FGE
FISCALÍA GENERAL DEL ESTADO
ECUADOR

CONSEJO DE LA JUDICATURA

Ministerio del Interior Ministerio de Gobierno

MANUAL DE ACTUACIÓN PARA LA RECOLECCIÓN, PRESERVACIÓN, TRATAMIENTO Y ANÁLISIS DEL CONTENIDO DIGITAL

Código: CSEIIMLCF-MLCF-MAN-2026-001

Versión: 2.0

FIRMAS DE ELABORACIÓN, REVISIÓN, VALIDACIÓN Y APROBACIÓN

Fase	Nombre / Cargo	Firma
Elaborado por:	**MSc. Ab. David Del Pozo Carrasco** ANALISTA ASESORIA JURIDICA 2 **FISCALIA GENERAL DEL ESTADO**	Validar únicamente en FirmaEC. Firmado electrónicamente por: DAVID DEL POZO CARRASCO
	Mrt. Patricio Guayaquil Proaño EXPERTO 1 **FISCALÍA GENERAL DEL ESTADO**	Validar únicamente en FirmaEC. Firmado electrónicamente por: PATRICIO GIOVANNI GUAYAQUIL PROANO
	Mgs. Jorge Néjer Guerrero ESPECIALISTA DE CIBERDELITOS **MINISTERIO DEL INTERIOR**	
	Ab. Paulo Haro Herrera JEFE DEPARTAMENTAL NACIONAL DE GESTIÓN PROCESAL GENERAL **CONSEJO DE LA JUDICATURA**	Nombre: PAULO CESAR HARO HERRERA Motivo: Firma Digital Localización Rumiñahui, Ecuador Fecha: 30/07/2026 08:59
	Mayr. Mgs. Luis Fernando Meza Cartagena JEFE DE COORDINACIÓN OPERACIONAL **UNIDAD NACIONAL DE ACOPIO DE INDICIOS Y EVIDENCIAS DE LA POLICÍA NACIONAL**	
	Mayr. Marco Pazmiño Montaluisa ASESOR ESTRATÉGICO OPERACIONAL **DIRECCIÓN NACIONAL DE INVESTIGACIÓN TÉCNICO CIENTÍFICA DE LA POLICÍA NACIONAL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: MARCO AURELIO PAZMINO MONTALUISA
	Sbte. Ing. Diego Fernando Cevallos Troya PERITO DE INGENIERÍA INFORMÁTICA FORENSE-Z9-JCRIM **DIRECCIÓN NACIONAL DE INVESTIGACIÓN TÉCNICO CIENTÍFICA DE LA POLICÍA NACIONAL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: DIEGO FERNANDO CEVALLOS TROYA

	Ing. Leonardo Chuquiguanca Vicente ESPECIALISTA EN AUDITORÍA FORENSE **CONTRALORÍA GENERAL DEL ESTADO**	
	Ing. Santiago Cobos Navarrete, MSc. COORDINADOR DE MÉTODOS Y PROTOCOLOS DE SERVICIOS **SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES**	
	Ing. Karina Jácome Herrera, MSc. ANALISTA DE MÉTODOS Y PROTOCOLOS **SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES**	Validar únicamente en FirmaEC. Firmado electrónicamente por: KARINA ESTEFANIA JACOME HERRERA

Nota: El funcionario **Mgs. Danilo Quijo Palacios**, Especialista Legal de la Oficina de las Naciones Unidas contra la Droga y el Delito participó en calidad de elaborador del presente instrumento, sin embargo, no cuenta con firma electrónica para la suscripción del mismo.

Fase	Nombre / Cargo	Firma
	Mgs. Gabriela Valeria Díaz Peñafiel SUBDIRECTORA GENERAL **SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES**	
	Ab. Paulo Haro Herrera JEFE DEPARTAMENTAL NACIONAL DE GESTIÓN PROCESAL GENERAL **CONSEJO DE LA JUDICATURA**	Nombre: PAULO CESAR HARO HERRERA Motivo: Firma Digital Localización Rumiñahui, Ecuador Fecha: 30/07/2026 08:59
	MSc. Ab. José Andrés Bedón Paula DIRECTOR DE INVESTIGACIÓN CIVIL (e) **FISCALIA GENERAL DEL ESTADO**	Validar únicamente en FirmaEC. Firmado electrónicamente por: JOSE ANDRES BEDON PAULA

Revisado por:	**Mgs. Víctor Romero Rea** ESPECIALISTA EN CRIMINALÍSTICA **FISCALÍA GENERAL DEL ESTADO**	Validar únicamente en FirmaEC. Firmado electrónicamente por: VICTOR MANUEL ROMERO REA
	Mayr. Xavier Garzón Pérez DIRECTOR CIBERDELITOS **MINISTERIO DEL INTERIOR**	
	Mgs. María Espinosa Espinosa ANALISTA DE POLÍTICA INTEGRAL Y PROMOCIÓN DE DERECHOS HUMANOS **MINISTERIO DE GOBIERNO**	
	Crnl. De Policía de E.M. Dr. Henry Javier Coral Ramos DIRECTOR NACIONAL DE INVESTIGACIÓN TÉCNICO CIENTÍFICA POLICIAL **DIRECCIÓN NACIONAL DE INVESTIGACIÓN TÉCNICO CIENTÍFICA DE LA POLICÍA NACIONAL**	Validar únicamente en FirmaEC. Firmado electrónicamente por: HENRY JAVIER CORAL RAMOS
	Cptn. Mgs. Diana Castillo Lucio JEFE DEL DEPARTAMENTO DE PLANIFICACIÓN **DIRECCIÓN NACIONAL DE INVESTIGACIÓN TÉCNICO CIENTÍFICA DE LA POLICÍA NACIONAL**	
	Mgtr. Tcnl Esteban Valencia Valverde JEFE DE LA UNIDAD **UNIDAD NACIONAL DE ACOPIO DE INDICIOS E EVIDENCIAS DE LA POLICÍA NACIONAL**	
	Dr. Carlos Bedón Ortega Msc. DIRECTOR NACIONAL DE AUDITORÍA FORENSE E INFORMÁTICA **CONTRALORÍA GENERAL DEL ESTADO**	

Nota: Las funcionarias: **Carla Cohen**, Especialista en Investigación en Entornos Virtuales y **Agostina Miquelarena**, Experta Internacional en Criptoactivos y Blockchain del Programa Global sobre Cibercrimen de la Oficina de las Naciones Unidas contra la Droga y el Delito – Uruguay,

participaron en calidad de revisoras del presente instrumento, sin embargo, no cuentan con firma electrónica para la suscripción del mismo.

VALIDACIÓN. - El presente instrumento fue validado por los miembros del CODECO, mediante Acta de Validación Única.

APROBACIÓN. - La aprobación del presente instrumento se efectúa a través de la Resolución emitida por el Comité Directivo del Órgano de Gobierno del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forense.

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de creación y/o actualización
2.0	***Segunda*** **Versión: "***Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital***"**	
	Se modificó el acápite 5. Lineamientos con los siguientes cambios: • Se modifico el 5.1. Lineamientos técnicos • Se modifico el 5.2. Lineamientos metodológicos Y se integraron los siguientes numerales: • 5.3. Características de la Evidencia Digital • 5.4. Principios de admisibilidad jurídica • 5.5. Principios de la cadena de custodia • 5.6. Clasificación general de las fuentes de evidencia digital • 5.7. Niveles de Gestión • 5.8. Actores • 5.9. Acciones Según el Nivel de Gestión Se modificó el acápite 6. Contenido del Manual. Se modificó el acápite 8.1 Formulario Único de Cadena de Custodia	

ÍNDICE DE CONTENIDO

1. Información Básica 9
2. Marco Legal 9
3. Glosario de Términos y Abreviaturas 42
4. Alcance 47
5. Lineamientos 47
5.1. Lineamientos Técnicos 47
5.2. Lineamientos metodológicos 50
5.3. Características de la Evidencia Digital 51
5.4. Principios de admisibilidad jurídica 51
5.5. Principios de la cadena de custodia 51
5.7. Niveles de Gestión 54
5.8. Actores 54
5.9. Acciones Según el Nivel de Gestión 55
5.9.1. Primera Fase: Asegurar y proteger el lugar de los hechos 55
5.9.2. Segunda Fase: Procesamiento de la escena 56
5.9.3. Tercera Fase: Procesamiento de evidencia digital en laboratorio 57
6. Contenido del Manual 57
6.1. Metodología para el tratamiento de Evidencia Digital 57
6.1.1. Identificación 57
6.1.2. Recolección 58
6.1.2.1. Recolección de Dispositivos Electrónicos a Nivel Físico 58
6.1.2.2. Recolección y Preservación de Contenido Digital (Elementos Lógicos) 60
6.1.3. Adquisición 60
6.1.3.1. Métodos de adquisición: 60
6.1.3.2. Adquisición *In Situ* 62

6.1.3.3. Adquisición en Laboratorio 65

6.1.4. Análisis 71

6.1.5. Presentación de Resultados 73

6.1.5.1. Consideraciones para la presentación del informe pericial 75

6.1.6. Disposición Final 76

8. Anexos 79

8.1 Formulario Único de Cadena de Custodia 79

1. Información Básica

Nombre del Documento:	Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital.
Código del Documento:	CSEIIMLCF-MLCF-MAN-2026-001
Macroproceso al que pertenece:	Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses.
Responsables de la ejecución:	Entidades que componen el sistema especializado integral de investigación medicina legal y ciencias forenses.
Ejecutor:	Servidores de las áreas responsables de los procesos correspondientes a las entidades que integran el Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, así como servidores públicos o particulares que, por disposición legal o requerimiento de autoridad competente, deban preservar, asegurar, entregar o proteger contenido digital relacionado con una investigación penal.
Objetivo:	Establecer un marco integral que permita a todos los actores involucrados en casos con contenido digital, mediante la estandarización de los procesos de identificación, recolección, preservación, adquisición, análisis y presentación de resultados, actuar ante la autoridad competente con pleno respeto al debido proceso, la cadena de custodia, la legalidad, la integridad, la autenticidad y la utilidad probatoria de la evidencia digital, como apoyo técnico-científico a la investigación penal dirigida por la Fiscalía General del Estado.

2. Marco Legal

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
76	*"En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes*

	garantías básicas: *1. Corresponde a toda autoridad administrativa o judicial, garantizar el cumplimiento de las normas y los derechos de las partes. (…)* *4. Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria. (…)* *7. El derecho de las personas a la defensa incluirá las siguientes garantías: (…)* *b) Contar con el tiempo y con los medios adecuados para la preparación de su defensa. (…)* *i) Nadie podrá ser juzgado más de una vez por la misma causa y materia. Los casos resueltos por la jurisdicción indígena deberán ser considerados para este efecto".*
163	*"Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atenderla seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional.* *Los miembros de la Policía Nacional tendrán una formación basada en derechos humanos, investigación especializada, prevención, control y prevención del delito y utilización de medios de disuasión y conciliación como alternativas al uso de la fuerza.* *Para el desarrollo de sus tareas la Policía Nacional coordinará sus funciones con los diferentes niveles de gobiernos autónomos descentralizados (…)".*
169	*"El sistema procesal es un medio para la realización de la justicia. Las normas procesales consagrarán los principios de simplificación, uniformidad, eficacia, inmediación, celeridad y economía procesal, y harán efectivas las garantías del debido proceso. No se sacrificará la justicia por la sola omisión de formalidades."*
195	*"La Fiscalía dirigirá, de oficio o a petición de parte, la investigación preprocesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la*

	sustanciación del juicio penal. *Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial; dirigirá el sistema de protección y asistencia a víctimas, testigos y participantes en el proceso penal; y, cumplirá con las demás atribuciones establecidas en la ley.".*

CÓDIGO ORGÁNICO INTEGRAL PENAL	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
234.4	*"**Definiciones. -*** *a. Contenido digital. - El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.* *b. Datos de tráfico. - Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.* *c. Proveedor de servicios. - Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.* *d. Sistema informático. - Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital."*

442	*"**Fiscalía.** - La Fiscalía dirige la investigación preprocesal y procesal penal e interviene hasta la finalización del proceso. La víctima deberá ser instruida por parte de la o el fiscal sobre sus derechos y en especial, sobre su intervención en la causa".*
443	*"**Atribuciones de la Fiscalía. -** La Fiscalía ejerce las siguientes atribuciones:* *1. Organizar y dirigir el Sistema especializado integral de investigación, de medicina legal y ciencias forenses (…)".*
444	*"**Atribuciones de la o el fiscal. –** Son atribuciones de la o el fiscal, las siguientes:* *2. Reconocer los lugares, huellas, señales, armas, objetos e instrumentos con la intervención del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses o personal competente en materia de tránsito, conforme con lo dispuesto en este Código.* *4. Disponer al personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses o al personal competente en materia de tránsito, la práctica de diligencias tendientes al esclarecimiento del hecho, salvo la recepción de la versión del sospechoso.* *12. Ordenar el peritaje integral de todos los indicios que hayan sido levantados en la escena del hecho, garantizando la preservación y correcto manejo de las evidencias.* *16. El fiscal dispondrá en el tiempo máximo de tres meses el destino final de los indicios, artefactos, vehículos u otros objetos que sean ingresados en los centros de acopio o almacenamiento temporal, que no sean de interés pericial.* *En caso de indicios y evidencias de interés pericial, previo informe justificativo y detalle del o los peritajes cumplidos, el fiscal deberá pronunciarse en cuanto a su disposición final en un término no mayor a un año..."* *17. Para realizar los allanamientos, el fiscal solicitará al juez la orden para la preservación de la evidencia digital de los dispositivos de interés para la investigación o el proceso que se encuentren en la escena, los cuales se guardarán con cadena de custodia (…)".*

448	*"**Organización y dirección. -** En materia preprocesal y procesal penal, la Fiscalía organizará y dirigirá el Sistema especializado integral de investigación, de medicina legal y ciencias forenses que prestará servicios especializados de apoyo técnico y científico a la administración de justicia.* *El Sistema contará con el apoyo del organismo especializado de la Policía Nacional y personal civil de investigación, quienes llevarán a cabo las diligencias necesarias para cumplir los fines previstos en este Código, ejecutarán sus tareas bajo la dirección de la Fiscalía y dependerán administrativamente del ministerio del ramo".*
449	*"**Atribuciones. -** Son atribuciones del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses: (…)* *6. Vigilar, resguardar, proteger y preservar el lugar donde presuntamente se comete la infracción y recoger los resultados, huellas, señales, armas, objetos, instrumentos y demás vestigios. (…)* *8. Cumplir de acuerdo con los plazos señalados, las disposiciones para la práctica de diligencias investigativas de la o el fiscal.* *9. Cumplir las órdenes que les imparta la o el fiscal o la o el juzgador. (…)* *12. Solicitar a la o al fiscal la autorización judicial para la práctica de diligencias investigativas.* *Sobre las diligencias investigativas y sus resultados, se presentará un informe a la o al fiscal, dentro de los plazos señalados.* *En aquellos lugares donde no exista personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses, en el ámbito de la justicia penal, los servidores o servidoras de la Policía Nacional tendrán las atribuciones señaladas en este artículo.".*
453	*"**Finalidad**. - La prueba tiene por finalidad llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada".*
454	*"**Principios**. - El anuncio y práctica de la prueba se regirá por los siguientes*

	principios: *1. Oportunidad. - Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio. Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria 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 oral de juicio. Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de 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 penal 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 preacordadas. 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 prueba.* *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".
455	*"**Nexo causal. -** 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	*"**Cadena de custodia. -** 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.* *La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación".*
457	*"**Criterios de valoración. -** 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.* *En el caso de delito de desaparición involuntaria, la acumulación de indicios servirá de nexo causal vinculante siempre y cuando dichos indicios se relacionen con el hecho o circunstancia a probar y sean inequívocos respecto del hecho o circunstancia controvertida".*
458	*"**Preservación de la escena del hecho o indicios. -** La o el servidor público que intervenga o tome contacto con la escena del hecho e indicios será la responsable*

	de su preservación, hasta contar con la presencia del personal especializado. *Igual obligación tienen los particulares que por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo".*
459	*"**Actuaciones**. - Las actuaciones de investigación se sujetarán a las siguientes reglas:* *(…) 2. Las diligencias de reconocimiento constarán en actas e informes periciales.* *3. Las diligencias de investigación deberán ser registradas en medios tecnológicos y documentales más adecuados para preservar la realización de la misma y formarán parte del expediente fiscal.* *4. El registro que conste en el expediente fiscal deberá ser suficiente para determinar todos los elementos de convicción que puedan fundamentar la formulación de cargos o la acusación".*
460	*"**Reconocimiento del lugar de los hechos. -** La o el fiscal con el apoyo del personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, o el personal competente en materia de tránsito, cuando sea relevante para la investigación, reconocerá el lugar de los hechos de conformidad con las siguientes disposiciones: (…)* *5. La fijación y recolección de las evidencias, huellas, vestigios encontrados en el lugar ingresarán en cadena de custodia para la investigación a cargo de la o el fiscal, quien dispondrá las diligencias pertinentes. (…)* *8. Se realizarán diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos".*
470	*"**Comunicaciones personales. -** No podrán grabar o registrar por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido y autorizado dicha grabación o registro, salvo los casos expresamente señalados en la ley.* *La información obtenida ilegalmente carece de todo valor jurídico. Los riesgos, daños y perjuicios que genere para las personas involucradas, serán imputables a*

	quien forzó la revelación de la información, quedando obligada a efectuar la reparación integral de los daños".
471	*"**Registros relacionados con un hecho constitutivo de infracción.-** No requieren autorización judicial las grabaciones de audio, imágenes de video o fotografía relacionadas a un hecho constitutivo de infracción, registradas de modo espontáneo al momento mismo de su ejecución, por cámaras de vigilancia o seguridad, por cualquier medio tecnológico, obtenidos a través de dispositivos de dotación de las servidoras y servidores de las entidades de seguridad ciudadana y orden público o de las Fuerzas Armadas, por particulares en lugares públicos y de libre circulación, por los medios de comunicación social o en los casos en que se divulguen grabaciones de audio o video obtenidas por uno de los intervinientes, en cuyo caso se requerirá la preservación de la integralidad del registro de datos para que la grabación tenga valor probatorio.* *En estos casos, las grabaciones se pondrán inmediatamente a órdenes de la o el fiscal en soporte original y servirán para incorporar a la investigación e introducirlas al proceso y de ser necesario, la o el fiscal dispondrá la transcripción de la parte pertinente o su reproducción en la audiencia de juicio".*
472	*"**Información de circulación restringida**. - No podrá circular libremente la siguiente información:* *1. Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley.* *2. La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por la o el juzgador.* *3. La información producida por la o el fiscal en el marco de una investigación previa y aquella originada en la orden judicial relacionada con las técnicas especiales de investigación.* *4. La información acerca de niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código Orgánico de la Niñez y Adolescencia y la Constitución.*

	5. La información calificada por los organismos que conforman el Sistema nacional de inteligencia".
475	*"**Retención de correspondencia.** - La retención, apertura y examen de la correspondencia y otros documentos se regirá por las siguientes disposiciones:* *1. La correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código.* *2. La o el juzgador podrá autorizar a la o al fiscal, previa solicitud motivada, el retener, abrir y examinar la correspondencia, cuando haya suficiente evidencia para presumir que la misma tiene alguna información útil para la investigación.* *3. Para proceder a la apertura y examen de la correspondencia y otros documentos que puedan tener relación con los hechos y circunstancias de la infracción y sus participantes, se notificará previamente al interesado y con su concurrencia o no, se leerá la correspondencia o el documento en forma reservada, informando del particular a la víctima y al procesado o su defensor público o privado. A falta de los sujetos procesales la diligencia se hará ante dos testigos. Todos los intervinientes jurarán guardar reserva.* *4. Si la correspondencia u otros documentos están relacionados con la infracción que se investiga, se los agregará al expediente fiscal después de rubricados; caso contrario, se los devolverá al lugar de donde son tomados o al interesado.* *5. Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará el desciframiento por peritos en criptografía o su traducción (…)".*
476	*"**Interceptación de las comunicaciones o datos informáticos**. - La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal, cuando existan indicios que resulten relevantes a los fines de la investigación y la medida sea idónea, necesaria y proporcional, de conformidad con las siguientes reglas:* *1. La o el juzgador determinará la comunicación interceptada y el tiempo de intercepción, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga*

	hasta por un plazo de noventa días. Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses. *2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen.* *3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código.* *4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes.* *5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a preservar el secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones.* *6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa.* *Toda información que no resulte útil o relevante a los fines de la investigación será eliminada de oficio por parte del fiscal y se remitirá el acta que deje constancia de este hecho a fin registrarlo en el expediente respectivo. La destrucción de la información se realizará bajo la supervisión del juez competente, el cual podrá ordenar la eliminación de la información que no haya sido considerada relevante o*

	útil para probar la materialidad o responsabilidad de una infracción. *7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio.* *8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio.* *9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros".*
477	*"**Reconocimiento de grabaciones. -** La o el juzgador autorizará a la o al fiscal el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento.* *La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos".*
477.1	*"**Aseguramiento de datos. -*** *Para el aseguramiento de datos se observará las siguientes reglas:* *1. El fiscal a cargo de la investigación, sin necesidad de autorización judicial, podrá ordenar a una o varias personas naturales o jurídicas la conservación expedita de datos informáticos específicos, incluidos los datos de abonado y de tráfico, que hayan sido almacenados mediante un sistema informático o en un dispositivo de almacenamiento informático, en particular cuando haya motivos para sospechar*

	que los datos informáticos son especialmente vulnerables a la pérdida o a la modificación. La orden deberá establecer la obligación de preservar y mantener la integridad de los datos informáticos durante el tiempo necesario hasta un máximo de noventa días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden. De la misma manera y en virtud del principio de celeridad, esta conservación podrá ser solicitada por la Policía Nacional en delito flagrante, cuando medie una investigación previa, instrucción fiscal, actuaciones fiscales urgentes, actos administrativos e investigación de noticias de personas desaparecidas; en este caso se notificará a la Fiscalía en el plazo máximo de ocho horas posteriores a la solicitud. *2. La persona natural o jurídica procurará los medios necesarios para preservar de inmediato los datos en cuestión y queda obligada a mantener la confidencialidad de la orden recibida durante el tiempo que dure la medida, bajo el apercibimiento de incurrir en responsabilidad penal.* *3. El proveedor de servicios de una comunicación que haya recibido la orden o solicitud de preservación de datos relativos al tráfico de una comunicación informará de inmediato a la autoridad que emitió la orden o solicitud cuando advierta que la comunicación bajo investigación ha sido efectuada con la participación de otros proveedores de servicios a fin de que se puedan arbitrar las medidas necesarias para solicitar a dichos proveedores la conservación de los datos".*
477.2	*"**Orden de presentación. -** El juez, a pedido del fiscal, podrá ordenar a cualquier persona natural o jurídica con domicilio en el territorio nacional o que ofrezca sus servicios en el territorio nacional, que presente, remita o entregue datos de contenido alojados en un sistema informático o en un dispositivo de almacenamiento de datos informáticos que esté bajo su poder o control y que se vinculen con la investigación de un delito concreto. La orden podrá contener la indicación de que la medida deberá mantenerse con confidencialidad bajo el apercibimiento de sanción penal.* *El fiscal, sin autorización del juez, podrá ordenar a cualquier persona natural o jurídica con domicilio en el territorio nacional o que ofrezca sus servicios en el territorio nacional, que presente, remita o entregue datos de abonado y de tráfico*

	alojados en un sistema informático o en un dispositivo de almacenamiento de datos informáticos que esté bajo su poder o control y que se vinculen con la investigación de un delito concreto. La orden podrá contener la indicación de que la medida deberá mantenerse con confidencialidad bajo el apercibimiento de sanción penal".
477.3	*"**Búsqueda, registro, acceso y secuestro de datos informáticos. -*** *El juez podrá ordenar a requerimiento del fiscal, la búsqueda, registro, acceso de un sistema informático o de una parte de éste, de los datos informáticos almacenados en él o de un medio de almacenamiento de datos informáticos o electrónicos. Podrá, además, disponer:* *1. Incautar y secuestrar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura;* *2. Hacer u obtener copia íntegra de los datos en cualquier medio de almacenamiento o autónomo disponible; y,* *3. Acciones que permitan hacer inaccesibles los datos informáticos o eliminar los mismos.* *La orden del juez podrá extenderse o ampliarse a otros sistemas que contengan los datos buscados o se encuentren almacenados en otro u otros dispositivos a los que se tenga acceso lícito desde el dispositivo o sistema inicial.* *Regirán en cuanto sean aplicables las normas generales y las mismas limitaciones dispuestas para el secuestro de documentos y correspondencia epistolar".*
477.4	*"**Cooperación internacional**. - Las autoridades nacionales competentes cooperarán con las autoridades extranjeras competentes en las investigaciones o procedimientos en caso de delitos relacionados con las tecnologías de la información y comunicación, así como para la obtención o tratamiento de evidencia digital; o requerir esta información a las autoridades extranjeras, de conformidad con los instrumentos internacionales suscritos por el Ecuador y la ley".*

477.5	*"**Reglas para la preservación y divulgación expedita de contenido digital en la cooperación internacional. -** Las autoridades nacionales competentes están obligadas a preservar y divulgar, de manera expedita, el contenido digital cuando así sea requerido por una autoridad extranjera, de conformidad con los instrumentos internacionales suscritos por el Ecuador y la ley, para lo cual se observarán las siguientes reglas:* *1. La solicitud de preservación de contenido digital almacenado en un sistema informático ubicado en el territorio nacional se realizará por cualquier vía expedita de comunicación entre la parte requirente y la parte requerida.* *2. La divulgación del contenido digital almacenado en un sistema informático ubicado en el territorio nacional, se realizará previa solicitud de asistencia penal internacional.* *3. En la ejecución de una solicitud internacional de preservación de contenido digital, la autoridad competente dará la respectiva orden a quién tenga el control o disponibilidad de este contenido, incluido el o los proveedores y prestadores de servicios.* *4. En la ejecución de una solicitud de asistencia penal internacional de divulgación de contenido digital, la autoridad judicial competente dará la respectiva orden a quién tenga el control o disponibilidad de este contenido, incluido el o los proveedores y prestadores de servicios.* *5. La orden de preservación especificará: a) La naturaleza del contenido digital; y, b) El tiempo de preservación del contenido digital que podrá ser hasta un máximo de noventa días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden.* *6. En cumplimiento de la orden de preservación, quien tenga el control o la disponibilidad del contenido digital preservará, de inmediato, el contenido digital por el período especificado, protegiendo y conservando su integridad. Esta regla es aplicable a los proveedores o prestadores de servicios u otros.* *7. El contenido digital preservado y divulgado en virtud del presente artículo se concederá únicamente a:*

	a) La o el fiscal a cargo, en la ejecución de la solicitud de asistencia penal internacional con fines de divulgación de contenido digital. *b) La autoridad nacional que emitió la orden de preservación, en las mismas condiciones que podrían realizarse en un caso similar nacional.* *Estas reglas serán aplicadas, según corresponda, a las peticiones formuladas por las autoridades del Ecuador cuando actúen como requirentes.".*
477.6	*"**Motivos de denegación. -** La solicitud de preservación o divulgación expedita de contenido digital será denegada cuando:* *1. El contenido digital se refiera a un delito político o delito conexo, de conformidad con la legislación ecuatoriana.* *2. Atente contra la soberanía, seguridad, orden público u otros intereses del Ecuador.* *La solicitud de preservación y divulgación expedita de contenido digital podrá ser denegada si existieren motivos razonables para creer que la ejecución de la solicitud será rechazada por falta de comprobación del principio non bis in idem.".*
477.7	*"**Búsqueda, registro, acceso y secuestro de contenido digital en cooperación internacional.-** En ejecución de una solicitud de autoridad extranjera competente, la autoridad judicial nacional podrá disponer la búsqueda, el registro, el acceso o secuestro del contenido digital, así como, la divulgación de contenido almacenado en un sistema informático ubicado en el Ecuador, cuando se trate de una situación en que el registro y/o secuestro son admisibles en un caso nacional de características similares.* *La autoridad judicial competente actuará tan pronto como sea posible, cuando existieran razones para creer que el contenido digital es especialmente vulnerable a su pérdida o modificación, o cuando la cooperación expedita esté prevista en un instrumento internacional aplicable.* *Estas disposiciones serán aplicadas, según corresponda, a las peticiones formuladas por las autoridades del Ecuador cuando actúen como requirentes".*

477.8	*"**Acceso transfronterizo a contenido digital de acceso público o con consentimiento. -** Las autoridades extranjeras competentes, sin previa petición a las autoridades del Ecuador, podrán:* *1. Acceder a contenido digital almacenado en un sistema informático ubicado en el Ecuador, cuando este esté a disposición del público; y,* *2. Recibir o acceder, por medio de un sistema informático ubicado en su territorio, a contenido digital almacenado en el Ecuador, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos".*
477.9	*"**Punto permanente de contacto para la cooperación internacional. -** Con fines de cooperación internacional, el Ecuador mantendrá una estructura que garantice un punto de contacto disponible en todo momento, las veinticuatro horas del día, los siete días de la semana.* *El punto de contacto podrá ser contactado por otros puntos de contacto, con arreglo a los acuerdos, tratados o convenios a los cuales el Ecuador está obligado, o en ejecución de protocolos de cooperación internacional con organismos judiciales o policiales.* *La asistencia inmediata que ofrece este punto de contacto permanente incluye:* *1. La prestación de asesoramiento técnico a otros puntos de contacto;* *2. La preservación expedita de contenido digital en casos de urgencia o peligro en el retraso, en conformidad con este Código;* *3. La recopilación de evidencia digital en casos de urgencia o de peligro en el retraso;* *4. La localización de sospechosos y el suministro de información de carácter jurídico en casos de urgencia o de peligro en el retraso; y,* *5. La transmisión inmediata a la autoridad judicial competente de las solicitudes referentes a medidas de la competencia, en vista de su pronta ejecución".*
477.10	*"**Interceptación de las comunicaciones en la cooperación internacional.-** En ejecución de una petición de una autoridad extranjera competente, puede ser*

	ordenada la intercepción de transmisiones de datos informáticos realizadas por medio de un sistema informático ubicado en el Ecuador, sí así se prevé en acuerdo, tratado o convenio internacional y si se trata de situación en las que dicha interceptación está permitida en un caso nacional de características similares, respetándose el procedimiento y observándose los límites y garantías del artículo 476 del Código Orgánico Integral Penal".
478	*"**Registros**. - Los registros se realizarán de acuerdo con las siguientes reglas:* *1. Los registros de personas u objetos e incautación de los elementos relacionados con una infracción que se encuentren en viviendas u otros lugares, requerirán autorización de la persona afectada o de orden judicial. En este último caso deberá ser motivada y limitada únicamente a lo señalado de forma taxativa en la misma y realizado en el lugar autorizado.* *2. El consentimiento libremente otorgado por la persona requerida para registrar un espacio determinado, permitirá realizar el registro e incautación de los elementos relacionados con una infracción. Únicamente podrán prestar el consentimiento personas capaces y mayores de edad. Se deberá informar a la persona investigada sobre su derecho a no permitir el registro sin autorización judicial".*
483	*"**Operaciones encubiertas.-** En el curso de las investigaciones de manera excepcional, bajo la dirección de la unidad especializada de la Fiscalía, se podrá planificar y ejecutar con el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, una operación encubierta y autorizar a sus agentes para involucrarse o introducirse en organizaciones o agrupaciones delictuales ocultando su identidad oficial, con el objetivo de identificar a los participantes, reunir y recoger información, elementos de convicción y evidencia útil para los fines de la investigación.* *El agente encubierto estará exento de responsabilidad penal o civil por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma, caso contrario será sancionado de conformidad con las normas jurídicas pertinentes".*

483.1	*"**Agente encubierto informático.-** La o el fiscal podrá autorizar al personal del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses, realizar tareas de gestión investigativas ocultando su verdadera identidad, asumiendo identidad supuesta, para lo cual deberán realizar patrullajes o acciones digitales en el ciberespacio, penetrándose e infiltrándose en plataformas informáticas como foros, grupos de comunicación o fuentes cerradas de información o comunicación, con la finalidad de hacer seguimiento de personas, vigilar cosas, realizar compras controladas y/o descubrir, investigar o esclarecer hechos delictivos cometidos o que puedan cometerse con el uso o en contra de las tecnologías de la información y comunicación, esto es ciberdelitos puros o replicas o cualquier otro tipo de delito.* *En el desarrollo de sus actividades, podrá intercambiar, enviar de manera directa archivos, ficheros con contenido ilícito o aplicar técnicas para preservar y descifrar información recolectada que sea útil para la investigación. Además, podrá obtener imágenes y realizar grabaciones en audio o video, de las conversaciones que podría llegar a mantener con el o los investigados, dependiendo de la naturaleza y modus operandi de la organización, con la utilización de cualquier medio tecnológico, en cualquier lugar, para lo cual el fiscal previamente obtendrá la respectiva autorización judicial.* *Para el desarrollo de estas actividades, el agente encubierto informático observará además las reglas del siguiente artículo".*
484	*"**Reglas. - Las operaciones encubiertas deberán observar las siguientes reglas:*** *1. La operación encubierta será dirigida por la unidad especializada de la Fiscalía. Podrá solicitarse por el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, entregando a la o al fiscal los antecedentes necesarios que la justifiquen.* *2. La autorización de la o el fiscal deberá ser fundamentada y responderá al principio de necesidad para la investigación, se deberá imponer limitaciones de tiempo y controles que sean de utilidad para un adecuado respeto a los derechos de las personas investigadas o procesadas.* *3. No será permitido al agente encubierto, persona jurídica encubierta y agente*

	encubierto virtual impulsar delitos que no sean de iniciativa de los investigados, salvo en el caso de compras controladas, para lo cual el fiscal tendrá la facultad de definir la proporcionalidad y cantidad de la sustancia o bien a adquirir. *4. La identidad otorgada al agente encubierto, persona jurídica encubierta y agente virtual encubierto será mantenida hasta después de la audiencia de juicio en el proceso. La autorización para utilizar la identidad no podrá extenderse por un período superior a dos años, prorrogable por dos años más mediante debida justificación. El agente encubierto y el agente encubierto informático podrá desarrollar compras controladas de sustancias catalogadas a fiscalización; dentro de un proceso investigativo el fiscal a través del sistema especializado de investigación podrá disponer la práctica de compras controladas de sustancias catalogadas sujetas a fiscalización, a persona o personas que oferten estas sustancias. (…)* *6. Las versiones del agente encubierto servirán como elementos de convicción dentro de la investigación (…)".*
484.1	*"**Compras controladas de sustancias catalogadas sujetas a fiscalización, flora y fauna silvestre, falsificación de moneda, falsificación de medicamentos u otros a consideración del agente fiscal.*** *Dentro de un proceso investigativo el fiscal a través del sistema especializado de investigación, podrá disponer la práctica de compras controladas, a persona o personas que oferten el objeto ilícito, con el fin de conocer, personas, lugares, modos de operación, de estos objetos. Estas prácticas podrán ser desarrolladas únicamente por un agente encubierto o agente encubierto virtual, debidamente delegado y en el marco de una investigación. Los dineros u otros instrumentos utilizados para este fin gozarán de legalidad, podrán también ser, marcados y/o señalados para el beneficio de la investigación".*
497	*"**Asistencia judicial recíproca. -** Las o los fiscales podrán solicitar asistencia directa a sus similares u órganos policiales extranjeros para la práctica de diligencias procesales, pericias e investigación de los delitos previstos en este Código. Esta asistencia se refiere entre otros hechos, a la detención y remisión de procesados y acusados, recepción de testimonios, exhibición de documentos inclusive bancarios,*

	recuperación de contenido digital, inspecciones del lugar, envío de elementos probatorios, identificación y análisis de sustancias catalogadas sujetas a fiscalización e incautación y comiso de bienes. *Asimismo, la o el fiscal podrá efectuar actuaciones en el extranjero dirigidas a recoger antecedentes acerca de hechos constitutivos de alguna infracción, a través de la asistencia penal internacional.* *Las diligencias señaladas serán incorporadas al proceso, presentadas y valoradas en la etapa del juicio."*
499	*"**Reglas generales. -** La prueba documental se regirá por las siguientes reglas: (…)* *6. Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código (…)".*
500	*"**Contenido digital.** - El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.* *En la investigación se seguirán las siguientes reglas:* *1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.* *2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.* *3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.*

	4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto".
511	*"**Reglas generales. -** Las y los peritos deberán:* *1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.* *2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.* *3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.* *4. Las o los peritos no podrán ser recusados, sin embargo, el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.* *5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.* *6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.* *7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.* *8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por estas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.* *De no existir persona acreditada como perito en determinadas áreas, se deberá*

	contar con quien tenga conocimiento, especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje. Para los casos de mala práctica profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organismo rector de la materia. *Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados como prueba, a través de testimonios anticipados o podrán ser receptados mediante video conferencias de acuerdo a las reglas del presente Código".*
560	*"**Oralidad. -** El Sistema procesal penal se fundamenta en el principio de oralidad que se desarrolla en las audiencias previstas en este Código. Deberán constar o reducir a escrito:* *1. La denuncia y la acusación particular.* *2. Las constancias de las actuaciones investigativas, los partes o informes policiales, informes periciales, las versiones, testimonios anticipados, testimonios con juramento y actas de otras diligencias.* *3. Las actas de audiencias.* *4. Los autos definitivos siempre que no se dicten en audiencias y las sentencias.* *5. Interposición de recursos".*
616	*"**Exhibición de documentos físicos u objetos. -** Los documentos u objetos que pretendan ser incorporados como prueba, serán leídos en su parte relevante o exhibidos según corresponda, siempre que estén directa e inmediatamente relacionadas con la materia del juzgamiento, previa acreditación por quien lo presenta, quien deberá dar cuenta de su origen.* *Las partes procesales podrán solicitar la lectura parcial o resumida de los documentos físicos, cuando sea conveniente y se asegure el conocimiento de su contenido".*
616.1	*"**Reglas para la exhibición de contenido digital. -** El contenido digital que pretenda ser incorporado como prueba digital seguirá las siguientes reglas:*

	1. El contenido digital debe estar almacenado en cualquier elemento óptico o sistemas de almacenamiento como discos, cintas, memoria extraíble, entre otros. *2. El contenido digital será exhibido y/o reproducido en su formato original por cualquier medio tecnológico que lo permita, previa acreditación de quien lo presenta a través del testimonio de la o el perito correspondiente, quien dará cuenta de la cadena de custodia, integridad y autenticidad conforme a las técnicas digitales forenses.* *El contenido digital que haya sido obtenido mediante Asistencia Penal Internacional ingresará al Centro de Acopio del Sistema Nacional de Investigación Integral, Medicina Legal y Ciencias Forenses o el que haga sus veces, para el sometimiento a las respectivas pericias de ser necesario; y, en la etapa de juicio serán presentadas conforme a las reglas del presente artículo. En todo momento se garantizará la cadena de custodia".*
Disposición General Primera	*"En lo no previsto en este Código se deberá aplicar lo establecido en el Código Orgánico de la Función Judicial y el Código Orgánico General de Procesos, si es aplicable con la naturaleza del proceso penal acusatorio oral."*

CÓDIGO ORGÁNICO DE LAS ENTIDADES DE SEGURIDAD CIUDADANA Y ORDEN PÚBLICO - COESCOP	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
60	*"**Misión. -** Tiene como misión la protección interna, la seguridad ciudadana, el mantenimiento del orden público y, dentro del ámbito de su competencia, el apoyo a la administración de justicia en el marco del respeto y protección del libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional, a través de los subsistemas de prevención, investigación de la infracción e inteligencia antidelincuencial".*
61	*"**Funciones. -** La Policía Nacional tiene las siguientes funciones: (…)* *12. Garantizar la cadena de custodia, vestigios y los elementos materiales de la*

	infracción en la escena del delito; (…)".
70	*"**Investigación preprocesal y procesal penal**. - Las actividades que desarrolle la Policía Nacional, a través de los subsistemas relacionadas con la investigación preprocesal y procesal penal, estarán bajo la dirección de Fiscalía General del Estado, en el marco del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses".*
77	*"**Componente de Investigación de la Infracción. -** El componente de la investigación de la infracción es la unidad que se encarga de coordinar las acciones para la implementación de la política pública y planificación estratégica institucional en el ámbito de la investigación operativa de la infracción. Realiza la investigación técnica y científica de la infracción, bajo los lineamientos y la coordinación del Servicio Nacional de Investigación, Medicina Legal y Ciencias Forenses.* *Es responsable del registro, análisis y control de la información relacionada con la identificación biométrica y balística a nivel nacional.* *En el cumplimiento de sus funciones, dispondrá de equipos multidisciplinarios conformados por servidoras y servidores policiales especializados en investigación, medicina legal y ciencias forenses".*
136	*"**Naturaleza. -** El Sistema es el conjunto articulado y coordinado de subsistemas, instituciones, políticas, normas, programas y servicios de investigación, de medicina legal y ciencias forenses, creado para apoyar a la administración de justicia.* *Su funcionamiento se implementa a través de los siguientes subsistemas:* *1. Subsistema responsable de la investigación operativa de los delitos de ejercicio público de la acción; y,* *2. Subsistema responsable de la investigación técnica y científica en materia de medicina legal y ciencias forenses."*
142	*"**Entidades Operativas. -** En calidad de entidades operativas, el Sistema contará con la participación del ente especializado en investigación operativa del ejercicio público de la acción penal de la Policía Nacional y con el Servicio Nacional de*

	Medicina Legal y Ciencias Forenses".
146	*"**Naturaleza. -** Es un servicio público de carácter civil, técnico y especializado que tiene a su cargo la investigación técnica y científica de la infracción a nivel nacional en materia de medicina legal y ciencias forenses. Prestará apoyo técnico y científico a los órganos de la administración de justicia.* *Estará adscrito al ministerio rector de orden público, protección interna y seguridad ciudadana. Tendrá personalidad jurídica y autonomía administrativa, financiera y de gestión. En materia pre procesal y procesal penal actuará bajo la dirección de la Fiscalía General del Estado".*
149	*"**Funciones del Servicio. -** El Servicio tiene las siguientes funciones:* *1. Gestionar la investigación técnica y científica pre procesal y procesal penal en materia de medicina legal y ciencias forenses bajo la instrucción de la Fiscalía General del Estado;* *2. Realizar las actividades técnico-periciales bajo los procedimientos estandarizados, reglamentos, manuales y protocolos técnicos y científicos nacionales e internacionales y demás normativa emitida por el Comité Directivo;* *3. Prestar servicios especializados y asesoramiento técnico-científico a la administración de justicia, de conformidad con las normas legales de la actividad pericial y administrativa;* *4. Mantener actualizada la información de la gestión técnica y científica realizada por el Servicio; y,* *5. Las demás que consten en este Código y sus reglamentos, o las que le sean asignadas por el Comité Directivo dentro del ámbito de sus competencias".*
151	*"**Personal. -** El Servicio está integrado por personal civil y servidoras o servidores policiales especializados en la investigación técnica y científica, en materia de medicina legal y ciencias forenses, que, habiendo aprobado los procesos de selección correspondientes, obtienen esta calidad, de conformidad con el plan de carrera".*

163	***"Obligaciones. -*** *Son obligaciones de las y los servidores, a más de las establecidas en la ley que regula el servicio público y la normativa pertinente, las siguientes:* *2. Desempeñar las disposiciones ordenadas por la autoridad judicial el fiscal y juez competentes; (…)* *7. Actuar, interpretar y manejar objetivamente la información obtenida durante la investigación operativa del delito, estudio de campo o estudio pericial, conforme a criterios técnicos, éticos y jurídicos, basados en principios científicos vigentes; y, (…)".*

CÓDIGO ORGÁNICO GENERAL DE PROCESOS	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
202	*"**Documentos digitales.** Los documentos producidos electrónicamente con sus respectivos anexos, serán considerados originales para todos los efectos legales.* *Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original. Los documentos originales escaneados, serán conservados por la o el titular y presentados en la audiencia de juicio o única, o cuando la o el juzgador lo solicite.* *Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código."*
221	*"(…) **Perito.** Perito. Es la persona natural o jurídica que, por razón de sus conocimientos científicos, técnicos, artísticos, prácticos o profesionales está en condiciones de informar a la o al juzgador sobre algún hecho o circunstancia relacionado con la materia de la controversia.* *Aquellas personas debidamente acreditadas por el Consejo de la Judicatura estarán autorizadas para emitir informes periciales, intervenir y declarar en el proceso. En el caso de personas jurídicas, la declaración en el proceso será realizada por el*

	perito acreditado que realice la pericia. *En caso de que no existan expertos acreditados en una materia específica, la o el juzgador solicitará al Consejo de la Judicatura que requiera a la institución pública, universidad o colegio profesional, de acuerdo con la naturaleza de los conocimientos necesarios para la causa, el envío de una terna de profesionales que puedan acreditarse como peritos para ese proceso en particular".*
222	*"(…)* ***Declaración de peritos. -*** *La o el perito será notificado en su dirección electrónica con el señalamiento de día y hora para la audiencia de juicio o única, dentro de la cual sustentará su informe. Su comparecencia es obligatoria.* *En caso de no comparecer por caso fortuito o fuerza mayor, debidamente comprobado y por una sola vez, se suspenderá la audiencia, después de haber practicado las demás pruebas y se determinará el término para su reanudación.* *En caso de inasistencia injustificada, su informe no tendrá eficacia probatoria y perderá su acreditación en el registro del Consejo de la Judicatura.* *En la audiencia las partes podrán interrogarlo bajo juramento, acerca de su idoneidad e imparcialidad y sobre el contenido del informe, siguiendo las normas previstas para los testigos.* *Las partes tendrán derecho, si lo consideran necesario, a interrogar nuevamente al perito, en el orden determinado para el testimonio.* *En ningún caso habrá lugar a procedimiento especial de objeción del informe por error esencial, que únicamente podrá alegarse y probarse en la audiencia.* *Concluido el contrainterrogatorio y si existe divergencia con otro peritaje, la o el juzgador podrá abrir el debate entre peritos de acuerdo con lo previsto en este Código.* *Finalizado el debate entre las o los peritos, la o el juzgador, abrirá un interrogatorio y contrainterrogatorio de las partes, exclusivamente relacionado con las conclusiones divergentes de los informes. La o el juzgador conducirá el debate".*
223	*"****Imparcialidad del perito. -*** *La o el perito desempeñará su labor con objetividad e imparcialidad.*

	Durante la audiencia de juicio o única, podrán dirigirse a la o al perito, preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico o científico de sus conclusiones, así como cualquier otra destinada a solventar o impugnar su credibilidad".
224	*"**Contenido del informe pericial. -** Contenido del informe pericial. Todo informe pericial deberá contener, al menos, los siguientes elementos:* *1. Nombres y apellidos completos, número de cédula de ciudadanía o identidad,* *dirección domiciliaria, número de teléfono, correo electrónico y los demás datos que faciliten la localización del perito.* *2. La profesión, oficio, arte o actividad especial ejercida por quien rinde el informe.* *3. El número de acreditación otorgado por el Consejo de la Judicatura y la declaración de la o del perito de que la misma se encuentra vigente.* *4. La explicación de los hechos u objetos sometidos a análisis.* *5. El detalle de los exámenes, métodos, prácticas e investigaciones a las cuales ha sometido dichos hechos u objetos.* *6. Los razonamientos y deducciones efectuadas para llegar a las conclusiones que presenta ante la o el juzgador.* *Las conclusiones deben ser claras, únicas y precisas".*
225	*"**Solicitud de pericia. -** Solicitud de pericia. Cuando alguna de las partes justifique no tener acceso al objeto de la pericia, solicitará en la demanda o contestación, reconvención o contestación a la reconvención, que la o el juzgador ordene su práctica y designe el perito correspondiente. El informe pericial será notificado a las partes con el término de por lo menos diez días antes de la audiencia, término que podrá ser ampliado a criterio de la o del juzgador y de acuerdo con la complejidad del informe".*
227	*"**Finalidad y contenido de la prueba pericial.** La prueba pericial tiene como propósito que expertos debidamente acreditados puedan verificar los hechos y*

	objetos que son materia del proceso. (…)".

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
2	*"**Ámbito de aplicación material**. - La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a: (…)* *f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y (…)".*
18	*"**Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad**. - Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, en los siguientes casos: (…)* *6) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas; (…)".*

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 2002-67)	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
2	*"**Reconocimiento jurídico de los mensajes de datos.** - Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento".*
52	*"**Medios de prueba.** - Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código Orgánico General de Procesos".*
53	*"**Presunción.** - Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la Ley, y que, por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario".*

REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL (RESOLUCIÓN No. 216-2024)	
ARTÍCULO	**DETALLE DEL ARTÍCULO**
25	*"**Obligaciones generales. -** Las y los peritos calificados se desempeñarán como auxiliares de la justicia con objetividad, imparcialidad, independencia, responsabilidad, oportunidad, puntualidad, rectitud, veracidad, corrección, confidencialidad y honestidad. Su experticia deberá enmarcarse en todo momento en la ética, con la presentación de su criterio técnico y especializado.* *La obligación de la o el perito es única e integral y comprende las siguientes*

	actividades: *a) Cumplir con la designación dispuesta por la autoridad competente;* *b) Presentar el informe verbal y/o escrito;* *c) Presentar aclaraciones, ampliaciones u observaciones al informe;* *d) Defender y/o exponer el informe de manera fundamentada en las audiencias correspondientes; y,* *e) Cualquier otra actividad necesaria, dispuesta por autoridad judicial competente.* *En el caso de las personas jurídicas, tendrán responsabilidad solidaria del cumplimiento de las obligaciones de los peritos vinculados."*
26	*"**Obligaciones específicas. -*** *1. Cumplir la orden de la autoridad competente una vez que han sido designados. En caso de vencimiento de la calificación del perito, luego de la designación, éste tendrá la obligación de presentar ante la autoridad respectiva su informe y cumplir con todos los deberes inherentes a la orden dispuesta. El informe y las actuaciones periciales cumplidas en este supuesto tendrán toda la validez legal y procesal que el caso lo amerite.* *2. Presentar el informe correspondiente oportunamente, en la forma, plazos y términos previstos por la normativa o por la autoridad correspondiente. En caso de dificultad o complejidad en la experticia, tendrá la posibilidad de solicitar fundamentadamente a la autoridad competente, un tiempo adicional al antes establecido de forma excepcional para presentar su informe, con la ampliación o aclaración al mismo.* *3. Presentar el informe correspondiente con los requisitos mínimos establecidos en este reglamento y la ley, subirlo al Sistema Pericial Integral de la Función Judicial suscrito electrónicamente. En el caso de informes de avalúos de bienes, obligatoriamente se subirán también las fotografías de estos.* *4. Las aclaraciones se presentarán de forma verbal y escrita según la normativa que lo establezca, los cuales deberán ser elevados al Sistema Pericial Integral.* *5. Explicar y fundamentar el informe presentado y sus conclusiones en las*

	audiencias respectivas. *6. Presentar conjuntamente con su informe, la factura electrónica de honorarios correspondientes.* *7. Abstenerse de cobrar valores adicionales a los incluidos en la factura presentada, por el informe, cuyo valor será establecido por la autoridad competente respecto de sus aclaraciones y ampliaciones correspondientes.* *8. Aprobar el curso básico de peritos por año fiscal determinado en el presente reglamento; y,* *9. Cualquier otra obligación establecida en la normativa legal, en este reglamento y/o por la o el administrador del Sistema Pericial Integral de la Función Judicial."*
33	*"**Designación de peritos servidores del sector público para procesos específicos. -** Las y los peritos que pertenezcan a instituciones del sector público cuando sean designados por la jueza o juez o la o el fiscal de la causa, actuarán de conformidad al perfil profesional y la necesidad requerida de la materia en litigio.* *En los procesos de familia, mujer, niñez, adolescencia, violencia contra la mujer o miembros del núcleo familiar; en procesos judiciales que se sustancien en las Unidades de Flagrancia de la Función Judicial; o, cualquier otro considerado por el Pleno del Consejo de la Judicatura, la autoridad judicial podrá designar directamente como perito exclusivamente a las y los servidores judiciales pertenecientes a la Función Judicial, a las instituciones del sistema de salud pública y a la Policía Nacional del Ecuador, que se encuentren previamente calificados como tales para desarrollar su labor en este tipo de procesos.* *En el caso de que la o el fiscal requiera peritos de la Policía Nacional, del Servicio Nacional de Medicina Legal y Ciencias Forenses o de otras instituciones u organismos del sector público, solicitará directamente a esas instituciones para su respectiva designación.* *Los peritos designados del sector público, para el cumplimiento de sus funciones, contarán con los permisos necesarios por parte de la unidad o dirección de talento humano de cada institución, como asuntos oficiales."*

39	*"**Contenido del informe pericial.** - Los requisitos mínimos obligatorios de todo informe pericial son los siguientes:* *1. Antecedentes: Se delimitará el objeto del peritaje, especificando el tema sobre el que informará con base en lo ordenado por la jueza o juez, la o el fiscal y/o lo solicitado por las partes procesales;* *2. Consideraciones técnicas o metodología a aplicarse: Explicación clara del análisis y cómo aplican sus conocimientos especializados de una profesión, arte u oficio, al caso, el objeto pericial o encargo materia de la pericia;* *3. Conclusiones: luego de las consideraciones técnicas, se procederá a emitir la opinión técnica o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. La conclusión será clara y directa en relación con la pericia realizada. Se prohíbe todo tipo de juicios ambiguos, así como cualquier tipo de juicio de valor sobre la actuación de las partes en el informe técnico; y,* *4. Inclusión de documentos de respaldo, anexos o explicación de criterios técnicos: deberá sustentar sus conclusiones, ya sea con documentos y objetos de respaldo (fotos, láminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.) y/o con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se deben exponer claramente las razones especializadas de la o el perito para llegar a las conclusiones correspondientes debidamente fundamentadas. (…)".*

3. Glosario de Términos y Abreviaturas

TÉRMINO	DEFINICIÓN
Algoritmo HASH	Procedimiento matemático diseñado para convertir cualquier dato digital en una cadena de caracteres de longitud fija, llamada código hash, que identifica de forma única ese dato.
Archivos .OST, .PST, .MSG, Outlook,NFS. EML. EMLX. MBOX.	Formatos de archivos relacionados con el correo electrónico, metadatos y sistemas de archivo. Fundamentales en investigaciones forenses para reconstruir comunicaciones, identificar remitentes,

	destinatarios, fechas y otros relativos a buzones de correo.
Cadena de custodia	Es el conjunto de actividades y procedimientos secuenciales que se aplican en la protección y aseguramiento de los indicios y/o evidencias físicas y digitales, desde la localización en la escena del delito o lugar de los hechos, hasta su presentación ante el juzgador y/o disposición final.
Cifrado	Proceso que convierte información legible en un formato codificado e ilegible con el fin de protegerla de accesos no autorizados para lo cual se utilizan algoritmos matemáticos.
Códigos Hash	Cadena única de caracteres generada por un algoritmo hash que sirve para identificar y verificar la integridad de archivos o contenido digital, asegurando que no han sido alterados.
Contenido digital	Dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
Criptoactivos	Representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión.
Datos volátiles	Datos residentes en la memoria temporal de un dispositivo, se pierden cuando se apaga o reinicia el equipo.
Dirección IP	Protocolo de Internet, es un número único que identifica a cada dispositivo conectado a una red informática, como Internet o una red local. Sirve para localizar y comunicar dispositivos entre sí dentro de la red, existen dos tipos direcciones IP. • IP pública: Permite que los dispositivos sean accesibles desde cualquier lugar a través de Internet. • IP privada: Solo permite la comunicación dentro de una red interna; los dispositivos con IP privada no son accesibles directamente desde Internet.

Dispositivo de almacenamiento digital	Dispositivos de hardware usados para almacenar datos de manera electrónica, usados en computadoras y otros dispositivos electrónicos.
Dispositivo móvil	Dispositivo electrónico portátil, equipado con capacidades de procesamiento, memoria y conectividad inalámbrica (como 3G, 4G, Wi-Fi, Bluetooth o datos móviles), almacenan gran cantidad de información como mensajes, llamadas, correos, ubicaciones, fotos, contraseñas y datos de aplicaciones.
Disponibilidad	Refiere a la garantía de que los recursos digitales y sistemas estén disponibles y accesibles cuando sea necesario. Este es uno de los tres pilares fundamentales de la seguridad de la información.
Evidencia	Es cualquier dato, objeto o información obtenida y preservada legalmente que puede ser utilizado para demostrar hechos relevantes en una investigación o proceso judicial. La evidencia forense sirve para esclarecer un delito, identificar a los responsables o exonerar a inocentes, y debe ser confiable, íntegra y verificable.
Evidencia Digital	Es cualquier tipo de datos en tránsito o en reposo que se encuentra en formato digital y que puede ser utilizada en investigaciones legales, forenses o en otros contextos para respaldar o refutar afirmaciones o acusaciones.
Forense	Conjunto de técnicas, procedimientos y metodologías especializadas utilizadas para la identificación, adquisición, preservación, análisis y presentación de evidencia digital, con el fin de que dicha información pueda ser utilizada en procesos legales.
Función Hash	Aplicación práctica del algoritmo hash sobre un dato específico. Conocida como "hash", es única para cada conjunto de datos de entrada.
Hardware forense	Se refiere a la categoría de herramientas y dispositivos especializados utilizados en el campo de la informática forense, son esenciales para llevar a cabo las tareas de recuperación, análisis y preservación de evidencia digital de manera efectiva.
Indicio	Todo elemento físico, químico, biológico o digital que ha sido utilizado o generado durante la comisión de un hecho

	presuntamente delictivo, y que se recolecta en la escena para que, mediante su análisis técnico, pueda esclarecerse el hecho.
Integridad	Principio que garantiza que los datos se mantienen completos, exactos y sin alteraciones no autorizadas durante su almacenamiento, transmisión o procesamiento.
Licenciamiento	Es el derecho a utilizar el software y servicios, las licencias de software suelen ser de 3 tipos: propietarias, libres o de código abierto.
Perito	Experto en una disciplina o materia relacionada a un arte o profesión. Dentro del campo de las ciencias forenses o criminalística, se define como el experto que analiza desde un punto de vista técnico y científico la totalidad o parte de un hecho.
RAM	Memoria de acceso aleatorio utilizada en los dispositivos informáticos, memoria volátil usada para almacenar temporalmente los programas y datos que están siendo utilizados activamente por el sistema operativo y las aplicaciones en ejecución.
RFC (request for comment)	Documentos de referencia y directrices para el desarrollo y la implementación de tecnologías de Internet, incluidos protocolos de red, aplicaciones de software y estándares de seguridad.
Transferencia de la escena	Procedimiento técnico, documental y legal mediante el cual la responsabilidad sobre el lugar de los hechos, indicios o evidencias es entregada formalmente de un servidor policial, autoridad competente o equipo técnico a otro funcionario autorizado, garantizando la continuidad del control, preservación, integridad y trazabilidad de los elementos materiales relacionados con la investigación.
Trazabilidad	Capacidad de registrar y seguir de manera cronológica, documentada y verificable todas las acciones realizadas sobre la evidencia digital.
Volcado de Memoria RAM	Proceso de copiado de todo el contenido de la memoria volátil (RAM) de un dispositivo para su posterior análisis. En informática forense, este procedimiento es fundamental porque la RAM puede contener evidencia digital valiosa y temporal, como contraseñas, sesiones activas, procesos en ejecución y datos no almacenados en

	disco. Analizar el volcado de memoria permite a los expertos recuperar información crítica que puede ser clave en una investigación digital

ABREVIATURA	DEFINICIÓN
AFU	“After First Unlock” por sus siglas en inglés, después del primer desbloqueo
BFU	“Before First Unlock” por sus siglas en inglés, Antes del primer desbloqueo
CCTV	Circuito cerrado de televisión
CD	“Compact Disc” por sus siglas en inglés, Disco Compacto
DEFR	“First Head of Digital Evidence” por sus siglas en inglés, Primer Responsable de Evidencia Digital
DES	“Digital Evidence Specialist” por sus siglas en inglés, Especialista en evidencia digital
DVR	“Digital Video Recorder”
ED	Evidencia Digital
IMEI	“International Mobile System Equipment Identity” por sus siglas en inglés, Sistema Internacional para la Identidad de Equipos Móviles
iOS	“iPhone Operating System” por sus siglas en inglés, Sistema operativo iPhone
IoT	“Internet of Things” por sus siglas en inglés, Internet de las Cosas
IP	“Internet Protocol” por sus siglas en inglés, protocolo de Internet
ISO/IEC	Organización Internacional de Estandarización / Comisión Electrotécnica Internacional.
NVR	“Network Video Recorder” por sus siglas en inglés, Grabador de vídeo en red
OS	“Operating System” por sus siglas en inglés, sistema operativo

RFC	"Request for Comments" por sus siglas en inglés, documentos de referencia
SEIIMLCF	Sistema Especializado Integral de Investigación en Medicina Legal y Ciencias Forenses
USB	"Universal Serial Bus" por sus siglas en inglés.
UTC	"Coordinated Universal Time" por sus siglas en inglés, Hora universal coordinada
VPN	"Virtual Private Network" por sus siglas en inglés, Red privada virtual

4. Alcance

El presente manual constituye un instrumento técnico-metodológico de observancia obligatoria para el personal perteneciente al Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses que intervenga en el manejo integral de contenido digital, dentro del ámbito de sus respectivas atribuciones y competencias, con sujeción a las disposiciones fiscales, autorizaciones judiciales y normativa legal aplicable.

5. Lineamientos

5.1. Lineamientos Técnicos

a) Las disposiciones del presente manual regulan exclusivamente actuaciones técnicas y metodológicas para la identificación, recolección, preservación, adquisición, análisis y presentación de evidencia digital.

b) Su ámbito de aplicación comprende procedimientos considerados desde la comisión de un delito flagrante o desde el inicio de una investigación penal, siempre que existan dispositivos, sistemas, medios de almacenamiento, cuentas, servicios digitales o cualquier otro elemento que pudiera contener evidencia digital relacionada con un hecho investigado.

c) Este manual proporciona la metodología para el tratamiento de contenido digital en sus diferentes fuentes o escenarios de evidencia digital, desde el momento de su hallazgo en la escena del delito hasta cada etapa del proceso de investigación penal, con base a los estándares internacionales y normativa legal vigente.

d) Los procedimientos técnicos aplicados por cada actor vinculado al tratamiento del contenido digital deberán garantizar el respeto a los derechos constitucionales, principalmente aquellos relacionados con confidencialidad de las comunicaciones, protección de datos personales, derecho a la intimidad, debido proceso y derecho a la defensa.

e) Todo el contenido inherente a la gestión del contenido digital deberá mantenerse con irrestricta confidencialidad para su uso en actuaciones judiciales debidamente requeridas por la autoridad competente.

f) Las instituciones y actores intervinientes en la gestión y tratamiento del contenido digital actuarán con base a la metodología citada en el presente instrumento, de acuerdo con sus atribuciones y competencias, conforme a la normativa legal vigente.

g) Las entidades que forman parte del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, cuando resulte necesario, podrán emitir instrumentos metodológicos institucionales propios en concordancia con las disposiciones del presente manual.

h) Ante cualquier interacción física y/o lógica del indicio informático, se deberán considerar las características inherentes al contenido digital (volátil, duplicable, eliminable y alterable), adoptando las medidas técnicas forenses y procedimientos de seguridad de la información, que garanticen su autenticidad, integridad y admisibilidad.

i) Se deberá garantizar en todo el proceso la observancia de los principios que rigen la cadena de custodia para indicios físicos, electrónicos y/o contenido digital, de conformidad con la normativa legal vigente.

j) En la escena del hecho, la interacción, extracción y/o adquisición del contenido digital de dispositivos móviles, informáticos y/o electrónicos solo podrá ser realizado por personal del Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses o por quien cuente con competencias técnicas suficientes y actúe bajo disposición expresa de la autoridad competente.

k) Los servidores del Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses, cuando su intervención corresponda a actuaciones periciales

deberán acreditar los perfiles mínimos para su actuación y contar con formación especializada en técnicas de investigación digital forense.

l) Los servidores del Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses emitirán una respuesta técnica fundamentada cuando los requerimientos del operador de justicia se contrapongan con la metodología establecida para el tratamiento de contenido digital.

m) La intervención de peritos privados o provenientes de organismos de cooperación internacional, deberá realizarse en estricto cumplimiento de la normativa legal vigente, asegurando que sus actuaciones se ajusten a los procedimientos y requisitos establecidos por la ley, con el fin de garantizar la validez y la integridad de los resultados periciales dentro del proceso investigativo.

n) Solo las personas autorizadas por la autoridad competente podrán asistir de manera presencial a la exhibición de contenido digital, conforme la normativa legal vigente.

o) Se establecerá una reunión de coordinación entre el personal del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses que intervengan en la investigación, con la finalidad de orientar y definir los aspectos operativos y técnicos de la intervención, que servirán de base para la gestión de las autorizaciones judiciales, conforme a la normativa legal vigente.

p) Para efectos de este manual se entenderá por *"contenido digital"* a todo dato que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

q) Corresponde al Subsistema responsable de la investigación técnica y científica en materia de Medicina Legal y Ciencias Forenses gestionar un repositorio integrado de información especializada destinada a la investigación forense en evidencia digital, a efectos de constituir un sistema informático estadístico para la investigación del delito e inteligencia forense.

r) El contenido digital está compuesto por el indicio físico (contenedor/equipo). A partir del análisis del indicio físico, se realiza la extracción de la información digital, misma

que constituye la evidencia digital, sobre la cual se deberá observar las reglas de los artículos 500 y 616.1 del Código Orgánico Integral Penal.

5.2. Lineamientos metodológicos

a) La recolección, preservación y análisis del contenido digital se basarán en metodologías, técnicas digitales y utilización de herramientas que cumplan con las mejores prácticas, normas, tipos de licenciamientos y estándares validados a nivel nacional e internacional, así como trabajos investigativos publicados en revistas indexadas de alto impacto. Estas actividades garantizarán la integridad, autenticidad y admisibilidad de la evidencia en procesos judiciales.

b) Tanto el Primer Responsable de Evidencia Digital (DEFR) como el Especialista en Evidencia Digital (DES) deberán considerar que la gestión del contenido digital, en los procesos de extracción y preservación de datos, puede requerir, dependiendo del estado y las características de los elementos contenedores de evidencia digital, una interacción física y/o lógica con los equipos; dicha interacción deberá realizarse aplicando técnicas digitales forenses, con el fin de garantizar la integridad y validez de la evidencia, y evitar cualquier tipo de alteración o pérdida de la información. Los procedimientos utilizados deben estar debidamente documentados y ajustarse a estándares reconocidos en la materia.

c) Tanto el Primer Responsable de Evidencia Digital (DEFR) como el Especialista en Evidencia Digital (DES), en caso de aplicar técnicas invasivas para la extracción y preservación de evidencia digital, deberá contar previamente con la autorización de la autoridad correspondiente. Los procedimientos utilizados deben estar debidamente documentados y ajustarse a estándares profesionales y buenas prácticas.

d) Previo a ejecutar una orden de allanamiento o preservación de datos, se deberá coordinar con la fiscalía, las unidades investigativas y el personal técnico especializado, a fin de definir los aspectos operativos y técnicos necesarios para el tratamiento del contenido digital. Esta coordinación deberá contemplar según corresponda los procedimientos aplicables en casos de triaje, inspección manual de dispositivos, volcados de memoria RAM, manejo de claves de acceso, acceso a datos en la nube, capacidades del personal interviniente y recursos disponibles, sin perjuicio de que las disposiciones fiscales y autorizaciones judiciales que

correspondan, se emitan y tramiten de conformidad con la normativa legal vigente.

5.3. Características de la Evidencia Digital

- **Volátil:** El contenido digital se pierde por completo cada vez que un dispositivo se apaga o pierde su suministro eléctrico, ya que reside en memorias temporales como la RAM. **Duplicable:** La evidencia digital puede ser copiada las veces que sean necesarias sin afectar el original, lo que permite trabajar con replicas para preservar el elemento original.
- **Alterable:** La evidencia digital puede ser modificada de forma voluntaria, por ejemplo, por un atacante, o involuntaria, por un usuario o incluso durante el análisis forense, por lo que es crucial garantizar la integridad de los elementos bajo estudio.
- **Eliminable:** Puede ser eliminada fácilmente no solo por acción humana sino también por acción del ambiente o daños físicos, razón por la cual se debe conservar y custodiar en debida forma para evitar pérdidas, daños o manipulación no autorizada.

5.4. Principios de admisibilidad jurídica

- **Legalidad:** La evidencia digital debe ser obtenida, extraída y procesada con sujeción a la constitución, la ley y la normativa aplicable, asegurando el respeto al debido proceso y la validez jurídica.
- **Confiabilidad**: Los procedimientos, herramientas, técnicas forenses utilizadas para la recolección, preservación y análisis de la evidencia deben ser científicamente validas, reconocidos por la comunidad forense y auditables.
- **Suficiencia:** Cualidad que hace referencia a la cantidad y calidad de la evidencia digital, la suficiencia garantiza que la información digital recolectada permita sustentar el análisis forense acorde el objeto de la investigación.
- **Pertinencia:** Está directamente relacionada con el hecho investigado, ser útil para probar o descartar una hipótesis y no ser excesiva ni irrelevante.

5.5. Principios de la cadena de custodia

- **Autenticidad:** Cualidad que garantiza que los datos provienen de su fuente original y no han sido alterados, manipulados o falsificados desde su creación o recolección.

- **Integridad:** Principio que establece que el manejo de los indicios informáticos no debe generar alteraciones que comprometan su validez o admisibilidad como prueba. En este contexto, la integridad implica que la evidencia digital recolectada se mantenga inalterada, completa, exacta y fiable a lo largo de todas las etapas del proceso forense, garantizando así su autenticidad y valor probatorio.
- **Auditabilidad:** Cualidad del proceso forense que permite establecer trazabilidad en todas las etapas de obtención, preservación y análisis de la evidencia digital. Este principio implica la existencia de registros detallados y documentados de cada acción realizada, lo que posibilita la evaluación del procedimiento ejecutado y, cuando sea necesario, su reproducción en casos específicos.

5.6. Clasificación general de las fuentes de evidencia digital

A efectos de estandarizar la actuación pericial y establecer criterios técnicos uniformes para la identificación, priorización e intervención sobre dispositivos electrónicos, se establece la siguiente clasificación general. Esta categorización tiene por objeto orientar a los diferentes actores descritos en este manual, en la determinación del orden de intervención, el protocolo de adquisición aplicable y las consideraciones técnicas particulares de cada tipo de dispositivo, en función de su naturaleza, capacidad de almacenamiento y tipo de contenido digital que pudiera contener.

Tabla 1. Clasificación general de las fuentes de evidencia digital

CATEGORÍA	TIPO DE DISPOSITIVO	CONTENIDO DIGITAL
SISTEMAS INFORMÁTICOS	Computadoras de escritorio.	Datos ofimáticos, archivos multimedia, cuentas de usuario, base de datos, datos de máquinas virtuales, configuración y/o registros de sistema operativo, licencias de software, configuración de red, artefactos de navegación web, aplicaciones, respaldos de datos.
	Computadoras portátiles.	
	Servidores físicos o virtualizados	
	Sistemas de video vigilancia	
	Sistemas electrónicos automotrices.	
	Consolas de video juegos	
	Cámaras digitales.	
	Impresoras	
	Rig de Minería	

DISPOSITIVOS DE ALMACENAMIENTO	Discos Duros externos.	Datos Ofimáticos, archivos multimedia, registros del sistema de archivos, datos eliminados, volumen, número de serie lógica, metadatos.
	Dispositivos USB	
	Memorias externas.	
	Dispositivos ópticos.	
	Grabadoras digitales (audio y/o video).	
	Sistema de respaldos	
	Sistemas de reproducción multimedia.	
DISPOSITIVOS TELEMÁTICOS	Enrutador	Tablas de enrutamiento, configuración de protocolos de comunicación y red, registros, entre otros.
	Conmutador	
	Módems	
	Equipos de seguridad informática	
	Teléfonos satelitales	
	Equipos de radio digital	
DISPOSITIVOS MÓVILES	Teléfonos inteligentes o smartphones.	Contactos, registro de llamadas, mensajes SMS, servicios de mensajería instantánea, ubicación, archivos multimedia, redes sociales, correos electrónicos, documentos, contraseñas, tokens de conexión, firma electrónica, datos de proveedor de servicios, rutas de navegación, respaldos, información de las APP, entre otros.
	Tabletas digitales o PDA.	
	Dispositivos y consolas de navegación no tripulada.	
	Reloj inteligente.	
SISTEMAS BASADOS EN LA NUBE (CLOUD)	Software como servicio (SaaS).	Redes Sociales, sitios web, mensajería instantánea y electrónica, almacenamiento, registros de servicios de dominio, datos de suscriptor, tráfico y contenido.
	Plataforma como servicio (PaaS).	
	Infraestructura como servicio (IaaS).	
	Nube de datos (Pública, Privada e Híbrida)	
TECNOLOGÍAS	Realidad extendida.	Trazabilidad de transacciones e información de billeteras digitales, cuentas de usuario, datos de registro y/o
	Blockchain y Activos Digitales.	
	Computación Cuántica.	
	Big Data.	

DISRUPTIVAS	Inteligencia Artificial (IA). Equipos de IOT (internet de las cosas).	conexión, base de datos, tablas de hash, datos geográficos de ubicación, datos de Inter operatividad, datos de entrenamiento, metadatos, entre otros.

5.7. Niveles de Gestión

Para el tratamiento de la evidencia digital se establecen tres niveles de gestión:

- El primero corresponde a la preservación inicial en escena.
- El segundo corresponde al procesamiento técnico de campo.
- El tercero corresponde al procesamiento técnico especializado en laboratorio.

5.8. Actores

- **Primer Respondiente**

Perfil que pueden cumplir los servidores pertenecientes o no al Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses y personas particulares que, por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo, que actúan bajo la figura de primer actor o persona que llega a la escena del delito, su obligación principal es preservar, asegurar y proteger el lugar de los hechos, evitar alteraciones y activar el escalamiento técnico correspondiente.

- **Personal competente en materia de procesamiento de la escena**

Es el servidor del Sistema Especializado que ejecuta actividades de búsqueda y recolección de indicios físicos y/o electrónicos, siempre que tales actividades no impliquen tratamiento lógico del contenido, además, serán los encargados de evaluar las condiciones para seguir el escalamiento a otros especialistas según el tipo y estado del indicio informático.

- **Primer responsable de Evidencia Digital (DEFR)**

Es el servidor que, dentro del ámbito de su formación académica, capacidades y competencias, identifica, recolecta, preserva y documenta la posible evidencia digital en la escena del delito, en

cumplimiento a los principios de admisibilidad y cadena de custodia.

- **Especialista en Evidencia Digital (DES)**

Es el profesional especializado que aporta conocimientos técnicos para extraer, procesar, analizar e interpretar la evidencia digital, con fundamentación científica y con base al requerimiento de la autoridad competente.

5.9. Acciones Según el Nivel de Gestión

Una vez identificados los actores, se procederá a realizar las acciones correspondientes según el nivel de gestión para el tratamiento de la evidencia digital, siguiendo estas tres fases principales:

- **Primera Fase (primer respondiente y personal competente en materia de procesamiento de la escena):** Asegurar y proteger el lugar de los hechos.
- **Segunda Fase (personal competente en materia de procesamiento de la escena y/o DEFR):** Procesamiento de la escena.
- **Tercera Fase (DES):** Procesamiento de evidencia digital en laboratorio.

5.9.1. Primera Fase: Asegurar y proteger el lugar de los hechos

El primer respondiente asegurará y protegerá la escena con los medios disponibles, por lo que deberá tomar las precauciones y el uso del equipo de protección necesario, realizando las siguientes actividades:

- **Preservación y No Interacción:** Su obligación principal es asegurar y proteger el lugar de los hechos, evitando cualquier interacción, salvo disposición de autoridad competente.

- **Escalamiento Técnico:** El primer respondiente deberá activar el escalamiento técnico correspondiente, solicitando la presencia del Primer Responsable de Evidencia Digital (DEFR) o del personal técnico especializado para que ellos realicen las actividades que implican el tratamiento lógico del contenido.

- **Transferencia de la escena:** Realizará la entrega del lugar de la intervención, la cual deberá contener como mínimo, el registro de la hora, fecha y circunstancias en las que se deja el lugar de intervención bajo la responsabilidad del personal competente en materia de investigación, de acuerdo a los principios de cadena de custodia.

El primer respondiente también comunicará por cualquier medio a la Fiscalía General del Estado, del hecho delictivo con el fin de realizar las primeras diligencias investigativas de estos delitos, conforme a lo dispuesto por la autoridad competente y la normativa nacional vigente, a fin de establecer los elementos de convicción, en apoyo a la administración de justicia.

5.9.2. Segunda Fase: Procesamiento de la escena

Se identifican y aseguran de inmediato todos los dispositivos electrónicos relevantes, documentando su estado original y evitando cualquier alteración, además corresponde a las actividades inherentes a la intervención en el sitio del suceso, ya sea en casos de flagrancia o mediante disposición de autoridad competente. Las acciones para desarrollar incluyen la protección de la escena, Identificación de indicios, ingreso de indicios a centro de acopio y en el caso de requerir asistencia técnica especializada.

La recolección, preservación y tratamiento de contenido digital en el procesamiento de la escena se presenta en los siguientes casos:

1) **Primer Escenario:** Comunicado por parte del Servicio Integrado de Seguridad ECU 911 de la existencia de un hecho delictivo que implique la recolección, procesamiento y tratamiento de evidencia digital.
2) S**egundo Escenario:** Por disposición del operador de justicia o en casos de allanamientos para la búsqueda, registro, acceso y secuestro de datos informáticos e incautación de indicios tecnológicos.

En los dos mecanismos de actuación los servidores pertenecientes al Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, de conformidad a sus competencias deberán acudir al lugar de los hechos o territorio digital a gestionar el procesamiento especializado de los elementos materiales probatorios, la transferencia de la escena o de los indicios informáticos y/o electrónicos en cumplimiento con la normativa legal vigente, donde se deberá generar el correspondiente Formulario Único de Cadena de Custodia. **(Ver Anexo 8.1).**

En estos dos escenarios aparece la figura del primer respondiente, quienes realizarán lo siguiente:

a) Protección del lugar

Ejecutarán las actividades de su competencia conforme a la normativa vigente que regula el procedimiento de cadena de custodia, garantizando la integridad, autenticidad y trazabilidad de los indicios y/o evidencias.

b) Identificación de indicios

De acuerdo con la tipología del delito, se debe establecer los dispositivos electrónicos y/o elementos contenedores de evidencia digital, que se encuentren involucrados en el hecho a investigar, con base a lo determinado en el acápite 6.1.1. Identificación.

c) Ingreso de indicios al centro de acopio

En caso encontrarse en la capacidad de gestionar los dispositivos electrónicos y/o los elementos contenedores de evidencia digital y de no requerir personal técnico se suscribirá el Parte Policial, incluyendo la ubicación en donde se encuentran los equipos, dispositivos y/ o elementos a ser incautados o secuestrados y el Formulario Único de Cadena de Custodia.

d) Solicita escalamiento técnico

En el caso de requerir la presencia del personal técnico se deberá gestionar y coordinar la asistencia de más unidades con capacidades para procesamiento de la escena y de la evidencia digital.

Cuando se prevea adquirir datos volátiles, ordenes de preservación o se efectúen operaciones urgentes de triaje, el perito de Inspección Ocular Técnica, podrá solicitar acompañamiento del Primer Responsable de Evidencia Digital (DEFR), a efectos de recolectar y/o preservar la evidencia digital, debiéndose en todos los casos documentar e informar a fiscalía el proceso realizado.

5.9.3. Tercera Fase: Procesamiento de evidencia digital en laboratorio

Corresponde a la ejecución sistemática de las actividades descritas en la sección 6. Contenido del Manual: "*Metodología para el tratamiento de Evidencia Digital"* del presente manual.

6. Contenido del Manual

6.1. Metodología para el tratamiento de Evidencia Digital

6.1.1. Identificación

Corresponde a la observación, búsqueda, localización, reconocimiento y documentación de fuentes de evidencia digital asociada a un hecho investigado. En esta fase se deberá observar y documentar el estado del dispositivo, determinar si se encuentra encendido o apagado, registrar gráficamente pantallas activas cuando existan, preservar documentos físicos asociados a

credenciales de acceso, diagramas de red, direcciones IP, tokens, llaves privadas, alias u otros elementos relevantes, y valorar riesgos de pérdida, cifrado o alteración.

Los actores asociados a la identificación que comprende al personal competente en materia de procesamiento de la escena y/o DEFR deberán realizar las siguientes actividades mínimas:

- Asegurar el entorno en el que se encuentran los indicios y verificar, así como documentar, el estado de conservación del indicio informático.
- Realizar fijación fotográfica y/o videograbación tanto de la escena como de los dispositivos involucrados.
- Identificar el usuario y/o propietario asociado a los dispositivos, de ser factible.
- Documentar como mínimo, las características del dispositivo: tipo, marca, modelo, número de serie, color y dispositivos periféricos conectados.
- Identificar y documentar la ejecución de técnicas anti forenses, dentro de las diferentes fuentes de evidencia digital.
- Determinar el estado de los dispositivos electrónicos (encendidos o apagados), priorizando aquellos que almacenan o pudieran registrar contenido digital, acorde lo detallado en el numeral **5.6. Clasificación general de las fuentes de evidencia digital.**
- En caso de dispositivos encendidos procurar el aislamiento electromagnético y solicitar la presencia de personal técnico especializado según el nivel de escalamiento correspondiente (DERF o DES).

6.1.2. Recolección

Corresponde al personal competente en materia de procesamiento de la escena y/o DEFR la colección de elementos materiales probatorios que pudieran contener información electrónicamente almacenada o evidencia digital asociada a un hecho investigado, los cuales puedan estar almacenados dentro de un elemento físico o a nivel lógico.

6.1.2.1. Recolección de Dispositivos Electrónicos a Nivel Físico

Este proceso se ejecuta con base a las siguientes actividades determinadas de manera mínima:

- Asegurar el o los dispositivos a nivel físico, protegiendo de interfaces de entrada/salida y conectores de energía.

- Asegurar los dispositivos a nivel lógico mediante el aislamiento de redes y señales electromagnéticas, adoptando las medidas técnicas necesarias para impedir el acceso remoto, la modificación, eliminación o sincronización no autorizada de la información digital. Para este efecto, se deberán ejecutar, como mínimo, las siguientes actividades, las cuales podrán aplicarse de manera individual o combinada, conforme a las condiciones técnicas del dispositivo:
    - Activar el modo avión del dispositivo, con el propósito de deshabilitar todas las comunicaciones inalámbricas disponibles.
    - Proceder con al retiro de la tarjeta SIM, siempre que esta acción no comprometa la integridad del dispositivo o de la información contenida.
    - Emplear contenedores o fundas tipo Faraday, a fin de garantizar el bloqueo de señales electromagnéticas entrantes y salientes.
    - En ausencia de los medios especializados descritos, se deberá utilizar material aislante, como papel aluminio, como medida de contingencia para la mitigación de comunicaciones inalámbricas.

De no ser posible la ejecución de una o más de las actividades descritas en los puntos citados, se deberá documentar de manera expresa, detallada y debidamente justificada las razones técnicas, operativas o de seguridad que impidieron el aislamiento del dispositivo.

- Los indicios deben embalarse conforme a su naturaleza y categoría, utilizando contenedores adecuados que cuenten con protección antiestática y antigolpes. Como contenedor primario, se deberá emplear fundas o sobres de papel, evitando el uso de materiales plásticos; estos favorecen la acumulación de cargas electrostáticas, la condensación de humedad y la exposición visual de las pantallas. Este nivel de embalaje categorizado es fundamental para prevenir cualquier tipo de interacción con los dispositivos que pueda alterar, modificar o eliminar la información contenida en ellos.
- Etiquetar cada indicio documentando al menos con los siguientes datos:
    - **Número de indicio,**
    - **Fecha** (a/m/d),
    - **Hora de recolección** (00H00),
    - **Lugar** (Coordenadas Geográficas),
    - **Causa** (IP, IF, Acto Administrativo, Acto Urgente),

- **Responsable** (Grado/Nombre/Institución).

- Generar el Formulario Único de Cadena de Custodia correspondiente.
- Realizar el traslado e ingreso de los indicios mediante cadena de custodia a las Unidades de Acopio de Indicios y Evidencias de la Policía Nacional.

6.1.2.2. Recolección y Preservación de Contenido Digital (Elementos Lógicos)

Esta actividad tiene como base la ejecución de un proceso sistemático de triaje mediante el cual se asignan niveles de importancia a los datos con el fin de categorizar la relevancia de la información, así como establecer la pertinencia de los componentes físicos del sistema a ser incautados y/o secuestrados, donde se plantean los siguientes escenarios:

a) Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura crítica, se realizará su adquisición en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

b) Al tratarse de la incautación y/o secuestro se deberá cumplir los preceptos descritos en el acápite 6.1.2.1. Recolección de Dispositivos Electrónicos a Nivel Físico.

6.1.3. Adquisición

Lo realizará el DEFR y DES, un proceso controlado orientado a la obtención, preservación y aseguramiento de datos provenientes de sistemas o dispositivos informáticos, con el objetivo de garantizar su integridad y autenticidad. Para ello se emplearán métodos, técnicas y herramientas que aseguren una intervención no invasiva ni intrusiva, evitando cualquier tipo de alteración de los datos originales. Además, el proceso debe incluir mecanismos de verificación, como el uso de funciones hash, que permitan la reproducibilidad y auditabilidad en todas las etapas de la investigación.

6.1.3.1. Métodos de adquisición:

Existen diferentes métodos que pueden emplearse según las características del dispositivo, el nivel de acceso disponible y el tipo de análisis requerido. A continuación, se describen las principales técnicas utilizadas:

a) Imagen Forense: Método que consiste en obtener una copia exacta, bit a bit, del contenido de un dispositivo de almacenamiento, creada con técnicas y herramientas especializadas en informática forense, la cual puede realizarse mediante**:**

- **Adquisición Física**: Se realiza una imagen física en la que se incluyen todos los datos (bit a bit) del dispositivo. La adquisición física a nivel del disco o unidad de almacenamiento consiste en copiar la totalidad de la información contenida en el dispositivo, abarcando el esquema de particiones, así como el espacio asignado y no asignado del volumen.

- **Adquisición Lógica**: Se genera una copia lógica o personalizada que incluye únicamente un subconjunto específico de datos asignados. La adquisición lógica a nivel de disco consiste en copiar únicamente una porción lógica particionada, como puede ser un sistema de archivos, una partición completa, carpetas o archivos individuales, sin capturar el espacio no asignado ni el esquema completo de particiones.

- **Duplicación Forense:** Proceso mediante el cual se realiza una copia exacta de un dispositivo, también a nivel de bits, pero su enfoque principal está en la replicación del contenido completo

b) Extracción de datos: Proceso de recuperación de información directamente desde el dispositivo, utilizando diferentes niveles de acceso:

- **Extracción Física**: Técnica que consiste en generar una copia íntegra de toda la memoria del dispositivo móvil, incluyendo sectores no visibles al usuario y datos eliminados. Esta modalidad es equivalente a una adquisición física y permite realizar extracciones avanzadas mediante métodos como Hex Dump, JTAG, Chip-off, Micro Read entre otras. Algunas de estas técnicas exigen la intervención física del dispositivo.

- **Extracción Lógica**: Proceso mediante el cual se extraen datos específicos almacenados en un dispositivo móvil, utilizando comandos del sistema operativo o herramientas especializadas, sin intervenir directamente en la memoria física del dispositivo.

- **Extracción Manual**: Método basado en la revisión visual directa del contenido del dispositivo, documentado mediante registros fotográficos o fijaciones, excluyendo el uso de capturas de pantalla generadas en el propio equipo. Se emplea en escenarios en los que no es posible realizar extracciones automatizadas o cuando se requiere una inspección rápida y limitada de la información visible.

c) Copias de Seguridad: Se refiere al uso de respaldos del sistema como fuente de evidencia digital. Estas copias pueden realizarse de acuerdo con las siguientes modalidades:

- **Copia automática:** Creación programada y sistemática de duplicados de archivos, datos o sistemas, sin intervención manual directa. Se ejecuta mediante herramientas o servicios configurados previamente.

- **Copia manual**: Duplicación de archivos, carpetas o sistemas realizada sin automatización, en la que una persona inicia, controla y supervisa directamente el proceso.

6.1.3.2. Adquisición *In Situ*

La adquisición *in situ*, realizada en el lugar de los hechos, debe llevarse a cabo considerando la criticidad de la información y siguiendo el orden de volatilidad de los datos. Para ello, se recomienda, siempre que sea posible, realizar un triaje previo, que permita priorizar la captura de la evidencia más vulnerable y relevante.

- **Triaje**

Es el proceso mediante el cual se asignan niveles de prioridad con base en su criticidad u orden de volatilidad, para determinar el orden óptimo de adquisición y/o preservación. Este procedimiento es esencial, ya que permite identificar los elementos tecnológicos relevantes para la investigación, al tiempo que descarta aquellos que no aportan valor, optimizando las fases del análisis forense.

El personal encargado de la recopilación de evidencias en el lugar de los hechos debe actuar con base a la aplicación de técnicas digitales forenses que guíen la búsqueda e incautación de contenido digital y dispositivos electrónicos, garantizando su autenticidad, integridad y manejo de cadena de custodia.

Si bien existen fases recomendadas para este proceso (*como las descritas a continuación*), su aplicación puede variar según las circunstancias del escenario o categoría de dispositivos. Por ejemplo, puede priorizarse la adquisición de datos volátiles antes de documentar físicamente el dispositivo, si se considera que dicha información está en riesgo de perderse por su naturaleza transitoria.

a) Reconocimiento Inicial

- Inspección visual del escenario conforme la categorización de dispositivos detallados en la Tabla 1. "**Clasificación por tipo y contenido de dispositivos electrónicos**".
    - **NOTA**: se deberá tener en cuenta la detección de la utilización de técnicas anti forenses.
- Análisis de conectividad y mapeo de red a nivel cableado o inalámbrico.
    - **NOTA**: se deberá tener en cuenta posibles redes falsas u ocultas como táctica antiforense.

b) Identificación

- Observar y localizar los elementos electrónicos presentes en la escena conforme la categorización de dispositivos detallados en la Tabla 1. "**Clasificación por tipo y contenido de dispositivos electrónicos**".
- Identificar qué dispositivos están conectados a la red, ya sea interna o externa.
- Inspeccionar físicamente cada dispositivo en busca de signos de manipulación, daños o alteraciones que puedan afectar la integridad de la evidencia.
- Detectar posibles dispositivos o mecanismos que puedan representar una técnica antiforense (VPN, borrados seguros, cifrados, esteganografía, etc.).

c) Documentación

- Documentar cualquier tipo de daño físico visible en los dispositivos electrónicos o medios de almacenamiento.

- Documentar gráficamente (vídeo, fotografía) el escenario en cual se recogen los dispositivos electrónicos o medios de almacenamiento, del mismo modo documentar cualquier dispositivo electrónico (marca, modelo, número de serie, color y dispositivos periféricos conectados) conectado físicamente previo a su desconexión bajo criterio forense.

- Se debe limitar la interacción (físico, lógico) con los dispositivos, salvo que ésta haya sido previamente planificada y autorizada.

- Etiquetar las evidencias para su correcta identificación visual, al menos con los siguientes datos:

    - **Fecha** (a/m/d),
    - **Hora de recolección** (00H00),
    - **Lugar** (Coordenadas Geográficas),
    - **Causa** (IP, IF, Acto Administrativo, Acto Urgente),
    - **Responsable** (Grado/Nombre/Institución).

d) Aseguramiento

I. Preservar documentos impresos o manuscritos asociados a credenciales de acceso, diagramas de red, direcciones IP, tokens, llaves privadas, nickname o alias, etc., que puedan ser relevantes para la investigación.

II. Determinar si los dispositivos se encuentran apagados o encendidos. En el caso de dispositivos encendidos, la pantalla podría mostrar información de interés, la cual debe ser documentada gráficamente.

III. Intentar obtener información volátil si el dispositivo lo permite, para lo cual se deben considerar los lineamientos del Request For Comments - RFC 3227, “Guía para Recolectar y Archivar Evidencia volátil”.

IV. Apagar los dispositivos de manera controlada, únicamente si las condiciones del dispositivo y escena lo exigen (por ejemplo, para la extracción física de un disco duro) para lo cual se registrará la fecha y hora de su apagado.

V. Para la protección y aislamiento electromagnético de los indicios se deberá considerar lo estipulado en el apartado 6.1.2.1. Recolección de Dispositivos Electrónicos a Nivel Físico

Cuando el sistema informático o dispositivo de almacenamiento de datos forme parte de un sistema en operación crítica que impida su apagado (ejemplo: servidores en producción, sistemas que formen parte de un servicio público, sistemas con llaves USB, entre otros.), se realizará la adquisición in situ, aplicando técnicas forense-digitales que aseguren la integridad y autenticidad lo cual deberá documentarse y registrarse en el formulario de cadena de custodia.

6.1.3.3. Adquisición en Laboratorio

La adquisición en laboratorio, lo realizará el DES considerando el tipo de sistema, equipo, dispositivo informático, características y condiciones técnicas del o los dispositivos. Este proceso implica la creación de una imagen forense, la extracción de datos o copias de seguridad, duplicado de datos u otras que considere el perito, este proceso implica la utilización de herramientas y técnicas especializadas, garantizando en todo momento la integridad y autenticidad de la información.

En esta etapa se debe considerar la Tabla de clasificación por tipo y contenido de dispositivos electrónicos, para la determinación del tipo de adquisición que deba aplicarse; es importante indicar que, en esta etapa, los sistemas operativos, equipos y dispositivos se encuentran en estado pasivo y aislados de cualquier tipo de conexión (No aplica para dispositivos Telemáticos, sistemas en la nube y tecnologías disruptivas).

a) Adquisición de Sistemas Informáticos

- Extraer la fuente de almacenamiento de datos del sistema informático del cual se va a realizar el proceso de adquisición.
- Utilizar bloqueadores de escritura a nivel de hardware o software, previo a realizar los procesos de adquisición y/o extracción forense, con el fin de garantizar en todo momento la integridad de la evidencia.
- Realizar el proceso de adquisición a través de la duplicación de discos o la generación de una imagen forense, para lo cual se deben utilizar herramientas especializadas a nivel de hardware o software.

- Almacenar la extracción forense en un sistema o medio tecnológico seguro.
- Generar valores hash de la imagen forense adquirida para garantizar su integridad.
- Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

b) Adquisición de dispositivos de almacenamiento

- Utilizar bloqueadores de escritura a nivel de hardware o software para el proceso de adquisición con el fin de garantizar en todo momento la integridad de la evidencia.
- Realizar el proceso de adquisición a través de la generación de una imagen forense, para lo cual, se puede utilizar herramientas especializadas a nivel de hardware o software.
- Almacenar la extracción forense en un sistema o medio tecnológico seguro.
- Generar valores hash de la imagen forense adquirida para garantizar su integridad.
- Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

c) Adquisición de dispositivos telemáticos

El valor forense de recolección de datos de este tipo de dispositivos puede presentarse en dos instancias tanto in situ como en el análisis de laboratorio para lo cual se determina las actividades mínimas a desarrollarse:

- Identificar la configuración del dispositivo (Dirección IP, credenciales de acceso de ser necesario, protocolos de comunicación).
- Aislar el dispositivo (Desconectar de la red, usar bloqueadores de señal).
- Identificar la existencia de datos volátiles, realizar el proceso de adquisición de datos de la memoria, registros en tiempo real y configuraciones.
- Realizar el proceso de adquisición de datos no volátiles a través de la generación y exportación de imágenes forenses, respaldo u copia de seguridad, para lo cual se deben utilizar herramientas especializadas a nivel de hardware o software.
- Utilizar bloqueadores de escritura a nivel de hardware o software para el proceso de adquisición, con el fin de garantizar en todo momento la integridad de la evidencia.
- Almacenar la extracción forense en un sistema o medio tecnológico seguro.

- Generar valores hash de la extracción forense para garantizar su integridad Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

d) Adquisición de dispositivos móviles

En dispositivos configurados con acceso por PIN, patrón, clave o biometría, se deben ejecutar procesos de desbloqueo o bypass de seguridad, haciendo uso de herramientas especializadas y técnicas forenses, este proceso será documentado e incorporado al informe pericial.

I. Adquisición Lógica

- Activar modo avión y aislar de cualquier tipo de conexión.
- Sincronizar el dispositivo al equipo de extracción forense.
- Realizar la extracción de datos soportados.

II. Adquisición Física (Si es soportada)

- Activar modo avión y aislar de cualquier tipo de conexión.
- Seleccionar herramientas forenses compatibles con los dispositivos móviles.
- Sincronizar el dispositivo al equipo de extracción forense.
- Realizar la extracción de datos.

III. Adquisición Manual

Este método de adquisición se ejecuta cuando no es posible realizar extracciones automatizadas, la adquisición manual implica generar un registro fotográfico o fijaciones, excluyendo el uso de capturas de pantalla generadas en el propio equipo. Este proceso debe ser realizado a través de herramientas forenses o mediante equipos externos de captura de imágenes, esta información debe ser validada a través de valores hash.

IV. Adquisición de dispositivos bloqueados modo (AFU)

Este procedimiento exige mantener el dispositivo móvil encendido, considerando que el apagado o reinicio, podrían activar algoritmos de cifrado, borrado de datos o alteración de información. Se deberán seguir los siguientes pasos para garantizar una adquisición segura:

- Usar un dispositivo de carga externa o conexión a fuente de poder.
- Sincronizar el dispositivo al equipo de extracción forense.
- Realizar la extracción de datos soportados.

V. Adquisición de dispositivos bloqueados modo (BFU)

Si no es posible desbloquear el dispositivo, se realizará una adquisición parcial o limitada que permita la obtención de datos sin desbloqueo.

- Usar un dispositivo de carga externa o conexión a fuente de poder.
- Sincronizar el dispositivo al equipo de extracción forense.
- Realizar la extracción de datos soportados.

Para concluir el proceso de extracción de datos, se deben ejecutar las siguientes actividades complementarias:

- Verificación exitosa de la extracción en el equipo o software utilizado.
- Validación de acceso exitoso a los datos extraídos.
- Almacenar la extracción en un sistema o medio tecnológico seguro.
- Generar valores hash de la adquisición forense para garantizar su integridad. Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

e) Adquisición de sistemas basados en la nube (Cloud)

I. Páginas y sitios web.

- **Manual:**
  - El proceso manual se enfoca para páginas web estáticas.
  - Exportar y preservar la página web de manera parcial o total, utilizando extensiones de navegadores o aplicaciones especializadas.

- **Automatizada:**

  - Utilizar herramientas especializadas para adquirir y obtener un respaldo íntegro del contenido del sitio web y otros recursos.

- Asegurar que la herramienta respete los archivos robots.txt (a menos que se tenga autorización para ignorarlos).

- **De contenido dinámico:**
  - Para sitios web dinámicos, utilizar herramientas especializadas que permitan capturar datos o interacciones en tiempo real.
  - Si el caso lo amerita, registrar el proceso integro, utilizando herramientas de grabación de pantalla o dispositivos de grabación externa.

f) Sistemas informáticos y/o plataformas digitales con factores de autenticación

Si la información requerida corresponde a datos de abonado o de tráfico, su requerimiento se realizará por disposición fiscal conforme al régimen legal aplicable. Respecto a datos de contenido, especialmente en sistemas o plataformas digitales con mecanismos de autenticación administrados por el usuario, el acceso, preservación, registro, extracción, copia o presentación de dichos datos deberán sujetarse a la normativa legal vigente, autorización judicial y, si corresponde, mecanismos de cooperación internacional.

g) Desde un servicio hosting

- En caso de contar con las credenciales de acceso al servidor, proceder con la adquisición de una réplica exacta de los datos con el uso de herramientas especializadas.
- En caso de no contar con credenciales de acceso al servidor, se deberá contactar formalmente al proveedor del servicio del hosting y solicitar una copia exacta de los datos requeridos.
- En ambos casos se adquirirá y/o solicitará los archivos de registro (logs) del servidor.

Para los tres escenarios planteados se deberá considerar las siguientes acciones finales:

- Generar valores hash de la adquisición forense para garantizar su integridad,
- Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

h) Correos electrónicos

I. Buzón en servicios de correo web externos (por ejemplo: Gmail, Outlook, Yahoo)

Según las condiciones del caso, se optará por una o más de las siguientes acciones:

- Solicitar una copia del buzón de correo al proveedor del servicio, para lo cual se seguirán los canales legales establecidos, cumpliendo con los requisitos formales de cada plataforma.
- Solicitar las credenciales de acceso del titular de la cuenta (usuario y contraseña), asegurando que sea registrado y documentado.
- Utilizar herramientas especializadas, para la descarga del buzón en formato compatible para el análisis forense (ejemplo: PST, EML, MBOX).

II. Buzón en servidores de correo locales

- En caso de contar con las credenciales de acceso al servidor, proceder con la adquisición completa del buzón de la cuenta de correo electrónico, con el uso de herramientas especializadas.
- En caso de no contar con credenciales de acceso al servidor, se deberá contactar formalmente a la institución o entidad solicitando se brinde las facilidades para la adquisición completa del buzón de la cuenta de correo electrónico.

En todos los casos:

- Almacenar la adquisición en un sistema o medio tecnológico seguro.
- Generar valores hash de la adquisición forense para garantizar su integridad,
- Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

III. Adquisición en tecnologías disruptivas

La adquisición forense de datos en entornos que integran tecnologías disruptivas comprende metodologías y procedimientos técnicos de identificación y obtención de evidencia digital, aplicados a sistemas no convencionales, caracterizados por su complejidad, descentralización, virtualización, cifrado o alto nivel de automatización. Estas innovaciones transforman

radicalmente industrias, mercados financieros y la vida cotidiana, desplazando métodos y modelos tradicionales los cuales necesitan tratamientos especiales de investigación forense digital.

Estas tecnologías como la realidad extendida (XR), blockchain (criptoactivos), activos digitales, computación cuántica, computación en nube, big data, inteligencia artificial (IA) y el Internet de las Cosas (IoT) presentan particularidades que exigen enfoques especializados de adquisición, debido a la diversidad de formatos, niveles de cifrado y ubicaciones (locales o en la nube).

Considerando la evolución de las tecnologías disruptivas, los procedimientos de adquisición deben adaptarse de manera flexible a los distintos escenarios contemplados en las secciones previas de este manual, en función del tipo de entorno involucrado como **sistemas informáticos, dispositivos móviles, sistemas basados en la nube**, **entre otros**, garantizando siempre la integridad, autenticidad y trazabilidad de la evidencia digital.

En todos los casos:

- Almacenar la adquisición en un sistema o medio tecnológico seguro.
- Generar valores hash de la adquisición forense para garantizar su integridad,
- Documentar todo el proceso e incluirlo en el informe técnico pericial.
- Considerar los lineamientos de cadena de custodia.

6.1.4. Análisis

El análisis de evidencia digital es una etapa crítica dentro del proceso forense digital, ya que permite identificar, examinar, interpretar y correlacionar la información recolectada durante la adquisición.

Durante esta fase, los peritos forenses y/o DES deberán examinar minuciosamente la información relevante para el caso, con técnicas y herramientas especializadas, de acuerdo con el objeto de la investigación. Para lo cual, se deberá considerar el siguiente procedimiento:

I. Procedimiento del Análisis

- Verificar la integridad de las adquisiciones y/o extracciones mediante funciones HASH.
- Crear una línea de tiempo con los hallazgos relevantes identificados.

- Analizar de particiones, identificación de particiones eliminadas y espacio no asignado en discos duros.
- Configurar la zona horaria adecuada y ajustar en las herramientas para correlación temporal precisa.
- Identificar volúmenes lógicos contenidos en la imagen forense, describiendo sus características: capacidad de almacenamiento, sistema de archivos, número de serie lógico, etiqueta del volumen, entre otros.
- Identificar volúmenes recuperados, considerando las etiquetas asignadas por el sistema (ejemplo: “Recovery”, “C”, “Datos, Unallocated”, etc.).
- Identificar el Sistema Operativo, versiones, actualizaciones, aplicaciones relevantes para la investigación, registros y otra información clave.
- Recuperar archivos y carpetas eliminadas, mediante procedimientos manuales o utilizando herramientas especializadas.
- Calcular códigos hash para cada archivo contenido en la imagen forense.
- Exportar de manera selectiva los archivos según el tipo, extensión u otros criterios definidos en el proceso investigativo.
- Extraer información de perfiles de usuario, como nombres, ID de usuario, fecha de creación y último acceso.
- Extraer datos de dispositivos móviles, mediante adquisición física, lógica o manual.
- Analizar firmas digitales, extensiones de archivo y códigos de cifrado.
- Analizar correos electrónicos, considerar trazabilidad de encabezados, direcciones IP, autenticidad y correspondencia.
- Montar y analizar archivos, incluir archivos comprimidos (ZIP, RAR, etc.), correo electrónico (PST, XML, etc.), máquinas virtuales (OVA, VMDK, etc.), imágenes de disco (ISO), esteganografía, entre otros.
- Generar de reportes que incluyan metadatos, atributos y demás propiedades significativas de los archivos examinados.
- Virtualizar de entornos para escaneo y análisis de archivos maliciosos.
- Búsqueda avanzada de palabras clave, mediante expresiones regulares o patrones específicos.
- Documentar de manera integral el caso.

6.1.5. Presentación de Resultados

Debe enfocarse al cumplimiento del objeto de pericia, el cual debe ser planteado de manera clara, precisa y técnica por los operadores de justicia para definir los límites del análisis pericial, además proporcionar al perito designado y/o el equipo multidisciplinario la información específica que oriente de lo que se debe investigar, analizar, determinar y presentar.

El perito designado deberá cumplir con todas las formalidades legales, técnicas y metodológicas contempladas en el presente Manual, el Reglamento del Sistema Pericial Integral de la Función Judicial, Código Orgánico Integral Penal y/o el Código Orgánico General de Procesos con base en la normativa legal vigente.

El perito una vez designado y posesionado legalmente, realizará todas las actividades inherentes a la acción pericial. Una vez culminadas, se incorporará al informe, toda la información relativa a la solicitud/delegación, recolección/recepción de indicios, metodología para el tratamiento de la evidencia digital aplicada, presentación de resultados, conclusiones y anexos.

El formato de informe pericial se deberá regir acorde el Reglamento del Sistema Pericial Integral de la Función Judicial, dicho formato estará disponible en la página web del Consejo de la Judicatura.

Otros aspectos importantes que debe incluirse en la presentación de resultados y sustento del informe pericial son:

- Número de juicio, Número de noticia del delito, Noticia de Persona Desaparecida, Número del Acto Administrativo, Estado Procesal (Investigación Previa, Instrucción Fiscal) o trámite administrativo, que dispone la realización de la experticia, tomando en consideraciones los preceptos legales para la designación.

- Código de acreditación judicial del perito designado.

- Incluir el nombre, cargo, ciudad y dependencia de la autoridad competente solicitante de la experticia.

- Transcripción textual de la disposición de la autoridad competente, para garantizar una interpretación precisa del requerimiento y evitar ambigüedades en el desarrollo de la experticia.

- Enumeración y descripción precisa y detallada de los elementos materiales probatorios e indicios físicos que fueron examinados.

- El perito deberá considerar si es pertinente incluir al informe el nombre y características y versión de las herramientas de hardware y software empleadas en la realización de la experticia; por ejemplo, tipo de licenciamientos o certificados de mantenimiento y vigencia de equipos, si la investigación lo amerita.

- Se debe realizar una narración cronológica del procedimiento, técnica o guía empleada con cada uno de los elementos materiales probatorios e indicios físicos objeto de la pericia.

- Verificar los elementos materiales probatorios e indicios físicos, registro fotográfico, ficha de actividad técnico-científica que se realizó a cada elemento objeto de análisis.

- El resultado del análisis debe ser descrito de forma clara y con un lenguaje adecuado para la interpretación de la autoridad solicitante y, para el proceso judicial donde interactúan profesionales del derecho y otras áreas no técnicas.

- Si el análisis pericial contempla una gran cantidad de información relevante, se recomienda indexar la información en un reporte y adjuntar al informe como anexo en un dispositivo de almacenamiento digital con las medidas de seguridad físicas y digitales, en cadena de custodia, permitiendo que el operador de justicia pueda hacer uso en cualquier instancia del proceso judicial.

- El dispositivo del almacenamiento a ser adjunto al informe pericial, deberá ser debidamente rotulado con el número de caso o investigación y con su respectiva seguridad digital. Aplicar el cálculo de la función HASH para garantizar la integridad de la información contenida en estos dispositivos, dato que deberá incorporarse como anexo al informe pericial, con las características y especificaciones del dispositivo de almacenamiento.

- Se debe dejar constancia que, con el informe, se hace entrega o se hace la devolución de los elementos materiales probatorios e indicios físicos analizados, los cuales deben ser entregados, embalados, rotulados y registrados en el formulario de cadena de custodia, manteniendo el embalaje original a medida de lo posible.

- Comparecencia ante los tribunales de justicia para la defensa de su informe con base en la normativa legal vigente.

El perito debe presentar los resultados de la investigación pericial con precisión, objetividad y ética; resultados con alto valor probatorio que aporten a la autoridad competente en la administración de justicia.

6.1.5.1. Consideraciones para la presentación del informe pericial

Previo a la entrega del informe pericial (físico o digital), se propone la incorporación de procedimientos internos de verificación y revisión por pares u otra herramienta metodológica que permita validar el uso de métodos y técnicas así como aspectos de forma asociados a la redacción, coherencia, ortografía, legalidad, correcto diligenciamiento de los ítems estipulados, formato de cadena de custodia, presentación de resultados e incorporación de anexos; para lo cual se levantará un procedimiento interno y registro de actividades que permitan identificar el trabajo y aporte de los actores, como un mecanismo de control de calidad de la gestión pericial.

El informe pericial debe cumplir como mínimo con las siguientes características:

- **Preciso:** La información debe ser clara, exacta y detallada, evitando ambigüedades o interpretaciones erróneas, para reflejar fielmente los hallazgos de la investigación.
- **Oportuno:** Los resultados deben presentarse en el momento adecuado, garantizando que sean útiles y relevantes para el proceso judicial.
- **Imparcial:** El informe debe basarse únicamente en evidencia técnica y científica, sin sesgos ni influencias externas, asegurando objetividad en las conclusiones**.**
- **Completo:** Debe incluir toda la información relevante sobre la investigación, documentando cada procedimiento, metodologías, hallazgos y análisis realizado, conforme a las normativas y estándares establecidos.

Las actividades de despacho y archivo de los informes periciales, anexos y reportes están sujetas a las directrices de la unidad de gestión de cada Institución, que permitan certificar su autenticidad y originalidad, así como la capacidad de reproducibilidad.

Una vez entregado el informe pericial y en el caso que corresponda, el perito debe cumplir los lineamientos de la cadena de custodia para la devolución de los indicios.

6.1.6. Disposición Final

La disposición final del contenido digital se sujetará a las disposiciones de la normativa legal vigente, así como, a la normativa secundaria que emita La Fiscalía General del Estado para que internamente se emitan los documentos pertinentes respecto a la eliminación y/o destrucción de la información derivada del análisis del contenido digital.

7. Fuentes

- Ballou, S. (Ed.). (2010). Electronic crime scene investigation: A guide for first responders. Diane Publishing.
- Cano, J. (2015). Computación forense. Alpha Editorial.
- Carvey, H., & Altheide, C. (2011). Digital forensics with open source tools. Elsevier.
- European Network of Forensic Science Institute ENFSI (2016). Best practice manual for the Forensics Examination of Digital Technology.
- Fish, J. T., Miller, L. S., & Braswell, M. C. (2010). Crime scene investigation. Routledge.
- Guide, N. I. J. (2001). A Guide for First Responders. National Institute of Justice, 4.
- INTERPOL (2021). Guidelines for Digital Forensics First Responders. Best practices for search and seizure of electronic and digital evidence.
- ISO/IEC 27001:2022 'Information technology – Security techniques– Information security management systems– Requirements'.
- ISO/IEC 27002:2022 'Information technology – Security techniques– Code of practice for information security management'.
- ISO/IEC 27037:2012 'Directrices para la Identificación, Recopilación, Adquisición y Preservación de Evidencia Digital.'
- ISO/IEC 27041 'Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method'.
- ISO/IEC 27042 'Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence'.
- ISO/IEC 27043 Information technology — Security techniques — Incident investigation principles and processes.
- Lázaro, F. (2013). Introducción a la informática forense. Editorial Ra-Ma.

- Maiorano, A. (2009). Criptografía: técnicas de desarrollo para profesionales. Alpha Editorial.
- Ministerio de Seguridad Argentina (2023). Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de Evidencia Digital.
- National Institute of Justice Forensic NIJ (2004). Examination of Digital Evidence: A Guide for Law Enforcement
- NIST Interagency Report [NIST IR 8387] - Digital Evidence Preservation Considerations for Evidence Handlers
- NIST Internal Report [NIST IR 8354] - Digital Investigation Techniques.
- NIST Interagency/Internal Report (NIST IR 8428) - Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT).
- NIST Technical Series Publication (NIST SP 800-101) – Guidelines on Cell Phone Forensics
- Pous, H. R., Ruiz, J. S., & López, J. L. R. (2009). Análisis forense de sistemas informáticos. Catalunya: Universidad Oberta de Catalunya.
- RFC 3227 - Guidelines for Evidence Collection and Archiving / Directrices para la recopilación de evidencias y su almacenamiento.
- Soriano, M. Criptografía, delitos cibernéticos.
- Standards Australia International. (2003). Guidelines for the management of IT evidence: handbook. Sydney: Standards Australia International

8. Anexos

8.1 Formulario Único de Cadena de Custodia

SISTEMA ESPECIALIZADO INTEGRAL DE INVESTIGACIÓN, DE MEDICINA LEGAL Y CIENCIAS FORENSES		
CODIGO:	**FORMULARIO ÚNICO DE CADENA DE CUSTODIA PARA INDICIOS Y/O CONTENIDO DIGITAL**	
Edición N° 01		**Pág. 1**

INFORMACIÓN GENERAL

Institución, (o persona):	
Servidor que interviene:	
Lugar del Hecho	
Zona/Sub zona:	Distrito:
Circuito: Las Cuadras	Sub circuito:
Dirección:	Coordenadas:
Fecha:	Hora:
Tipo de hecho:	Autoridad: Fiscal de Turno.

INDENTIFICACIÓN DE INDICIOS Y EVIDENCIA DIGITAL

Tipo de Elemento:		Nro. indicio:		Categoría:	Sistema Informático: ( )
Marca:		Modelo:			Dispositivo de almacenamiento: ( )
Nro. Serie:		Color:			Dispositivo telemático: ( )
IMEI:		IP/MAC:			Dispositivo móvil: ( )
Capacidad almacenamiento:					Sistema basado en nube: ( )
Estado de pantalla:	Bloqueado BFU ( ) Desbloqueado AFU ( )				Tecnología disruptiva (IOT/IA/Blockchain): ( )
Estado de hallazgo:	Encendido ( ) Apagado ( ) Hibernación ( ) Con daño físico ( )				
Descripción del daño físico:					

Localización física en la escena:					
Detalle del indicio y periféricos conectados:					
Medidas de seguridad aplicadas					
Aislamiento Electromagnético:	Modo de avión activado: ( )			Inhibidor de señal: ( )	
	Funda Faraday: ( )			Papel aluminio: ( )	
Sellado de puertos: ( )		Banco de energía: ( )			
Embalaje utilizado:		Cinta/sello:		Sellado por:	

TIPO DE ADQUISICIÓN REALIZADA

MODALIDAD		MÉTODO	
Adquisición in situ:		Imagen forense (adquisición física):	
		Imagen forense (adquisición lógica):	
Adquisición en laboratorio:		Duplicación forense:	
		Extracción física:	
Triaje previo realizado:		Extracción lógica:	
		Extracción manual:	
Volcado de memoria RAM:		Copia de seguidad/Backup:	
		Adquisición de sitios y páginas web:	
Herramientas utilizadas:			

VERIFICACIÓN DE INTEGRIDAD – VALORES HASH

Algoritmo	Valor Hash original	Valor Hash verificación	Coincidencia

TRAZABILIDAD DE INTERVINIENTES / MOVIMIENTO DE INDICIOS Y/O EVIDENCIAS

	INSTITUCIÓN	GRADO/NOMBRES Y APELLIDOS	C.C./C.I./PA	MOTIVO	FIRMA DE RESPONSABILIDAD
ENTREGA				Custodia ☐ Peritaje ☐ Traspaso ☐	
RECIBE				Devolución ☐	
ENTREGA: FECHA Y HORA:			OFICIO:		
OBSERVACIONES:.....					
	INSTITUCIÓN	GRADO/NOMBRES Y APELLIDOS	C.C./C.I./PA	MOTIVO	FIRMA DE RESPONSABILIDAD
ENTREGA				Custodia ☐ Peritaje ☐ Traspaso ☐	
RECIBE					
ENTREGA: FECHA Y HORA:			OFICIO:		
OBSERVACIONES:.....					