explicó en mayo y la hemos visto, imagen que se la ha visto, esta imagen, la misma que se presentaba como la prueba central, no se encontraba en el archivo del Fiscal, sus abogados quisieron obtener información de la foto, para saber que material se había extraído del teléfono, pero tardaron días, pero a cerca del teléfono nunca tuvieron acceso, no tuvieron acceso de las pruebas, al teléfono, les fue negado por el motivo de su integridad personal, lo que sigue sorprendiéndolo es como pudo sacar el Fiscal la información del teléfono sin su presencia; otras imágenes se presentaron, que luego se introdujeron al sistema del archivo; hasta el día de hoy siguen sin acceso al material del teléfono; es más nunca han tenido acceso a esta imagen, solamente han tenido acceso a lo que se ha imprimido, de una imagen de muy mala calidad, pero se trata de una imagen digital, para poder realizar su análisis es necesario tener acceso a ese archivo, análisis que sería importante para la defensa; por ejemplo sería ventajoso un análisis técnico del

archivo para ver si ha sido cambiado, por ejemplo sería bueno comparar la cámara que se usó para sacar la imagen y con la cámara del teléfono, luego sería oportuno determinar si es una imagen o una foto; sin acceso a este archivo sería imposible realizar estos análisis y nunca se los ha entregado, volvemos a los mismo derecho a la defensa violando; no sabe si nos hemos dado cuenta que se ha conversado de la imagen pública, pero de donde proviene esa imagen?, proviene del otro sitio de 4 Pelagatos, mirando esa imagen que hicieron pública, la calidad es superior, porque es más fácil leer esa imagen, es fácil se ve claramente que la imagen impresa, no tiene la misma calidad, eso nos lleva a suponer que esta plataforma digital ha tenido acceso al archivo digital, como puede ser que esa organización haya tenido acceso a una prueba necesaria para su defensa cuando su defensa no ha tenido acceso a la misma; 2 días antes de finalizar los 30 días añadidos a la Instrucción, fueron llamados a una audiencia, un jueves 29, audiencia de reformulación cargos remitidos contra él, la acusación anterior era ataque a un sistema informático, ahora en cambio se hace uso de la imagen para alegar que había tenido acceso a un sistema informático; 118 días de investigación, estaba acusado por un delito; CNT la empresa no había formado parte de esta acusación, pero esta última semana aparece en conjunto con el Fiscal y presenta estas acusación; es decir dos días antes de finalizar el tiempo de investigación cambia la acusación y presentan otra; si ven registrado en esta audiencia han presentado mucha argumentación para refutare el hecho; son mucho factores importantes, pero la imagen no indica que se hubiere cometido el delito, pero otra cosa es importante, con el derecho a la defensa, en la reformulación tuvo dos días para preparase contra esta nueva acusación, uno de estos días era sábado, ahora ya sabe que en Fiscalía se trabaja los sábados y se ingresa a los archivos; pero que piensan ustedes si sus abogados quieren incorporar documentos después de las cinco? Es decir no tenía dos días para preparar la defensa; ve que esta argumentación se merece respuesta por parte del Juez, el Juez de entonces se dirige al Fiscal pidiendo su opinión, puede ver en el registro la respuesta del Fiscal, afirmó que se trata del mismo capítulo donde se encuentran estos dos delitos tipificados, con lo cual no es necesario para tener más tiempo aunque se trata de otro delito; fue un tiempo muy duro el mes de agosto, a su amigo le había vinculado al proceso y su vida se estaba destruyendo por persecución, pero aún seguía en agosto sin tener claro de que estaba acusado; dos días antes de finalizar el tiempo de investigación se reformuló para investigar otro delito; solamente deja claro en esta segunda nueva formulación de cargos, no se especifica la hora, o dirección IP, y si se había tenido acceso no consentido; sin embargo el Fiscal dijo que se trataba de un sistema de información; estamos muy cerca del fin, prepararon la defensa como mejor pudieron, presentaron testigos para tratar como se conecta a internet para determinar lo absurda de la acusación; trabajaron duro el día viernes a hasta las 4h45 y Fiscalía no quiso que se agregue más documentos; es un buen momento para rebobinar: empezamos desde el final, en su vida nunca se accedió no consentidamente a un sistema informático, nunca lo ha intentado, nunca lo ha hecho a CNT, nunca ha sido miembro de Wikileaks, no ha trabajado con Julián Assange, ahora menciona esto y eso se debe que el Fiscal presenta estos hechos una y otra vez, sin especificar que tiene que ver con el hecho acusado; aprovecha para mencionar lo que dijo la Ministra del Interior, no ha intentado desestabilizar gobierno alguno y nunca ha encontrado a la Ministras del Interior; además aprovecha para decir lo que

se pronunció el Presidente, nunca he intentado acceder a ningún sistema ni a nada, nunca desestabilizar a su gobierno, ni del presidente ni de esta País; que en mayo existen personas que realizan la tarea de profesionales, brindar acceso a sistemas informáticos para comprobar cual seguro son, él nunca ha tenido ese tipo de trabajo ni remunerada ni no, construye muros, no los derrumba, construye puertas, no las cierra; se está diciendo que por el mero hecho de que porque conoce de sistemas informáticos, debería saber cómo brindar un acceso no consentido, eso no es correcto , sería como decir que una persona que maneje un vehículo sabría cómo construirlo, sería como decir que por tener conocimientos de construir un edificio, pudiere abrir puerta sin que se deje rastro, es lo mismo con decir que si uno es policía tiene tendencia a ser delincuente; es inocente, ni ha hecho nada de esas cosas acusadas, y aunque las acusaciones no quedan claras , pero lo dice es que no lo ha hecho:: para empezar gracias por la pausa; estaba hablando de que llegaron al fin de la investigación, pero durante el mes de noviembre hubo novedades en el archivo del Fiscal, y además en los videos de masa, aparecieron nuevos dato e imágenes, en el mes de octubre el Presidente habló a los medios afirmando de que habría accedido no consentidamente en Ecuador y en otros Países también, pero en el material del Fiscal ahí no había ningún signo, sigue sin saber de dónde provenía esa información; durante los años posteriores pasaba a menudo ser acusado por medios de comunicación, de otros delitos no de accesos no consentidos, cuando personas conocidas de miembros de comunicación dijeron que se habría accedido no consentidamente, que se usaban para las elecciones y que había alterado el resultado de las elecciones; es un ejemplo de las cosas que ha tenido que sufrir desde su arresto y su reputación se ha denigrado; en el mes de noviembre apareció material de índole personal en los archivos, por ejemplo, como hemos visto, por testigos se trataba de chats de índole personal, recordarán que se le negó acceso su teléfono para proteger si integridad personal, y eso lo dijo la misma persona que por su parte agregó cientos de páginas de conversaciones privadas de aplicaciones donde se tiene citas; y durante ese tiempo seguía la persecución, pero no solamente dirigida hacia él, la persecución de los días siguientes contra sus amigos, contra sus compañeros de entrenar, también fueron perseguidos, sus colegas de trabajo, sus abogados, se ven perseguidos hasta sus padres cuando lo viene a visitar, periodistas que se encuentran en calidad de veedores también están supervisados en citas con él; intentaron abrir nuevos procesos de los hechos, tener comprensión sobre las acusaciones, su amigo además intentó comprender al verse involucrado, y a la vez personas cercanas a él que le habrían brindado ayuda, fueron investigados por procesos legales; la organización de la que forma parte también sometida a persecución; hemos sufrido accesos ilegales a nuestros locales, de forma extraña, donde no se llevan objetos de valor, se les ha negado servicios por seguros, bancos y parecidos; y además siempre sin una explicación al porque se les niega; sus colegas, ex novia, investigadas y en el material investigativo se encuentra material personal de esas personas; en el mes de abril del 2022, tres años de ser privado de la libertad, fueron víctimas de una redada por parte de otro Fiscal en otra causa, se llevaron todas las computadoras, pero estas computadoras terminaron en bolsas con su nombre; se presentaron supuestamente investigando otro caso, pero llevaban consigo bolsas con el caso Ola Bini; si le creen pueden ir a la cuenta de tuitter de Fiscalía, subieron una foto con las bolsas caso Ola Bini; hemos dado muchas vueltas

el proceso lleva más de un año, debido a la persecución constante, sigue temiendo por su vida, hace dos semana su equipo de seguridad personal identificó a un policía armado, persiguiéndole; sigue sin saber quién ha dado instrucción de que sea como es, sigue sin porque, y cuantos años más estará perseguido; el 11 de abril de su detención en el 2019, su sobrina cumple un año, lleva años muy lejos de su hogar, aun así su familia es importante para él, siempre viajaba mucho y podía verlos, pero debido a la situación actual no puede ver a sus familiares ni amigos ha sido así durante 4 años; hemos intentado varias veces en foros legales que se le haga justicia, la única vez que ha sido así es el 20 de junio del 2019 cuando se dio el habeas corpus, porque ahí se dictó claro que sus derechos han sido violados; pero aún desde que salió de la cárcel la situación a seguido de forma igual; está sentado aquí casi un año de inicio de audiencia con la esperanza de que usted escuchen y vean las pruebas y comprendan de que no puede seguir de esta forma; pero también en este procesado actual se siente confundido con cosas que han llegado a pasar, usted recuerdan que tendríamos que iniciar esta audiencia en octubre del 2021, habían venido sus padres junto con los abogados; llevaban semanas preparándose para mostrar los detalles para que se comprenda su inocencia, 2 días antes de empezar se les informa que no se celebraría la audiencia, si lo comprendió, el Jefe de la CNT tenía que presentarse, pero tenía otra reunión importante y pidió que se aplase el juicio; cuando se inició la audiencia en enero del 2022 vio con curiosidad a tal jefe, también en el mes de mayo, hoy también, él no se encuentra presente aquí, lo que no comprende si no es necesaria su presencia porque se llegó a posponer y vivir otros meses en esta situación; hay otras cosas, por ejemplo hemos escuchado a testigos que hablan sobre su visado, pero no tiene nada que ver con las acusaciones, hemos escuchado sobre un servidor que alquiló de una empresa, pero nunca se alegó que tenga que ver con el delito acusado, la verdad es que los Jueces se ha dirigido hacia el Fiscal para que diga cuándo hablará de los asuntos relativos a la acusación; y cada vez que se le preguntó, ya que no es él el único que no entiende que ver con las acusaciones; escucharon al inicio que no tiene formación profesional, es esa clase de personas que en EEUU los dicen EOPRS discontinued mix; pero muchos de los testimonios las preguntas han tenido que ver con educación, y de nuevo esto le tiene confundido, que tiene que ver la educación con estos delitos; y bueno ya lo sabemos que han presentado un montón de información, centenares de páginas explicando el equipo técnico que tenía, se nos ha leído números de series, de billetes, le tienen confundido, lo que tiene que ver con el presunto delito; puede adivinar, la sensación que le da es que por parte de Fiscalía es dar tantísima información para que los jueces no se den cuenta de la información del presente delito; y como lo que sintió ese primer día al ver noticia, es sensación se está intentando describirlo como un criminal o una mala persona; sabe que no tiene una buen pinta, es sueco, más alto de la mayoría, es rubio aunque se pinta el pelo, las uñas, lleva vestimenta negra, hasta tiene un sombrero negro y se han hecho preguntas del sombrero, a él le parece un intento de hacer que se enfoquen esos detalles que no tienen que ver con ese delito; es una persona igual que ustedes, tiene sentimientos, perspectiva, lo que desea es que ustedes hagan lo que espera, si es desde el primer momento que lo ayuden para defender su derechos humanos; el sistema judicial d Ecuador no ha respetado sus derechos; estos son hecho no es lo que opina; está basado por el Tribunal superior; muchas organizaciones

internacionales han dicho lo mismo; llevo 4 años sin poder preparar una defensa verdadera, ya han escuchado el por qué ha sido imposible presentar una verdadera defensa, porque han violado sus derechos; entonces para acabar pide que escuche, les piden que miren las pruebas presentadas y que miren las pruebas no presentadas y que además tomen en cuenta los derechos violados; teniendo en cuenta que hasta la actualidad el sistema jurídico de Ecuador no ha respetado sus derechos, ahora les toca a ustedes y les pide que respeten sus derechos. **PRUEBA DOCUMENTAL:** Incorpora: 1) Investigación previa, 1er. impuso fiscal de 11 abril del 2019; Dr. Chávez da inicio a la fase pre-procesal indagación previa que tiene el carácter de reservada; delito: ejercicio público de la acción; mediante llamada telefónica, alias Marco..... conocer a Ola Bini, con vínculo con Julián Assange, una de las persona que la Min In nombró; impídase por 8 horas se ausente del lugar en el que se encuentra; 499.2 oficio a Migración certificación del movimiento migratorio de OB; 2) Solicitud de Fiscalía al Juez de turno, parte pertinente; a llegado a conocimiento el parte policial, refiere noticia del delito 180 delito.... ; Jacker Ruso y o Suizo miembro de Wikilick. 530 y 5232 detención para investigación; 3) Resolución a Fiscalía, autorización dada por Gloria Mayorga y secretaria: autoriza detención con fines investigativos; reconocimiento y extracción de información que contengan los dispositivos en poder de OB; como allanamiento en líneas anteriores; 4) Formulario de acta de allanamiento, siendo las 03:30 del 12 de abril del 2019, Edgar Chávez Fiscal con Tnte. Ricardo Muñoz en el sector de Ñaquito, se ha llevado a cabo allanamiento, encontrando...; concluye 08:30; 5) Otro formulario de acta de entrega de inmueble Andrés Ayala Tejada se entrega el departamento cerrado, firmado por Fiscal Chávez; 6) Oficio Policía Nacional 2019-499.UIDT-DNP-J 12 abril del 2019, documento acreditar al Cónsul que ha sido notificado, lo firma Mayor David Andrade al Cónsul de Suecia, sin recibido; 7) Informe de UAFE 2019-013 12 de abril del 2019 recibido en Fiscalía esa fecha a las 16:24 horas, establece que en base solicitud de 12 de abril, informe ampliado de Ola Bini, anexado a dicho oficio; información general, financiera, tributaria, complementaria, movimientos migratorios; 8) Razón sentada por Secretario de Fiscalía donde se dice que ha sido descargada del SATJE, que no existen peritos traductores en el Suecos en el 2019; 12 de abril del 2019; 9) Escrito presentado por la defensa 29 abril del 2019 19:00, petitorio se ponga en conocimiento los hechos que se imputan, no hay como ejercer la defensa sin conocer los hechos fácticos; pide saber los cargos que se le imputan, los hechos, conducta punible; 10) Oficio suscrito por el Cal Center DELITO, 2019-257-1800-DELITO-DNP-JEI 3 de mayo del 2019 y recibido en Fiscalía el 6 de mayo del 2019; atento a oficio se remita copia de grabación de 11 de abril del 2019: mediante oficio suscrito por el informe elaborado por Roberto Herrera dando a conocer que el 1° de marzo del 2019 los servidores instalados en el Cal Center habrían colapsado; no hay grabaciones, mantenimiento el viernes 4 de abril del 2019; la información del 11 de abril del 2019 no se puede remitir; 11) Impulso Fiscal 16 de mayo del 2019 establece 2.1. en atención al primer escrito ha sido, revisar el acta de audiencia de formulación de cargos La Fiscalía es la titular de la acción para lo cual ha fijado algunas líneas de investigación; 12) Memorando MINEL 0062M 14 de mayo del 2019 recibido por Fiscalía, subsecretario de Telecomunicaciones Se entrega un reporte de ataques 11-15 de abril del 2019 que recibió, dando el origen de los ataques; 13) Consta Memorando suscrito Directora Gestión procesal de Fiscalía dirigida al Fiscal

01549, 6 de junio del 2019, parte pertinente: establece que mediante Memorando de 14 de mayo del 2019, el Fiscal Chávez emite resolución en instrucción remitirá certificación de información; denuncia a Ola Bini 1 o 12 de abril por autoridades del Ministerio del Interior; denuncia 11 o 12 abril por pate de María paula Romo, si existe investigación previa de Wikilick o sospechoso Julián Assange; denuncia para desestabilizar el gobierno o denuncia que dañen de sistemas de tratamiento de información; la señora Gestión procesal elabora informe que adjunta: revisado el sistema no se encuera denuncia en contra de Ola Bini del 11 y 12 abril de 2019; María Paula Romo no se encuentra denuncia presentada; si existen denuncia en contra de María Paula Romo; investigación contra Wikiliks no hay investigación, ni contra Julián Assange; no denuncia para desestabilizar al gobierno ninguna autoridad ha denunciado; 14) Carta firmada por Ex Presidente Moreno Garcés: 11 de julio del 2019, oficio al Fiscal de la causa y dice: rinda versión, libre y voluntariamente dice: debe indicar que únicamente conoce la información pública dada por María Romo; 15) Oficio suscrito por Dra. María Paula Romo, informa: dice que cuando el gobierno del Ecuador analizó el retiro de asilo a Julián Assange, se contempló potenciales aliados de Assange, por asiduo visitante residía en Ecuador, Ola Bini lo visitó 12 veces, tenía contratado internet, su visa había sido solicitud por empresa contratista de la SENAI, arrojaba una serie de coincidencias de viajes con Patiño, ; 28 de octubre del 2018; la madrugada del 11 de abril retiró asilo a Julián Assange , informaron a medios la decisión soberana de dar terminado Asilo, que tiene un ciudadano extranjero vinculados a él, con antecedentes de haber jackeado , fue informada que un ciudadano Marco había dicho; 16) Oficio Director Diario Universo 20 de junio del 2019, entrega copias certificadas de la nota Lenin Moreno dice que se sorprendió a Ola Bini jackeando... ..; en Washington se la ha sorprendido a Ola Bini jackeando; 17) Oficio No. 25 junio del 2019 recibido en Fiscalía el 26 gestión procesal de Fiscalía dirigido al Fiscal Fabián Chávez, información de Ola Bini: sistema fiscal: no consta noticia de delito en contra de OB, por presunto delito de ataque a sistemas informáticos; 18) Oficio suscrito por Lenin Moreno: al Dr. Chávez: 2 de julio del 2019; pliego de preguntas del procesado, responde: no considera pertinente ampliar la versión; 19) Escrito de la defensa 10 de julio del 2019: solicita despachar pedido no despachados c) peritos en informática manifestaron que no podía acceder a la información de lo USB, requiere se entregue copia espejo; 7) oficie ECU911 a que autoridad se hizo conocer la llamada de denuncia; 20) Impulso Fiscal Ha solicitado la autorización judicial concedida en el momento oportuno, no se vulnera el derecho a la intimidad; 21) Impulso Fiscal: no ha lugar petición se autorizó se otorgue las copias espejos, impertinente otorgar copias espejos se revoca y se niega la entrega de copias espejo; 22) Resolución Fiscal: No. 8 el peticionario diga qué tipo de pericia se refiere y no sobre copias de fotografías; 23) Impulso Fiscal: has sido de manera secreta y privada, secretario no ha revisado, no existe registro documental para el efecto; 24) Oficio CNT 465, suscrito Wilson Falcón Rodríguez 4 agosto del 2019, recibo en Fiscalía 4 septiembre del 2019, pone en conocimiento que si la CNT puso en conocimiento del Ministerio una posible vulneración de sistemas 6 de octubre del 2015; CNT certifica que de la revisión de bitácoras NO REGISTRA el 6 de octubre del 2015; 25) Materialización certificación de página Web, notariada; 30 de agosto del 2019, correo electrónico en donde solicita se materialice Shodaw páginas públicas; fundación TOR IP es pública;

26) Copias certificada del habeas corpus; resolución de primera instancia; Jueces aceptan Habeas Corpus, declara vulnerado el der a la libertad, detención ilegítima y arbitraria, se vulneró el debido proceso en la garantía de la defensa: impugnada por Fiscal y Jueza; Corte Nacional acepta parcialmente dejando sin efecto los oficios de sanción para los empleados judiciales y fiscales. **4.3. EL DEBATE: FISCALÍA:** Dijo que al inicio de la audiencia, Fiscalía ofreció demostrar que el procesado había adecuado su conducta como autor del delito tipificado en el 234 del COIP, esto es el acceso no consentido a un sistema de telecomunicaciones de la CNT, en contra de su voluntad y sin su consentimiento; que el bien jurídico tutelado es la seguridad de los activos, vulnerado por el procesado; que por la complejidad del delito, ha hecho mención a datos de información técnica que comprueban la materialidad de la infracción y la responsabilidad del procesado, que en ese sentido se ha llegado a probar que el 6 de octubre del 2015, el hoy procesado sin autorización accede al sistema de telecomunicaciones de la CNT, ingresa en contra de la voluntad de quien tiene el legítimo derecho sobre el sistema, ilícito que fue descubierto una vez que se abrió y se extrajo la información del teléfono del procesado marca I Phone 8, modelo 10.4, color negro, incautado el 11 de abril del 2019 mediante el procedimiento adoptado por Fiscalía y la Policía, amparados todos en la legitimidad constitucional y legalidad de las respectivas ordenes de autoridad competente; procedimiento detallas por cada uno de miembros policiales, a través de los testimonios del Mayor David Andrade Daza Jefe de la Unidad de Delitos Cibernéticos, y los agentes William Molina, el sargento Ángel Guarnizo, teniente Ricardo Muñoz y sargento José Luis Vásquez, quienes relatan el procedimiento de la detención del ciudadano Ola Bini en el aeropuerto Mariscal Sucre y posterior allanamiento de su domicilio, encontrando una gran cantidad de dispositivos informáticos y electrónicos, más de 150, los cuales fueron fijados, etiquetados e ingresados bajo cadena de custodia; indicios que fueron acumulados en la cadena de custodia No. 1772-2019, lo que fue corroborado por los peritos de Criminalística como el Mayor Diego López, Capitán Ariel Velasco Albán, quienes practicaron las diligencias de inspección ocular técnica, el reconocimiento del lugar de los hechos y el reconocimiento de evidencias; para lo cual fue necesaria la intervención de peritos informáticos que describieron 68 dispositivos electrónicos, entre los cuales se encontraban 19 equipos de cómputo, 13 de almacenamiento de datos externos, 3 discos duros internos, 31 dispositivos USB y tarjetas de memoria SD, nano llaves con claves primaria y secundaria; así mismo los peritos de audio y video destacaron dispositivos móviles, tablet, IPhod, 5 celulares que necesitaban código para su desbloqueo, dispositivos electrónicos que estaban cifrados o encriptados, siendo imposible su acceso, pese a que en la audiencia privada el procesado no dio las claves en el momento oportuno para abrirlos, en caso de no encontrarse algo ilícito en su interior, sin embargo no los dio cuidando celosamente su contenido, en tales circunstancias se logró obtener la clave de un dispositivo, del teléfono celular del procesado y la apertura de otro de ellos mediante la asistencia penal internacional; el teléfono I phone, 8 del procesado, donde en audiencia privada se obtuvo la calve de acceso a dicho celular, al observar las cámaras de seguridad del edificio donde vive el procesado, las que fueron remitidas en una USB por la administración del edificio; que el Capitán William Castro señaló con lujo de detalle como obtuvo la calve de acceso, lo que se pudo verificar por la ampliación de imágenes; clave que fue probada en todos los

dispositivos móviles, logrando el acceso al teléfono y procediendo a su extracción, en un dispositivo USB, donde consta información en formato PDF, en la cantidad de 42.864 páginas, pericia en la cual se pudo obtener una fotografía digital cuya materialización de la imagen, corresponde al archivo A95079D384EDBE1B75A21A558A22383C, misma que se encuentra en la fs. 33.115 del informe de extracción, materializado todo lo relevante y que fue introducido en el expediente y al alcance de las partes procesales; fotografía digital que determina el acceso al sistema de telecomunicaciones de CNT, en la data se observa según lo dijo el perito Ing. Galo Cárdenas Calderón, que el protocolo TELNET, lenguaje de bajo nivel TOR, el COMAN PRO interface para ingreso de protocolos, el aviso de la CNT, en el que dice que el acceso es no autorizado, se considera un acto criminal, PETROECUADOR SENAI INTERNET, además dentro de la foto consta el usuario /home/Ola Bini, y un quipo físico, una laptop Lenovo, además la dirección IP 181.113.57.169, el ingreso al sistema de telecomunicaciones que corresponde al enlace de internet desde el Data Center principal de la Presidencia de la República del Ecuador, hacia el Data Center de contingencia ubicando en Guayaquil, el cual fue corroborado por el testigo de la CNT Ing. Carlos Medina, quien dijo que entre sus funciones coordinaba con los sitios de contingencia; que estuvo presente además en esta audiencia el funcionario de la Presidencia de la República Kléver Salguero, el líder del área de red de la Presidencia, quienes determinaron el proceso para la obtención de la IP; así también tiene relación a la pericia de extracción de los respaldos de los correos electrónicos carlosmedina, del cual se extrajo del dispositivo electrónico perteneciente a Carlos Medina, correos como asunto consta el Data Center, Contingencia, remitente yepezedy, de fecha 24 de julio del 2015, correos que específicamente tratan sobre la instalación de los data center de contingencia de la Presidencia y Petroecuador, cuyo proveedor está a cargo de la CNT, cuyos destinatarios fueron los funcionarios de la Presidencia, Petroecuador y por supuesto CNT; pericia realizada por el sargento Carlos Ninacuri y el Ing. Fabián Silva; de lo que se trata el Data Center de contingencia, nos habló Kléver Salguero Sosa, de la Presidencia, quien básicamente señaló que el Data Center Principal se encuentra alojado en le ex Secretaría de Inteligencia SENAIN, por observaciones de Contraloría se estableció que la Presidencia no contaba con un Centro de Datos alternos para la emergencia; por eso realizan un contrato entre empresas públicas; indicó que el Centro de Contingencia estaba operativo y en funcionamiento desde el 24 julio del 2015, esto corroborado por el ing. Carlos Medina, la que permaneció activa desde el 18 de julio del 2013; que los datos de conexión son reservados, de conocimiento sólo del área técnica de la Institución, para el público por su relevancia es reservada; solo el proveedor de CNT y funcionarios de la Presidencia podía tener acceso lícito a la información y acceso a los equipos; que en la fotografía de acceso a la página de CNT, consta la computadora Lenovo, lo que fue corroborado con las varias computadoras de esta marca, al parecer las preferida por el profesado, conforme lo señaló el cabo Henry Yépez, quien describió uno a uno todos los dispositivos incautados en el aeropuerto como en el departamento del procesado; así mismo esta fotografía fue reconocida y aceptada por Marco Arguello, quien asintió haber recibió la fotografía el mismo día de los hechos a su celular y que generó un archivo tuns mails, que es una imagen más pequeña que se almacena en la aplicación WathsApp, esto lo indicó el Capitán William Castro; la imagen en

WathsApp fue enviada por WathsApp al teléfono de Marco Arguello el 6 de octubre del 2015, al teléfono 593995494579, quien además indicó que este número lo tenía varios años, chat enviado desde el 593968942120, el teléfono de Ola Bino a Ricardo Arguello el 6 de octubre del 2015; lo que fue corroborado además con los chats extraídos de los mismos celulares, que fueron leídos por la perito traductora María Casco, cuyos interlocutores eran en procesado Ola Bini y el señor Ricardo Arguello, lo que tiene correspondencia incluso con el testimonio rendido por Ricardo Arguello; incluso de los testigos del procesado como el señor Mirtza, asintió que se trataba de una fotografía e indicó que se podía ver el reflejo y que podía haber sido tomada por una cámara, se ve el fabricante de Lenovo; así mismo estuvo presente el Ing. Galo Cárdenas quien señaló que el lenguaje Tor no es muy conocido, cuya finalidad es ocultar la identidad de quien lo utiliza y a la vez no dejar rastros de las conexiones, lo que concuerda con lo mencionado por el funcionario de CNT, además el perito señaló que se realizó un acceso no consentido a un sistema de telecomunicaciones, no a un sistema informático, como aquí se lo trata de decir; en este sentido solicita considerar toda la prueba evacuada; que de acuerdo al artículo 455 del COIP, existe el nexo causal, es decir la prueba y los elementos de prueba tienen un nexo causal entre la infracción y el procedo, el fundamento se basa en hechos reales introducidos a través de medios de prueba y no en base de presunciones; se ha cometido un acto típico, antijurídico y culpable, por lo que Fiscalía ha presentado pruebas contundentes e irrefutables, que llevan al convencimiento de los hechos, más allá de toda duda razonable; en tal virtud Fiscalía al haber probado la materialidad y la responsabilidad del procesado, solicita se declare su culpabilidad y se le imponga el máximo de la pena establecida en el 234, inciso 1, numeral 1 del COIP; en calidad de autor directo, conforme al artículo 42.1, literal a) de la citada norma. **LA ACUSACIÓN PARTICULAR:** Dijo que la ignorancia deliberada no es más que la negación del más elemental conocimiento, pretendiendo reducir así el dolo, la intención, el propósito; para ejemplificar tenemos que un joven conoce que las notas de su último semestre serán publicadas el día viernes, sin embargo prefiere aplazarlas hasta el día lunes para evitar un sinsabor, en caso de que haya reprobado; otro ejemplo sería que una persona sospecha que su cónyuge le es infiel, sin embargo no realiza averiguaciones para no corroborar estas sospechas; los ejemplos dados no tienen relevancia jurídica, pero muestran dos escenarios, en los cuales las personas prefieren mantenerse en zozobra, ante la realidad o verdad; esto lo dice para reafirmar los argumentos expuestos por Fiscalía; en este contexto debe mencionar que la empresa pública CNT, tiene dentro de sus varios servicios cuatro grupos, el primero la telefonía, segundo la televisión satelital, tercero servicio de datos y el cuarto de internet; para que un cliente pueda recibir los servicios, específicamente los dos últimos, es necesario que CNT proporcionen e instalen, así como configuren, los equipos necesarios de acuerdo al diagrama del servicio, que responde a las recomendaciones de seguridad que se encuentran dentro de la IZO 127 2001-2013, así como estándares internacionales de las organizaciones, los cuales determinan cuáles son los rangos de las IP públicas y privadas; de los testimonios rendidos por los peritos, el Ing. David Cárdenas realizó la pericia y análisis integral de conclusiones técnicas al informe presentado por la acusación particular, y el Ing. Carlos Medina quien por su formación académica nos han podido determinar cuál es la diferencia entre un sistema de telecomunicaciones y un sistema

informático, destacando que el sistema de telecomunicaciones es un conjunto de dispositivos que permite la transmisión y recepción de señales en diferentes formatos a quienes lo requieran y está compuesto por elementos activos y pasivos como ruteadores, firewall, ONT, cables de última milla, entre otros; por lo que considerando el tipo penal y ante la negativa para la presentación de un gráfico, solicita poner los equipos de manera física ante el Tribunal; señala que haciendo relación a los oficios del 13 de agosto del 2019, suscrito por el Mayor de Policía Rubén Terán, en el que se adjuntó el informe pericial de audio video y afines, de la extracción del iPhone 8, color negro, perteneciente al ciudadano Ola Bini, así como el oficio de 15 de agosto del 2019, suscrito por el Capitán William Castro, al cual se adjunta la materialización de la imagen signada con el número A95079D384EDBE1B75A21A558A22383C; han sumado varias horas en que la defensa técnica del señor Ola Bini, han desviado nuestra atención, dando a conocer, bajo testimonio de los calificados como expertos, temas referentes a derechos digitales, derechos humanos, herramientas para proteger la privacidad, los orígenes y función de la herramienta TOR, sin embargo refiriéndose al diagrama antes mencionado, nuevamente quiere mencionar que estos responde a estándares internacionales, los cuales fueron instalados en el cliente denominado Petroecuador, SENAÍ INTERNET, compuesto por los elementos expuestos en la sala, el primero corresponde a una ONT, que es el medio que sirve de interconexión, como alcance desde la central de la CNT hasta las instalaciones del cliente; el router permite tomar las decisiones sobre los envíos de paquetes de información a la dirección de destino y el cable que es el medio físico para la interconexión; debemos entender que lo que se encuentra expuesto, constituye un sistema de telecomunicación, sin embargo el sistema informático, es todo lo que se recibe en cada una de las computadoras; insiste en que el diagrama corresponde a las recomendaciones establecidas en el RFC 1918 y a los de seguridad de la IZO 27.001-2013; en consecuencia, de los hechos develados en este proceso, se puede determinar que el señor Ola Bini de manera planificada, organizada y ocultándose bajo la red de anonimato TOR, utilizando un protocolo TELNET, accedió en todo al sistema de telecomunicaciones de la CNT de manera remota desde su computador, utilizando sin autorización todos los elementos que constituyen el diagrama de servicio de internet de fibra óptica GIPON, en cuanto a telecomunicaciones, de propiedad de la acusación particular, manteniéndose dentro del mismo en contra de su voluntad, y una vez dentro del sistema de telecomunicaciones, como resultado de su acceso no consentido hasta el router, último elemento físico del sistema, se obtiene un pron que es el elemento objetivo del tipo penal, demostrando el acceso no consentido al sistema de telecomunicaciones por parte del hoy acusado, quien además remitió la fotografía del pron, según constan de las conversaciones que fueron referidas, al señor Ricardo Arguello; cabe mencionar que la defensa técnica de la contra parte ha tratado de desvirtuar la veracidad y existencia de esta imagen, sin embargo en el testimonio de Carlos Arguello, respondió de manera afirmativa de que si recibió o no la fotografía en su teléfono 0945497579. Con lo expuesto se encuentra demostrada la materialidad de la infracción y la responsabilidad, en la comisión del delito tipificado y sancionado en el artículo 234 del COIP, acceso no consentido a un sistema telemático. **LA DEFENSA DEL PROCESADO:** Cree que es pertinente partir por establecer de que se viene a defender, pero fue el Fiscal, en la reformulación de

cargos dijo que esto se trataría del acceso no consentido de un sistema informático y luego hábilmente se refiere a telemático y de telecomunicaciones, vulnerando con eso la posibilidad de defenderse, de tener claramente de que se trata el caso; delito o no delito, se vienen a defender de un supuesto acceso no consentido a un sistema informático y después de telecomunicaciones y todo nace de una supuesta fotografía, que viene a ser el elemento probatorio clave; en ese orden de ideas, el caso planteado por Fiscalía y la acusación particular tiene varios problemas y el primero es la no idoneidad de la prueba presentada, el Tribunal acredita un asesinato con la foto de una persona aparentemente fallecida?, esa es la prueba en un delito contra la vida?; estamos aplicando analogías? De esa supuesta fotografía se tiene que acreditar si sucedió o no sucedió, al igual que el delito contra la vida, y no tiene lógica jurídica, porque así lo manda la norma, el artículo 500 fija las reglas que tiene que realizarse cuando se trate de contenido digital, nos habla de una técnica digital forense; el Fiscal ha dicho que sí, que el señor William Castro vino y dijo que eso es una foto digital, pero escuchen el testimonio completo, dijo que era un elemento digital porque se tomó con una cámara digital, es decir que si toma una foto en este momento, la imprime y sería una evidencia digital, porque la tomé con un celular; tan cierto es esto que cuando se le preguntó al señor Castro que ahí había una foto de una pizza y que si era una evidencia digital, dijo que si, que era una evidencia digital, es esa la idoneidad de la prueba?, no, porque incluso el código penal en su artículo 460.8 manda a hacer reconocimiento digital, es decir la posibilidad de acreditar que eso que aquí nos han expuesto, supuestamente pasó el puntito rojo del uno al otro, efectivamente pasó, porque no puede quedar en una mera afirmación; tenía que verificarse por mandato normativo; es más cuando se quiso presentar como prueba de la defensa una materialización digital, el Fiscal dijo una dirección web debía presentarse a través de una técnica pericial forense, no a través de un documento; pasa lo mismo y es que dentro de las pruebas aceptadas, la que consta a fs. 2.659, el pronunciamiento fiscal, que ese documento llamado fotografía no es más que un documento; el otro argumento es que hay una pericia del señor Galo Calderón, que determina si efectivamente sucedió o no tal cosa, pero analizando el contexto de esa pericia, primer elemento una fotografía, segundo elemento CNT haciendo un informe documental sobre la supuesta fotografía, tercer elemento un perito haciendo un informe documental, del informe documental de CNT de esa supuesta fotografía, donde está la pericia informática en ese acto realizado, es la primera problemática y el por qué en este caso no se puede hablar de un delito, es la insuficiencia de la prueba, es su aspecto normativo, para probar un hecho: pero supongamos que el puntito pasó de ahí y que la norma no lo mandaría, así se podría demostrar una muerte con una pericia contable, o de cualquier forma; pero incluso los técnicos de la acusación vinieron y dijeron que no pueden demostrar si efectivamente sucedió el acto que supuestamente consta en la fotografía, al señor Galo Cárdenas se le pregunto si con el número de IP, que es lo que hay en la fotografía, puede acreditar si se accedió o no a un sistema, dijo que no puede; le pidieron que analice materialmente los equipos?, dijo que no, solo le pidieron que analice un informe documental; al señor Medina, experto de la CNT, que vino a presentar el informe y al cual se referirá más adelante, le preguntaron si le pidieron que analice los equipos, como estaban configurados, que había dentro o lo supuestamente sucedido? Dijo que no, simplemente querían información del número IP 181.113.57.169; le

preguntaron entonces ante esta necesidad de efectivamente demostrar si había o no un acceso y como lo probaría?, y respondió que necesita el equipo, su configuración y los logs o registros, los datos que quedaron, pero eso nunca le pudieron verificar; al señor Medina, le pidieron verificar el equipo, la configuración y los logs, respondió que no, que no le pidieron; a costa de quien tiene que ir la insuficiencia técnica de la prueba técnica presentada? A costa de quien tiene que ir la conformidad con una supuesta fotografía, acosta del procesado? Pero en realidad es a costa de Fiscalía, por un factor clave, se presentó dentro de la prueba documental por parte de la misma Fiscalía, el Informe de CNT, en este informe Fiscalía le dice que necesita saber cuál es el equipo que tiene la IP 181.113.57.169, CNT puntualmente le dice el equipo es de serie tal, que se realizó la búsqueda del sistema, verificándose que corresponde a un equipo ONT, hoy nos dicen que no, que el número está en el otro grande, no en la ONT; y no se quedan ahí y para justificar la falta de datos técnicos dicen retengan este equipo, con el propósito de que sea levantado, por un perito informático forense, quien deberá extraer los LOGS del mismo con el fin de determinar las conexiones entrantes a fecha 6 de octubre del 2015 y verificar la información contenida en el mismo, la misma Fiscalía sabía que se debía hacer; y que le contesta CNT aquí está el equipo para cuando lo necesite, se pregunta dónde está el perito que tomó el equipo, quien se refirió a más de describir la capa externa; una foto, no es más, al tal punto llega esto, que el señor Cárdenas no dijo que fue un acceso, dijo "si hubiera pasado la ONT, constituía un acceso no consentido"; irónicamente el señor Medina en su informe documental le preguntan "determine si al acceder a este dispositivo sin la autorización correspondiente y explícita de un usuario denominado Ola Bini constituye acceso no consentido a un sistema informático, telemático o de telecomunicaciones" y el responde: en el caso (supuesto) que un usuario no identificado ingrese y cree usuarios, constituiría un acceso no consentido; entonces supongamos que lo que está en esa supuesta fotografía sucedió o no sucedió?; segundo problema de la prueba presentada, no es jurídicamente válida y no es técnicamente válida, pero considerando que estamos jugando a supuestos, que todo fue ordenado y planificado el 6 de octubre, ya que todos estamos suponiendo en contra del reo, entonces supongamos que la fotografía nunca fue suficiente; señala que él también quiere hacer un ejercicio, el internet es un carro, a través de ese carro se puede llegar a distintos lugares, en unos lugares para entrar les van a pedir identificarse y en otros no, en el parque La Carolina no le van a pedir nada, en la Presidencia les van a pedir identificación, así de fácil, todos estos lugares, de acuerdo a los mismos testimonios del señor Cárdenas, del señor Dingeldon, del señor Bonifaz, Pazmiño, Agmad, han dicho que todos estos lugares tiene inicio en números distintos a 10., la otra variable es 172.16, y la tercera variable 192.168, a ninguno de esos tres inicios se puede llegar, en ese carro, a través del camino, es como querer llegar a Galápagos en carro, eso quiere decir que el número que lamentablemente 181.113.57.169, es un número al que se puede llegar con su vehículo y tocar la puerta, sí hay puerta; El Comercio, Google, ESPN Deportes, todos esos son portales que van a responder esos números a los que ustedes ponen enter y llegan; dice que ahora, la acusación en sus dos variables, dice que no importa eso, que este número 181., es privado, que no se puede acceder, mientras que todos y cada uno de los testigos han sido coherentes y concordantes al decir, que allá se puede llegar en el carro, pero el señor Cárdenas dijo algo que es muy importante,

que estos lugares pueden tener tres facetas o tres variables, la una, puede entrar cualquier persona, la segunda que le pidan un acceso, el sistema Satje de la Función Judicial les pide un acceso, se necesita ingresar los datos para poder acceder, si no ingresan datos no acceden, eso nos ha dicho el mismo testigo de la acusación, perito especializado, el señor Cárdenas, y hay otros que son totalmente restringidos; analicemos que tenemos en la foto, primero tenemos el número 181.113.57.169, al que puede llegar con su carro a través de internet, que tipo de lugar es?, uno que te pide usuario y contraseña, si quieres acceder tienes que ingresar un usuario y contraseña, y cada uno de los testigos ha dicho esto, que no se ingresó ningún dato de usuario y contraseña, llegó, no accedió y se fue, eso es lo que se ha probado en esta audiencia, a través de cada uno de los testimonios, sumándole algo, ese TOR esa red de anonimato con TH según el perito informático, el otro del superhéroe, que tan mal lo han hecho ver, pero esa red, dicho por el mismo fundador, estuvo aquí y dijo que solo puede llegar a espacios públicos, no salta muros, solo puede llegar a estos números y siempre que estos no tengan ninguna restricción, porque al contrario cuando pasa, llega y le piden usuario y contraseña, como en cualquier otro lugar que necesite identificación, esto además de que el /Ola Bini, lo aclararon cada uno de los expertos, no es un usuario sino una carpeta que puede tener cualquiera; por otro lado nos han dicho que no ha sido acceso a un sistema informático, ahora dicen que ha sido al sistema de telecomunicaciones y pasó del aparatito chiquito al aparato grande, aquí se tiene varios problemas, el testigo explicó cuál era el sistema, cómo funcionaba?, el número como estaba configurado? O lo explicó el abogado, en lo que hay una gran diferencia, pero hay algo más importante, cada uno de los testigos, específicamente Roger Lingelang y Agmad les han dicho que los sistemas de telecomunicaciones son efectivamente son los equipos, quien los conecta?, CNT como lo acaba de decir el abogado, Yo en mi vehículo no hago el puente, no hago el camino, Yo solo transito, si a través de internet Yo puedo transitar por esos caminos, es porque alguien puso los caminos ahí, esa es la CNT, ahora resulta que dicen que configuré el internet, que hice los caminos, se pueden conectar pero no lleguen acá, a pesar de que puse el camino, es lo que están tratando de imponer, el señor Dilgedan les dijo al preguntarle cuantos cables hay en su conexión?, dijo que imposible saber, dijo que incluso puede haber un cable por debajo de tierra, no podemos elegir el camino, simplemente ponemos una dirección y luego enter, y llegamos o no llegamos. Pero afirma que el tercer problema en materialidad es efectivamente accedió?, dice que la única teoría posible para mantener ese acceso es la que han dicho supuestamente: pasó de la ONT, pasó del chiquito al grande, pero no es lo que dice el informe presentado por el señor Cárdenas, se dice que ese número 181.113.57.169 es el chiquito y ahí es donde se ha fijado la necesidad de acceso y usuario y de una clave, el supuesto router no ha sido identificado, no se ha dicho que número tenía, y si el router tenía el número entonces cual es la ONT, porque nos han hablado de uno; señala que hay un problema más, citando la ignorancia deliberada, que si bien como elemento subjetivo no es aceptado por nuestra Corte Nacional, ignorancia deliberada es con respecto a los elementos objetivos del tipo, la necesidad de probar un tipo penal, es más el calificaría la ignorancia deliberada como que un artículo no esté vigente al momento de darse el hecho, eso es ignorancia deliberada; pide que se tenga mucha atención en esto, por su relevancia: pide que se verifique la norma vigente a la fecha, porque Fiscalía ha

dicho que cometió el delito contemplado en el artículo 234 numeral primero del COIP, pero ese no es el tipo penal a la época, a la época decía “para explotar ilegítimamente el acceso logrado, modificar un portal web ...”, ese es realmente el tipo penal, entonces Fiscalía no pudo configurar el tipo penal de la época, y se va al actual donde tiene una ultra finalidad que tiene que ser comprobado como todo el tipo, porque no lo habló, ni siquiera lo refirió, no hubo una sola pregunta en toda la audiencia dirigida a la finalidad por la cual, supuestamente la foto si hubiere sucedido, ninguno; entonces analicemos el de la época, primero sin autorización acceda, acceso no hay, es un paso previo donde se pide identificación; a un sistema informático, telemático o de telecomunicaciones, aparentemente ese; en la audiencia no fue demostrado nada más que la fotografía del supuesto sistema y luego viene esa parte que no fue materia de esta audiencia y que por verdad procesal restringe totalmente lo que fue la acusación, “para explotar ilegítimamente el acceso logrado, modificar ...”, algún elemento probatorio sobre esto?, es más, lo único que se podría decir además es saber si en ese lugar había información “crítica”, pero el señor Salguero dijo que a la época el sitio de contingencia estaba funcionando, pero que entró en funcionamiento el siguiente año 2016, lo que es concordante con lo que dijo el señor Ninacuri Macas quien leyó los correos, se puso en funcionamiento un años después, en el 2016, que además no prueba la supuesta finalidad; el señor Ricardo Arguello estuvo aquí sentado como testigo de Fiscalía, respondió una pregunta de cara a comprobar el tipo penal, no dijo que sí me mandó la foto, dijo que se publicó en la prensa una conversación que habríamos tenido, eso fue lo que él dijo; esto es importante porque el artículo 234 actual, por el que se le está tratando de acusar sí tiene dos variables, el numeral 1 donde consta el acceso sin una finalidad ultra subjetiva, más allá de que complemente ese dolo, y el numeral 2 dónde está esa ultra finalidad, es decir se dividió el antiguo 234 en dos, pero a la época era uno solo y eso era lo que se tenía que demostrar; con todo ello hasta estos momentos ustedes pueden notar que la prueba presentada no cumple con presupuestos normativos, ni técnicos, ni siquiera el alcance de la teoría del caso presentada por la acusación, cumplen con los elementos objetivos de manera que podamos hablar de un supuesto delito; esa supuesta foto, no especializada, no técnica, muestra una realidad totalmente distinta y el señor que dice que supuestamente sería un acceso no consentido, se contradice en la misma prueba documental que consta del expediente; señala que la decisión que se debe tomar ya no es solamente si es culpable o inocente, a pesar de todos los excesos que han existido en la tramitación y ejercicio de esta causa: artículo 457 del COIP: se ha verificado la ilegalidad de la prueba obtenida, donde se puede verificar la detención ilegítima, arbitraria y una vulneración al derecho a la defensa, por no conocer los cargos, ese habeas corpus ha sido complementado con la prueba documental, donde se solicita reiteradamente conocer los cargos, los que no se les ha hecho conocer en los momentos procesales correspondientes; ese habeas corpus que ya es cosa juzgada, lo único que se debe hacer es respetar la decisión y determinar si se puede valorar o no la prueba presentada, no sin eso resaltar que los agentes que vinieron acá, no pudieron decir que decía el documento como delito y se ha escuchado la noticia críminis, que el señor Daza dijo que el motivo de la detención es porque lo nombró la Ministra, al igual que el señor Molina, quienes afirmaron además que no le habían escuchado que dijo; María Paula Romo, Lenin Moreno, el señor Roldán, todos hablando del

supuesto caso, imagínense que les dijo la Fiscalía en su alegato final: se describió una vez que pudimos acceder al celular, entonces dicen que empezaron si caso, salí a pescar algo sin relevancia, un teléfono celular, y en esta audiencia se ha repetido sistemáticamente el intento de estigmatizar al señor Ola Bini, Fiscalía ha dicho: sombrero negro, “supuesto” desarrollador de software”, Wikilikcs, que tiene que ver Wikilikcs acá, “estuvo en el País para posiblemente obtener información”, eso no es estigmatizar?; el señor Daza, quien lideró toda la detención dijo “hay muchas personas que vienen de otro país a cometer irregularidades y a ratos sinvergüenzas” y el Tribunal no le permitió seguir; Marco Aurelio Pazmiño quien expuso los dispositivos dijo “68 dispositivos”, fue tal el impacto de la estigmatización que el Tribunal le preguntó: eso es malo que tenga tantos dispositivos?; se le preguntó al señor Muños la razón por la que cogieron libros?, porque Fiscalía le dijo que tomen los libros en un delito informático; Galo Cárdenas dijo lenguaje de bajo nivel TOR, el THOR de superhéroe pero de bajo nivel; cuando el relator de las NNUU en el año 2015 dijo que se promueva el uso de TOR, busquen que los ciudadanos protejan si identidad, es esa la estigmatización a la que se le ha llevado; 9 de 17 testigos presentados, más el alegato de Fiscalía, tienen algún elemento estigmatizante y eso va en contra del artículo 22 del COIP, se suponía que se juzgaban actos, no la persona Ola Bini, ni como se viste ni su sombrero; además en la audiencia se ha podido evidenciar como se ha vulnerado el derecho a la defensa en el curso de la causa, inicia la investigación previa sin noticia criminal; se pide una copia espejo, respuesta no, no le voy a dar la copia espejo; Fiscalía diciendo a la defensa de Ola Bini que está llevando la investigación de una manera privada y secreta, de la cual no está dejando ninguna constancia documental, eso se va a permitir?; sin perjuicio de lo que se dijo, que Fiscalía maneja varias líneas de investigación, esto es la investigación previa? Investigar personas?; con todo esto, habiéndose evidenciado como fue obtenido ese dispositivo celular, que el habeas corpus declara esa detención como ilegal y la regla es no darle eficacia probatoria, porque así lo establece el artículo 454.6 del COIP, el no acceso al informe; prueba que el Tribunal no la podía excluir, pero no la puede, por respeto a la Constitución, los derechos fundamentales, de un marco jurídico vigente; con lo dicho, sin una prueba técnica, sin el cumplimiento normativo, la supuesta foto no demuestra la comisión delito, el no cumplimiento de los elementos del tipo penal, el inicio de un proceso a través de una detención arbitraria, la violación de derechos fundamentales en el proceso, solicita al Tribunal se ratifique la inocencia del señor Ola Bini, lo hagan no solo por él, ya que él ha sido muy claro en lo que es y representa, lo hagan por el sistema, por el derecho penal, que no deliberadamente ignoremos las partes que no nos conviene, para no ver las calificaciones que veremos después en la resolución.

V. FUNDAMENTACIÓN. En un Estado constitucional de derechos y justicia, como es el Ecuador, el Derecho Penal, dentro del ordenamiento jurídico, se convierte en un medio de control social teniendo como función principal la protección y tutela de los bienes jurídicos, los que pueden ser vulnerados por ciertas conductas lesivas, generando la inmediata reacción del Estado en búsqueda de precautelar el orden jurídico y social vulnerado. Corresponde entonces a los Jueces de los Tribunales de Garantías Penales, en ejercicio de la potestad jurisdiccional, otorgada por el Estado, conocer la etapa del juicio y sancionar los delitos que devienen de una acción u omisión típica, antijurídica y culpable; cuando éstos presupuestos se cumplan a

cabalidad, logrando el convencimiento del juzgador de la culpabilidad de la persona procesada más allá de toda duda razonable; para lo cual el “onus probandi” está en manos del ente persecutor, que sustentado en hechos reales introducidos a través de un medio de prueba, deberá demostrar la comprobación del nexo causal entre la existencia de la infracción y la responsabilidad de la persona procesada, superando el máximo estándar de la presunción de inocencia, para lo cual el juzgador deberá valorar los medios probatorios presentados sustentándose en su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica, excluyendo todo medio de prueba obtenido con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la ley, los que carecerán de eficacia probatoria. La actividad probatoria ejercida en la audiencia de juzgamiento bajo los principios de oportunidad, inmediación, contradicción, libertad probatoria, pertinencia y exclusión permiten la búsqueda y acopio de los elementos necesarios para reconstruir un hecho delictivo y las circunstancias que lo rodean, permitiendo que el juez logre “el conocimiento del hecho que mejor responda a la realidad del mismo, a partir de los medios que dispone en el proceso y al amparo de un fin práctico y social no metafísico” (Manzini Vincenzo, Tratado de Derecho Procesal Penal. El Foro. Buenos Aires. 1996. Pag 260), logrando un grado de convencimiento propicio para resolver más allá de toda duda razonable. Siendo necesario que el juzgador al aplicar este estándar probatorio, que establece nuestra normativa penal, sustente su convencimiento, no solo en el campo subjetivo, sino en un examen lógico de los hechos y una apreciación ponderativa de los medios de prueba, previo a establecer como verdadera una hipótesis.

Por otro lado y dentro de las disposiciones relativas a la prueba, el Código Orgánico Integral Penal en su artículo 453 establece que éstas tienen como finalidad el convencimiento del juzgador en cuanto a los hechos y circunstancias, así como establecer la responsabilidad de la persona procesada, todo esto con observancia a los principios en cuanto a su anuncio y práctica en la audiencia de juicio, detallados en el artículo 454 ibídem, como son: 1. Oportunidad: Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio. (...) Las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia orla de juicio. Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido en forma anticipada. 2. Inmediación.- Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba. 3. Contradicción. Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada. 4. Libertad probatoria.- Todos los hechos y circunstancias pertinentes al caso se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas. 5. Pertinencia.- las pruebas, deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad de la persona procesada. 6. Exclusión.- Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución,

en los instrumentos internacionales de derechos humanos o en la ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal. Se inadmitirán aquellos medios de prueba que se refieran a las conversaciones que haya tenido la o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones pre-acordadas. Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones, siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como pruebas. 7. Principio de igualdad de oportunidades para la prueba.- Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal.” En cuanto a los medios de prueba el COIP en su artículo 499 señala “Los medios de prueba son: El documento, el testimonio, la pericia.” 455.- “La prueba y los elementos de prueba deberán tener un nexo causal entre la infracción y la persona procesada, el fundamento tendrá que basarse en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones.” 456.- “Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio.(...)” 457.- “La valoración de la prueba se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales. La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente.”; siendo por ello la prueba de suma importancia para la justificación de esos presupuestos, debiendo por tanto ser obtenida a través de mecanismos o medios lícitos.

VI CONSIDERACIONES Y FUNDAMENTACIÓN SOBRE LA EXISTENCIA DE LA INFRACCION Y LA RESPONSABILIDAD DEL PROCESADO.- El Tribunal considera, por mandato legal, que es obligación de la Fiscalía, sobre quien descansa el ejercicio de la acción penal y el impulso de la acusación en la sustanciación del juicio, probar su hipótesis de adecuación típica. Bajo esta premisa el Tribunal debe entrar a analizar si en el caso, de la prueba incorporada se ha demostrado o no la existencia del delito, entendido éste como un acto típico, antijurídico y culpable, donde cada categoría dogmática tiene sus propios elementos que le dan contenido material al injusto, debiendo por tanto demostrarse la existencia material de la infracción como la responsabilidad o la culpabilidad de quien la ha cometido, así como el nexo causal existente, por lo que la adecuación de la conducta del sujeto corresponde en inicio y como se refirió anteriormente, al representante de la sociedad quien a través de la acusación expresa la pretensión punitiva del Estado, la que será sometida en la etapa respectiva, al juicio de desvalor de la inocencia del enjuiciado y solo cuando el juzgador obtenga la certeza del cometimiento del delito y que el sujeto es el culpable del acto, establecerá el grado de responsabilidad, encaminado normalmente al tipo penal por el que ha sido traído a juicio, haciendo referencia a los hechos por los que ha sido investigado, garantizando de esta manera la tutela judicial efectiva, el debido proceso, la seguridad jurídica y el derecho

a la defensa.

En la presente causa al tratarse de un delito de “acceso no consentido a un sistema informático, telemático o de telecomunicaciones”, pues la resolución de llamamiento a juicio inicialmente referida así lo detalla, éste se encuentra descrito en la ley, específicamente en el artículo 234 del COIP, aplicable al caso, que describe: “La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con una pena privativa de libertad de tres a cinco años”; conducta punible determinada por los verbos rectores: ACCEDER, que según la Real Academia Española significa “entrar en un lugar o pasar de él”; acción que debe ejecutarse en todo o en parte; y, a sistemas informáticos, telemáticos o de telecomunicaciones; o MANTENERSE dentro de los mismos, en contra de la voluntad de quien tenga el legítimo derecho; tipo penal que además contempla una FINALIDAD específica: explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re-direccionar el tráfico u ofrecer estos servicios sin pagar a los proveedores; debiendo considerarse además que en esta acción de acceso indebido, se REQUIERE ESENCIALMENTE que el autor haya VULNERADO un sistema de protección o de seguridad para lograr este acceso al sistema informático, ya que necesariamente este debe ser RESTRINGIDO; como claramente lo explica el autor argentino Gustavo Eduardo Aboso: “... lo que acá se exige es el que el autor haya superado las medidas de seguridad que caracterizan a los sistemas informáticos con acceso restringido mediante el uso de programas para vulnerar los códigos de acceso, o bien utilizando los códigos auténticos de una persona autorizada.” (Gustavo Eduardo Aboso. Derecho Penal Cibernético. Editorial B de F. Montevideo-Buenos Aires. 2017. pág. 184).

El delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, exige que se lo haya cometido con conciencia y voluntad, debiendo considerarse además que es un delito doloso por expresa disposición del artículo 234 del Código Orgánico Integral Penal; al respecto el artículo 26 *ibídem* establece “Actúa con dolo la persona que tiene el designio de causar daño”; al referirse al dolo, los tratadistas Francisco Muñoz Conde y Mercedes García Arán, en la obra Derecho Penal, Parte General, 8va Edición, editorial Tirant lo Blanch, Valencia-2010, manifiestan que el dolo “se entiende simplemente como la conciencia y voluntad de realizar el tipo objetivo de un delito (...) el dolo está constituido por dos elementos: uno intelectual o cognitivo y otro volitivo. a) Elemento intelectual. Para actuar dolosamente, el sujeto de la acción debe saber qué es lo que hace y conocer los elementos que caracterizan su acción como conducta típica. (...) El intelectual del dolo se refiere, por tanto, a los (elementos objetivos del tipo): sujeto, conducta, resultado, relación causal o imputación objetiva, objeto material, etc; (...) b) Elemento volitivo. Para actuar dolosamente no basta con el mero querer realizarlos. Este querer no se confunde con el deseo o con los móviles del sujeto (...) el elemento volitivo supone la voluntad incondicionada de realizar algo (típico) que el autor cree que puede realizar”. Entonces el autor debe realizar necesariamente la acción de

acceder al sistema informático restringido, conociendo la ausencia de autorización para aquello (DOLO DIRECTO).

En el presente caso el Tribunal analiza el conjunto de pruebas producidas en el curso de la audiencia de juzgamiento, debiendo recalcar el hecho de que este Juez Pluripersonal no puede pronunciarse sino de la prueba que fue actuada por los sujetos procesales, dentro de la cual se tiene en primer lugar los testimonios de los agentes policiales que refirieron las causas que originaron o por las cuales se dio inicio a esta investigación; en primer lugar compareció el Mayor de Policía David Alexander Andrade Daza, quien dijo ser el Jefe de la Unidad de Delitos Tecnológicos de la Dirección Nacional de la Policía Judicial, con capacitación en delitos cibernéticos recibida en Brasil, Chile, República Dominicana y en el Ecuador; sobre el caso dijo que el 11 de abril del año 2019, a eso de las 13:20 llegó a la Unidad una denuncia telefónica de un “alias” Marco, en la que se decía que el ciudadano Ola Bini se trasladaba al aeropuerto y que había escuchado a la Ministra del Interior decir que dicho ciudadano tenía vínculos con Julián Assange, esta información recibida motivó a que “activara” a sus agentes de manera inmediata, al cabo de Policía Patricio Paredes, agente de la unidad de “capturadores” para que se encuentre pendiente; a los agentes de Policías Cristian Camacho y William Molina, quienes a eso de las 14:30 generaron un parte solicitando tomar versión al ciudadano Ola Bini y pedir la judicialización del caso ante la Fiscalía, es por esto que se dio a conocer al Fiscal doctor Fabián Chávez, quien dispuso la inmovilización del ciudadano Ola Bini; que a las 17:58 nuevamente el sargento Cristian Camacho y el cabo William Molina “generan” un documento en el cual solicitaban el allanamiento al domicilio del señor Ola Bini; dijo que a las 23:00 avanzaron al aeropuerto con el señor Fiscal, sus agentes de la Unidad de Delitos Tecnológicos y personal de Criminalística, así como con personal de Interpol, específicamente con el sargento Luis Vásquez, quien le dio a conocer los derechos al señor Ola Bini, en los dos idiomas, inglés y español; mientras tanto dijo que coordinó con el personal de Criminalística para que levanten indicios o evidencias en el aeropuerto; a las 02:30 junto al Fiscal y más personal, específicamente el subteniente Rodrigo Muñoz y el sargento Claudio Castillo, realizaron el allanamiento en el domicilio del señor Ola Bini, verificando un “sin número de dispositivos electrónicos” como pendrive, aparataje tecnológicos, cableado que estaba tendido y otros arrumados en el lugar; el Jefe de la Unidad de Delitos Tecnológicos fue claro en manifestar que “se trataba de un delito de conmoción social, porque así lo decía la Ministra del Interior” afirmando además que “hay muchas personas que vienen de otros países a cometer irregularidades en nuestro País”; aclaró luego que él desconocía si la Ministra mencionó el cometimiento de un delito informático, ya que él no escucho a la Ministra en el noticiero y que era un “procedimiento de magnitud y prontitud que tenían que realizar”, por eso casi toda la Unidad estuvo en ese procedimiento; finalmente dijo que la denuncia decía textualmente “Ola Bini de nacionalidad rusa, con vínculos con Julián Assange, que vive en la calle Juan Diguja, que es nombrado por la ministra y que se dirige al aeropuerto”. En segundo lugar comparecieron los agentes “activados” de la Unidad de Ciberdelitos: el cabo William Molina Valenzuela explicó que ese día 11 de abril del 2019, efectivamente recibió un memorando del Mayor David Andrade, al cual se adjuntaba la denuncia presentada y se le disponía que realice un análisis del caso y se proceda a su judicialización; explicó que el

denunciante era un “alias” Marco, quien decía conocer al señor Ola Bini Methodius, el cual tenía vínculos con el señor Assange, persona que la señora Ministra había nombrado en los medios de comunicación en esa mañana y quien estaba a punto de salir del país, mencionaba además su dirección domiciliaria en las calles Juan Diguja y Voz Andes; afirmó que junto al sargento Cristian Camacho, se trasladaron a dicho domicilio a eso de las 15:00, se contactaron con 2 personas que no quisieron identificarse y dijeron que el ciudadano Ola Bini Methodius vivía en el edificio Bertone, 4to. piso, departamento 12; aclaró que para poder cometer un delito informático en general, se necesita de una persona, un dispositivo móvil, un ordenador y acceso a internet, pero que en la denuncia recibida no se señalaban estas características; señaló finalmente que solicitó la detención para investigaciones del ciudadano Ola Bini por el reporte televisivo de la Ministra del Interior, a pesar de que él no vio esa noticia; y, que solicitó la detención para evitar el cometimiento de un delito flagrante, este era “la salida del País de Ola Bini”; por su parte el sargento José Patricio Paredes Ruiz dijo haber realizado dos partes: el primero dando cumplimiento a una orden Fiscal, el 11 de abril del 2019, la cual consistía en impedir que el ciudadano Ola Methodius Bini se ausente del lugar donde sea ubicado, por un tiempo no mayor a 8 horas, orden que le dio lectura a dicho ciudadano en español y con ayuda del sargento Vásquez, en idioma inglés en el aeropuerto eso de las 14:00 o 15:00, aclarando que no constaba ningún delito en el oficio de Fiscalía; el segundo procedimiento o parte, consistió en dar cumplimiento a la orden de detención con fines de investigación del ciudadano Ola Bini Methodius, dispuesto por la doctora Gloria Mayorga, Jueza de la Unidad Judicial de Garantías Penales, le leyó sus derechos en idioma español e inglés y a eso de las 02:00 del siguiente día, por disposición del Fiscal se trasladó con el detenido desde el aeropuerto hasta el exterior del domicilio del señor Ola Bini, lugar en el que el ciudadano Ola Bini dijo que no deseaba ingresar mientras se realizaba el allanamiento, posterior de lo cual, a eso de las 04:00 se trasladó a la Unidad de Flagrancia para realizar el procedimiento, obtener el parte médico y comunicar al consulado, hecho que lo hizo a eso de las 06:46; y, finalmente sobre este tema, compareció a rendir testimonio el agente de la INTERPOL Ángel Guarnizo Rosillo, quien dijo que él asiste en detenciones de personas en delitos internacionales o donde hay ciudadanos de lengua inglesa; señaló en lo principal que por disposición de la Jefa de su Unidad Capitana Vanesa Muñoz, colaboró en un procedimiento del sargento Segundo Luis Vásquez, para leerle los derechos constitucionales en inglés, a una persona extranjera de habla inglesa, Ola Methodius Bini, lo que ocurrió el 12 de abril del 2019, a las 05:30, en la Unidad de Delitos Informáticos de la Policía, ubicada en la Av. Amazonas y Roca de la ciudad de Quito, en el lugar tomó contacto con el señor Patricio Paredes y el detenido, quien se identificó como Bini Methodius, a eso de las 06:00 le leyó sus derechos en el idioma inglés, de acuerdo al artículo 77 de la Constitución de la República del Ecuador; afirmó que el señor Bini le indicó que había entendido lo que le leyó y que entendía tanto el idioma español como el idioma inglés; aclaró que no sabía de qué nacionalidad era el señor Bini, pero que hablaba el idioma inglés, idioma en el que le dijo que estaba siendo detenido por orden de autoridad competente, sin recordar de qué delito se le acusaba.

De los testimonios rendidos tanto por el Jefe, como por los agentes de la Unidad de Delitos Tecnológicos de la Dirección Nacional de la Policía Judicial, se puede

comprobar que el ciudadano procesado Ola Methodius Martín Bini, fue efectivamente detenido el 11 de abril del 2019, en el aeropuerto Mariscal Sucre de Tababela cuando se disponía a salir del País, esto debido a una “denuncia” de un ciudadano con el “alias” Marco, quien habría afirmado que “el ciudadano Ola Bini se trasladaba al aeropuerto y que había escuchado a la Ministra del Interior decir que dicho ciudadano tenía vínculos con Julián Assange”, siendo primeramente impedido de ausentarse del lugar donde fue ubicado (aeropuerto Mariscal Sucre, por un tiempo no mayor a 8 horas), para luego ser detenido por orden una jueza de la Unidad Judicial de Garantías Penales en dicho lugar; debiendo resaltarse el hecho de que para dichos agentes policiales “se trataba de un delito de conmoción social, porque así lo decía la Ministra del Interior”, llegando incluso a afirmar que “desconocían” si se trataba del cometimiento de un delito “informático” o algún otro delito específico, pero aseverando que tenían que realizar un “procedimiento de magnitud y prontitud”, ya que se trataba de un delito de conmoción social; advirtiéndole al Tribunal que de la supuesta denuncia de “alias” Marco, no se puede establecer acción ilícita alguna, pues viajar fuera del País, o tener vínculos de amistad con otras personas, no constituyen por sí y de forma alguna el cometimiento de una infracción penal, menos aún flagrante, la que motivó primero su detención e incluso se autorizó un allanamiento posterior a su domicilio; llamando además la atención de este juzgador pluripersonal que dichos actos: viajar fuera del País o tener relaciones de amistad con una persona, hayan “activado” a toda la Unidad de Delitos Tecnológicos de la Policía Nacional, sin conocerse el delito que supuestamente se estaba cometiendo, ni las circunstancias de dicha infracción.

Como consecuencia de la detención del ciudadano Ola Methodius Martín Bini y del posterior allanamiento a su vivienda, comparecieron una serie de peritos que participaron en estas diligencias; en primero lugar compareció a rendir testimonio el perito de Criminalística y Teniente de Policía Ricardo Martín Muñoz Navarrete, también perteneciente a la Unidad de Cibercrimitos, quien manifestó que por disposición del Jefe de la Unidad, acompañó al Fiscal doctor Chávez con su equipo conformado por el sargento William Frías, el sargento Claudio Castillo y el cabo Luis Aldáz, para dar cumplimiento a una orden de allanamiento dispuesta por la Jueza Gloria Mayorga, el 12 de abril del 2019 a las 03:00, inmueble ubicado en la calle Diguja, Edificio Bartone, 4to. Piso, departamento 12, ingresaron al domicilio y fijaron, etiquetaron y recolectaron más de 300 indicios, trasladándolos a la bodega de la Unidad de Flagrancia; aclaró que por disposición del Fiscal de la causa levantaron aparatos electrónicos como computadoras, tablet, celulares y memorias USB, así como también una caja fuerte sin identificar su contenido, libros, varios pasaportes y tarjetas bancarias a nombre de Bini Ola Methodius Martín; recordó que el 11 de abril 2019 a las 23:00, salió en precipitada carrera del domicilio de la calle Diguja, un vehículo no identificado, lo siguieron hasta la gasolinera Primax de la 9 de Octubre y Orellana y pidieron los datos al propietario del vehículo, el cual se identificó e indicó sus documentos y posterior se le solicitó que continúe su marcha, porque no presentaba ninguna novedad; finalmente dijo que por orden del Jefe de la Unidad, el domicilio quedó bajo vigilancia policial. En segundo lugar compareció el Capitán Diego López Tapia, perito del Departamento de Criminalística quien dijo que por orden de Fiscalía realizó la pericia de inspección ocular técnica en las oficinas de la INTERPOL del aeropuerto Mariscal Sucre de Tababela, el 11 de abril del 2019 a eso

de las 23:00, con el Capitán Ariel Velasco y los sargentos Lincango y Talabera; dijo que procedieron a realizar la inspección y fijación técnica de elementos electrónicos, informáticos y de telecomunicaciones de 4 maletas: la primera de color gris contenía varios documentos tipo tarjeta a nombre de Ola Bini y 90 dólares americanos, así como dos tarjetas plásticas con un logo que decía Visa; en la segunda maleta constató en lo principal, diferentes artículos informáticos, electrónicos y de telecomunicaciones, siendo los principales una computadora portátil, 2 tablet, 2 teléfonos celulares, 2 tarjetas plásticas con chip SIM, USD 1.200,00, 14 nano llaves de seguridad, 29 dispositivos tipo llaves, 23 dispositivos tipo USB y 23 contenedores y alambres tipo USB, una antena de recepción de señal; en la tercera maleta se encontraron dispositivos de conexión USB, cables auxiliares tipo USB y cables de conexión; y, en la cuarta maleta encontró un parlante portátil, dos modem de conexión a internet, 14 cables de conexión y dos cables de red; aclaró que él desconocía las causas que motivaron la investigación que llevaba Fiscalía.

Sobre este tema compareció además el perito del Departamento de Criminalística y Capitán de Policía Ariel Alexis Velasco Albán, quien dijo haber realizado las pericias de reconocimiento del lugar de los hechos y reconocimiento de evidencias encontradas en el departamento del hoy procesado Ola Martín Bini, ubicado en la calle Juan Diguja con numeración EO2-30, edificio Bartone, 4to. Piso, departamento No. 12; en cuanto al reconocimiento del lugar dijo que el inmueble se encuentra en el sector norte de Quito, que para su ingreso el edificio tiene una puerta de madera, luego por un pasillo, al lado izquierdo hay un ascensor, por donde suben al 4to. piso, al departamento 12, dentro del cual se observa los siguientes ambientes: cocina, sala, al costado derecho existe un dormitorio, seguido de un ambiente destinado para oficina, a continuación hay un baño y al fondo se encuentra un ambiente destinado para el dormitorio No. 2; en cuanto a los indicios fijados dijo que se trataba de varios dispositivos electrónicos, tarjetas, varias computadoras marca Lenovo, modem, dispositivos electrónicos, soporte de papel moneda, cables de poder, USB, detallando individualmente a cada uno de estos, así como también describió en lo principal a una caja fuerte metálica color plateada, varios discos duros de diferentes marcas, dispositivos de almacenamiento de datos, varios I pod, varios pasaporte a nombre de Ola Bini y varias tarjeta Visa a nombre de Ola Bini; detalló además varios libros con títulos como Privace Lod, Panamá Papers, Hackers Play Book, Hacker Coaccer, The Dark Red, The Black Book, Cyber Ware, Cyber Ware, Snowden y Wikileaks; cargadores de computadora, cables de poder, cables UTP, 12 cables de impresora; varios teléfono celulares marca Samsun y I pone; soporte de papel moneda de diferentes nominaciones y países; y, varias tarjetas a nombre de Ola Bini; aclaró que los agentes investigadores indicaron que libros debía fijar como evidencias, pues habían otros más que no fijaron; que no conoce cuál era la infracción que se investigaba. Sobre este mismo tema, esto es el reconocimiento de evidencias, compareció el perito del Departamento de Criminalística Henry Daniel Yépez Ortiz, quien afirmó ante el Tribunal haber realizado cinco pericias en la presente causa: **PRIMERA PERICIA:** realizó el reconocimiento de indicios que tienen relación con la aprehensión del señor Ola Bini y que se encontraban bajo cadena de custodia No. 177219, procediendo en la audiencia a exhibir las fotografía de cada uno de estos, los que consistían en: 10 tarjetas plásticas a su nombre; 3 billetes de 20 dólares y 3 de 10 dólares, una moneda de 0.50 euros; varios fragmento

de papel de diferentes colores; documentos de vacunación; un pasaporte a nombre de Ola Bini Metoduis Martin; 60 soportes de papel con similares características al billete de 20 dólares; una tarjeta plástica con chip; una tarjeta de presentación; 4 dispositivos de almacenamiento de datos electrónicos tipo USB, sellados; 8 concentradores de poder conocidos como PAV; 3 acumuladores de energía portables y un dispositivo de alimentación de energía; 7 adaptadores de puertos para transmisión de datos; 19 elementos de almacenamiento de datos tipo PAV; un adaptador; 5 lectores de tarjetas inteligentes; 10 dispositivos de autenticación de credenciales; 13 dispositivos de autenticaciones de credenciales; 12 nano dispositivos de identificación de credenciales; otros 2 nano dispositivos de identificación de credenciales; 14 dispositivos de almacenamiento de datos electrónicos tipo USB; 6 lectores de tarjetas inteligentes; un computador portátil marca Lenovo; 2 tablet tipo I pod marca Apple; un dispositivo de comunicación móvil tipo celular, marca Apple, color negro y un dispositivo color negro de comunicación móvil, marca Samsun; 2 soportes de papel con similares características al de papel moneda de 50 Euros; 2 monedas metálicas que se lee 2 Euros; 3 monedas metálicas que se lee un Euro; 3 monedas metálicas que se le 0.50 Euros; 5 monedas que le lee 0.10 Euros; 20 monedas metálicas que se lee 0.20 Euros; otras monedas que lee Euros; 12 cables de datos con diferentes interfaces; un conector de puertos; un acumulador de energía portable; 4 dispositivos de almacenamiento de datos tipo USB; dos cables de datos; un concentrador de puerto, dos enrutadores; 7 cables de datos; un altavoz inalámbrico; un dispositivo de alimentación de energía; 3 regletas de alimentación de energía; mientras que en la cadena de custodia No. 8851922 encontró los siguientes indicios: un Swift de 24 puertos, un modem, un computador portátil marca Toshiba, color plomo, con un dispositivo USB de 16 gigas, una caja fuerte metálica, color plateada, un dispositivo de almacenamiento disco duro marca Hitachi, un dispositivo de almacenamiento de datos, un disco duro externo marca G Drive de 3 Teras de capacidad, con cable de datos USB color negro; 4 dispositivos de almacenamiento de datos externos (disco duro), marca Lassie; dos dispositivos de almacenamiento de datos marca Wester Digital de 160 gigas; un dispositivo de almacenamiento de datos marca Lassie; dos unidades de almacenamiento de datos marca Hitachi, de 2 Teras de capacidad; un disco duro marca Digital: otro disco duro externo; una tarjeta de memoria marca Scan Disc de 4 gigas; 15 dispositivos de almacenamiento de datos electrónicos tipo USB; un computador portátil marca Lenovo; un computador portátil marca Lenovo color negro, sin batería, un computador portátil marca Lenovo; un computador portátil marca Lenovo, sin batería de alimentación; un computador portátil marca Lenovo, sin batería; un computador portátil marca Lenovo; un computador portátil marca Lenovo sin batería; un computador portátil marca Lenovo; un computador portátil marca Lenovo; un computador portátil marca Positivo; un computador portátil marca Apple; un computador portátil marca Apple; 6 tabletas tipo I pod, marca Apple; tres pasaportes a nombre de Ola Metodius Bini Martin; una tarjeta Visa a nombre de Ola Bini; otra tarjeta marca Visa a nombre de Ola Bini; una libreta color negro con textos manuscritos color azul; 12 libros con diferentes títulos en su pasta principal; un teléfono fio color negro; una computadora portátil marca Apple, un router, otro router; otro router inalámbrico marca Apple, un dispositivo electrónico color blanco con teclado; un disco duro externo marca Toshiva de 2 Teras; 40 tarjetas color blanco;

dos dispositivos electrónicos con teclado alfa numérico con puerto USB, con su respectivo cable de datos USB; 12 soportes de papel con textos impresos y manuscritos; un periódico que se lee El Comercio 13 de octubre del 2015, con 6 hojas; un periódico que se lee El Telégrafo martes 13 de octubre del 2015; 12 papeles tamaño A4 con textos manuscritos; un soporte de papel A5; 51 cables con diferentes interfaces; 5 adaptadores o cargadores marca Lenovo; 7 cables de alimentación; 2 router marca Apple; 2 router marca I pone, con capacidad de 2 Teras; un lector de unidades ópticas con cables USB; 4 cables de alimentación de energía con un adaptador marca Toshiva; un cargador marca Lenovo; un cargador marca Deline; un computador marca Lenovo; un computador portátil marca Lenovo; un computador Sistem 76; un reproductor de archivos multimedia marca I pone; dos teléfonos celulares, un teléfono celular marca Samsun; un router inalámbrico marca Apple; un router marca Apple; un cable de alimentación de energía color blanco; una tarjeta de memoria de 8 gigas; 6 dispositivo de almacenamiento de datos tipo USB; 54 soportes de papel con textos impresos y manuscritos; un soporte de papen con la leyenda 10 pesos argentinos; un soporte de papel con la denominación 10 pesos argentinos; dos soportes de papel con la denominación de 5 pesos argentinos; y, varios soportes de papel con la denominación de varias monedas extranjeras; un documento de identificación a nombre de Strain Ambas Longan; una tarjeta con la leyenda Visa a nombre de Samer Mary; una tarjeta con la leyenda que se lee Mastercard; una tarjeta con la leyenda Atlantic a nombre de Ola Bini; una tarjeta que se lee Asociación Computer Machine a nombre de Ola Bini y una tarjeta con la leyenda que se lee National Usa Number, a nombre de Ola Bini; prendas de vestir: una mochila de nylon color negra, con 6 libros de diferentes colores, con diferentes textos; un cable de poder y un audífono; una maleta de viaje color negro, en cuyo interior constaban 13 camisetas negras, 13 pares de medias color negro con plomo, 9 interiores tipo bóxer, 6 esferográficos y una chompa de tela color negro; dos pantalones, uno jean y otro de tela color negro; dos gafas marca Ray Ban; una tarjeta electrónica de color blanco; 6 tarjetas de presentación a nombre de Ola Bini; un bolso pequeño de nylon y un sombrero de color negro; un termo metálico color plateado, 4 frascos de plástico color blanco; una maleta de tela color negro conteniendo 40 paquetes de galletas; un estuche de nylon conteniendo útiles de aseo; un estuche conteniendo pastillas; tres cinturones color negro y uno amarillo; 2 pantalones de tela; dos chaquetas de tela color negro, dos buzos de licra color negro; un par de zapatos deportivos blancos, plomo y anaranjado, marca Adidas; 5 folletos de artes marciales, un cable color negro y un candado pequeño color amarillo; 9 pares de guantes; llega a la conclusión de que los objetos descritos existen y se encuentran Centro de Acopio del Laboratorio de Criminalística; sobre este informe aclaró que la mayoría de libros encontrados trataban de Hacking, que es el área de informática que se encarga de buscar y explotar ciertas vulnerabilidades de sistemas y redes; **SEGUNDA PERICIA:** Realizó la fijación, adquisición y preservación del contenido digital de los dispositivos electrónicos encontrados dentro de la caja fuerte que permanecía en el interior del departamento de Ola Bbini, hecho realizado a través de la generación de copias espejo e imágenes forenses; eran dos dispositivos de almacenamiento externo o discos duros: uno marca Toshiba identificado como DE01, serie 76EE7G06DPGC, de 2 teras de capacidad y, el otro identificado como DE02, disco duro marca Selgay, serie

NA8RA821, de 2 Teras; señalando que fijó además 15 dispositivos de almacenamiento de datos tipo flash memory, de los cuales 13 son de marca Kingston y 2 de marca Scan Disc; **TERCERA PERICIA:** esta consistió en realizar la fijación, preservación y extracción del contenido digital de 6 URL o direcciones electrónicas: 1) URL: https://www.youtube.com/wapch?ube=blorwlbvxvo*fearqre=youtuve.e: video no está disponible; 2) <https://www.youtube.com/wapch?ube=1210913100hbien>: video no está disponible; 3) <https://www.youtube.p/bhkeh4vbz6d>: no se puede acceder a este sitio; 4) <https://www.youtube.b/b36f9t4anq0>: no se puede acceder a este sitio; 5) <https://ww.eluniverso.com/noticias/2019/04/16/nota/7289255/lenin-moreno-dice-que-se-sorprendió-ola-bini-hakeando-cuentas>: página web del El Universo, que lleva como título: Lenin Moreno dice que se sorprendió a Ola Bini hackeando cuentas del gobierno y personales, de 16 de abril del 2019, a las 18h32; 6) <https://www.facebook.com/watch/?v=821680031522415>: SR radio, título: Entrevista a los Ministros de RR.EE e Interior del Ecuador, sobre retiro de Asilo a Julián Assange; **ACLARACIÓN:** al ser exhibidos los contenidos de los CD de estas direcciones electrónicas en la audiencia, se puede constatar que no corresponde a lo descrito por el perito, pese a que afirma que ese CD contiene el número de cadena de custodia que consta en el informe. **CUARTA PERICIA:** consistió en realizar la fijación, preservación y extracción del contenido digital de otra URL o dirección electrónica: https://www.youtube.com/wapch?v=0g9xolmoa6g*t=8155S: título verás29mapaularomo, de fecha 9 de junio del 2019, contiene entrevista Carlos Vera a María Paula Romo: asunto detención de Ola Bini; **QUINTA PERICIA:** consistió en realizar la fijación, preservación y extracción del contenido digital de otra URL o dirección electrónica: <https://www.amnesty.org/download/document/amr2808712919spanish.pdf>; sitio web de amnesty.org; título Ecuador violaciones de derechos humanos en proceso penal contra Ola Bini: <https://www.amnesty.org/es/lamnst/newps/2019/08/ecuador>: gobierno interfiere en proceso penal contra Ola Bini.

Analizando la prueba pericial descrita, el Tribunal observa que esta se refiere de manera específica, a la descripción de los bienes de propiedad del procesado Ola Bini, tanto los que lo llevaba consigo en cuatro maletas cuando pretendía viajar desde el aeropuerto Mariscal Sucre de Tababela, como los bienes que mantenía en su domicilio de la calle Diguja, norte de la ciudad de Quito, bienes que consisten principalmente de aparatos electrónicos como computadoras, Tablet, celulares, memorias USB, cables de conexión y otros, pudiendo apreciarse además que en calidad de “indicios” se habría retenido además una caja fuerte, libros, pasaportes, tarjetas bancarias y personales, sin que el Tribunal entienda la pertinencia de dichos “indicios”; de las pericias expuestas además se verifica la existencia tanto de las oficinas de la INTERPOL en el aeropuerto Mariscal Sucre, lugar en el que fue aprehendido el ciudadano Ola Bini, así como su lugar de vivienda, ubicada en el Edificio Bertone de la calle Diguja; por otro lado se debe señalar que en las pericias se describe pormenorizadamente a los dispositivos electrónicos, como sus marcas, número de series, color y demás características, sin que se llegue a explicar o determinar la pertinencias y conducencia de estas “evidencias”, así como tampoco se expuso ante el Tribunal el objetivo de retener libros, tarjetas bancarias, tarjetas de presentación y otros bienes personales, que no tienen conducencia con el delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones;

finalmente en cuanto a la materialización de varias “URL” o direcciones electrónicas, se debe resaltar el hecho de que cuatro de estas direcciones no tenían contenido alguno, mientras que otras dos tan solo tenían noticias de prensa, las cuales a criterio del Tribunal no constituyen prueba alguna, debiendo eso sí recalcar el Tribunal que incluso, al solicitarse se exhiban en la audiencia uno de los CD que contenían “estas pruebas” técnicas (contenidos de las direcciones electrónicas), se pudo establecer que su contenido no era el que el perito describió en la audiencia, se trataba de otro tema muy diferente y no relacionado con el caso investigado, pese a que el perito afirmó que se trataba de la misma cadena de custodia que constaba en el informe por él realizado, si saber explicar a los Jueces lo que sucedía.

OTROS TEMAS:

Sobre otros temas, compareció a rendir testimonio el Gerente Regional y apoderado de TELCONET Igor Krochin Lapenti, quien explicó que el 2 de abril del año 2015, firmó un contrato de “Housing” (servicio de data center) y de enlace de datos, en español, con el señor Ola Bini, mediante el cual se le dio un espacio en el Data Center y un enlace de datos de 10 MDT, afirmando que el 10 de abril procedieron a instalar los equipos, que consistían básicamente en un servidor de datos, afirmando luego que el contrato terminó el 15 de mayo del 2019, sin tener ningún tema especial que mencionar; explicó que un Data Center, es un lugar donde se almacenan muchos computadores, el cliente lleva su propio computador y éste es alojado en estas instalaciones, lo que permiten que dos o más puntos se interconecten entre sí, a través de la nube de internet; además dijo que el Data Center tiene capacidad de enfriamiento de las alas de las computadoras, las que deben mantenerse frías ya que miles de computadoras generan calor, cuenta con todo el equipo de enfriamiento, de disipación, más las instalaciones del edificio; refirió además los equipos del señor Ola Bini en el Data Center están ubicados en la calle Los Aceitunos E5-85 y Av. Eloy Alfaro, al norte de Quito, donde tienen un edificio de dos pisos, sus equipos se ubican en el piso 2, en la fila 3, en el RAP 6, aclarando que no conoce el propósito de los equipos de sus clientes; dijo que el señor Ola Bini recibió una factura por el servicio de USD 2.800,00, pero que en la factura el pago total mensual es de USD 4.360,00 más IVA; expresó que tiene muchos clientes del sistema financiero, cooperativo, entidades del gobierno y personas naturales; finalmente refirió que Fiscalía dispuso que los equipos del señor Ola Bini le fueran entregados, un servidor y un ruteador.

Por otro lado compareció a rendir testimonio Cristian Patricio Cruz Medina, funcionario del Ministerio de Relaciones Exteriores del Ecuador, quien dijo que en el año 2018 se desempeñaba como Coordinador Zonal 9 del MRE en la ciudad de Quito; que con respecto al señor Ola Bini, se había identificado 3 visados otorgados, el primero en el 2015 y otro en el 2016, visas de trabajo y el tercero y último, emitido en mayo del 2018, fue una visa especial de residencia temporal de excepción, cuya concesión es de competencia privativa de la autoridad de Movilidad Humana del Ministerio, son autorizadas por el Vice Ministro de Movilidad Humana; en cuanto a las visas de trabajo del 2015 y 2016, dijo que se emiten en virtud de un hecho generador, la existencia de un vínculo laboral que permite a los extranjeros, con contrato de trabajo recibir ese visado y que para el visado del 2018, se presentaron dos comunicaciones al auspiciante Ola Bini, uno de la compañía Soporte Libre y una comunicación de Autonomía Digita.

Sobre estos dos temas, el Tribunal puede constatar que el ciudadano procesado Ola Bini efectivamente habría contratado los servicios de un Data Center o Housing, así como de un enlace de datos con la empresa TELCONET, la misma que estaba representada por el ingeniero Igor Krochin Lapenti, empresa a la canceló mensualmente por dicho servicio y que a decir del representante de la Compañía nunca tuvo problema alguno su cliente, debiendo recalcar el hecho de que la Fiscalía fue la Institución que “solicitó” le sean entregados tanto el servidor de datos del señor Ola Bini, como el “ruteador” de TELCONET, sin que el Tribunal pueda relacionar estas “nuevas” evidencias con ninguna pericia practicada en ellas, o la obtención de alguna información que se relacione con estos dispositivos; lo mismo que ocurre con la información que sobre los visados obtenidos por el señor Bini en el Ministerio de Relaciones Exteriores, en los años 2015, 2016 y 2018, conforme lo refirió Cristian Cruz Medina, trámites realizados que no establecen nexo alguno con el presunto ilícito investigado, pues de manera alguna esta prueba es pertinente o conducente con la infracción, llamando nuevamente la atención del Tribunal su presentación en la audiencia de juicio, por las características que se han mencionado.

OTRAS PERICIAS:

Continuando con la descripción de más pericias que se presentaron en la audiencia de juicio, el Tribunal analiza el testimonio del Capitán Marco Aurelio Pazmiño Montaluisa, perito del Departamento de Criminalística, quien explicó a los Jueces que practicó cuatro pericias: PRIMERA: dijo que tenía que ver con una audiencia privada de exhibición del contenido digital de la cadena de custodia 1772-2019, contenida en 68 equipos: 19 de cómputo, 13 de almacenamiento externo, 3 de almacenamiento interno, 31 dispositivos de almacenamiento USB y 2 tarjetas de memoria SD; explicando que generó 72 imágenes forenses, resaltando el hecho de que los archivos que constaban en los dispositivos estaban basados en LINUS y tenían un proceso de cifrado de datos que no permitía que la información sea legible, solicitando a las “partes” proporcionar estos accesos y al no contar con ellos, solicitó a Fiscalía se haga una asistencia penal internacional para hacer que los datos sean legibles; sin embargo dijo que lo que hizo, se validó de manera aleatoria ciertos dispositivos, analizó una flash memory, una USB, un equipo de cómputo y un dispositivo de almacenamiento externo, vieron que todos manejaban sistemas operativos Linux y tenían algún tipo de distribución como Fedora, estas distribuciones sirven para hacer, por ejemplo de un estudio bibliográfico, permite hacer navegaciones seguras, anónimas, Teits tiene la característica de no instalarse directamente en el equipo, sino que utiliza un dispositivo ruteable y se instala en la memoria RAM del equipo, para que una vez que finalice la actividad del usuario, no quede ningún registro, es una forma de proteger los datos; SEGUNDA PERICIA: dijo haber realizado un informe de inspección ocular técnica del domicilio de señor Ola Bini, en el que además de haberse realizado el levantamiento de indicios, él hizo un diagrama de la red instalada, la que tenía 3 subredes: una que permitía acceso a internet; otra conectada a 4 NAS, lo que permite transformar de red física a inalámbrica y crear una copia de seguridad; y, una tercera subred conectada a computadores LENOVO sin disco duro, lo que permite proteger los datos y que nada de la navegación quede registrado; TERCERA PERICIA: Asociada a una audiencia privada, donde se generó imágenes forenses de un servidor ingresado con cadena de custodia, imagen forense que es una copia íntegra con un código de verificación

hash, que lo valida; explicó además varios conceptos utilizados en esta rama: dijo que DATA es la información utilizada en un disco de almacenamiento; que un sistema TAILS es un sistema operativo ruteable basado en LINUS, que sirve para realizar actividades de carácter anónimo y para proteger información; afirmó que cuando se apaga el equipo se pierde los datos, así como las actividades realizadas por el usuario; afirmó que los equipos sometidos a perica tenían llaves LLUVICO, que son credenciales de autenticación, con las cuales se puede validar el acceso de un usuario al computador, puedes cifrar la información que envías de un correo o de una red social o cifrar tema de la navegación web; y, que el cifrado de información es utilizado para que la información sea ilegible existiendo dos mecanismos de cifrados, el sistema simétrico y el cifrado asimétrico, el simétrico utiliza una clave pública o privada, el asimétrico se utiliza para volúmenes de información, en cambio el cifrado asimétrico se lo utiliza en volúmenes pequeños; que un sistema operativo ruteable implica que no necesita logiarse con un computador, sino a través de una USB, es un arranque distinto al convencional; finalmente refirió que el señor Ola Bini no quiso proporcionar ninguna contraseña de los equipos; CUARTA PERICIA: La que consistió en adquirir información almacenada en un servidor IBM y un Router, para así obtener una copia espejo o imagen forense con código Hash; finalmente comentó que la infraestructura encontrada y sus equipos, comprueban el propietario tiene un nivel técnico importante y al existir ese nivel de seguridad para acceder a esa información, en el País no existen personas que manejen ese tipo de cifrado de datos, es por eso que pidieron asistencia penal internacional.

Sobre la prueba técnica presentada, compareció además el perito del Departamento de Criminalística sargento Carlos Eduardo Ninacuri Macas, quien en lo principal dijo haber practicado dos pericias: PRIMERA PERICIA: Tuvo como objeto la fijación, preservación y materialización de una dirección electrónica o URL, la que se encontraba operativa el 14 de agosto del 2019, con contenido digital de acceso público, obteniéndose 2 archivos con nombre: reportes de vigilancia; título: "Develan como Assange transformó una embajada en un centro de operaciones para influir en las elecciones de EE.UU; aclarando que en dicha materialización y sus anexos, NO consta o se menciona al señor Ola Bini; SEGUNDA PERICIA: Para realizar esta pericia se trasladó a la Av. Amazonas y Japón el 22 de agosto del 2019, con el fin de fijar y extraer la información de un dispositivo de propiedad de la empresa CNT, computadora marca HP, Compac, modelo 8000, facilitado por Carlos Medina, responsables de las IP de dicha Institución, en el cual verificó la mensajería electrónica de carlos.medina@cnt.gov.ec y detalló 3 correos electrónicos recibidos; el primero con asunto Data Center Contingencia SIN SENAI-PETROECUADOR; remite tyépez, recibe comvanesa, de 25-07-2015; el segundo con asunto Instalación Data Internet Presidencia; remite trevelo; destinatario: aquinaana IT, de 29-11-2016; y, el tercero con asunto Instalación datos Internet Presidencia; remite mosqueraverónica; destinatario Marianela y Quevedo/ de 1-12-2016; correos que fueron validados mediante su código Hash, aclarando que ese dispositivo no se encontraba en cadena de custodia.

Del análisis de la prueba técnica detallada, se pueden establecer en primer lugar ciertos datos técnicos de los dispositivos electrónicos que reposan como evidencia, los cuales ya fueron descritos por pericias anteriores, debiendo resaltar el hecho de que con estas nuevas pericias, según lo manifestó el Capitán Marco Pazmiño, la

información que contenían estos dispositivos se encontraba cifrada, sin que se haya podido técnicamente, acceder a la misma; y, por otro lado el perito citado describe la red que tenía instalada el procesado Ola Bini, en su domicilio, la que le permitía un acceso directo al internet, contaba con dispositivos que permitían transformar la red física en inalámbrica y otra subred conectada a computadoras marca LENOVO, la que según el perito permitía a su usuario de manera general, proteger los datos de la navegación; explicando el perito ciertos datos técnicos en la audiencia, referente a la capacidad de almacenamiento de los dispositivos, sistemas operativos utilizados y su finalidad, así como describió las seguridades con la que contaban dichos dispositivos, como la utilización de credenciales de autenticación y formas de “cifrar” la información, señalando finalmente que la persona que manejaba estos dispositivos y equipos, debía tener un nivel técnico alto. Por otro lado y en cuanto al segundo perito que rindió testimonio, nuevamente el Tribunal debe hacer notar que la materialización de “URL” o direcciones electrónicas, en este caso concreto trata de asuntos totalmente ajenos a la investigación del delito de acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, lo que se comprueba de la simple lectura de su título “Develan como Assange transformó una embajada en un centro de operaciones para influir en las elecciones de EE.UU.”; debiendo recalcarse las afirmaciones del mismo perito en el sentido de que en dicha materialización y sus anexos, ni siquiera consta o se le menciona al señor Ola Bini, reiterando que estas “noticias de prensa”, a criterio del Tribunal no constituyen prueba alguna; y, finalmente la segunda pericia practicada por el perito Carlos Ninacuri Macas, tampoco aporta en nada en cuanto al cometimiento del ilícito, describiendo tan solo tres correos electrónicos recibidos por carlos.medina@cnt.gov.ec, los que trataban del Data Center Contingencia SIN SENAI-PETROECUADOR, correos que no tienen relación alguna con el procesado. Sobre este último tema, el Data Center Contingencia SIN SENAI-PETROECUADOR (Centro de Datos de Contingencia de la Presidencia de la República), compareció el ingeniero en sistemas y funcionario de la Presidencia de la República Klever Giovanni Salguero Sosa, quien dijo que en el año 2015 laboraba en la Dirección de Tecnologías, siendo el líder del área de redes y conectividad; sobre el Centro de Datos de Contingencia de la Presidencia de la República, dijo que éste nació por una observación realizada por la Contraloría General del Estado, que les informaron de la necesidad de tener un sitio alternativo o de contingencia, se buscaron sitios en Instituciones Públicas para poder alojarse en modalidad de hosting y que la empresa EP Petroecuador les presta o les da los equipos y la infraestructura tecnológica de ellos, para poder implementar este sitio alternativo de contingencia; señaló que sitio principal de su Data Center está ubicado en Lumbisi, en la ex Secretaría de Inteligencia, actual SIES; en cuanto al tipo de información que se registraba, al tratarse de un Data Center de contingencia, es un sitio presto a solucionar una emergencia del Data Center principal, en el posible en caso que sufra un siniestro el principal, tenían un sistema de decretos presidenciales y compromisos, se replicó el mail bock, que es su servidor de correo electrónico institucional; reitera que en el sitio alternativo se replicaba la información, una vez que la proveedora, en este caso CNT, proveía los datos como el de internet, que unía los dos Datas Center, se empezó a copiar la información del lugar principal al Centro de Contingencia Alternativo, el mismo que estaba ubicado en la ciudad de Guayaquil, el cual estaba operativo pero no en

producción, se cumplió la primera fase de entrelazar y replicar de información mas no en producción; señaló que se implementaron dos enlaces, uno de datos y un enlace de internet, el de internet tiene una dirección pública IP, el proveedor da la dirección IP pública que es la 181.113.57.169, esa dirección IP la configura el proveedor en su equipo de comunicación; aclaró que el convenio se firmó a finales del 2015 e inicio del 2016, esto quiere decir que estaba operativo pero no en producción, desde finales del año 2015 y comienzo del año 2016; señaló que el Data Center de Contingencia tiene varios equipos, servidores, equipos de almacenamiento que ellos los denominan Storash, de seguridad perimetral, farwoods y de comunicación que provee CNT y que Fiscalía no pidió información de esos equipos, tampoco le solicitaron las IP de esos equipos, no les pidieron remitir los accesos, no les pidieron posible accesos no consentidos a esos equipos del Data Center; finalmente señaló que sí se encontraba instalado un cortafuegos en los equipos, ubicado en el centro de datos de Petroecuador y que como equipo técnico hicieron pruebas tanto del equipo técnico de Presidencia, como de EP Petroecuador, que el corta fuegos estuvo configurado de acuerdo necesidades de Presidencia y operativo desde el inicio.

Sobre este testimonio del funcionario líder del área de redes y conectividad de la Presidencia de la República, se pueden establecer varios aspectos relevantes con relación a Centro de Contingencia: en primer lugar que este fue creado por una observación realizada por la Contraloría General del Estado y que fue la EP Petroecuador quien prestó a facilito los equipos e infraestructura tecnológica; se establece además que el sitio principal de su Data Center está ubicado en Lumbisi, en la ex Secretaría de Inteligencia, actual SIES, mientras que el Data Center de Contingencia está ubicado en la ciudad de Guayaquil; que el convenio para su creación se firmó a finales del 2015 e inicio del 2016, esto quiere decir que estaba operativo pero no en producción, desde finales del año 2015 y comienzo del año 2016; que en el sitio alterno se replicaba la información, una vez que la proveedora CNT les proveía los datos y el internet, que unía los dos Datas Center, luego de lo cual se empezó a copiar la información del lugar principal al Centro de Contingencia Alterno; y, que el Data Center de Contingencia contaba con varios equipos: servidores, equipos de almacenamiento o Storash, equipos de seguridad perimetral, farwoods y de comunicación que provee CNT y que Fiscalía no pidió ni obtuvo información de esos equipos, ni la IP de esos equipos, no les pidieron verificar los accesos, así como tampoco les pidieron verificar posible accesos no consentidos a esos equipos del Data Center.

OTRAS PERICIAS

Continuando con la descripción de otras pericias que se presentaron en la audiencia de juicio, el Tribunal analiza el testimonio del Mayor de Policía William Danilo Castro Acosta, perito del Departamento de Criminalística, quien explicó a los Jueces que practicó cuatro pericias: **PRIMERA PERICIA:** Un informe de audio, video y afines No. DCP-2019-01010, cuyo objeto consistían en la extracción de la información de varios dispositivos móviles constantes en las evidencias: 8 Tablet: 1) Marca Apple, color plomo con negro, modelo A1701, serie DMPDR03GHP83, sin tarjeta SIM (Chip), ni dispositivo de memoria externa; 2) Marca Apple, color ploma, modelo A1701, serie DMPBB1GZHP83, sin tarjeta SIM, ni memoria externa; 3) Marca Apple, color plomo, modelo A1673, serie DMPRR024H1MM, sin tarjetas; 4) Marca Apple, de color plomo,

modelo A1403, serie BLXHD1PVDNQV sin tarjetas; 5) Marca Apple, color plomo, modelo A1474, serie BMPLM47FK13, sin tarjetas; 6) Marca Apple, color plomo, modelo A1701, serie DMPVM5W7HP83, sin tarjeta; 7) Marca Apple, color plomo, modelo A1673, serie DMPSR0JXH1MM, sin tarjetas; 8) Marca Apple, color plomo, modelo A1566, serie DMPNR2KAG5W1; y, 5 teléfonos celulares: 1) Marca Apple, color negro, con tarjeta SIM de la operadora Claro, serie 9308955100054920382; 2) Marca Samsun, color azul, modelo GT-I9300, i mail 352993/05/639690/6, sin tarjeta SIM, ni tarjeta de memoria; 3) Marca Samsun, color negro con plomo modelo GT-E100W, con i mail 355874/04/900584/5, con tarjeta SIM o chip, de la compañía COMVIQ, serie 89462046110005771752IQ851; 4) Apple, color negro, modelo A1387, sin i mail, sin tarjetas; y, un dispositivo marca Apple, color negro, modelo A1574, serie CCQQ402WGM1C, sin tarjetas; señaló que utilizó el dispositivo de extracción forense el Universal Forense Extraction Devise UFER: concluyendo que los dispositivos tenían el sistema bloqueado (Enter Passcode); excepto el teléfono celular No. 2 Marca Samsun, color azul, modelo GT-19300, del cual extrajo 132 hojas en formato PDF; que del teléfono celular No. 3, marca Samsun, obtuvo números telefónicos, números de contactos y mensajes de texto. **SEGUNDA PERICIA:** Un informe de audio, video y afines, cuyo objeto consistían en la exhibición y extracción del contenido digital de los dispositivos de almacenamiento y electrónico, que se encontraba bajo cadena de custodia No. 3082-2019, aclarando que previamente existió una audiencia privada; señaló que los dispositivos eran: 1) Un dispositivo de almacenamiento óptico marca ADATA, tipo USB, el cual presenta una carpeta de archivos de nombre “grabaciones”, con 756 archivos de audio y 756 archivos de texto; de los cuales dijo haber obtenido 6 archivos considerados “relevantes” para la causa: los archivos: CH05_20190403065610, CH05-20190405065818, CH0520190406094621, CH0520190406154623, CH0520190408190405, CH05_20190409065738, en los cuales se aprecia en general “a una persona de género masculino acercarse a un ascensor, manipula su acceso, manipula además un dispositivo de comunicación móvil (teléfono)”, al ser recurrente esta actividad, permite apreciar la combinación 55373571, clave que acciona el aparato”; dijo que como se aprecia de los videos, se infiere una contraseña de desbloqueo de un equipo de comunicación móvil, contraseña que es ingresada en todos los dispositivos móviles que constan dentro de esta cadena de custodia contando con la autorización judicial para la extracción, logrando el desbloqueo de un teléfono celular marca Appel, color negro, modelo MQ7C2ZD/A, con i mail 352993090817594, con tarjeta SIM de la operadora Claro, de serie 895930100054920382, sin tarjeta de memoria, equipo en buen estado de conservación y funcionamiento, óptimo para ser sometido a peritaje; en cuanto a la extracción de la información, esta se le remitió en otro informe pericial, por la cantidad de información que existía y como anexo a este informe pericial, en el cual constaba toda la información extraída y el reporte en PDF que estaba conformado por 42.864 páginas; 2) Un DVD R marca Berbatin, con el nombre de 190612_2120, que contiene 2 archivos de audio y video de nombres 0204-19, Bc hacker Sueco MP 11 abr 2019, donde se aprecia a dos persona una de género masculina y otra de género femenino, los logotipos identificativos de Tele Amazonas, 24 horas, entrevista al Secretario de Presidencia Sebastián Roldán, sobre Julián Assange y aprehensión de Ola Bini en el aeropuerto de Quito; 3) Un DVD R marca Maxell, serie

WEH607100350L10, de nombre canal 1 y www.canal1tv.com, VERAS 9 de junio 2019; contiene un archivo audio y viendo de nombre VERAS, domingo 9 de junio 2019-MA. Paula Romo, entrevista a María Paulo Romo; 4) Un CDR marca Maxell rotulado Videos, posee 7 archivos de audio y video; el nombre del video WhatsApp 2019-06-27 AT91937AM, donde fundamentalmente se aprecia a varias personas que inspeccionan la cajuela de un vehículo color rojo, con persona vestida de Policía y personas con ropa formal; y, se puede ver a una persona en el interior de un vehículo, otra persona que se encuentra afuera con una chompa refractivo, interaccionan en un diálogo; 5) De un dispositivo de almacenamiento óptico, disco duro marca SEAGATE, serie NA9QA8H3, contiene 2 carpetas de archivos y dos archivos propios del dispositivo, en los que se aprecia la estructura de un corredor, unas bandas transportadoras, se trata de un aeropuerto, se observa además a varias personas portando varios objetos, al parecer equipajes, un counter y varias personas caminando por el lugar; en sus CONCLUSIONES determinó que los dispositivos de almacenamiento tanto ópticos como externos tipo USB, están en el Centro de Acopio del Departamento de Criminalística, bajo cadena de custodia 3082-19, de los cuales se determinó su integridad física y que son aptos para ser sometidos a peritaje.

TERCERA PERICIA: Cuyo objeto era la de extraer la información contenida en el teléfono celular de marca I Pone, modelo I Pone 8, color negro, con número 352993090817594; el cual se pudo desbloquear utilizando la clave obtenida 55373571 (descrita en la segunda pericia, dispositivo 1); obteniendo información que se la almacena en un dispositivo USB marca Kinston No. 04715-554A00LE; se almacena además un archivo en PDF con 42.864 páginas; señaló que la información fue exhibida en una audiencia privada y dada a conocer a las partes procesales, aclarando que Fiscalía, a petición de la defensa del procesado, dijo que para garantizar la privacidad de la información, solicitaría se materialice únicamente lo pertinente con la investigación; lo que fue solicitado mediante varios oficios, por lo que materializó 147 fojas que contenían chat y mensajes de una red social, cuyos participantes principalmente son: MENSAJES: De Ola Bibi con: Karina de 17-04-2017; con Veng Ake Verg, de 24-03-2018; con Daniel Spiewak, de 10-11-2011; con Estella Sandel, de 10-11-2011 y 16-11-2011; con Emma Bret, de 19-12-2014 y 06-03-2015; con Adoración Guamán; con Cristian Cruz, de 15-09-2017 y 22-09-2017; con Stella Sandell, de 20-06-2018; con Sara, de 11-04-2019; y, con Leslie Jarrín/ 11-04-2019. **CUARTA PERICIA:** Cuyo objetivo fue realizar la materialización de la imagen que consta a fs. 33.115 de su TERCER informe, señalando que su ruta era: IPONE/APPLICATIONS/GROUP.NET.WHATSAPP.WHATSAPP.SHARE/MESSAGE/MEDIA/599995404579@WHATSAPP.NET/A/9/A95079D384EDBE1B75A21A558A22383C.JPG; que el nombre de la imagen es: A95079D384EDBE1B75A21A558A22383C.JPG; que el contenido de la imagen es:

[/HOME/OLABINI] (1004) V TORSOCKS2 TELNET 181.113.57.169
[OCT0612:51:56] ERROR TORSOCKS [23473]: UNABLE TO RESOLVE.

STATUS REP

TRYING 181.113.57.169...

CONNECTED TO 181.113.57.169.

ESCAPE CHARACTER IS, Y (invertida)]

C*****

EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTÁ PROHIBIDO

Usted debe tener permiso explícito para acceder/o
Configurar este dispositivo. Todas las actividades realizadas
son almacenadas
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
YOU MUST HAVE EXPLICIT PERMISSION TO ACCESS OR
CONFIGURE THIS DEVICE. ALL ACTIVITIES PERFORMED ON THIS
DEVICE
ARE LOGGED

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT E.P. CNT
(Logo)
EL ACCESO O USO NO AUTORIZADO SE CONSIDERA UN ACTO
CRIMINAL
PETROECUADOR SENAIN INTERNET

USER ACCESS VERIFICATION
USER NAME: % USER NAME: TIME OUT EXPIRED ; CONECTION CLOSED
BY FOREIGN HOST. [/HOME/OLA BINI] (1005) Y (invertida)
LENOVO.

Explicó finalmente que la fotografía es digital, es una captura realizada en una cámara oscura; que las imágenes que terminan en JPG: tienen una extensión y propiedades para almacenar fotografías; que las imagen (como la fotografía) que termina en JPG si se puede capturar de internet; dijo que los archivos THUMBNAILS, traducidos quieren decir en miniatura; explicó que el código MD5 es una forma de archivo hash, es un código alfanumérico conformado por 32 caracteres, que permite a cualquier archivo digital de cualquier extensión, darle una extensión fija, este código le da una identidad a esta imagen de acuerdo a las propiedades y a cómo está conformada, así como la cantidad de pixeles que tiene; que en la ruta de la fotografía se lee WhatsApp, Share, Mensaje, Media y un número telefónico, por lo que refiere que si existió una conversación de WhatsApp; y, que remitiéndose al informe de extracción, se puede saber si fue un mensaje enviado, recibido, si la imagen fue cargada como archivo adjunto y otras circunstancias; señala, que la palabra "share", traducida quiere decir compartido, esto es enviado o recibido.

Sobre estas pericias practicadas por el Mayor de Policía William Castro Acosta, el Tribunal advierte que en la primera de ellas, se le dispuso obtener la información constante en varios dispositivos móviles encontrados en el domicilio y poder del señor Ola Bini, estableciéndose que de 8 Tablet no se obtuvo información alguna, a no ser sus características como marcas y números de series; mientras que de los 5 teléfonos celulares, se pudo concluir que estos tenían un sistema de bloqueo que no permitía obtener la información constante en estos, excepto del marca Samsun azul, modelo GR19300, del cual se obtuvo 132 hojas en formato PDF y del otro teléfono Samsun se obtuvo varios números de contactos y mensajes de texto, información que no tiene relevancia alguna con el delito acusado; en la segunda pericia detallada se procedió a la extracción de la información de varios dispositivos de almacenamiento óptico que se encontraban bajo cadena de custodia, de los cuales y en lo principal, en el dispositivo 1), se pudo obtener la clave 5537357, luego de

verificar que una persona (Ola Bini) lo digitaba en un dispositivo móvil en repetidas ocasiones al subir a un ascensor, luego de lo cual se le dispuso al perito ingresar dicha clave a todos los dispositivos que se encontraban como evidencias, logrando el desbloqueo del teléfono celular marca Appel, color negro, modelo MQ7C2ZD/A, con i mail 352993090817594, con tarjeta SIM de la operadora Claro, de serie 895930100054920382, del cual se procedió a extraer su información y elaborar un reporte en PDF de 42.864 páginas, el cual será analizado posteriormente; en cuanto a los otros dispositivos de almacenamiento óptico analizados, nuevamente el Tribunal advierte que estos tan solo contienen noticias de prensa, específicamente entrevistas realizadas en los canales Tele Amazonas y Canal 1, en los cuales se comentan temas como la terminación del asilo político al ciudadano Julián Assange, así como sobre la detención del ciudadano Ola Bini en el aeropuerto Mariscal Sucre, noticias que a criterio del Tribunal no constituyen medios de prueba; finalmente y sobre un CD que contiene el archivo WhatsApp 2019-06-27 AT91937AM, donde se aprecia a varias personas con uniforme de la Policía Nacional, quienes realizan el registro de un automotor, este video se relaciona con los hechos relatados en el testimonio del Teniente de Policía Ricardo Muñoz Navarrete, quien como ya se lo analizó precedentemente, dijo que el día de la detención del señor Bini, el 11 de abril 2019, siendo las 23:00, salió en precipitada carrera del domicilio del señor Ola Bini, ubicado en la calle Diguja, un vehículo no identificado, dijo que lo siguieron hasta la gasolinera Primax de la 9 de Octubre y Orellana y pidieron los datos al propietario del vehículo, acto que quedó registrado en un video y que fue periciado por el Mayor Castro; y, finalmente sobre el contenido del dispositivo de almacenamiento óptico marca SEAGATE, serie NA9QA8H3, tan solo se puede apreciar por varias horas, diferentes secciones de un aeropuerto, sin que de dichos videos se obtenga información relevante sobre el delito acusado.

Sobre el tercer informe pericial practicado por el Mayor William Castro Acosta, el mismo que dijo haber materializado 147 fojas del teléfono celular marca Appel, color negro, modelo MQ7C2ZD/A, que contenían chat y mensajes de una red social, cuyos participantes son el procesado Ola Bini y diferentes personas identificadas como Karina, Veng Ake Verg, Daniel Spiewak, Estella Sandel, Emma Bret, Adoración Guamán, Cristian Cruz, Sara y Leslie Jarrín; se dispuso la práctica de dos pericias que tuvieron como objeto, la traducción de dichos chat y mensajes; en primer lugar compareció la **perito traductora María Soledad Casco Rueda**, quien dijo que fue designada para realizar dos traducciones, la primera relacionada con conversaciones en varias plataformas de mensajería como WhatsApp o Tinder constantes en un dispositivo móvil (33 fojas); y, la segunda pericia una traducción del inglés al español, de varios audios contenidos en un CD; sobre la **PRIMERA PERICIA**: detalló conversaciones de Ola Bini (propietario del teléfono del cual se extrajo la información) con varias personas, entre las principales: **Adoración Guamán**, de 22-06-2017: buenos días, ahora conoceré a Assange y estoy feliz, tengo mi presentación esta mañana con él y estoy tratando de escribir algo interesante, también conoceré a Garzón; Ola Bini: Garzón está en Ecuador?, buena suerte con todo; Adoración Guamán: sigo pensando que decir; Ola Bini: como estas, te extraño; estoy en Ciespal todo el día, ahora en casa a trabajar un rato; Adoración Guamán: si, también te extraño; Adoración Guamán: y Garzón estuvo ayer en Riobamba con el Mashí?; Ola Bini: que bueno escuchar eso, escucharlo fue bueno?; Ola Bini:

adjuntos, la vista de la casa de mis padres a las 9; (texto ilegible); Adoración Guamán: si estuvo realmente bien; 26-07-2017 Ola Bini: usualmente tengo para esta semana reuniones políticas, pero esta vez es demasiado; podría perder mi visa y posibilidad de hogar en Ecuador en 5 semanas: Ola Bini: y hay algunas otras cosas de las que no puedo hablar; Adoración Guamán; hay; Ola Bini: entonces, extraño Ecuador ahorita; vivo para esta semana para relaciones políticas pero esta vez es demasiado; **Katherine Gim**: hola me encanta eso, quien es el pájaro afortunado que financia tu trabajo?, si puedes revelarlo; ya has encontrado todo tus compañeros de equipo; Ola Bini: los fondos provienen de un fondo político confiable llamado people soporte foundation y tengo un montón de gente que viene conmigo, pero espero encontrar gente nueva; 29-09-2017: Katherine Gin: viste la orden de Trump de recopilar información de todos los inmigrantes en las redes sociales, pensé, Ola tenía mucha razón en irse; Ola Bini: si es loco; **con Cristian Cruz**: 26-10-2017: o podrías intentar darle una visa; lo que significa que recibe dinero; procedente de fuentes nacionales o internaciones; en este caso de la Organización; pero necesita pensar correctamente esta acción; Ola Bini: ah, ya veo, entonces la visa de residencia no es posible?; no sé a cerca de la visa rentista; Cristian Cruz; podría ser posible si me visitas por favor; para un análisis más sólido de su situación; Ola Bini: sí, seguro, estaría bien el jueves?; buenos días, cuando debería visitarte; Cristian Cruz: podrías visitarme a las 11:00 hoy? en la Av. 10 de Agosto frente al edificio principal del Ministerio; estamos ubicados en un edificio con ventana verde; Ola Bini: lo siento tengo reuniones hasta la 13h00, sería posible después; Cristian Cruz: sí, puede ser a las 15:00?; Ola Bini: perfecto; cuál es la dirección, tengo tiempo; Cristian Cruz: nuestra oficina es la Coordinación Zonal 9, frente al edificio principal; es un edificio de 5 pisos con ventana verde; en la Av. 10 de Agosto, estamos en planta baja, por favor informe que tiene reunión conmigo; Ola Bini: gracias, te veo hoy; Cristian Cruz: perfecto; Ola Bini: hola, espero que te encuentres bien, estoy en el procesado de conseguir empleo en una empresa aquí en el Ecuador, pero los abogados nos dicen que es imposible para mí, obtener una visa de residencia permanente, ya que cambié mi empleo; estoy trabajando con algunos abogados diferentes, que se preguntaban sobre la sugerencia que usted me dio, pueden llamarle para aclarar las cosas, gracias; Cristian Cruz: hola, hoy conocí un abogado enviado para mi oficina para el análisis de su caso; una posibilidad podría ser una solicitud de visa de trabajo con un nuevo empleador; mantendrás un estado de visa temporal por 2 o 3 meses y luego solicitarás el estado permanente; de acuerdo con la regla de los 21 meses; Ola Bini: ah, ya veo gracias, vale la pena intentar; **con Estela Sandel**: me estás escuchando ahora?; si definitivamente; como lo sabes; he estado del otro lado; cómo se siente; muy norma; **con Sonia Alcívar**: buenos días, este es Ola Bini, el amigo de Iván Orosa, como estás; Sonia Alcívar: hola querido; Ola Bini: voy a tener todos los documentos listos a las 11 A.M. hoy, a qué hora es bueno para venir a las Cancillería; Sonia Alcívar: podría ser a eso de las 16:00 por fa; Ola Bini: perfecto; veamos; Sonia Alcívar: te espero; Ola Bini: piensas que necesito adjuntar antecedentes también?; Sonia Alcívar: si los tienes, está bien traerlos; Ola Bini: ok, gracias, estamos en camino finalmente, tuvimos unos problemas, ja ja; Sonia Alcívar: al menos ya se resolvió; Ola Bini: sí; Sonia Alcívar: como te fue en el Sur; Ola Bini: fue muy bien; ahora solo necesitamos esperar, pero solo la terminación; Sonia Alcívar: muy bien, ya le hacemos seguimiento; Ola Bini: muchas, muchas gracias;

Ola Bini: hola, recibe un correo sobre mi visa, parece que hay un problema, tienes un i mail?; Sonia Alcívar: hola Ola, mi correo sonialacivar@gotmail.com; Ola Bini: gracias lo he enviado; Sonia Alcívar: no te preocupes aquí hay feriado lunes y martes, el miércoles lo resolvemos; Ola Bini: ah, gracias; Sonia Alcívar: hola Ola, estás en Quito, ya tengo resuelto tu tema; Ola Bini: no puedo estar en Quito este viernes, que pasa?; Sonia Alcívar: ya tengo tu visa aprobada, cuando vienes; Ola Bini: en serio, uohhh, el lunes; Sonia Alcívar: sí, entonces así lo hacemos, está bien; Ola Bini fantástico, gracias; **con Ricardo Arguello:** Ola Bini: viste que Lenovo envía una cuenta tercera de temporal a los usuarios de Windows? (carita triste); 06-10-2015: de Ola Bini para Ricardo Arguello: si lo encontré; Ricardo Arguello: eso tiene que ser un enrutador le preguntaré a mi contacto de CNT; **con Sara:** ha sido arrestado (carita triste), Sara: mierda; es horrible; Ola Bini (carita triste), plena cooperación de Ecuador; Sara: viendo las noticias en Ecuador, absolutamente esto es muy muy malo; Ola Bini: sí, me siento bastante deprimido; Sara: tengo miedo de lo que pasará ahora, lo entiendo cariño; los principales medios ecuatorianos lo justifican diciendo que Ecuador es un país soberano; Ola Bini: sí, por supuesto que lo hacen; a pesar de que rompe todas las convenciones internaciones; y es una mierda (cara triste); ya hay confirmación de que hay una orden de extradición de EEUU, muy malo; Sara: oh mierda, he escuchado declaraciones de diplomáticos que dicen mire a Many, sufrió tortura, no, EEUU no lo va a lastimar de ningún amanaera; Sara: esto es una locura; Ola Bini: oh mi dios, muy estúpido (cara triste); yendo al aeropuerto; Sara: te iba a preguntar eso, va bien hasta ahora?; Ola Bini: todavía estoy esperando que me dejen entrar en el área de check in, nada fuera de lo común, hasta ahora; Sara: eso es bueno, estoy feliz; voy a ver las noticias ahora; Ola Bini: 30 minutos todo bajo control; Sara: bien, bien, nada nuevo hasta aquí; ok, bien, solo estoy en espera de las noticias; Sara: esperemos que no sean malas, al menos para ti; Ola Bini: sí, las noticias ya son malas; Sara: estoy cruzando los dedos por tí; Ola Bini: ok, acabé con el check in, pasando por seguridad ahora, estaremos en contacto después; Sara: ok, buena suerte; Ola Bini: seguridad listo, ahora inmigración; Sara: todo en orden?; Ola Bini: bien, inmigración listo, horario de 30 minutos comienza de nuevo; Sara: ok; Sara: estoy almorzando ahora; Ola Bini: espero que tengas un buen almuerzo; Ola Bini: voy a mi puerta ahora; Sara: por favor ten cuidado, buena suerte con todo cariño; Ola Bini: por supuesto, te dejo saber cuándo haya abordado; Sara: muchos abrazos; Ola Bini: abrazos, abrazos; chequeo de equipaje, te dejo saber cuándo haya terminado; Sara ok, buena suerte; debo hacer algo; Ola Bini: no todavía, gracias, solo estoy esperando que me llame un abogado; Sara: ok, por favor mantenme al tanto; Sara: cariño mantente fuerte; Ola Bini: gracias; Sara: muchos abrazos; cual es la explicación que te dan?; Ola Bini: nada todavía, digo que quiero un abogado una traducción al inglés para estar seguro; Sara: bien, están contigo ahora?; Ola Bini: están afuera, se ha publicado mi nombre; **con Leslie Jarrín: 11-04-2019:** Ola Bini: buenos días, hay noticias acerca de Julián (cara triste), entonces esto; no estoy ciento por ciento seguro que estén hablando de mí, algunos detalles no concuerdan, pero no es imposible; Leslie Jarrín: (ilegible) estamos .. no estoy segura de que sea la expresión correcta; Ola Bini: sí, tampoco me gusta, pero quien sabe; Leslie Jarrín: hablaste con Jasón por si acaso; Ola Bini: no, voy a esperar y ver; Leslie Jarrín: estás en Japón?; Ola Bini: estoy viajando esta tarde; por favor llama cuando tengas un segundo; Ola Bini: pasando inmigración y seguridad ahora,

no hay problemas hasta ahora; Leslie Jarrín: disfruta de Japón, espero poder ir algún día; Ola Bini: gracias, gracias; Leslie Jarrín: adjuntos; Pablo Encalada, teléfono +593991805859; Ola Bini: hablé con él, no estoy seguro si él enviará a alguien o puede venir; Leslie Jarrín: lo sabré en 5 minutos; Ola Bini: gracias, estoy un poco asustado, me quieren quitar el teléfono, necesito ayuda en el aeropuerto; Leslie Jarrín: ilegible; Ola Bini: no sé si él me puede ayudar; Leslie Jarrín: sí, acabo de hablar con David Ochoa, él o su compañero están yendo; te confirmo en un segundo; Ola Bini: no van a permitir más textos, solo pueden llamarme los abogados, mensaje final; **SEGUNDA PERICIA:** sobre la traducción de 17 audios que contenía el teléfono celular marca Appel, color negro, modelo MQ7C2ZD/A, se pueden escuchar conversaciones relacionadas principalmente con: 1) Es una restricción temporal de movimiento de hasta 8 horas en el aeropuerto, ah el abogado enviará a alguien; 2) Hey, me alegro de que ya lo tengas, eso es algo importante en caso de que ocurra algo y no te preocupes, ya sabes, siempre te he dicho que si puedo hacer algo por ti, házmelo saber, es mi deber como amiga, así que no te preocupes, ah bueno, por supuesto que vamos a estar en contacto, ahora estamos, Yo estoy yendo a la oficina, así que espero que las cosas vayan bien; 3) hey hey, perdón por no decir adiós correctamente, ah, pero Leslie me decía que está obteniendo la información del abogado, así que lo tendré cuando llegue al aeropuerto al menos, así que en caso de que ocurra algo, tengo un abogado al que puedes llamar, de cualquier forma y gracias de nuevo querida, realmente lo aprecio; 4) ok, acabo de llamar a Leslie, me están llevando lejos y no se me permitirá viajar, Leslie se pondrá en contacto del abogado, no estoy detenido, pero no tengo permitido salir del aeropuerto, eso es todo lo que sé ahora; 5) estaba leyendo nuevamente el artículo, habla de 4 personas, los dos rusos, el miembro de Wikileaks y la persona cercana a Julián, así que son cuatro, no tres, así que es algo en tener en cuenta; 6) hola Ola, así que hay un nuevo artículo en el Universo, aclara eso o tal vez no sé si en la conferencia de prensa, se dijo esto claramente, pero aclara que los hacker rusos estaban viajando con Patiño y de que se trataban estas preocupaciones, las afirmaciones es que los dos hacker rusos estaban trabajando en estrecha colaboración con Patiño, por lo que puedo decir las cosas sobre el miembro de Wikileaks no estaban asociadas con los países o con Patiño, están separadas de eso, así que tal vez eso explique algo de la confusión sobre las cosas; 7) hablé con Leslie, en este momento aparentemente ella está tratando de encontrar un abogado que pueda ir para ayudarte en este momento, si no puede encontrar a la persona que está buscando, ahora va a hablar con David, así que sí; 8) lo bueno de esto podría ser, que no estaba claro que si la Ministra del Interior transmitiría la información de todas esta gente a la Fiscalía, o si se trataba principalmente de los hacker rusos, es posible que solo se trate de los hackers rusos; 9) sobre eso entonces sí, cuando vi el comunicado de prensa ella estaba hablando de los rusos, dijo que no permitiremos que este tipo de actividades se cometan en Ecuador y también tenemos la información sobre estas otras dos personas, ella pidió los detalles y dijo que en las próximas horas les darían toda la información que tenía a Fiscalía para que tomaran todas las medidas.

El Tribunal al analizar el contenido de las traducciones realizadas a las conversaciones existentes en la mensajería WhatsApp o Tinder, extraídas del teléfono celular del ciudadano Ola Bini, advierte que se habla de temas diversos y con diferentes personas; se habla de que una persona (Adoración Guamán)

conocerá a Assange y también a Garzón, ente lo cual el ciudadano Ola Bini pregunta si Garzón está en Ecuador y le desea buena suerte con todo; se habla de ciertas actividades laborables y quien financia su trabajo (con Katherine Gim), contestando el ciudadano Ola Bini “los fondos provienen de un fondo político confiable llamado people soporte foundation”; en el mes de septiembre del 2019 comentan sobre noticias internacionales y hablan sobre una orden de Trump de recopilar información de todos los inmigrantes en las redes sociales, pensó, Ola tenía mucha razón en irse; Ola Bini: si es loco; se detalla además conversaciones relacionadas a los trámites para obtención de un visa, las clases de visas a las que podría acceder, los requisitos que se necesitarían, las diferentes citas en las que trataran estos asuntos, temas tratados por el ciudadano Ola Bini con Cristian Cruz y la ciudadana Sonia Alcívar; además se habla (Con Sara) sobre otras noticias internacionales, específicamente sobre el arresto de una persona (Assange), comentando que los principales medios ecuatorianos lo justifican y afirmando que se rompen todas las convenciones internacionales; además se detalla que el ciudadano Ola Bini se dirige al aeropuerto, que pasa por el check in y que luego es detenido; hecho éste, el de la detención del ciudadano Ola Bini que es tratado con Leslie Jarrín de manera amplia, primero se refieren a las noticias de la prensa, luego del itinerario en el aeropuerto, para posteriormente referir su detención (Ola Bini) y solicitar que le ayuden consiguiendo una abogado; temas estos que son totalmente ajenos al delito que se acusa, pues este se refiere al acceso no consentido a un sistema informático, telemático o de telecomunicaciones, o a la explotación ilegítima de ese acceso, pero el Tribunal no encuentra relación alguna con la prueba presentada, ni pertinencia con los temas tratados en estas conversaciones en las mensajerías WhatsApp o Tinder; y, sobre la segunda pericia practicada, fue la misma traductora María Soledad Casco Rueda, quien aseveró que de los audios peritados, no podía ella saber quiénes eran los intervinientes ni en qué fecha se produjeron, ya que solo tradujo las conversaciones, sin embargo de lo cual se puede apreciar conversaciones sobre la “restricción temporal de movimiento de hasta 8 horas en el aeropuerto”; o conversaciones banales como que “por supuesto que vamos a estar en contacto, ahora estamos, Yo estoy yendo a la oficina, así que espero que las cosas vayan bien”, o la que refiere que “ah, pero Leslie me decía que está obteniendo la información del abogado, así que lo tendré cuando llegue al aeropuerto al menos”, finalmente “ok, acabo de llamar a Leslie, me están llevando lejos y no se me permitirá viajar, Leslie se pondrá en contacto del abogado, no estoy detenido, pero no tengo permitido salir del aeropuerto, eso es todo lo que sé ahora”, temas estos que seguramente corresponden al día de la detención del ciudadano procesado Ola Bini, el 11 de abril del 2019, en el aeropuerto de Tababela, sin que exista relación alguna con el acceso no consentido a un sistema informático o de telecomunicaciones ocurrido, según la acusación oficial y particular como 4 años antes; conversaciones en las que además se relata “las afirmaciones es que los dos hacker rusos estaban trabajando en estrecha colaboración con Patiño, por lo que puedo decir las cosas sobre el miembro de Wikileaks no estaban asociadas con los países o con Patiño”, o comentarios sobre una noticia televisa “cuando vi el comunicado de prensa ella estaba hablando de los rusos, dijo que no permitiremos que este tipo de actividades se cometan en Ecuador y también tenemos la información sobre estas otras dos personas, ella pidió los detalles y dijo que en las

próximas horas les darían toda la información que tenía a Fiscalía para que tomaran todas las medidas”; hechos que nuevamente se recalca, no tienen pertinencia ni conducencia con el delito acusado; finalmente sobre estas “traducciones”, la defensa del ciudadano Ola Bini requirió que se presenten otras conversaciones que constan en la pericia, las que referían temas que tampoco guardan relación alguna con los hechos juzgados, como la conversación de 17 de abril del 2017 entre Ola Bini y Karina “hola, encantado de conocerte, no estoy seguro de qué decir en un primer mensaje como este, leer tui perfil me hizo sentir curiosidad, de qué manera eres horrible (carita feliz); Karina; hola, encantada de conocerte también, ja ja ja, tómalo con calma, es una broma; Ola: ja ja ja, entonces no lo eres, bueno saber; Ola: eres de Quito originalmente”; debiendo resaltarse que los únicos mensajes que presuntamente estarían relacionados con el delito investigado, son los realizados con el ciudadano Ricardo Arguello: “ Ola Bini: viste que Lenovo envía una cuenta tercera de temporal a los usuarios de Windows? (carita triste); 06-10-2015: de Ola Bini para Ricardo Arguello: si lo encontré; Ricardo Arguello: eso tiene que ser un enrutador le preguntaré a mi contacto de CNT”; conversación que será analizada posteriormente. Sobre este mismo tema, compareció otra perito traductora, Gerer Anouchka quien dijo que realizó la traducción del inglés al español de dos documentos, el primero era una apostilla con un certificado laboral, y el segundo documento contenía unos chats; en cuanto la **PRIMERA PERICIA**: refirió tratarse de una apostilla de los EEUU, el cual contenía un certificado de la empresa Top Word, con fecha 26 septiembre del 2019, en la que indica: a quien corresponda: Esta carta sirve para verificar que el señor Ola Bini fue empleado por Top Word, como el desarrollador principal desde el 10 de febrero del 2010 hasta el 30 de septiembre del 2016, el señor Bini fue asignado para trabajar a Ecuador desde el 11 de noviembre del 2013 hasta su último día de empleo hasta el 30 de septiembre del 2017, su sueldo anual fue de USD 220.000,00, durante su empleo su salario pagado por Top Word, con depósito directo a su cuenta bancaria en Estados Unidos, atentamente firma ilegible, Jeremy Gordon, Consejero Asociado General y Vicepresidente de Top Word; como se aprecia de la pericia, se trata de la traducción de un certificado laboral en favor de Ola Bini, su tiempo de trabajo y sueldo; mientras que la **SEGUNDA PERICIA**: derivado de un documento del FBI que contiene chats entre Ola Bini y personas generalmente no identificadas, chats que dijo, comienzan en el mes de octubre del 2013 y continúan hasta el 17 de julio del 2015; el Tribunal analiza los principales, en los cuales se habla de variados temas como la visita a una embajada (11 de octubre 2013), “estaba en la embajada, aparentemente hiciste una buena impresión; Bini respondió: oh me alegro de oír; la pasaste bien en la embajada?; sí, pero nuevo embajador nuevos reyes, los invitados se van a las 12; que hacker tan antipático; ah eso apesta”; de un contrato de trabajo y del viaje a Ecuador 6 de noviembre del 2013: “Ola Bini: como te va pase muchas horas con abogados de hoy y fundamentalmente lo más importante que descubrí, es que es importante que el contrato sea conmigo como persona y no con Top Word; pero a excepción de eso todo parece estar bien, estoy listo para empezar tan pronto como podamos; buenas noticias, solo tengo que descubrir todo de mi parte, especialmente con la nueva empresa, pero suena genial, fantástico; me avisas si hay algo que pueda hacer algo para acelerar el proceso, y por su puesto mis abogado tendrán que ver el contrato, pero estoy mentalizado y listo cuando sea; también mi mudanza a Ecuador será la próxima semana; así que

después de eso las cosas serán mucho más simples; como va todo con la nueva empresa?; todo está avanzando bien, tiene alguna idea del marco de tiempo calculado de las cosas?"; otro chat de 12 de diciembre del 2013: envían mensajes OB: alguna noticia?; GG: hola, nada todavía, sé que es lento pero todavía no hemos llegado al punto de la discusión sobre trabajar con personas externas con contratos, pero lo haremos; cómo estás; GG: estoy bien, como está Ecuador; OB: buen trabajo en las reanudaciones de Suecia; Ecuador es muy bueno, es bastante emocionante; GG: así, de gustan las cosas de Suecia?; GG: Ecuador es interesante?, quiero ir ahí; OB: logramos derogar un artículo insidioso en un nuevo Código Penal, que habrían hecho las cosas realmente malas aquí y, realmente es así y estamos recibiendo mucha consideración de los políticos locales; sería fantástico sacarlo lo más pronto, hay una ola de indignación en este momento y el gobierno está tratando de implementar planes para hacer algo al respecto y nos han pedido ayuda; GG: lo intentaré, es difícil, tengo la presión de todos para hacer todos los países, pero puedo intentarlo; del 11 de febrero del 2014: FR: Dios, estoy ansioso que nos veamos, aunque te pueda parecer frustrante, las preguntas que hago; OB: no te preocupes, también tenemos algunos días, no tengo realmente nada planeado para Londres, excepto visitar a ¿??, tengo algunas cosas e ideas, desde Hamburgo, el 21 tomaré el tren de regreso a Berlín con Mitri, y veré a Assange; OB: Ah, genial; estoy en Hamburgo el 21 y tomo el tren a Berlín el 22, pasaré tiempo con Mitri y Sara; FR: oh, bien; del 4 y 16 de abril del 2014: FR: Julián recibió el mapa que le envié y le encanta tanto que lo está enmarcando, presente exitoso; está confirmado para el último panel, quería que tratara de ponerlo en el grupo de ¿??; Kimi respondió grandes cosas; 16 abril del 2014: OB: acabo de hablar con el australiano; FR: oh bien; espero que este bien lo extrañe; OB: sí, pero aparentemente no hay muchos cambios con el embajador; FR: maldita sea, voy a pedirle al embajador que envíe una carta solicitando un trato especial, para que podamos quedarnos más tarde y beber wiski; OB: genial; traducción de fs. 7 y 8, de 18 de noviembre 2014 F, Rubí y Bini, se enviaron mensajes: OB: el ex ministro de defensa del Ecuador, que aparentemente es una buena persona, es el nuevo embajador de la ONU en Ginebra; OB: deberían ponerlos a los dos juntos; FR: oh, bien; OB: sí, se lo diré gracias; FR: sí; OB pensé que te gustaría; FR: sí, es una noticia increíblemente buena; permíteme compartir contigo mi último trabajo para los Wikileaks, niños mal humorados con los que todavía no estoy hablando porque estoy en huelga por su nieto; OB: enviaré un correo electrónico a Iván pidiéndole que lo haga; FR: Ecuador y posibilidades; OB: seguro; FR: sí, eso sería genial, me preocupo por el Iván; OB: está mucho mejor, logramos podernos al día; ha podido despegar totalmente el tema de Chevrón, por lo que tiene mucho más tiempo para hacer estrategia, el único problema es que el ministro Luano y que está haciendo un trabajo fantástico para él, convirtiéndose en el asesor más confiable de los ministros; FR: es una bendición muy contradictoria, tengo que irme; OB: sí, cuídate; traducción de fs. 19 y 20, chat de 10 de octubre del 2013: Bini envía mensaje a una persona cuya identidad es desconocida, hasta para el Departamento de Justicia; UI: mientras tanto, malas leyes y prácticas en todo lugar, incluso Ecuador a punto de aprobar una disposición de represión de datos, malo, malo, malo; OB: sí, parece que podríamos ayudar al gobierno ecuatoriano con seguridad, ver cómo se desarrolla y obtuve mi visa ecuatoriana de todos modos, desearía que tuvieras alguna noticia que pudieras

animar; UI: bueno Ecuador aprenderá bien o mal que romper la privacidad no es bueno, entre nos, estaban planeando comprar software para ingresar a las computadoras el año pasado, que los detuvo; traducción de fs. 21, 22, y 23, del chat de 24 octubre del 2013: Bini envió un mensaje Diane, cuyo verdadero nombre puede ser Diane Bareto y que puede ser un empleado de Sor Word: D: hola, hola, espero que estés bien, me preguntaba cómo va Ecuador, quería que Andy fuera a echar un vistazo, Mitri es muy escéptico, no presione aquí, sobre todo el asunto aquí, tal vez haya un poco de documentación a fines de noviembre cuando llegue Mitri, vayan ahí, con quien debo hablar según su opinión'; OB: hola, Ecuador se acerca, me mudaré a mediados de noviembre; D: genial, que pasa con la reforma del Código Penal en la que uno tiene que registrar la actividad en línea de los vecinos para evadir la responsabilidad, de todos modos odio ser tan audaz, tuviste la amabilidad de mencionar que podrías hablar algo por mí, creo que es una gran historia y en Europa, qué está sucediendo ahí, alguno de los mejores pensadores van a Ecuador para trazar una nueva utopía y nadie se entera de esto?; OB: sí, no estoy contento con la aprobación de parte de la legislación, es bastante mala.

Como se puede observar de la primera pericia, esta se trata de la traducción de un certificado laboral de la empresa TOP WORD en favor de Ola Bini, el tiempo de duración de dicha relación laboral, el sueldo que percibe y la forma como le realizarán los pagos por su salario; mientras que la segunda pericia consiste en una nueva traducción de chats, en los cuales se trata de diversos temas como la visita a una embajada y la forma como fue recibido; se habla de un contrato de trabajo, el cual deberá ser revisado por sus abogados y de un posible viaje para trabajar en Ecuador; se habla así mismo de que la empresa requerirá contratar a personas externas para poder funcionar; se hace mención de que se ha derogado un artículo del Código Penal, lo cual lo estiman relevante, y se menciona que se realizará un viaje a Londres y podrá visitar a Assange, viajará además a Berlín y que podrá pasar tiempo con Matri y Sara; que Julián recibió el mapa que le envió y le encantó tanto, que lo está enmarcando; comentan que el ex ministro de defensa del Ecuador, que aparentemente es una buena persona, es el nuevo embajador de la ONU en Ginebra; comentan que el tema de Chevron ha despegado, por lo que tiene mucho más tiempo para hacer estrategia, el único problema es que el ministro Luano y que está haciendo un trabajo fantástico para él; en otro tema comentan sobre malas leyes y prácticas en todo lugar, incluso que Ecuador está a punto de aprobar una disposición de represión de datos, lo que consideran malo; para finalmente comentar que Ecuador se acerca, se mudará a mediados de noviembre, y que alguno de los mejores pensadores van a Ecuador para trazar una nueva utopía y nadie se entera de esto; hechos que nuevamente el Tribunal tiene que recalcar, que no tienen pertinencia ni conducencia con el delito acusado, esto es con el delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, así como tampoco tiene relación con la finalidad que debe tener este acceso no consentido, como es el de explotar ilegítimamente dicho acceso o realizar otras actividades tendientes a modificar un portal, re-direccionar el tráfico de datos o aprovecharse de los servicios que ofrecería el sistema.

SOBRE EL ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES

Sobre este tema, Fiscalía General del Estado y la acusación particular recalcan que

este hecho se habría dado y que la prueba para establecerlo sería la fotografía digital encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594; el cual como ya se lo refirió, se lo pudo desbloquear utilizando la clave obtenida 55373571 (descrita en la segundas pericia del mayor William Castro Acosta, dispositivo 1); información que se la almacenó en un dispositivo USB, y cuya materialización se la realizó en otra pericia, especificando que el nombre de la imagen es: A95079D384EDBE1B75A21A558A22383C.JPG; y su contenido es:

```
[/HOME/OLABINI] (1004) V TORSOCKS2 TELNET 181.113.57.169
[OCT0612:51:56] ERROR TORSOCKS [23473]: UNABLE TO RESOLVE.
STATUS REP
TRYING 181.113.57.169...
CONNECTED TO 181.113.57.169.
ESCAPE CHARACTER IS, Y (invertida)]
```

```
C*****
EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTÁ PROHIBIDO
Usted debe tener permiso explícito para acceder/o
Configurar este dispositivo. Todas las actividades realizadas
son almacenadas
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBIPET
YOU MUST HAVE EXPLICIT PERMISSION TO ACCESS OR
CONFIGURE THIS DEVICE. ALL ACTIVITIES PERFORMED ON THIS
DEVICE
ARE LOGGED
```

```
*****
*****
CORPORACIÓN NACIONAL DE TELECOMINCAIONES CNT E.P. CNT
(Logo)
EL ACCESO O USO NO AUTORIZADO SE CONSIDERA UN ACTO
CRIMINAL
PETROECUADOR SENAIN INTERNET
```

```
*****
USER ACCESS VERIFICATION
USER NAME: % USER NAME: TIME OUT EXPIRED ; CONECTION CLOSED
BY FOREIGN HOST. [/HOME/OLA BINI] (1005) Y (invertida)
LENOVO.
```

Sobre esta imagen comparecieron en primer lugar el Ingeniero en electrónica y telecomunicaciones de la Corporación Nacional de Telecomunicaciones Carlos Andrés Medina Montalvo, empleado de dicha Institución desde el año 2009 y cuyo campo de trabajo son las áreas de redes IP, persona con conocimientos avanzados en redes de telecomunicaciones de equipos marca Cisco; explicó al Tribunal que la empresa pública CNT EP cuenta con certificaciones de seguridades desde el año 2013, con la certificación ISO2701-2013; señaló que por disposición del gerente de operaciones, él elaboró “un informe” de análisis de ejecución, Open OIM Redes IP, el 16 de agosto del 2019, afirmando que la IP 181.113.57.169 se asignó en base a una solicitud del área comercial, el 23 julio del 2015, a la empresa Petroecuador Senai

Internet, en el equipo de CNT, estaba ubicado en las instalaciones Boyacá, en la ciudad de Guayaquil, para posteriormente realizar un traslado de esta configuración el 24 de julio del 2015, hacia las instalaciones de CNT en el edificio Correos de Guayaquil; dijo que CNT EP realiza la instalación de la última milla y la configuración de la ONT asignada al cliente, bajo los estándares de seguridad de la información; que la IP que mencionó no es de conocimiento público, esa asignación está en conocimiento solo de personal de CNT y del cliente; explicó que la diferencia entre una IP pública y una privada, básicamente es que la IP pública tiene acceso a internet y la IP privada no lo tiene; recalcó que la IP 181.113.57.169 corresponde a un sistema de telecomunicaciones que difiere de un sistema informático y que la diferencia que básicamente consiste en que el sistema informático es el que permite almacenar o procesar información, como una o varias computadoras, servidores, los usuarios del sistema, mientras que un sistema de telecomunicaciones, es el medio físico que se usa para transportar información desde un origen a un destino; aclaró que quienes tienen autorización para acceder a la ONT son el cliente y el personal autorizado de CNT, esto de manera física, el otro es de manera remota, en ese caso únicamente el personal de CNT tiene la autorización para realizar esa conexión; señaló que como protocolos de seguridad tienen varias protecciones como bloquear el puerto ASL y otras; concluyó que la conexión de un tercero, es hacer uso como medio de paso para ingresar al ROUTER, y que eso era para él un acceso no consentido; explicó que el informe básicamente es un análisis de ejecución de funciones OPEN, ahí solo se detalla el equipamiento instalado y como fue el flujo en el sistema transaccional OPEN, no se detallan ni consta la configuración de ninguno de los dos equipos; explicó de forma detallada que una IP pública es aquella que permite la conexión a internet, si una persona tiene internet puede conectarse a esa IP, en el caso de que se lo admita, pero para que no se admita a esa conexión IP puede haber una restricción en su configuración, depende de los niveles de seguridad que tenga el servicio, también es posible poner un fire word, también se puede pedir un usuario y una contraseña, lo que forma parte de los elementos básicos de seguridad de un equipo; finalmente señaló que los equipos que pueden conectarse a esta ONT, así como a la distribución y asignación interna del direccionamiento público, son de responsabilidad del cliente y que si en el caso de que un usuario no autorizado, ingrese, cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático, telemático o de telecomunicaciones, aclarando que en el informe por él realizado no se verificó la creación de usuarios.

Sobre este mismo tema, compareció el perito en electrónica y telecomunicaciones Galo David Cárdenas Calderón, quien dijo además ser master en tecnología de la información con mención en informática, que posee un certificado en LINUS, otro en telefonía IP y que actualmente es docente de la carrera de maestría en la Universidad SEC; en lo principal expuso que realizó “un análisis integral” y elaboró conclusiones respecto del informe presentado por el ingeniero Carlos Medina Montalvo, empleado de la CNT, concluyendo que: a) Existe un enlace de internet con el nombre de Petroecuador SENAI, creado en el mes de julio del año 2015; b) Que los elementos técnicos no son suficientes para determinar la creación de usuarios en el equipo de la CNT; y, c) Que el equipo está en custodia de la CNT; explicó que un sistema de telecomunicaciones es un conjunto de dispositivos que permite brindar servicios digitales, compuesto por elementos activos y pasivos, como routeadores,

firewalls, ONTS, fibra óptica y todos los cables de última milla; mientras que un sistema informático está compuesto por servidores y aplicaciones que permiten brindar el servicio digital; que la infraestructura, permite el camino para conectar a estos servicios o medios digitales; en cuanto a la imagen (fotografía digital) encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594 y la cual consta en la página 33.115 del informe de perito William Danilo Castro Acosta, dijo que esta contiene una ventana para ingresar comandos, el protocolo utilizado es TELNET, realizado desde una computadora marca Lenovo, ejecutada en lenguaje de bajo nivel TOR, donde consta la dirección IP: 181.113.57.169, esta dirección según informe de CNT a julio del 2015, es de la empresa Petroecuador EP; explicó al Tribunal que para “acceder” a un sistema de comunicaciones (según las buenas prácticas y según la norma ISO27.001), existían tres formas: 1) Acceso totalmente restringido o bloqueado, donde todas las conexiones que se realicen son rechazadas; 2) Acceso libre: sistema que no tiene configurado ningún tipo de credencial, se puede “acceder” al mismo sin contraseñas, es un acceso con privilegios; 3) Acceso que requiere usuario y contraseña y demás factores de seguridad que tenga implementado el sistema; concluyó que “la imagen motivo de análisis”, la que consta en la página 33.115 del informe de perito William Danilo Castro Acosta y que fuera obtenida del teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594, es de acceso que requiere usuario y contraseña, en la cual se aprecia que existe una petición de conectividad hacia el ruteador (la imagen del anexo 3, se puede garantizar que hubo conectividad al equipo routeador) y éste devuelve una solicitud pidiendo usuario y contraseña; como ejemplo dijo que se tiene una propiedad, voy a ingresar para ver si la puerta está abierta o cerrada, sin embargo para hacer esta prueba, he tenido que atravesar el patio de la propiedad primero, por lo tanto cuando abro o cierro la puerta, quiere decir que ya entré al patio, es una analogía de la conectividad al ruteador; el perito explicó además que nunca tuvo acceso ni a la máquina Lenovo, ni al ruteador, ni revisó ningún equipo informático, lo que hizo tan solo fue un análisis del informe de la CNT O&M-REDES-IP-2019-08-016, “aclarando además” que la fotografía ni siquiera constaba dentro de ese informe; mencionó además que en el “informe” de la CNT no se podía evidenciar si había configurada seguridades para acceder a la IP 181.113.57.169, no siendo parte de la “pericia” determinar si la IP estaba protegida o si el router de la CNT tenía algún tipo de seguridad en la red; afirmó puntualmente que solo el cliente puede establecer si alguien se conectó o desconectó a esa red, en este caso el cliente era Petroecuador EP; explicó que de la documentación que analizó no se pudo determinar la creación de usuarios en el equipo routeador de la CNT, pero que lo que sí sería verificable en el LOCK del sistema, es que quedan todos los usuarios creados para la posterior revisión de los LOCKS, entonces si una persona accede a un dispositivo asignado a un IP, si quedaría grabado en el LOCK del dispositivo; señaló claramente que “si en el caso de que un usuario no autorizado ingrese y cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático”, aclarando que en el Informe de la CNT no consta que se hayan creado esos usuarios; señaló además que en su informe no pudo concluir que existió un acceso no consentido al sistema informático, que la información constante en el informe de la CNT no la pudo validar informáticamente, por lo que en su informe no se pudo demostrar lo que sucedió en realidad, porque para hacerlo,

necesitaría que el ruteador esté en línea y la configuración esté en línea, no solo tener la fotografía, resaltando que de la fotografía no se puede verificar si los comandos fueron ingresados, NO hay constancia del ingreso de algún usuario, solo aparece que el tiempo de validación terminó (no se ingresa usuario y contraseña) y se cierra la sesión automáticamente

ANÁLISIS

El Tribunal necesariamente tiene que realizar un análisis de lo mencionado por los dos “técnicos” que han rendido sus testimonios, el primero Ingeniero en electrónica y telecomunicaciones, empleado de la Corporación Nacional de Telecomunicaciones (Acusador Particular en la causa), Carlos Andrés Medina Montalvo, quien por disposición del “gerente de operaciones” de dicha Institución, elaboró “un informe” de análisis de ejecución, Open OIM Redes IP, el 16 de agosto del 2019, señalando en primer lugar y en lo relevante, que la IP 181.113.57.169 se le asignó el 23 julio del 2015, a la empresa Petroecuador Senai Internet; sobre el sistema de comunicaciones específicamente mencionó que como protocolos de seguridad tienen varias protecciones como bloquear el puerto ASL y otras; dijo textualmente que “la conexión de un tercero, es hacer uso como medio de paso para ingresar al ROUTER, y que eso era para él un acceso no consentido”; quedando en evidencia para este Juzgador Pluripersonal, una serie de contradicciones y vacíos en la elaboración de este “informe”: así, en primer lugar dijo que no se detallan ni consta la configuración de ninguno de los equipos de la CNT en el referido informe, las razones no las expuso; sobre la conectividad y seguridad del sistema, aclaró que una IP pública es aquella que permite la conexión a internet, si una persona tiene internet puede conectarse a esa IP “siempre que se lo admita”, pero para que no se admita a esa conexión IP puede haber una “restricción en su configuración”, dependiendo de los niveles de seguridad, también es posible poner un “Fire Word” y finalmente dijo que “se podía pedir un usuario y una contraseña”, todos estos elementos básicos de la seguridad de un equipo; quedando muy claro que esta “posibilidad de conectarse”, dependerá de los niveles de seguridad del sistema, como por ejemplo “se podía pedir un usuario y una contraseña”; afirmando finalmente que “si en el caso de que un usurario no autorizado, ingrese, cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático, telemático o de telecomunicaciones”, aclarando que en el informe por él realizado “no se verificó la creación de usuarios”, quedando entonces establecido que según el mismo “experto” del área de redes IP de la Corporación Nacional de Telecomunicaciones, al no verificarse la creación de usuarios en el sistema de telecomunicaciones de la CNT, NO existió un acceso no consentido a un sistema informático, telemático o de telecomunicaciones, conclusión a la que se arriba según lo dicho por el mismo experto.

Por otro lado, estas conclusiones a las que llega el encargado del área de redes IP de la Corporación Nacional de Telecomunicaciones, son incluso concordantes con lo señalado por el perito en electrónica y telecomunicaciones Galo David Cárdenas Calderón, master en tecnología de la información con mención en informática, que posee un certificado en LINUS, otro en telefonía IP y además docente de la carrera de maestría en la Universidad SEC; el que, sin embargo no realizó pericia alguna en la presente causa, pues se limitó a explicar que tan solo realizó “un análisis integral” y elaboró conclusiones, respecto del informe presentado por el ingeniero Carlos Medina Montalvo, empleado de la CNT, concluyendo de manera concordante con lo

dicho por el autor del informe que existía un enlace de internet con el nombre de Petroecuador SENAI, creado en el mes de julio del año 2015; que los elementos técnicos no son suficientes para determinar la creación de usuarios en el equipo de la CNT; y, que el equipo está en custodia de la CNT; se debe recalcar la afirmación realizada por el perito en electrónica y telecomunicaciones de que “los elementos técnicos no son suficientes para determinar la creación de usuarios en el equipo de la CNT”, lo que equivale a decir que NO existió un acceso no consentido a un sistema informático, telemático o de telecomunicaciones, según lo afirmó además el experto del área de redes IP de la Corporación Nacional de Telecomunicaciones y autor de este “informe”; por otro lado es relevante señalar que en cuanto a la imagen encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594 y la cual consta en la página 33.115 del informe de perito William Danilo Castro Acosta, el perito describió lo que se aprecia de ésta: dijo que contiene una ventana para ingresar comandos, el protocolo utilizado es TELNET, realizado desde una computadora marca Lenovo, ejecutada en lenguaje de bajo nivel TOR, donde consta la dirección IP: 181.113.57.169, esta dirección según informe de CNT a julio del 2015, es de la empresa Petroecuador EP; y, sobre el “acceder” a un sistema de comunicaciones, dijo que “existían” tres formas: un acceso totalmente restringido o bloqueado, donde todas las conexiones que se realicen son rechazadas; un acceso libre, donde el sistema no tiene configurado ningún tipo de credencia, se puede “acceder” al mismo sin contraseñas, es un acceso con privilegios; y, un acceso que requiere usuario y contraseña y demás factores de seguridad que tenga implementado el sistema, CONCLUYENDO que la “la imagen motivo de análisis”, es de acceso que requiere usuario y contraseña, quedando claramente establecido que el sistema de comunicaciones de CNT requería necesariamente de un usuario y contraseña para que se pueda acceder al mismo; tanto más cuanto que fue el mismo perito quien describió lo que se puede “apreciar” de la fotografía: una petición de conectividad hacia el router, el cual “devuelve” la solicitud pidiendo usuario y contraseña, por tanto al acceso al sistema de CNT nunca se dio; debiendo el Tribunal recalcar el hecho de que el perito nunca tuvo acceso ni a la máquina Lenovo, ni al router, ni revisó ningún equipo informático, se limitó solamente a “hacer un análisis” del informe de la CNT O&M-REDES-IP-2019-08-016; señalando incluso que no fue parte de la “pericia” determinar si la IP o el router tenían algún tipo de seguridad; llama la atención además al Tribunal las afirmaciones del perito en el sentido de que solo “el cliente”, en este caso Petroecuador EP, podía establecer al revisar sus equipos, si alguien se conectó o desconectó a esa red, lo que nunca ocurrió, pues como lo señaló el ingeniero Galo Cárdenas, nunca le dieron acceso a los equipos para comprobarlo, lo que fue corroborado incluso por el ingeniero en sistemas y funcionario de la Presidencia de la República Klever Giovanni Salguero Sosa, quien dijo que en el año 2015 laboraba en la Dirección de Tecnologías, siendo el líder del área de redes y conectividad, quien expuso, como ya se lo refirió precedentemente, que el Data Center de Contingencia tiene varios equipos, servidores, equipos de almacenamiento que ellos los denominan Storash, de seguridad perimetral, farwords y de comunicación que provee CNT y que “Fiscalía no pidió información de esos equipos, tampoco le solicitaron las IP de esos equipos, no les pidieron remitir los accesos, no les pidieron posible accesos no consentidos a esos equipos del Data Center”, comprobándose

entonces que nunca los equipos fueron siquiera revisados, menos aún practicada pericia alguna; por otro lado ha quedado plenamente establecido que de la simple “revisión de la documentación” realizada por el perito, NO se determinó la creación de usuarios en el equipo routeador de la CNT, lo que a criterio del perito sí hubiera sido factible determinar mediante la revisión de los equipos, ya que si una persona accede a un dispositivo asignado a un IP, siempre queda grabado en el LOCK del dispositivo este acceso, no encontrando explicación alguna de la razón por la cual no se realizó una “pericia” a los equipos instalados en el Data Center de Contingencia del a Presidencia de la República, lo que hubiera permitido determinar la existencia de la creación de usuarios en el routeador; conclusión que además se relaciona con lo dicho por el perito informático en el sentido de que “si en el caso de que un usuario no autorizado ingrese y cree usuarios alternos, esto constituye un acceso no consentido a un sistema informático”, reiterando que ni siquiera en el Informe de la CNT, consta que se hayan creado esos usuarios; finalmente se debe considerar lo afirmado por el propio perito: no pudo concluir que existió un acceso no consentido al sistema informático; que la información constante en el informe de la CNT no la pudo validar informáticamente; que no se pudo demostrar lo que sucedió en realidad; que para hacerlo necesitaría que el ruteador esté en línea y la configuración esté en línea; que de la fotografía no se puede verificar si los comandos fueron ingresados, NO hay constancia del ingreso de algún usuario, solo aparece que el tiempo de validación terminó y se cierra la sesión automáticamente; conclusiones determinantes en cuanto a la inexistencia del “acceso no consentido” a un sistema informático, telemático o de telecomunicaciones.

CRITERIO DE TESTIGOS EXPERTOS:

Sobre el tema específico de los sistema informático, telemático o de telecomunicaciones, así como de la imagen encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594 y que consta en la segunda pericia practicada por el mayor William Castro Acosta, comparecieron además varios testigos presentados por la defensa del ciudadano procesado Ola Bini, quienes aportaron información técnica sobre este tema; en primer lugar compareció el ingeniero en sistemas informáticos y computación, además desarrollador de sistemas y herramientas para la protección de la privacidad, **IVÁN PAZMIÑO MAZÓN**, quien explicó la importancia de la privacidad y las formas o herramientas existentes para protegerla, para conservar chats, para cifrar mensajes, ocultar direcciones de un computador cuando se conecta al internet, etcétera; explicó que un ROUTER es un dispositivo informático que ayuda a que los mensajes lleguen a un destino; que HACKER para él, es alguien que encuentra una solución a un problema técnico; IANA: es el Grupo de Trabajo de Ingeniería de Internet, trabajan para crear estándares de la WEB; que la dirección IP es la forma de encontrar un computador (como su número de teléfono); en cuanto a los tipos de direcciones IP, dijo que existen las públicas (utilizadas para servidores que están en el internet abierto) y privadas, que son para las redes internas de una institución; que TOR es una herramienta gratuita que sirve para proteger la privacidad de la gente, protege la IP de la computadora y que no sirve para saltarse seguridades; que TEILS es un sistema operativo que no tiene códigos ocultos, ni maliciosos; que los dispositivos LLUVICO, son como una llave que contiene códigos y sirve para desbloquearlos; que la CRIPTOGRAFÍA en el ámbito digital permite la trasmisión segura de un mensaje,

siendo similar a un cifrado, lo que hace que un mensaje sea ilegible; que el algoritmo HASH genera un identificador para un mensaje; sobre la imagen encontrada en el teléfono celular marca I Pone, dijo que esta circulaba en internet, en la cual se aprecia como un mensaje de bienvenida al servidor y el apuntador espera que se ingresen credenciales al servidor y después un mensaje que dice no ingresó credenciales, así que se cierra la conexión; que en la fotografía se ve una IP pública, que se utiliza las herramientas TOR y TELNET, aclara que no existe acceso, solo establecimiento de una conexión, no se presentan credenciales para acceder al sistema y se cierra la conexión; finalmente dijo que conoció a Ola Bini en una empresa consultora de EEUU, fueron compañeros de trabajo en el año 2015 donde se creó un equipo para crear herramientas para la privacidad; que Ola Bini es un desarrollador de Software abierto, lo conoce más de 9 años es un programador famoso, desarrollo uno de los proyectos más famosos para la simulación del comportamiento de cédulas u otros de relevancia. Sobre estos temas el Máster en seguridad Informática e ingeniero en sistemas **RAFEL BEJAMÍN BONIFAZ PALLARES**, empleado de la Organización de Derechos Digitales dijo sobre el derecho a la privacidad, que este se refiere al derecho a decidir que parte de nuestros datos se pueden compartir; dijo haber trabajado en seguridad informática desde el año 2012 y luego obtuvo una maestría en Seguridad Informática en Buenos Aires; reiteró que TOR es una herramienta que permite transitar por internet y mitigar el riesgo de ser vigilado por periodistas, abogados, etc.; explicó que un ROUTER es un dispositivo que permite conectar dos redes; que conoce a Ola Bini desde el año 2013, él era parte de la Asociación de Software Libre del Ecuador y la empresa Thought Works quería abrir oficinas en el Ecuador; que ha trabajado con él y compartido varios seminarios, afirmando que Ola Bini es un programador reconocido a nivel internacional, experto de seguridad informática; comento que IANA es la organización que se encarga de distribución de las direcciones IP públicas en internet; que la IP es una dirección dentro de una red de computadoras, existiendo públicas y privadas; expuso que la IP 181.113.57.169 es una dirección pública; que SHODAN es un sistema que permiten hacer escaneos para encontrar los servicios que se presten; sobre la CRIPTOGRAFÍA, dijo que es la utilización de las matemáticas para proteger información; sobre la imagen encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594 y que consta en la segunda pericia practicada por el mayor William Castro Acosta, dijo que esta circulaba en internet y que en esta se puede observar que se quiere acceder a través del sistema TELNET, en la imagen se lee: ingreso no permitido, pide nombre y usuario para autenticarse, no se ingresa el nombre de usuario, el sistema responde con un time out, tiempo de espera terminó y se corta la conexión; finalmente dijo que no se puede saber si la imagen es real, por lo que se debería contrastar con el sistema al que se quiso ingresar, ya que este sistema debería guardar esos registros, para establecer que alguien quiere ingresar al sistema en esa fecha:

Comparecieron además otros expertos en sistemas como **ROGER LINUS NORBERG**, quien dijo ser uno de los investigadores del proyecto TOR; ciudadano con pregrado en ciencias informáticas, ingeniero en matemáticas y en ciencias informáticas e ingeniera eléctrica; habló sobre la privacidad en el entorno digital, sobre el software libre y quien lo desarrolla, aclaró que es el creador de la

herramienta TOR junto a los ciudadanos Matisen y Saibersen, proyecto que fue financiado por el Departamento de Defensa de EEUU, la Organización Nacional de Ciencia de EEUU, el Ministerio de RREE de Suecia y otros países europeos; aclarando que TOR es un software que funciona en una computadora; que el programa SHODAN es una página web, la que recolecta un mapa o una vista de cada servicio que está en internet, es utilizado para seguridad en la red y su meta es la de tener un mapa de ver como se ve el internet; que la IANA es la autoridad que asigna los números en internet; que una IP es como un número telefónico pero para internet; dijo que la red 181.113.57.169 es una dirección pública; que un cable de FIBRA ÓPTICA es una forma de transmitir datos en el internet a largas distancias; que un ROUTER es el aparato que envían el tráfico de internet de un lado a otro; TELNET es un programa para conectarse a los servicio de internet, es como un navegador para visitar sitios web; que la red ONE es una red de área ancha (conexión de internet a larga distancia); red LAN es una red de área local (dos computadores comunicándose); un FIREWORD, dispositivo que bloquea la conexión a ciertos servicios; HACKER lo considera a una persona con conocimientos sobre un tema; HACKING ÉTICO es un movimiento de expertos en seguridad informática, que utilizan su conocimiento para mejorar la seguridad de internet; CRIPTOGRAFÍA en el ámbito digital es el estudio de las matemáticas para proteger información como el cifrado o la firma digital; sobre este juicio, señalan que vio un artículo de la EFF (organización sin fines de lucro en los EE.UU) sobre un imagen publicada, en la que se aprecia una conexión por internet a una dirección IP pública, se utiliza TOR, la dirección es alcanzable, se realiza la conexión y sale un banner que es un aviso, que dice que el acceso es prohibido y en la parte inferior de la imagen hay una opción de ingresar el nombre de usuario para hacer el login, y luego dice que venció el tiempo y que la conexión fue cerrada por un anfitrión ajeno, eso quiere decir que se hizo una conexión pero que no se hizo el login, no se ingresó y luego se desconectó, de la imagen se establece que no hubo ningún intento de acceder; expresa además que todas las actividades realizadas en este dispositivo son registradas; sobre Ola Bini, dijo que lo conoce desde el año 2013, en una reunión de expertos en seguridad informática; que ha trabajado en un proyecto con Ola Bini, él fue voluntario y desarrollador de TOR para mejorar su diseño, para que sea más seguro para el usuario; aclaró sobre la diferencia entre un sistema informático y uno de telecomunicaciones: el sistema informático se enfoca en datos y tráfico y el sistema de telecomunicaciones habla de la infraestructura, cables etc.; que la herramienta TOR permite que el usuario elija cual información compartir; finalmente dijo que de acuerdo con la RPS 1918, las IP públicas son ruteables de forma pública, cualquier persona puede enviar tráfico a través del internet, ahora, si existe un firework, puede ser que no llegue ese tráfico, pero una dirección IP pública es algo que es públicamente ruteable. Finalmente y sobre este tema, comparecieron además **LINUS NORBERG**, de nacionalidad sueca, consultor informático y ejecutor de software; habló en lo principal sobre la privacidad y como se garantiza este derecho, las herramientas y dispositivos que se utilizan para garantizarla, como la herramienta TOR; explicó varios términos técnicos como IANA: organización que vigila los números en internet; AITF: organización que crea los estándares en el internet; habló de las IP y sus clases: públicas y privadas, de la RED ONE, que es una red ancha, RED LAN que son redes locales; dijo que FIREWORK es un dispositivo para

filtrar el tráfico; expresó que SHODAN es una herramienta que se usa como motor de búsqueda de direcciones IP; que IFF es una organización responsable de emitir estándares sobre dispositivos; habló de la criptografía y el cifrado; explicó que conoce a Ola Bini quien es un desarrollador de software libre; sobre la imagen que vio en el sitio web EFE, dijo que de la misma se aprecia una conexión a un sistema vía internet, este sistema responde con un banner que dice CNT, ese banner dice que el acceso es prohibido y sale un crow que pide usuario y password, no se ingresa nada y el sistema remoto caduca; **DENIS ROGER** de nacionalidad italiana, con un PHD en Filosofía, maneja y dirige el desarrollo de software, además es criptográfico y desarrollador de sistemas de autenticación; quien en lo principal expuso sobre la privacidad en el campo digital, la que dijo, permite no revelar sus datos cuando no lo desea o elegir el contexto donde se desea compartirlos, existiendo herramientas para protegerla como el GPG que es un software de privacidad, TOR que es una herramienta que permite conexiones de red a través del internet, BPN que es una red privada virtual; explicó ciertos conceptos como IANA: institución de asignación de direcciones IP públicas en el internet; ROUTER: enruta paquetes entre diferentes máquinas o conecta más de una máquina sin cables; TELNET: es una forma antigua pero activa de conectarse con una terminal por red en el internet; SHODAN: utilizado por investigadores de seguridad, sirve para revisar las direcciones IP, ver cuales están abiertas y las enumera en una página; FIREWALL: es un sistema que bloquea conexiones desde afuera; CIFRADO SIMÉTRICO: es un sistema protegido por una contraseña; dijo conocer al ciudadano Ola Bini desde hace 6 años, en el desarrollo de un proyecto de privacidad ciudadana y datos, financiados por la Comisión Europea, que Ola Bini es coautor de varios tipos importantes de software importantes, además de desarrollador de software e investigador de seguridad; sobre la imagen que la ha visto en un artículo de la EFF, lo que recuerda es que hay una conexión de Telnet a través de TOR, hay una IP pública y hay un banner que dice CNT, banner de texto que dice que el acceso es no autorizado, entonces informa de una conexión y luego una desconexión; y, **DAVID RAFIC MIRZA AHMAD**; ciudadano de nacionalidad canadiense, Presidente de una Compañía de Seguridad Informática, quien habló de la privacidad, las herramientas para protegerla como BPN o TOR; explicó conceptos como IANA: organización que asigna los números de internet; AITF: grupo de ingenieros que publican las especificaciones técnicas para el internet; dirección IP: es un número único asignado a un computador y a una red como un número de teléfono; una ONT: es una interfase física, el computador se conecta con una óptica a través de puerto físico; TELNET; es un protocolo que se utiliza para conectar un computador con otro, ya no es muy utilizado porque es muy expuesto; SHODAN: herramienta de escaneo masivo, utilizado para reunir estadísticas y medir el internet, FIREWALL: es como una cerca que se pone en una red que restringe el acceso; CRIPTOGRAFÍA: es la ciencia de crear súper códigos; RED ONE: red de área amplia; red LAN: es una red área local; dijo conocer al ciudadano Ola Bini desde el año 2013, miembro importante del Software Libre; sobre la fotografía filtrada en el año 2019, en ella aparece una pantalla de un terminal de un computador, se indica una línea de comando, luego sale una advertencia, pero no hay intento ni acceso al sistema informático, hay una captura de pantalla donde se muestra que la conexión caduca. Finalmente y sobre la prueba documental presentada por Fiscalía General del

Estado, el Tribunal tiene que remitirse necesariamente a uno de los principios esenciales de la prueba, esto es su pertinencia; conforme lo señala el artículo 454 del COIP, norma que en su numeral 5 establece: “5. Pertinencia.- Las pruebas, deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad de la persona procesada”; pertinencia de la prueba hace alusión a la relación que debe existir entre los hechos acusados y los medios con los cuales se pretende probarlos, debiendo aclararse que si nada tienen que ver con estos hechos, entran en el campo de la impertinencia; debiendo recalcar que su utilidad se refiere al aporte concreto que pueda presentar, sobre el objeto de la investigación; mientras que la conducencia de la prueba consiste en la aptitud del contenido intrínseco y particular para demostrar los hechos que se alegan; deberá referirse directa o indirectamente a los hechos o circunstancias y su idoneidad legal está determinada o encaminada a demostrar un determinado hecho; sin embargo de lo cual la prueba documental presentada de Fiscalía se refiere a hechos totalmente ajenos al delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, refiriéndose más bien a los movimientos migratorios que registra el procesado Ola Bini en el período comprendido entre los años 2013 y 2019; un contrato de Housing y de enlace de datos, suscrito por el Ing. Iván Croshi y el procesado Ola Bini, de 2 de abril del 2015, contrato mediante el cual la empresa Telconet daba un espacio en su Data Center y un enlace de datos de 10 MDT al procesado Ola Bini; una certificación del Viceministro de Relaciones Exteriores del Ecuador, en el cual se certifica las visitas del ciudadano Ola Bini, al entonces asilado en la embajada de Ecuador en Londres Julián Assange, en el período 2015-2019; un oficio suscrito por la Viceministra de RR.EE. del Ecuador, en el cual se remiten copias certificadas de la emisión de visas a nombre del ciudadano Ola Bini, así como copias certificadas de los expedientes para la obtención de la visa de 26 de noviembre del 2015, del 27 de noviembre del 2016, así como el expediente de la visa de excepción, de 8 mayo del 2018, a favor de Ola Bini; un oficio de la Dirección de Prevención de Lavado de Activos de la Superintendencia de Compañías, en el que se certifica que el ciudadano Ola Bini no es socio, accionista o representante legal de compañía alguna, así como otro oficio de la Secretaria General de la Intendencia Regional de Quito de la Superintendencia de Compañías, en la que se certifica que Ola Bini no figura como socio o administrador en ninguna sociedad de comercio; un oficio de la SENA en el que se certifica que Ola Bini no registra declaraciones de dinero en el período 2011-2019; un memorando de 14 de mayo del 2019, suscrito por el Subsecretario del Ministerio de Telecomunicaciones, en el cual se adjunta un reporte de ataque cibernéticos del 11 al 15 de abril del 2019; un certificado del IESS, que contiene el historial laboral de Centro de Economía Digital y otro certificado con el historial de la empresa Tour Word, en el cual no consta el ciudadano Ola Bini; un oficio de 5 de junio del 2019, suscrito por la Directora de Asesoría Legal de la Corte Constitucional, al cual se adjunta el Informe Técnico NO. 044-DTI, título: ataque informático de 22 de mayo del 2019, describe la caída del portal Institucional, donde se puede observar el mensaje OUT Net Julián Assange; oficio de 6 de junio del 2019, suscrito por la Coordinadora Jurídica del Ministerio de Telecomunicaciones, al cual se adjuntan copias certificadas del expediente de la Asociación Centro de Autonomía Digital, en cuya Directiva se nombra como vicepresidente al señor Ola

Bini; oficio de la UAFE, suscrito por la Coordinadora de Prevención de la UAFE, al cual se adjunta un informe de TOUR WORDS S.A.; oficio de 14 de junio del 2019 suscrito por el Gerente de TOUR WORD Ecuador, mediante el cual se remiten información sobre los ingresos del señor Ola Bini, en los años 2013-2017; oficio de 20 de junio del 2019, remitido por la Dirección Zonal 9 del SRI, al cual se adjuntan informes ejecutivos ampliados de la empresa Tour Word y Soporte Libre: el Informe No. OIM-REDES-IP2019-08-016 de 16 agosto del 2019, suscrito por el Ing. Carlos Medina, funcionario del CNT; Memorando de fecha 14 de junio del 2019, suscrito por la Directora de Asuntos Internacionales de la Fiscalía General del Estado, al cual se adjunta respuesta parcial de requerimientos de la Asistencia Penal Internacional de traducción; la Asistencia Penal Internacional con la traducción de chats del señor Ola Bini; un oficio suscrito por procurador judicial de EP Petroecuador, al cual se adjunta el memorando en el que se señala que el comando TELNET a la IP 181.113.57.169, no se realizó desde la IP Petroecuador; un oficio firmado electrónicamente por el Ministerio de RR.EE. del Ecuador, al cual acompaña un detalle de visitas al señor Julián Assange en los años 2015 y 2019, en la embajada de Ecuador en Londres, entre los cuales consta el señor Ola Bini y funcionarios de TOP WORDS.

ANÁLISIS DE LA PRUEBA

El Tribunal en este análisis final, parte realizando un análisis del tipo penal acusado “Acceso no consentido a un sistema informático, telemático o de telecomunicaciones”, que como se lo dijo precedentemente está tipificado en el artículo 234 del COIP aplicable al caso, que describe: “La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con una pena privativa de libertad de tres a cinco años”; teniendo el tipo penal dos acciones específicas contenidas en los verbos ACCEDER (entrar en un lugar o pasar de él) o MANTENERSE (contra la voluntad de quien tenga el legítimo derecho), en un sistema informático, telemático o de telecomunicaciones; y, además el tipo penal contempla una “finalidad” de ese acceso, claramente detallada en la norma: explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re-direccionar el tráfico u ofrecer estos servicios sin pagar a los proveedores.

Por otro lado, estas dos acciones descritas, las de “acceder” o “mantenerse” en un sistema informático, telemático o de telecomunicaciones, requiere esencialmente la vulneración de un sistema de protección o de seguridad para lograr estos objetivos, pues si el sistema no tiene estas características (protección o seguridad), querría decir que su “acceso” es libre, que no requeriría del consentimiento del titular para ingresar al mismo, pudiendo hacerlo cualquier persona y de cualquier forma; entonces queda claro para este Juzgador Pluripersonal que el sistema informático, telemático o de telecomunicaciones es “restringido” para las personas en general y por tanto requieren contar con un sistema de “protección o seguridad”, lo que le da precisamente esa calidad; en otras palabras y basándonos en la doctrina mencionada anteriormente (Gustavo Eduardo Aboso. Derecho Penal Cibernético. Editorial B de F. Montevideo-Buenos Aires. 2017. pág. 184), “se exige que el autor

haya superado las medidas de seguridad que caracterizan a los sistemas informáticos con acceso restringido mediante el uso de programas para vulnerar los códigos de acceso, o bien utilizando los códigos auténticos de una persona autorizada”.

En la causa y de la prueba analizada, se establece sin que exista duda alguna, la existencia del Data Center de Contingencia de la Presidencia de la República, creado a finales del año 2015 e inicios del 2016, el cual contaba con servidores, equipos de almacenamiento, de seguridad perimetral farwood y de telecomunicaciones, equipos que fueron “prestados” por la empresa EP Petroecuador y cuyo proveedor de enlaces era la Corporación Nacional de Telecomunicaciones, estando ubicado el sitio principal en Lumbisí, en la Secretaría de Inteligencia, mientras que el sitio alterno estaba ubicado en la ciudad de Guayaquil, servidores que en lo principal contenían los correos institucionales de la Presidencia de la República; todo esto según lo expuso el ingeniero en sistemas de la Presidencia de la República Klever Giovanny Salguero, quien además señaló puntualmente que el Centro de Contingencia a finales del 2015 estaba ya operativo, “pero no en producción”, entendiendo con esta afirmación que si bien el sistema estaba en funcionamiento, no contaba todavía con dato alguno.

El Tribunal analiza además lo afirmado por el ingeniero en electrónica y telecomunicaciones Carlos Medina Montalvo, funcionario de la CNT, empresa proveedora de enlaces al Centro de Contingencia de la Presidencia de la República y autor del Informe Open OIM, redes IP, de 16 de agosto del 2019, quien explicó que efectivamente la IP 181.113.57.169 fue asignada el 23 de julio del año 2015, a la empresa EP Petroecuador SENAI Internet, en uno de los equipos de la CNT ubicado en las instalaciones de la calle Bocayá en Guayaquil y posteriormente se la trasladó al edificio Correos de Guayaquil; funcionario quien aseveró que el sistema tenía implementado un protocolo de seguridad y que a su criterio “un acceso no sentido” se da, cuando existe la conexión de un tercero, quien hace uso como medio de paso para ingresar al ROUTER; informe al que se le realizó “una pericia” por parte del ingeniero Galo Cárdenas Calderón, quien recalcó que él tan solo hizo un análisis del Informe O&M-REDES-IP-2019-08-016 presentado por la CNT, estableciendo que efectivamente existía el enlace de internet con nombre EP Petroecuador-SENAI, creado en el mes de julio 2015, equipo que estaba en custodia de la CNT; en cuanto a establecer si se produjo a no un “acceso no consentido” a un sistema informático telemático o de telecomunicaciones, el perito Cárdenas explicó de forma amplia las formas como se puede conseguir este acceso, describiendo las únicas formas en que se puede producir; la primera cuando se tiene un sistema con acceso totalmente restringido, dijo que estos sistemas se encuentran totalmente bloqueados, y cuando se pretende acceder al mismo, todas las conexiones son rechazadas; en segundo lugar y contrario al primer caso, existen sistemas con accesos totalmente libres, los cuales no tienen configurado ningún tipo de credencia, a estos sistemas dijo, se puede acceder sin ningún tipo de contraseña; y, finalmente, dijo que existían los sistemas que tenían implementado un nivel de seguridad y que para cuyo acceso se requería ingresar un usuario y una contraseña, aclarando que el sistema descrito en el Informe O&M-REDES-IP-2019-08-016 presentado por la CNT, era un sistema de este tipo, que para su acceso requería el ingreso de un usuario y contraseña.

Pese a lo afirmado por el perito Galo Cárdenas Calderón, la Fiscalía General del

Estado y la acusación particular afirman que el acceso no consentido al sistema de telecomunicaciones que estaba en custodia de la CNT, si se produjo, lo que se probaría únicamente con una fotografía digital encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594 y que consta descrita en la segunda pericia practicada por el mayor William Castro Acosta, imagen que a criterio del mismo perito Cárdenas, contiene una ventana para ingresar comandos, dijo que se utiliza el protocolo TELNET, se lo realiza desde una computadora LENOVO, ejecutada en lenguaje TOR, donde consta la IP 181.113.57.169, la que según CNT pertenece a la empresa EP Petroecuador desde el año 2015; perito que sobre la misma aclaró que de esta no se puede verificar si los comandos fueron ejecutados, NO hay constancia del ingreso de algún usuario, solo aparece que el tiempo de validación terminó y se cierra la sesión automáticamente, recalcando que en su informe NO puede concluir que haya existido un acceso no consentido y que la información contenida en la imagen, no se la pudo validar informáticamente, por tanto NO se puede determinar qué sucedió en la realidad, ya que no era parte de pericia, ya que para establecer un acceso al sistema analizado, necesitaría que el ruteador esté en línea y la configuración esté en línea, en otras palabras realizar “una pericia” al sistema y no solo tener la fotografía, afirmando que nunca se le facilitó los equipos para analizarlos, lo que fue corroborado por el ingeniero Klever Salguero, funcionario de la Presidencia quien dijo Fiscalía no le solicitó información de ninguno de los equipos, ni de las IP de los equipos, ni los accesos realizados a los equipos, ni de accesos no consentidos, que pudieron haber ocurrido, recalcando el hecho de que todo “acceso” queda registrado en los equipos; criterios mantenidos además por varios testigos con conocimientos amplios en el tema, como el ciudadano Iván Pazmiño Mazón, ingeniero en sistemas informáticos y de computación quien sobre la fotografía digital encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, dijo que lo que se aprecia es un información desplegada por la CNT, se refiere a lo que un servidor muestra como pantalla de bienvenida, en el cual se pide el usuario y contraseña y se acaba el tiempo de espera, sale un mensaje que se corta la comunicación, reiterando que no existe acceso al sistema; o como Roger Linus Rorberg, Denis Roger y David Mirza Ahamed, quienes concordantemente dijeron sobre la imagen, que en esta se aprecia una conexión a un sistema informático, el sistema responde con un Baner CNT, el Baner indica que wel sistema remoto caduca y se cierra; llegándose a concluir que de la prueba analizada, no se ha demostrado en forma alguna, que se haya vulnerado un sistema de protección o seguridad, para lograr el acceso al sistema informático.

Por otro lado y en cuanto a la finalidad que debe tener este “acceso no consentido”, el que según lo detalla norma se refiere a la explotación ilegítima del acceso, modificar un portal web, desviar o re-direccionar el tráfico u ofrecer estos servicios sin pagar a los proveedores, no se presentó prueba alguna, debiendo recalcar en primer lugar lo dicho por el ingeniero en sistemas de la Presidencia de la República Klever Giovanni Salguero, en el sentido de que su Centro de Contingencia estuvo operativo a finales del año 2015, pero no en producción, por lo tanto no contaba con información alguna que podría haber sido “explotada” ilegítimamente, es decir acceder ilegalmente al conocimiento existente en el sistema y extraer la información de dichos datos; y, en segundo lugar volver a resaltar el hecho de que tanto el

“perito” designado (quien no realizó ninguna pericia), el mismo autor del Informe de la CNT y varios expertos en el tema de sistemas, determinaron que tan solo con la fotografía digital encontrada en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594, era imposible establecer la existencia del acceso a al sistema de la CNT, ni establecer lo que verdaderamente sucedió en el realidad, pues para poder establecerlo, debían contar con los aparatos que componen dicho sistema, en el cual además todo acceso realizado debe quedar registrado.

El Tribunal concluye señalando que la prueba incorporada por Fiscalía y la acusación particular, con la cual se pretendió justificar la responsabilidad del ciudadano Ola Metodiuos Martín Bini en el cometimiento del delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, es insuficiente y no justifica de forma alguna que dicho acceso se haya producido, ni que el ciudadano Ola Bini se haya beneficiado o explotado información constante en dicho sistema, tampoco se ha comprobado que se haya modificado un portal web ni que se haya re-direccionado el tráfico de datos o voz, ni que se haya beneficiado de forma alguna de la información constante en el sistema; debiendo recalcar más bien que de la prueba presentada, tanto de cargo como de descargo, se establece de manera unívoca que el presunto “acceso no consentido” al sistema que funcionaba en el Centro de Contingencia de la Presidencia de la República y que estaba a cargo de la CNT nunca se dio, sin que la prueba presentada determine acción alguna realizada con ese objetivo, a no ser la fotografía digital que consta en el teléfono celular marca I Pone, modelo I Pone 8, color negro, con i mal 352993090817594, la cual fue descrita en el informe pericial del mayor William Castro Acosta, imagen que fue analizada tanto por el perito nombrado por Fiscalía Galo Cárdenas Calderón, así como varios expertos en el tema informático, quienes concluyen señalando que de dicha imagen, no se puede verificar si ha existido un acceso al sistema de CNT, ni establecer siquiera lo que en la realidad sucedió, según el análisis previamente realizado, estableciéndose por tanto que no existe acción ilícita alguna imputable el procesado, acción que según el concepto causal se refiere a un “comportamiento humano dependiente de la voluntad que produce una determinada consecuencia en el mundo exterior”, y que en el presente caso tenía como finalidad logra un acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Finalmente el Tribunal observa que se debe garantizar un principio necesario y fundamental para el derecho penal “la presunción de inocencia” que, como lo refiere Ferrajoli “el principio de jurisdiccionalidad al exigir en su sentido lato que no exista culpa sin juicio, y en sentido estricto que no haya juicio sin que la acusación sea sometida a prueba y a refutación postula la presunción de inocencia del imputado hasta prueba en contrario sancionada por la sentencia definitiva de condena” (Ferrajoli, Luigi. 2001, Derecho y razón, quinta edición, Madrid, Ed. Trotta página 549); presunción de inocencia que es un derecho fundamental y por tanto forma parte del bloque constitucional de derechos, la que se encuentra asegurada y garantizada tanto en la Convención Americana de Derechos Humanos como en el Pacto Internacional de Derechos Civiles y Políticos: artículo 11.1 de la Declaración Universal de Derechos Humanos, aprobada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, dispone que: “toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se pruebe su

culpabilidad, conforme a la ley y en juicio público en el que se hayan asegurado todas las garantías necesarias para su defensa”; por su parte, el Pacto Internacional de Derechos Civiles y Políticos, aprobado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966, establece en su artículo 14.2 que “toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad conforme a la ley”.

VII RESOLUCIÓN. Por las consideraciones expuestas, en mérito de la prueba aportada en la audiencia oral de juzgamiento, de conformidad con lo establecido en los Artículos 622 y 625 del Código Orgánico Integral Penal, **ADMINISTRANDO JUSTICIA, EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR, Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPUBLICA**, éste Tribunal de Garantías Penales de Pichincha dicta sentencia, RATIFICANDO EL ESTADO DE INOCENCIA de la persona procesada: **OLA METODIOS MARTIN BINI**, cuyo estado y condición constan en esta sentencia; a efectos del presente pronunciamiento, se revocan todas la medida cautelares dictadas en la presente causa en contra del citado procesado, medidas cautelares constante en el auto de llamamiento a juicio inicialmente referido. La acusación particular presentada no es maliciosa ni temeraria. Actúe el doctor Edwin Cárdenas Vargas, Secretario de este despacho jurisdiccional. NOTIFÍQUESE.

f).- MAROTO SANCHEZ MILTON IVAN, JUEZ; ALTAMIRANO CARDENAS FANNY ISABEL, JUEZA; COELLO SERRANO PABLO MARCELO, JUEZ.

Lo que comunico a usted para los fines de ley.

CARDENAS VARGAS EDWIN VINICIO
SECRETARIA