Resolución Ministerial

N° 0066-2026-IN

Lima, 21 ENE 2026

VISTO; el Informe N° 000690-2025-IN-VOI-DGCO-DCO de la Dirección Contra Delitos de Crimen Organizado de la Dirección General Contra el Crimen Organizado del Ministerio del Interior; el Informe N° 000137-2025-DIRASJUR-DIVDJPN/PNP de la Dirección de Asesoría Jurídica de la Policía Nacional del Perú; el Informe N° 000015-2026-IN-OGPP-OMD de la Oficina de Modernización y Desarrollo Institucional de la Oficina General de Planeamiento y Presupuesto; el Memorando N° 000063-2026-IN-OGPP de la Oficina General de Planeamiento y Presupuesto; y, el Informe N° 000190-2026-IN-OGAJ de la Oficina General de Asesoría Jurídica y,

CONSIDERANDO:

Que, el artículo 1 de la Constitución Política del Perú establece que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado;

Que, el artículo 44 de la Constitución Política del Perú, establece que son deberes primordiales del Estado: defender la soberanía nacional, garantizar la plena defensa de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación;

Que, en el artículo 166 de la Carta Magna, prescribe que la Policía Nacional del Perú tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Prestar protección y ayuda a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras;

Que, la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, garantiza el derecho fundamental a la protección de los datos personales, previstos en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen;

Que, la Ley N° 30096, Ley de Delitos Informáticos, tiene por objeto prevenir y sancionar las conductas ilícitas de delitos cometidos utilizando las tecnologías de la información y las comunicaciones, que vulneran no solo los sistemas y datos informáticos, sino también otros bienes jurídicos penalmente relevantes con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia;

Que, mediante Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú, se establece la estructura, organización, competencias, funciones y atribuciones de la Policía Nacional del Perú, así como sus regímenes especiales. Depende del Ministerio del Interior; con competencia administrativa y operativa para el ejercicio de la función policial en todo el territorio nacional, en concordancia con el artículo 166 de la Constitución Política del Perú;

Que, el artículo 224 del Reglamento del Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú, aprobado por Decreto Supremo N° 012-2025-IN, determina que la Dirección de Investigación de Cibercrimen es la unidad orgánica especializada, de carácter sistémico, técnico-normativo y operativo; responsable de proponer, formular, aprobar, planificar, coordinar, comandar, ejecutar, supervisar y evaluar las actividades y operaciones policiales de prevención, investigación, combate y denuncia de los Delitos Contra el Patrimonio (delitos informáticos), Delitos Contra La Libertad (violación del secreto de las comunicaciones, violación de la intimidad - uso indebido de archivos computarizados -) previstos en el Código Penal y leyes penales especiales; las conductas previstas como ciberdelitos en los convenios internacionales en materia de cibercrimen suscritos por el Perú, los delitos cometidos por medio de las tecnologías de la información y comunicación, y las tecnologías emergentes; así como realizar acciones de localización y geolocalización de terminales móviles;

Que, en el marco de las disposiciones legales antes referidas, se evidencia la necesidad de contar con un documento orientador, siendo este, una guía, que coadyuve al personal policial para el desarrollo de las investigaciones especializadas en materia de delitos informáticos;

Que, la Guía para la investigación de los Delitos Informáticos, tiene como objetivo principal establecer lineamientos que orienten el accionar de la Policía Nacional del Perú en la prevención, detección, investigación y persecución de los delitos informáticos, en concordancia con el marco legal vigente y los estándares internacionales en la materia;

Que, conforme a lo señalado en los documentos de vistos, resulta necesario aprobar la Guía para la investigación de los Delitos Informáticos, que brindará al personal policial una herramienta completa con procedimientos técnicos que servirán de apoyo, al personal policial en las investigaciones relacionadas con la Ley N° 30096 - Ley de Delitos Informáticos y sus modificatorias, así como con la legislación penal y los convenios internacionales que el Perú ha suscrito;

Con el visado del Despacho Viceministerial de Orden Interno, de la Comandancia General de la Policía Nacional del Perú, de la Dirección General Contra el Crimen Organizado, de la Oficina General de Planeamiento y Presupuesto y de la Oficina General de Asesoría Jurídica del Ministerio del Interior; y,

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; el Decreto Legislativo N° 1266, Ley de Organización y Funciones del Ministerio del Interior; y el Reglamento de Organización y Funciones del Ministerito del Interior, aprobado por Resolución Ministerial N° 1520-2019-IN;

SE RESUELVE:

Artículo 1.- Aprobar la "Guía para la investigación de los Delitos Informáticos", que como Anexo forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Disponer la publicación de la presente Resolución Ministerial y su Anexo en la sede digital del Ministerio del Interior (www.mininter.gob.pe) y de la Policía Nacional del Perú (www.policia.gob.pe).

Regístrese y comuníquese.

VICENTE TIBURCIO ORBEZO
Ministro del Interior

PERÚ | Ministerio del Interior

Páginas: 140

Resolución N° 0066-2026-IN

Fecha de Aprobación: 21 ENE 2026

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"

MINISTERIO DEL INTERIOR

"GUÍA PARA LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS"

V°B° J. DE LA CRUZ Q.

ÍNDICE

OBJETIVO 4
FINALIDAD 4
ALCANCE 4
BASE LEGAL 4
PRESENTACIÓN 6
CAPITULO I 7
LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS 7
1.1. Procedimiento de Investigación de los Delitos Informáticos 7
1.2. Diligencias para investigación de los delitos informáticos 8
1.2.1. Delito contra el Patrimonio - Fraude Informático (Transferencias Ilícitas de dinero vía internet) 8
1.2.2. Delito Informático contra la Fe Pública – Suplantación de identidad. 17
1.2.3. Delito contra la integridad de datos y sistemas informáticos 20
1.2.4. Delito contra la Indemnidad Sexual de Menores 22
1.2.5. Delito de préstamo informático extorsivo 25
CAPÍTULO II 29
TRATAMIENTO DE INFORMACIÓN DE PERFILES DE USUARIOS DE REDES SOCIALES 29
2.1. Procedimiento de identificación e individualización de perfiles de usuarios de redes sociales 29
2.1.1. Identificando e individualizando un perfil de Facebook 29
2.1.2. Identificando e individualizando un perfil de Instagram 32
2.1.3. Identificando e individualizando un perfil de WhatsApp 37
2.1.4. Identificando e individualizando un perfil de TikTok 38
2.2. Procedimiento para preservación de información en redes sociales 39
2.2.1. Preservación para perfiles de Facebook e Instagram 40
2.2.2. Preservación para perfiles de WhatsApp 44
2.2.3. Preservación para perfiles de TikTok 49
2.3. Procedimiento de solicitud de registros de información en redes sociales. 56
2.3.1. Procedimientos para *Facebook* e *Instagram* 56
2.3.2. Procedimientos para *WhatsApp* 60
2.3.3. Procedimientos para *TikTok* 64
2.4. Solicitud de registro con Resolución Judicial 65
2.4.1. Procedimientos para Facebook e Instagram 65
2.4.2. Procedimientos para *WhatsApp* 67

2.4.3. Procedimientos para *TikTok* 69
CAPÍTULO III 71
PROCEDIMIENTOS PARA PRESERVAR UNA PÁGINA WEB Y/O DOMINIO WEB 71
3.1. Uso del software HTTRACK Website Copier 71
3.1.1. Descarga e Instalación del software HTTRACK Website Copier 71
3.1.2. Configuración del software HTTRACK Website Copier para descargar página web y/o sitios web 76
3.1.3. Verificación de la descarga y preservación de la página web y/o sitio *web* 82
3.2. Procedimiento para obtener información sobre dominios web y direcciones IP 85
3.2.1. Obtención de información técnica de sitios *web* 86
3.2.2. Obtención de información técnica de direcciones IP 88
CAPÍTULO IV 90
ASEGURAMIENTO DE LA EVIDENCIA DIGITAL 90
4.1. Aspectos legales 90
4.1.1. Resolución N° 729-2006-MP-FN del 15 junio del 2006 90
4.1.2. Decreto Supremo N° 010-2018-JUS del 25 de agosto del 2018 90
4.2. Fases para el aseguramiento de la evidencia digital 91
4.2.1. Fase inicial 91
4.2.2. Fase de ejecución 92
BIBLIOGRAFÍA 127
ANEXOS 128
Anexo I Definición de Términos 128
Anexo II 133
Anexo III 134
Anexo IV 135
Anexo V 136
Anexo VI 137
Anexo VII 138
Anexo VIII 139
Anexo IX 140

S. DE LA CRUZ Q.

"GUÍA PARA LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS"

OBJETIVO

Establecer lineamientos que orienten el accionar de la Policía Nacional del Perú en la prevención, detección, investigación y persecución de los delitos informáticos, en concordancia con el marco legal vigente y los estándares internacionales en la materia.

FINALIDAD

Brindar al personal policial una herramienta que contenga los procedimientos técnicos-operativos que sirvan en las investigaciones policiales por hechos delictivos sancionados en la Ley N° 30096-Ley de Delitos Informáticos y su modificatoria Ley N° 30171[1], el Código Penal y convenios internacionales de los que el Perú es parte.

ALCANCE

La presente guía está diseñada para fortalecer las capacidades operativas y técnicas de la Policía Nacional del Perú en materia de investigación de delitos informáticos, contribuyendo a la prevención, detección y neutralización de las diversas manifestaciones de la criminalidad organizada que hacen uso de la tecnología para la comisión del delito.

BASE LEGAL

Normativa internacional:

1. Convenio contra la Ciberdelincuencia (Budapest-2019).

Normativa nacional:

1. Constitución Política del Perú, artículo N° 166.
2. Ley N° 29733, Ley de Protección de Datos Personales.
3. Ley N° 29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
4. Ley N° 30077, Ley Contra el Crimen Organizado.
5. Ley N° 30096, Ley de Delitos Informáticos.
6. Ley N° 30171, que modifica la Ley N° 30096, Ley de Delitos Informáticos.
7. Ley N° 31146, Ley que modifica el Código Penal, el Código Procesal Penal y la Ley N° 28950, Ley contra la Trata de Personas y Tráfico Ilícito de Migrantes, con la finalidad de sistematizar los artículos referidos a los delitos de trata de personas y de explotación, y considerarlos estos delitos contra la indemnidad humana.
8. Ley N° 32130, Ley que modifica el Código Procesal Penal, Decreto Legislativo 957, para fortalecer la investigación del delito como función de la Policía Nacional del Perú y agilizar los procesos penales.
9. Ley N° 32183, Ley que modifica el Código Penal para incorporar la modalidad de préstamos extorsivos en el tipo penal de extorsión.
10. Decreto Legislativo N° 635, Código Penal (Art. 129-M).

[1] Publicada el 10 de marzo de 2014, en el diario oficial "El Peruano".

11. Decreto Legislativo N° 957, Nuevo Código Procesal Penal.
12. Decreto Legislativo N° 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.
13. Decreto Legislativo N° 1267 Ley de la Policía Nacional del Perú y su modificatoria Ley N° 31379.
14. Decreto Legislativo Nº 1338, que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana.
15. Decreto Legislativo N° 1412- que aprueba la Ley de Gobierno Digital.
16. Decreto Legislativo N° 1614, que modifica la Ley Nº 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la ciberdelincuencia.
17. Decreto Legislativo N° 1625, que modifica los artículos 154-B y 158 del Código Penal e incorpora el artículo 5-A en la Ley N° 30096, Ley de Delitos Informáticos para fortalecer el marco normativo sobre el uso de tecnologías digitales relacionado a la difusión de imágenes, materiales audiovisuales o audios con contenido sexual.
18. Decreto Supremo Nº 090-2013-EF, Reglamento de la Ley Nº 29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
19. Decreto Supremo Nº 012-2025-IN, que aprueba el Reglamento del Decreto Legislativo N° 1267 Ley de la Policía Nacional del Perú.
20. Decreto Supremo Nº 007-2019-IN, Reglamento Decreto Legislativo Nº 1338, que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana
21. Decreto Supremo N° 17-2019-IN, que aprueba la Política Nacional Multisectorial de lucha contra el Crimen Organizado 2019-2030.
22. Resolución de la Fiscalía de la Nación N° 729-2016-MP-FN, Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados.
23. Resolución Ministerial N° 848-2019-IN, que aprueba el Manual para el Recojo de la Evidencia Digital.
24. Resolución Directoral N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016, que aprueba el Manual de Documentación Policial.
25. Resolución de Comandancia General de la Policía Nacional del Perú - RGC N.º 79-2024-CG-PNP/EMG, del 09MAR2024, que aprueba el Manual de Análisis de Evidencia Digital

PRESENTACIÓN

Desde la masificación del internet, se ha transformado profundamente la educación, el comercio y la participación ciudadana, pero también ha aparecido nuevos riesgos como la pérdida de privacidad, la manipulación de información y la ciberdelincuencia. Organismos internacionales como UNESCO, CEPAL y el Foro Económico Mundial vienen advirtiendo sobre la necesidad de regulaciones sólidas y estrategias contra la concentración de poder en grandes corporaciones tecnológicas.

En América Latina, el acceso desigual a la conectividad persiste, afectando principalmente a sectores vulnerables. La arquitectura abierta de internet y la ausencia de un sistema global de verificación de identidad facilitan la suplantación y el fraude digital. Esto ha permitido que la ciberdelincuencia se expanda a escala transnacional, afectando bienes jurídicos fundamentales.

En Perú, las denuncias por delitos informáticos como suplantación de identidad, fraude, extorsión digital y difusión no consentida de imágenes se han incrementado desde 2018, intensificándose durante la pandemia. La respuesta estatal exige fortalecer la ciberseguridad pública, actualizar el marco legal y promover educación digital preventiva.

El auge del internet, los teléfonos inteligentes y la digitalización de servicios financieros, laborales y personales, surgieron nuevas formas de criminalidad que afectan tanto a individuos como a empresas. El fraude bancario electrónico, el ciberacoso, la extorsión virtual o la difusión no consentida de imágenes íntimas no solo causan daños económicos, sino también psicológicos y sociales profundos.

La promulgación de la Ley N° 30096, tipifico los delitos informáticos y alineo la legislación penal a los estándares internacionales establecidos en la Convención de Budapest. Esta norma busca proteger derechos fundamentales en el entorno digital y facilitar la cooperación judicial transnacional.

Las acciones contra el hackeo de sistemas, la interceptación de comunicaciones digitales, el uso malicioso de datos personales o la suplantación de identidad en redes sociales carecían de una regulación precisa. Este vacío limitaba las posibilidades de intervención efectiva por parte de la Policía Nacional y el Ministerio Público, lo cual colocaba en situación de indefensión a las víctimas.

La presente Guía para la investigación de los Delitos Informáticos, elaborada con apoyo de la Unión Europea, brinda técnicas y procedimientos actualizados para la Policía Nacional del Perú en la investigación de ciberdelitos que asegure la utilización de altos estándares en procedimientos técnicos y científicos para la obtención de la prueba digital.

La guía está estructurada en cuatro capítulos que comprenden: la investigación de los delitos informáticos, el tratamiento de información de los perfiles de usuarios de redes sociales, los procedimientos para preservar una página web y/o dominio web y el aseguramiento de la evidencia digital. Todo ello, garantiza un trabajo ordenado, minucioso y el éxito en las investigaciones, sin perder de vista el respeto de los principios procesales y los derechos fundamentales, que no sólo han costado tanto conseguir, sino que, su vulneración echaría a perder los diligentes esfuerzos de la policía en enfrentar los flagelos de la criminalidad en sus diferentes modalidades.

CAPÍTULO I

LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS

La presente Guía, contiene aspectos técnicos y operativos que son aplicables en la investigación policial de los delitos informáticos; con observancia de la normativa vigente; a fin de garantizar la protección y tratamiento de la evidencia digital, así como la eficacia del proceso de la investigación policial.

> *"La legalidad, la panoplia que conocemos como "debido proceso", la presunción de inocencia, la intimidad, entre otros, son elementos constitutivos de cualquier Estado de derecho que, si no se respetan rigurosamente echarán a perder los más denodados esfuerzos policiales" aspectos que sin duda son esenciales considerar cuando se pretende introducir una nueva política criminal con el ánimo de asegurar un mínimo normativo común que brinde previsión normativa al sistema de justicia en general*[2].

1.1. Procedimiento de Investigación de los Delitos Informáticos

Para la investigación de los delitos informáticos se puede considerar la secuencia propuesta, pudiendo considerarse otras diligencias de acuerdo con la modalidad y naturaleza del delito investigado conforme al avance tecnológico, los siguientes puntos:

a. Conocimiento del Hecho
b. Recepción de denuncia
c. Comunicación de la denuncia al Ministerio Público.
d. Diligencias urgentes e inaplazables.
e. Realizar las diligencias dispuestas por el Ministerio Público.
f. Desarrollo de la investigación.
g. Elaboración del documento policial correspondiente.

Preguntas generales para la recepción de denuncias por delito informático.
Estas preguntas específicas permiten ampliar el pliego interrogatorio para el esclarecimiento de los hechos materia de investigación.

i. Indique Ud. ¿Cómo tuvo conocimiento del hecho?
ii. Indique Ud. ¿Cuál es el nombre de la red social, aplicativo de mensajería instantánea, página web, correo electrónico o sala de chat, donde fue o presume, que fue víctima del delito?
iii. Indique Ud. ¿Cuál ha sido la dirección(es) de correo electrónico empleada(s) en dicha página web?
iv. Señale Ud. ¿Desde cuándo y cómo ha notado alguna actividad inusual en sus cuentas y/o redes sociales?
v. Indique Ud. ¿Si ha recibido notificaciones o alertas de seguridad (por parte de la plataforma o la entidad financiera) antes o después del incidente?
vi. Indique Ud. ¿Cuáles han sido las cuentas y/o redes sociales comprometidas y/o afectadas?

[2] BUSTAMANTE RÚA, Mónica María. Cibercriminalidad e investigación penal tecnológica. Una mirada desde la experiencia de la Cooperación Internacional para la persecución de la cibercriminalidad en Latinoamérica. Palestra, abril 2023.

vii. Indique Ud. ¿cuáles han sido los nombres de usuario (*nicknames*) u otros datos utilizados por la víctima y por el presunto autor?
viii. ¿Puede Ud. identificar y/o determinar la dirección electrónica del perfil de la red social o página web utilizada por el presunto autor?
ix. ¿Puede Ud. señalar si existe alguna respuesta, comunicación o intercambio de información por parte del presunto autor del delito?
x. Indique Ud. ¿si han sido afectadas sus cuentas bancarias (crédito y/o débito), de ser así desde cuándo?
xi. Indique Ud. ¿Presume a que teleoperadora pertenece el número del que recibió las llamadas o mensajes de la entidad financiera relacionada a su cuenta bancaria afectada?
xii. ¿Puede Ud. presentar los reportes o movimientos de las operaciones financieras no reconocidas por su persona que son materia de investigación?
xiii. Indique Ud. ¿cuándo fue la última vez que realizo operaciones físicas y/o virtuales con su tarjeta electrónica bancaria?
xiv. Indique Ud. ¿Cuál es el medio tecnológico utilizado por su persona mediante el cual realiza sus operaciones financieras (compras y/o transferencias por internet)?
xv. ¿Señale Ud. cuál es su proveedor de servicios de internet (ISP) u operadora de telefonía móvil?
xvi. ¿Indique Ud. si registra evidencia de los mensajes, correos electrónicos, números telefónicos, capturas de pantallas entre otros que sustenten su denuncia?
xvii. Otras preguntas que el funcionario considere pertinentes para la pesquisa.

S. DE LA CRUZ Q.

1.2. Diligencias para investigación de los delitos informáticos

1.2.1. Delito contra el Patrimonio - Fraude Informático (Transferencias Ilícitas de dinero vía internet).

Forma delictiva que tiene como fin el tener acceso a la información sensible de la víctima, para realizar operaciones fraudulentas con el empleo de herramientas tecnológicas que facilitan la comisión de indicado acto ilícito.
Sus modalidades son:

1.2.1.1. PHISHING - SMISHING

a. Recepción de denuncia

El efectivo policial, al entrevistarse con el agraviado, puede realizar las siguientes preguntas y acciones:

- Indique Ud. ¿ha recibido correos electrónicos, mensaje de texto u otros a través de aplicaciones de mensajería instantánea con direcciones electrónicas (URL) inusuales?
- Indique Ud. ¿ha ingresado a una página web o dirección electrónica de la entidad financiera donde es cliente, donde ingresó sus datos personales como número de tarjetas, clave o código de verificación?
- ¿Podría Ud. identificar cuál es el enlace o *link* donde ingresó?

- ¿Cómo tomó conocimiento de las operaciones no reconocidas (fraudulentas)?
- Indique Ud. la fecha y hora de registro de las transferencias no reconocidas (fraudulentas).
- Indique Ud. Si tiene los reportes de los últimos movimientos de su cuenta y hoja de reclamación del banco.
- Identifique Ud. las cuentas receptoras y los montos sustraídos.

b. Comunicación al Ministerio Público.

El instructor comunica la denuncia al Ministerio Público, de forma inmediata, sin exceder en ningún caso, el plazo legal correspondiente.

c. Diligencias urgentes e inaplazables

- Preservar la evidencia digital *(copia de los videos de seguridad, captura de pantalla, identificar direcciones web, URL e ID de redes sociales)*, cuentas de redes sociales incriminadas, captura de información volátil, entre otros, a fin de que estas no sean eliminadas, suprimidas o adulteradas por el delincuente informático.
- De ser necesario evalúa la incautación.
- El personal policial realiza las actas respectivas en presencia del agraviado.
- Otras diligencias necesarias para la investigación (geolocalización, solicitud de información a OSIPTEL, entre otras).
- Dar cumplimiento a las diligencias dispuestas por el Ministerio Público conforme a lo establecido en los dispositivos legales vigentes.

d. Desarrollo de la investigación policial.

- Tomar la declaración del agraviado; al momento de recibir la declaración especificar la fecha y hora, a fin de tener en cuenta si existe flagrancia delictiva y que narre detalladamente los hechos sucedidos.
- Identificar la dirección electrónica fraudulenta (URL) así como la ID, de existir un perfil de red social involucrado.
- Mediante una carta de autorización de la parte agraviada, solicitar a las entidades financieras información de las operaciones bancarias (IP con huso horario, correos eléctricos, teléfono, datos personales y otros) de las cuentas afectadas y las grabaciones de video vigilancia.
- Solicitar se practique la pericia o el análisis informático forense de los equipos involucrados, a fin de corroborar el rastro de páginas fraudulentas (Phishing), debiendo contar con autorización del titular del equipo o autorización judicial.
- Solicitar las medidas limitativas del secreto bancario relacionado a: (se adjunta formato modelo en el anexo II y III).
  - Detalles de las operaciones ilícitas – donde se especifican los titulares de las cuentas beneficiarias (receptoras) y así como las direcciones IP y códigos IMEI de donde se generaron las transacciones fraudulentas.
  - Detalles sobre el estado de cuenta receptoras, así como registro de sus datos personales, líneas telefónicas y correos electrónicos vinculados.

- Solicitar las medidas limitativas del secreto de las comunicaciones y documentos privados relacionados a: (utilizar el formato del anexo IV)
  - Datos de filiación de los titulares de los registros IP y códigos IMEI de las transacciones fraudulentas.
  - Datos de filiación de los titulares de los abonados telefónicos asociado a la cuenta receptora.
  - Datos de filiación de los usuarios de correos electrónicos asociados a la cuenta receptora.
  - Datos de filiación de los perfiles de usuarios en plataformas de redes sociales asociados a la cuenta receptora.

e. Elaboración del informe policial[3].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

1.2.1.2. FAKE APP

a. Recepción de denuncia.

El efectivo policial, al entrevistarse con el agraviado, puede realizar las siguientes preguntas y acciones:

- Indique Ud. ¿Si ha recibido algún mensaje donde le ofrecen algún tipo de préstamo y usted tenga que descargar algún archivo o ingresar a alguna página *web* desconocida?

- Indique Ud. ¿ha recibido correos electrónicos, mensaje de texto u otros a través de aplicaciones de mensajería instantánea con direcciones electrónicas (URL) inusuales?
- Indique Ud. ¿ha ingresado a una página *web* o dirección electrónica de la entidad financiera donde es cliente, donde ingresó sus datos personales como número de tarjetas, clave o código de verificación?
- ¿Podría Ud. identificar cuál es el enlace o *link* donde ingresó?
- ¿Cómo tomó conocimiento de las operaciones no reconocidas (fraudulentas)?
- Indique Ud. la fecha y hora de registro de las transferencias no reconocidas (fraudulentas).
- Indique Ud. Si tiene los reportes de los últimos movimientos de su cuenta y hoja de reclamación del banco.
- Identifique Ud. las cuentas receptoras y los montos sustraídos.

b. Comunicación al Ministerio Público.

El efectivo policial comunica la denuncia al Ministerio Público, de forma inmediata, sin exceder en ningún caso, el plazo legal correspondiente.

[3] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/7716945/6529039-manual-de-documentacion-policial.pdf

c. Diligencias urgentes e inaplazables

- Realizar la preservación de la cuenta de usuario en la plataforma de mensajería instantánea *WhatsApp*, para poder conservar a la información que pueda ser utilizada para las investigaciones.

- Preservar la evidencia digital *(copia de los videos de seguridad, captura de pantalla, identificar direcciones web, URL e ID de redes sociales)*, cuentas de redes sociales incriminadas, captura de información volátil, entre otros, a fin de que estas no sean eliminadas, suprimidas o adulteradas por el delincuente informático.

- De ser necesario evalúa la incautación.

- El efectivo policial realiza las actas respectivas en presencia del agraviado.
- Otras diligencias necesarias para la investigación (geolocalización, solicitud de información a OSIPTEL, entre otras).
- Dar cumplimiento a las diligencias dispuestas por el Ministerio Público.

S. DE LA CRUZ Q.

d. Desarrollo de la investigación policial.

- Tomar la declaración del agraviado; al momento de recibir la declaración especificar la fecha y hora, a fin de tener en cuenta si existe flagrancia delictiva y que narre detalladamente los hechos sucedidos.

- Identificar la dirección electrónica fraudulenta (URL) así como la ID, de existir un perfil de red social involucrado.

- Mediante una carta de autorización de la parte agraviada, solicitar a las entidades financieras información de las operaciones bancarias (IP con huso horario, correos eléctricos, teléfono, datos personales y otros) de las cuentas afectadas y las grabaciones de video vigilancia.

- Solicitar se practique la pericia o el análisis informático forense de los equipos involucrados, a fin de corroborar el rastro de páginas fraudulentas (*Phishing*), debiendo contar con autorización del titular del equipo o autorización judicial.

- Solicitar las medidas limitativas del secreto bancario relacionado a: (Se adjunta formato modelo en el anexo II y III).

  - Detalles de las operaciones ilícitas – donde se especifican los titulares de las cuentas beneficiarias (receptoras) y así como las direcciones IP y códigos IMEI de donde se generaron las transacciones fraudulentas.

  - Detalles sobre el estado de cuenta y movimientos de las cuentas receptoras, así como registro de sus datos personales, líneas telefónicas y correos electrónicos vinculados.

JURISPOL

- Solicitar las medidas limitativas del secreto de las comunicaciones y documentos privados relacionados a: (utilizar el formato del anexo IV)

  - Datos de filiación de los titulares de los registros IP y códigos IMEI de las transacciones fraudulentas.
  - Datos de filiación de los titulares de los abonados telefónicos asociado a la cuenta receptora.
  - Datos de filiación de los usuarios de correos electrónicos asociados a la cuenta receptora.
  - Datos de filiación de los perfiles de usuarios en plataformas de redes sociales asociados a la cuenta receptora.

e. Elaboración del informe policial[4].

Elaborar el documento policial, de acuerdo a lo establecido en el articulo 332 del D. Leg. N° 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

S. DE LA CRUZ Q.

1.2.1.3. THIEF TRANSFER

a. Recepción de denuncia.

El efectivo policial, al entrevistarse con el agraviado, debe realizar las siguientes preguntas y acciones:

- Indique Ud. ¿En qué parte o ubicación fue sustraída de su equipo móvil y en que circunstancia sucedió dicho evento delictivo?
- Indique Ud. ¿Indique usted que después del hecho noto algún tipo de modificaciones en sus cuentas de usuario que tiene en sus aplicaciones de su teléfono móvil?
- ¿Podría Ud. identificar si se efectuaron operaciones fraudulentas desde sus cuentas bancarias afiliadas a su móvil?
- Indique Ud. ¿Tiene usted conocimiento de la existencia de envios de mensajes enviados de sus cuentas de redes sociales a sus contactos?
- ¿Cómo tomó conocimiento de las operaciones no reconocidas (fraudulentas)?
- Indique Ud. la fecha y hora de registro de las transferencias no reconocidas (fraudulentas).
- Indique Ud. Si tiene los reportes de los últimos movimientos de su cuenta y hoja de reclamación del banco.

[4] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771694/5529039-manual-de-documentacion-policial.pdf

JURISPOL

- Identifique Ud. las cuentas receptoras y los montos sustraídos.

b. Comunicación al Ministerio Público.

El efectivo policial comunica la denuncia al Ministerio Público, de forma inmediata, sin exceder en ningún caso, el plazo legal correspondiente.

c. Diligencias urgentes e inaplazables

- El efectivo policial realiza las actas respectivas en presencia del agraviado.
- Otras diligencias necesarias para la investigación (geolocalización, solicitud de información a OSIPTEL, entre otras).
- Dar cumplimiento a las diligencias dispuestas por el Ministerio Público.

d. Desarrollo de la investigación policial.

- Tomar la declaración del agraviado; al momento de recibir la declaración especificar la fecha y hora, a fin de tener en cuenta si existe flagrancia delictiva y que narre detalladamente los hechos sucedidos.
- Identificar las cuentas bancarias que fueron destinadas para el cobro indebido de las solicitudes de dinero y operaciones no reconocidas.
- Mediante una carta de autorización de la parte agraviada, solicitar a las entidades financieras información de las operaciones bancarias (IP con huso horario, correos eléctricos, teléfono, datos personales y otros) de las cuentas afectadas y las grabaciones de video vigilancia.

- Solicitar las medidas limitativas del secreto bancario relacionado a: (utilizar el formato del anexo II y III).
  - Detalles de las operaciones ilícitas – donde se especifican los titulares de las cuentas beneficiarias (receptoras) y así como las direcciones IP y códigos IMEI de donde se generaron las transacciones fraudulentas.
  - Detalles sobre el estado de cuenta y movimientos de los beneficiarios (cuentas receptoras), así como registro de sus datos personales, líneas telefónicas y correos electrónicos vinculados.

- Solicitar las medidas limitativas del secreto de las comunicaciones y documentos privados relacionados a: (utilizar el formato del anexo IV)
  - Datos de filiación de los titulares de los registros IP y códigos IMEI de las transacciones fraudulentas.
  - Datos de filiación de los titulares de los abonados telefónicos asociado a la cuenta receptora.
  - Datos de filiación de los usuarios de correos electrónicos asociados a la cuenta receptora.
  - Datos de filiación de los perfiles de usuarios en plataformas de redes sociales asociados a la cuenta receptora.

V°B°
S. DE LA CRUZ Q.

JURISPOL

e. Elaboración del informe policial[5].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

1.2.1.4. SIM SWAPPING

a. Recepción de denuncia.

El efectivo policial, al entrevistarse con el agraviado, debe realizar las siguientes preguntas y acciones:

- Indique Ud. ¿ha recibido correos electrónicos, mensaje de texto u otros a través de aplicaciones de mensajería instantánea con direcciones electrónicas (URL) inusuales?
- Indique Ud. ¿ha ingresado a una página web o dirección electrónica de la entidad financiera donde es cliente, donde ingresó sus datos personales como número de tarjetas, clave o código de verificación?
- ¿Podría Ud. identificar cuál es el enlace o *link* donde ingresó?
- ¿Indique usted si tomo conocimiento de que su línea telefónica no se encontraba operativa?
- ¿De ser el caso, tuvo alguna respuesta de la empresa prestadora de servicios de telecomunicaciones?
- ¿Cómo tomó conocimiento de las operaciones no reconocidas (fraudulentas)?
- Indique Ud. la fecha y hora de registro de las transferencias no reconocidas (fraudulentas).
- Indique Ud. Si tiene los reportes de los últimos movimientos de su cuenta y hoja de reclamación del banco.
- Identifique Ud. las cuentas receptoras y los montos sustraídos.

b. Comunicación al Ministerio Público.

El efectivo policial comunica la denuncia al Ministerio Público, de forma inmediata, sin exceder en ningún caso, el plazo legal correspondiente.

c. Diligencias urgentes e inaplazables

- Preservar la evidencia digital *(copia de los videos de seguridad, captura de pantalla, identificar direcciones web, URL e ID de redes sociales)*, cuentas de redes sociales incriminadas, captura de información volátil, entre otros, a fin de que estas no sean eliminadas, suprimidas o adulteradas por el delincuente informático.
- De ser necesario evalúa la incautación.
- El efectivo policial realiza las actas respectivas en presencia del agraviado.
- Otras diligencias necesarias para la investigación (geolocalización, solicitud de información a OSIPTEL, entre otras).
- Dar cumplimiento a las diligencias dispuestas por el Ministerio Público.

V°B° S. DE LA CRUZ Q.

JURISPOL

[5] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771594/5529039-manual-de-documentacion-policial.pdf

d. Desarrollo de la investigación policial.

- Tomar la declaración del agraviado; al momento de recibir la declaración especificar la fecha y hora, a fin de tener en cuenta si existe flagrancia delictiva y que narre detalladamente los hechos sucedidos.
- Identificar la dirección electrónica fraudulenta (URL) así como la ID, de existir un perfil de red social involucrado.
- Mediante una carta de autorización de la parte agraviada, solicitar a las entidades financieras información de las operaciones bancarias (IP con huso horario, correos eléctricos, teléfono, datos personales y otros) de las cuentas afectadas y las grabaciones de video vigilancia.
- Solicitar las medidas limitativas del secreto bancario relacionado a: (Se adjunta modelo de formato en anexo II y III).

  - Detalles de las operaciones ilícitas – donde se especifican los titulares de las cuentas beneficiarias (receptoras) y así como las direcciones IP y códigos IMEI de donde se generaron las transacciones fraudulentas.
  - Detalles sobre el estado de cuenta y movimientos de las cuentas receptoras, así como registro de sus datos personales, líneas telefónicas y correos electrónicos vinculados.

- Solicitar las medidas limitativas del secreto de las comunicaciones y documentos privados relacionados a: (utilizar el formato del anexo IV)
  - Datos del usuario que realizó el registro de reposición de chip a nombre de la parte agraviada y lugar donde se efectuó.
  - Datos de filiación de los titulares de los registros IP y códigos IMEI de las transacciones fraudulentas.
  - Datos de filiación de los titulares de los abonados telefónicos asociado a la cuenta receptora.
  - Datos de filiación de los usuarios de correos electrónicos asociados a la cuenta receptora.
  - Datos de filiación de los perfiles de usuarios en plataformas de redes sociales asociados a la cuenta receptora.

e. Elaboración del informe policial[6].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

1.2.1.5. CARDING (compras fraudulentas por internet y vía telefónica).

a. Recepción de denuncia.

El efectivo policial, al entrevistarse con el agraviado debe realizar las siguientes preguntas:

[6] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771694/6529039-manual-de-documentacion-policial.pdf

- ¿Cómo Ud. tuvo conocimiento sobre las operaciones fraudulentas?
- Registrar la fecha y hora de las compras o pagos fraudulentos.
- Solicitar información sobre los reportes de los últimos movimientos de su cuenta y hoja de reclamación del banco.
- Identifica a él/los beneficiarios(s) de las operaciones fraudulentas.
- Preguntar al agraviado respecto a los últimos establecimientos comerciales y/o sitios *web*, donde utilizó su tarjeta de crédito y/o débito.
- Si proporcionó su tarjeta electrónica bancaria físicamente o proporcionó los datos de esta, a terceras personas.

b. Diligencias urgentes e inaplazables.

- Preservar la evidencia digital *(copia de los videos de seguridad, captura de pantalla, identificar direcciones web, URL e ID de redes sociales).* Preservación de las cuentas de redes sociales incriminadas, captura de información volátil, entre otros, a fin de que estas no sean eliminadas, suprimidas o adulteradas por el delincuente informático. De ser necesario evalúa la incautación.
- Si se trata de contenido de información se debe generar el código *hash*, con la finalidad de preservar la cadena de custodia de la evidencia digital.



c. Comunicación al Ministerio Público.

El efectivo policial comunica la denuncia al Ministerio Público en forma inmediata.

d. Cumplimiento de las diligencias dispuestas por el Ministerio Público.

Dar cumplimiento a las diligencias dispuestas por el Ministerio Público conforme a lo establecido en los dispositivos legales vigentes.

e. Desarrollo de la investigación policial.

- Declaración del agraviado; al momento de recibir la declaración especifica la fecha y hora, a fin de tener en cuenta si existe flagrancia delictiva y que narre con lujo de detalles los hechos sucedidos.
- Visualización de equipos y cuentas de correo electrónico: Se recaba la información adicional que permita identificar el hecho delictivo y sus autores.
- Identificar las empresas y sitios *web* donde se realizaron las compras fraudulentas.
- Mediante carta de autorización del agraviado (titular de la cuenta), resolución judicial de levantamiento del secreto bancario se debe solicitar a las entidades financieras, centros comerciales, tiendas virtuales o plataformas digitales, información de las operaciones fraudulentas *(IP con huso horario de donde se realizaron las operaciones ilícitas, correos electrónicos, números telefónicos, datos personales y otros de los beneficiarios o receptores)*. (se adjunta modelo de formato en anexo II y III).
- Mediante resolución judicial de levantamiento del secreto de las comunicaciones se debe solicitar a las empresas proveedoras del servicio de internet y telefonía, los registros del titular de la dirección IP y/o de



código IMEI del dispositivo electrónico que efectuó la operación fraudulenta (se adjunta modelo de formato en anexo IV).

- Declaración del investigado, en presencia del representante del Ministerio Público y su abogado defensor, la cual debe realizarse tomando en consideración sus referencias policiales y/o antecedentes, así como las informaciones proporcionadas por las entidades comerciales, bancarias, telefonía e internet; debiendo realizar la verificación domiciliaria. Si el Fiscal tiene conocimiento de la diligencia y no puede participar de forma presencial puede hacerlo de manera virtual, debiendo dejarse constancia de su participación.
- La declaración del investigado debe registrarse en audio y video, siempre que sea posible y asegurando su custodia, utilizando los medios logísticos proporcionados por la unidad policial.

f. Elaboración del informe policial[7].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

S. DE LA CRUZ Q.

1.2.2. Delito Informático contra la Fe Pública – Suplantación de identidad.

Forma delictiva que tiene como fin el tener acceso a los usuarios de alguna plataforma que son administrados por personas naturales o jurídicas, tales como redes sociales, correos electrónicos entre otros, poder realizar actos delictivos como: Estafas, Difamación, Fraudes Bancarios entre otros.

a. Recepción de denuncia.

El efectivo policial, realiza las siguientes preguntas al agraviado:

- Indique Ud. ¿Cómo tuvo conocimiento de la existencia de la cuenta de usuario o página web falsa que suplanta su identidad? (solicitar información del sitio web o red social incriminado de ser el caso).
- Indique Ud. ¿Días antes de tomar conocimiento del hecho, existieron eventos o antecedentes que puedan ser relacionados a la acción ilícita que le generaron una alerta? (llamadas telefónicas, mensajes de texto entre otros)
- Indique Ud. ¿Posee capturas de pantalla de conversaciones, publicaciones, envíos de audios u otros, de las acciones ilícitas realizadas desde las cuentas de usuario o páginas *web* falsas?
- Indique Ud. ¿Tiene conocimiento de la existencia de otros perfiles en plataformas web que estén suplantando su identidad? ¿Existen publicaciones adicionales relacionadas al acto suplantador?
- Otras preguntas que considere pertinentes.

[7] Manual de documentación policial. Pág 183. (R.D Nº 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771694/6529036-manual-de-documentacion-policial.pdf

b. Diligencias urgentes e inaplazables.

- Preservar la evidencia digital *(copia de los videos de seguridad, captura de pantalla, identificar direcciones web, URL e ID de redes sociales)*. Preservación de las cuentas de redes sociales incriminadas, captura de información volátil, entre otros, a fin de que éstas no sean eliminadas, suprimidas o adulteradas por el delincuente informático. De ser necesario evalúa la incautación.

- Visualización de equipos (del agraviado) y/o de cuentas de redes sociales con conocimiento y/o participación del representante del Ministerio Público, se debe recabar información adicional que permita identificar a los autores del hecho.

- El instructor debe elaborar las actas necesarias en presencia del agraviado y del representante del Ministerio Público.

- Si en la comisión del delito de suplantación de Identidad se ha utilizado cuentas incriminadas de *Facebook* y/o *WhatsApp* u otro, se debe de solicitar la preservación, así como el registro de direcciones IP de las cuentas implicadas a través de las plataformas legales de *Facebook* https://www.facebook.com/records/ y *WhatsApp* https://www.whatsapp.com/record respectivamente, o la que corresponda.

- Cuando se identifique una línea telefónica vinculada a los hechos investigados, se debe solicitar al área de apoyo técnico de la dependencia policial encargada de la administración del sistema RENTESEG de OSIPTEL, para solicitar la siguiente información:

  - Datos del titular de la línea telefónica implicada, incluyendo el operador y la fecha de activación.
  - Identificación del número IMEI en el cual fue insertado el SIM *card* correspondiente a la línea en cuestión.
  - Relación de líneas telefónicas que han sido insertadas en el IMEI implicado.
  - Datos de los titulares de todas las líneas telefónicas vinculadas al IMEI señalado.
  - Una vez obtenida la fecha de activación de la línea telefónica incriminada, se recomienda oficiar a través de la mesa de partes virtual (https://apps.reniec.gob.pe/MesaPartesVirtual/) del Registro Nacional de Identificación y Estado Civil (RENIEC) la información correspondiente al usuario que realizó la verificación biométrica (huella dactilar) del titular de dicha línea. La solicitud debe incluir, de manera precisa, la fecha y hora de la activación, así como los datos completos del titular de la línea. En respuesta, RENIEC proporciona la identificación del usuario (funcionario, sistema o entidad) que efectuó la consulta biométrica utilizada para validar la identidad al momento de activar la línea incriminada. La solicitud debe contener un texto similar al siguiente:

V°B° DE LA CRUZ Q.

JURISPOL

"Se solicita información del titular y/o usuario que realizó la consulta biométrica el día [D], a horas [H], correspondiente a la persona de JUAN PÉREZ PÉREZ, identificado con DNI N.° 88888888."

c. Comunicación al Ministerio Público.

El instructor comunica la denuncia al Ministerio Público, de forma inmediata, sin exceder en ningún caso, el plazo legal correspondiente.

d. Cumplimiento de las diligencias dispuestas por el Ministerio Público.

Dar cumplimiento a las diligencias dispuestas por el Ministerio Público.

e. Desarrollo de la investigación policial.

- **Declaración del agraviado**; al momento de recibir la declaración especificar la fecha y hora, (a fin de tener en cuenta si existe flagrancia delictiva) detallando los hechos sucedidos.
- **Identificar los sitios *web* o perfiles de las plataformas** de redes sociales donde presuntamente se realizan los actos de suplantación, así como, identificar plenamente la dirección URL, el ID del usuario y nombre de usuario.
- **Realizar la diligencia de visualización de las cuentas y perfiles en las plataformas digitales**, identificando su ubicación (IP)[8], identificación (nombre o título de la página) y contenido de las cuentas y/o perfiles, en las plataformas digitales utilizadas, precisando: nombres, correos electrónicos, líneas telefónicas, dirección URL, identificación de usuario (ID)[9], entre otros.
- **Efectuar la preservación de información** en cada una de las plataformas digitales con el fin de evitar que eliminen, modifiquen o supriman información de los perfiles incriminados, para ello se realizan las diligencias de acuerdo a lo establecido en el numeral 2.2 *Procedimiento para preservación de información en redes sociales* de la presente Guía

S. DE LA CRUZ Q.

[8] Kaspersky (10 de marzo de 2025) Qué es una dirección IP. https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address?srsltid=AfmBOoph9xleUDp0U_ApCtNcvt5j_aZBcZTFi6LHT31urQAQL8PaVtbR
"Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local." (...) "Una dirección IP es una cadena de números separados por puntos. Las direcciones IP se expresan como un conjunto de cuatro números, por ejemplo, 192.158.1.38. Cada número del conjunto puede variar de 0 a 255. Por lo tanto, el rango completo de direcciones IP va desde 0.0.0.0 hasta 255.255.255.255.
Las direcciones IP no son aleatorias. La Autoridad de números asignados de Internet (Internet Assigned Numbers Authority, IANA), una división de Internet Corporation para números y nombres asignados (Internet Corporation for Assigned Names and Numbers, ICANN), genera y asigna matemáticamente las direcciones IP.
ICANN es una organización sin fines de lucro que se estableció en los Estados Unidos en 1998 para ayudar a mantener la seguridad de Internet y permitir que todos puedan utilizarla. Cada vez que alguien registra un dominio en Internet, debe dirigirse a un registrador del nombre de dominio, quien paga una pequeña tarifa a ICANN para registrarlo."

[9] Google (10 de marzo de 2025) ID de usuario: Definición https://support.google.com/google-ads/answer/9004360?hl=es-419.
"Un ID de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web."

sobre procedimientos para la preservación de información en redes sociales.

- **Solicitar la medida de levantamiento del secreto de las comunicaciones**, ante el fiscal, a efectos de requerir (previa orden judicial), a las empresas prestadoras de servicios de comunicaciones, la información oficial, sobre la actividad del perfil incriminado, especificando datos como[10]: (Se adjunta modelo de formato en anexo IV).
  - Nombre y dirección del afectado por la medida.
  - Identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar.
  - Forma de la interceptación *(voz, datos o mensajes, en tiempo real o datos históricos)*. Su alcance *(de qué números o datos concretos, asegurando que el levantamiento del secreto se realice de forma estrictamente circunscrita a lo indispensable para el esclarecimiento de los hechos)*.
  - Su duración (Fecha de inicio – fecha de fin).
  - La dependencia
  - Los datos del personal policial o Fiscalía encargado de la diligencia de intervención y grabación o registro.

Adicional a ello, puede solicitar los datos complementarios que por la naturaleza de la investigación considere pertinentes, como, por ejemplo:

- Fecha de creación
- Registro de actividad de la cuenta incriminada
- Correos utilizados
- Registro de IP's y otros, como verificadores de la cuenta y actividades de la misma.
- Otros que considere convenientes (Se adjunta modelo de formato en anexo IV).

- Al identificar al presunto autor, se procede a notificar, conforme a ley, para la toma de su declaración y demás diligencias, entre ellas verificaciones domiciliarias (de ser el caso), sus antecedentes policiales, así como las informaciones proporcionadas por las plataformas web.

f. Elaboración del informe policial[11].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. N° 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

1.2.3. Delito contra la integridad de datos y sistemas informáticos.

Forma delictiva que tiene como fin el vulnerar los niveles de seguridad de un sistema informático y así como apropiarse los archivos que este contenga para con ello pedir rescate de su disponibilidad.

[10] Decreto legislativo N° 957 – Nuevo Código Procesal Penal, numeral 3 del Art. 230.- Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles". (https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H682695)

[11] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://con.www.gob.pe/uploads/document/file/771694/5529039-manual-de-documentacion-policial.pdf

a. Recepción de denuncia.

El efectivo policial (a fin de tener en cuenta si existe flagrancia delictiva), al entrevistarse con el agraviado, representante legal o encargado de los sistemas informáticos, debe realizar las siguientes preguntas:

- ¿Cómo tuvo conocimiento de la vulneración de la integridad de datos o sistemas informáticos?
- ¿Días antes de tomar conocimiento del hecho, existieron eventos o antecedentes que puedan ser relacionados a la acción ilícita (mensajes de texto, correos electrónicos, actualizaciones de sistemas, entre otros)?
- ¿Tiene conocimiento si su representada maneja protocolos y/o políticas del uso de equipos, sistemas informáticos y/o correos electrónicos?
- ¿Se encuentra documentada la configuración o las políticas de seguridad y privacidad de datos de su representada?
- ¿Los servicios implementados (servicio de correos, almacenamiento, entre otros) son administrados por su representada o se encuentran tercerizados? Si se encuentran tercerizados ¿Por qué empresa y quién es el encargado responsable en la misma?
- ¿Tiene identificado y/o cuantificado, el perjuicio de la acción ilícita relacionado a la vulneración de la integridad de datos o sistemas informáticos?

b. Diligencias urgentes e inaplazables

- El personal policial, con apoyo de personal técnico especializado, realiza la preservación de la evidencia digital, realizando la copia *bit* a *bit*, extracción de información de dispositivos informáticos, entre otros; relevantes al esclarecimiento de los hechos.
- Solicitar el informe técnico y/o de auditoría de ser el caso, relacionado a la vulneración de la integridad de datos o sistemas informáticos.
- El instructor elabora las actas respectivas en presencia del agraviado.

c. Comunicación al Ministerio Público.

El instructor comunica la denuncia al Ministerio Público de forma inmediata, dentro del plazo legal vigente.

d. Cumplimiento de las diligencias dispuestas por el Ministerio Público.

Dar cumplimiento a las diligencias dispuestas por el Ministerio Público.

e. Desarrollo de la investigación policial.

- Declaración del agraviado; especificar la fecha y hora del ilícito penal (a fin de tener en cuenta si existe flagrancia delictiva), detallando los hechos sucedidos.
- Visualización de equipos y/o servidores afectados: Se debe recabar información adicional que permita identificar a los autores del hecho.
- Solicitar el análisis informático forense de los dispositivos informáticos afectados con la vulneración de la integridad de datos o sistemas informáticos.

S. DE LA CRUZ Q.

JURISPOL

- De ser el caso, solicitar información a la empresa responsable de los sistemas informáticos de la compañía agraviada sobre la modalidad de ataque informático (ataques de denegación de servicios - DDOS, *ransomware, phishing*, entre otros), el cual, debe estar acompañado de un informe técnico que detalle las acciones realizadas. (Se adjunta modelo de formato en anexo V).
- Solicitudes de información a las entidades de telecomunicaciones que brindan los servicios telefonía e internet, sobre las identidades y actividades de las líneas celulares y direcciones IP vinculadas al ilícito penal. (Se adjunta modelo de formato en anexo IV).

f. Elaboración del informe policial[12].

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

S. DE LA CRUZ Q.

1.2.4. Delito contra la Indemnidad Sexual de Menores

Este tipo de delito tiene como objetivo el realizar insinuaciones a menores de edad, establecer contacto de manera virtual para ganar su confianza y con ello el poder obtener información intima de las víctimas para cometer abusos sexuales.

a. Recepción de denuncia policial:

El efectivo policial, al entrevistarse con la parte agraviada, padres, tutores del menor de edad o cualquier adulto que desea denunciar, le realiza las siguientes preguntas:

- ¿Cómo tuvo conocimiento de los hechos en agravio del menor de edad?
- Describir o mencionar la plataforma virtual, red social, juego *on line*, entre otros, utilizados para contactar con el menor de edad.
- ¿De qué equipo informático accedió al internet el menor de edad?
- Recabar información necesaria a fin de conocer si el menor de edad agraviado envió imágenes y/o videos íntimos de connotación sexual a su agresor.
- Recabar información necesaria a fin de conocer si el agresor del menor de edad, solicitó alguna dádiva u otros, realizando amenazas a cambio de no publicar sus imágenes y/o videos de connotación sexual y a través de qué medios.
- Requerir la información del usuario y contraseña de los equipos informáticos, plataformas virtuales, cuentas de redes sociales, juegos en línea entre otros del menor de edad agraviado.
- Recabar información necesaria a fin de conocer si el menor de edad agraviado conoce al agresor, si llegó a tener contacto físico con éste y si puede proporcionar las características física del agresor.

JURISPOL

[12] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771694S/6529039-manual-de-documentacion-policial.pdf

b. Abordaje de la víctima

- Considerando que la víctima es un menor de edad, el abordaje inicial es efectuado por personal policial especializado, aplicando técnicas de entrevista acordes a su edad, desarrollo y condición de vulnerabilidad, con la finalidad de recabar información mínima, básica e indispensable para la identificación preliminar de los hechos materia de investigación, evitando indagaciones reiterativas o innecesarias que puedan generar revictimización.
- El referido abordaje primigenio no constituye una entrevista única ni una diligencia de actuación probatoria, sino una intervención inicial de carácter orientador y protector, necesaria para la adopción de medidas inmediatas de protección, la comunicación oportuna al Ministerio Público y la conducción adecuada de la investigación.
- Dicha intervención se realiza en un ambiente adecuado, seguro y conforme a la edad del menor, garantizando un trato digno, respetuoso y empático, en observancia del principio del interés superior del niño, niña y adolescente, conforme a los lineamientos y la normativa vigente.

S. DE LA CRUZ Q.

c. Diligencias urgentes e inaplazables

Teniendo como primacía el interés superior del niño, se deben realizar las siguientes diligencias:

- Realizar la preservación en las plataformas virtuales, de los perfiles de redes sociales incriminados o vinculadas al caso.

- Realizar la solicitud de registro por emergencia en las plataformas de aplicación de la ley, de los perfiles de redes sociales incriminados o vinculadas al caso.

- Solicitud de preservación de información de las cuentas incriminadas de *Google* debe ser realizada a través de los canales oficiales, entre ellos, el correo oficial vigente **lis-global@google.com** y la obtención de información debe ser solicitada a través del convenio de Cooperación Judicial Internacional, por intermedio del Ministerio Público-

- Realizar el acta de visualización de los perfiles de redes sociales incriminados o vinculadas al caso, así como de los dispositivos tecnológicos utilizados por el menor de edad agraviado, por la volatilidad de la evidencia digital, de ser posible descargar la información del perfil teniendo en consideración el procedimiento señalado en el numeral 4 Descarga de información de perfil de Facebook, contenido en el Capítulo IV de Aseguramiento de la Evidencia Digital - numeral 4.2. Fases para el aseguramiento de la evidencia digital, página 103 de la presente guía.

- Visualizar los dispositivos y equipos informáticos vinculados a los hechos a fin de recabar el Material de Abuso Sexual de Niños, Niñas y Adolescentes (MASNNA) almacenado en los distintos dispositivos electrónicos empleados para la comisión del delito.

- En ningún caso dicho material se podrá compartir, distribuir o proyectar vía internet, bajo responsabilidad funcional.

- De ser el caso, solicitar la geolocalización de los números telefónicos incriminados o vinculados.

d. Comunicación al representante del Ministerio Público

- La comunicación se realiza una vez recibida la denuncia, en el día, adjuntando una copia de la misma y se coordina la remisión de la Disposición Fiscal mediante la Carpeta Fiscal, a fin de realizar las diligencias preliminares.

- Una vez que se tenga la Disposición Fiscal, se coordina con las partes procesales el desarrollo de las diligencias.

- Coordinación con la Fiscalía a cargo para las pericias respectivas (Médico legista, evaluación antropológica forense, evaluación psicológica forense, pericia informática forense, entre otras) y programación para la entrevista en Cámara Gesell.

e. Desarrollo de la investigación policial

- Declaración del denunciante a fin de especificar la fecha y hora del ilícito penal, detallando los hechos sucedidos.

- Declaración del menor agraviado acompañado de su padre o apoderado y con participación del representante del Ministerio Público, teniendo en consideración las técnicas de abordaje.

- Diligenciar los exámenes de ley como el examen de médico legista de integridad sexual, examen psicológico forense, entrevista única en cámara Gesell, pericia antropológica forense, entre otras.

- Solicitar al Ministerio Público la RESERVA de la investigación, a fin de evitar en poner de sobre aviso al denunciado, impidiendo que el investigado elimine o destruya el Material de Abuso Sexual de Niños, Niñas y Adolescentes (MASNNA).

- Visualizar los dispositivos y equipos informáticos vinculados a los hechos a fin de recabar el Material de Abuso Sexual de Niños, Niñas y Adolescentes (MASNNA) almacenado en los distintos dispositivos electrónicos empleados para la comisión del delito. En ningún caso dicho material es compartido, distribuido vía internet o en forma física, bajo responsabilidad funcional.

- Solicitar el análisis informático forense de los dispositivos informáticos vinculados a la comisión de los hechos

- Solicitar al fiscal, la medida limitativa del secreto de las comunicaciones, documentos privados y/o interceptación, a efectos de obtener información de la empresa prestadora de servicios de telefonía o internet, sobre los

S. DE LA CRUZ Q.

JURISPOL

datos de titularidad de las líneas telefónicas o direcciones IP incriminadas, la cual debe contar con la respectiva resolución judicial (se adjunta modelo de formato en anexo IV).

- Realizar la solicitud de registro de información técnica (relacionados a los registros de direcciones IP de inicio de sesión, el IP primigenio de registro, número de teléfonos vinculados, correos electrónicos vinculados, entre otros) en las plataformas de aplicación de la ley de las redes sociales, de los perfiles incriminados o vinculados al caso, la cual debe contar con la respectiva resolución judicial del levantamiento del secreto de las comunicaciones, documentos privados y/o interceptación.

- Solicitar información a OSIPTEL (Organismo Supervisor de Inversión Privada de Telecomunicaciones) sobre los datos de titularidad de las líneas telefónicas incriminadas, a través de la plataforma RENTESEG (Sistema Nacional de Equipos Terminales Móviles para la Seguridad). Para ingresar al RENTESEG, el jefe de unidad policial debe contar con usuarios de acceso, los cuales se solicitan previamente, mediante el oficio respectivo al OSIPTEL.



- Solicitar información a OCN - INTERPOL Lima de las imágenes y/o videos incriminados, a fin de establecer si se encuentran reportados como Material de Abuso Sexual de Niños, Niñas y Adolescentes (MASNNA) en otras investigaciones nacionales e internacionales.

- Solicitar al Ministerio Público la aplicación de las técnicas especiales de investigación entre éstas, la Observación, Vigilancia y Seguimiento (OVISE) de los investigados plenamente identificados; agente encubierto; entre otros, debiendo ser realizada por un equipo especial de agentes de inteligencia de la División de Ciber Protección Infantil o en coordinación con la misma, a efectos de mantener la reserva de la investigación.

- Requerir las medidas limitativas de derecho como: la detención preliminar del investigado; el allanamiento con descerraje e incautación de bienes y equipos electrónicos (celulares, computadoras, laptops, Tablet, entre otros necesarios para la investigación); el levantamiento del secreto de la comunicaciones y documentos privados para la visualización *in situ*, el análisis informático forense o extracción de información de los dispositivos incautados, entre otras necesarias.

f. Elaboración del informe policial[13]

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. N° 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

1.2.5. Delito de préstamo informático extorsivo

[13] Manual de documentación policial. Pág 183. (R.D N° 776-2016-DIRGEN/EMG-PNP de fecha 27 de julio de 2016). https://cdn.www.gob.pe/uploads/document/file/771894S/6529039-manual-de-documentacion-policial.pdf

a. Recepción de denuncia policial:

El efectivo policial (a fin de tener en cuenta si existe flagrancia delictiva), al entrevistarse con el agraviado, representante legal, debe realizar las siguientes preguntas:

- ¿Cómo tuvo conocimiento del préstamo informático extorsivo?
- ¿Días antes de tomar conocimiento del hecho criminal, existieron eventos o antecedentes que puedan ser relacionados a la acción ilícita (mensajes de texto, mensajes de *WhatsApp*, llamadas telefónicas, correos electrónicos, entre otros) y de ser así, mencione el medio o el numero con el que se contactaron?
- Realizo la descarga de algún aplicativo (App) y/o página *web* para solicitar un préstamo de dinero en línea.

b. Diligencias urgentes e inaplazables

- Visualizar los dispositivos y equipos informáticos vinculados a los hechos a fin de recabar información criminal, suscribiéndose la respectiva acta de visualización con participación del denunciante, como diligencia de urgencia, conforme lo establece el **articulo 67 del NCPP. - Función de investigación de la Policía Nacional.**

- Cuando se identifique una línea telefónica vinculada a los hechos investigados, se debe solicitar al área de apoyo técnico de la dependencia policial encargada de la administración del sistema RENTESEG de OSIPTEL, para solicitar la siguiente información:

  - Datos del titular de la línea telefónica implicada, incluyendo el operador y la fecha de activación.
  - Identificación del número IMEI en el cual fue insertado el SIM *card* correspondiente a la línea en cuestión.
  - Relación de líneas telefónicas que han sido insertadas en el IMEI implicado.
  - Datos de los titulares de todas las líneas telefónicas vinculadas al IMEI señalado.
  - Una vez obtenida la fecha de activación de la línea telefónica incriminada, se recomienda oficiar a través de la mesa de partes virtual (https://apps.reniec.gob.pe/MesaPartesVirtual/) del Registro Nacional de Identificación y Estado Civil (RENIEC) la información correspondiente al usuario que realizó la verificación biométrica (huella dactilar) del titular de dicha línea. La solicitud debe incluir, de manera precisa, la fecha y hora de la activación, así como los datos completos del titular de la línea. En respuesta, RENIEC proporciona la identificación del usuario (funcionario, sistema o entidad) que efectuó la consulta biométrica utilizada para validar la identidad al momento de activar la línea incriminada. La solicitud debe contener un texto similar al siguiente:

    "Se solicita información del titular y/o usuario que realizó la consulta biométrica el día [D], a horas [H], correspondiente a la persona de

V°B° S. DE LA CRUZ C.

JURISPOL

JUAN PÉREZ PÉREZ, identificado con DNI N.° 88888888."

- Identificar la aplicación utilizada, así como el dominio web utilizado a fin de solicitar al proveedor de *hosting* información del administrador de la página web incriminada. (punto 2.6 Procedimiento para obtener información sobre dominios *web* y direcciones IP).

- Si en la comisión del delito de préstamo informático extorsivo se ha utilizado cuentas incriminadas de *Facebook* y/o *WhatsApp* u otro, se debe de solicitar la preservación, así como el registro de direcciones IP de las cuentas implicadas a través de las plataformas legales de:
  Facebook: https://www.facebook.com/records/
  WhatsApp: https://www.whatsapp.com/record o la que corresponda.

- Otras diligencias que, por la naturaleza del caso, puedan ser realizadas por el instructor, siempre que se encuentren dentro del marco legal correspondiente.

S. DE LA CRUZ Q.

c. Comunicación al representante del Ministerio Público

- La comunicación se realiza una vez recibida la denuncia, en el día, adjuntando una copia de la misma y se coordina la remisión de la Disposición Fiscal mediante la Carpeta Fiscal, a fin de realizar las diligencias preliminares.
- Una vez que se tenga la Disposición Fiscal, se coordina con las partes procesales el desarrollo de las diligencias.
- Coordinación con la Fiscalía a cargo para las pericias respectivas (pericia informática forense, entre otras).

d. Desarrollo de la investigación policial

- **Declaración del agraviado**; al momento de recibir la declaración especificar la fecha y hora, detallando los hechos sucedidos.

- Identificar **los sitios *web* o perfiles de las plataformas** de redes sociales donde presuntamente se realizan los actos de préstamo informático extorsivo, así como, identificar plenamente la dirección URL, el ID del usuario y nombre de usuario.

- **Realizar la diligencia de visualización de las cuentas y perfiles en las plataformas digitales**, identificando su ubicación (IP), identificación (nombre o título de la página) y contenido de las cuentas y/o perfiles, en las plataformas digitales utilizadas, precisando: nombres, correos electrónicos, líneas telefónicas, dirección URL, identificación de usuario (ID), entre otros.

- **Efectuar la preservación de información** en cada una de las plataformas digitales con el fin de evitar que eliminen, modifiquen o supriman información de los perfiles incriminados, para ello se realizan las diligencias de acuerdo a lo establecido en el numeral *2.3 Procedimiento para preservación de información en redes sociales* de la presente Guía

JURISPOL

sobre procedimientos para la preservación de información en redes sociales.

- **Solicitar la medida de levantamiento del secreto de las comunicaciones**, ante el fiscal, a efectos de requerir (previa orden judicial), a las empresas prestadoras de servicios de comunicaciones, la información oficial, sobre la actividad del perfil incriminado, especificando datos como: como: (se adjunta modelo de formato en anexo IV).

  - Nombre y dirección del afectado por la medida,
  - Identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar,
  - Forma de la interceptación (voz, datos o mensajes, en tiempo real o datos históricos).
  - Su alcance (de qué números o datos concretos, asegurando que el levantamiento del secreto se realice de forma estrictamente circunscrita a lo indispensable para el esclarecimiento de los hechos).
  - Su duración (fecha de inicio – fecha de fin).
  - La dependencia
  - Los datos del personal policial o Fiscalía encargada de la diligencia de intervención y grabación o registro.

- Adicional a ello, puede solicitar los datos complementarios que por la naturaleza de la investigación considere pertinentes, como, por ejemplo:
  - Fecha de creación
  - Registro de actividad de la cuenta incriminada
  - Correos utilizados.
  - Registro de IP's y otros, como verificadores de la cuenta y actividades de la misma.
  - Otros que considere convenientes (se adjunta modelo de formato en anexo IV).

- Solicitar las medidas limitativas del secreto bancario relacionado a: (se adjunta modelo de formato en **anexo II y III).**

  - Detalles de las operaciones ilícitas – donde se especifican los titulares de las cuentas beneficiarias (receptoras) y así como las direcciones IP y códigos IMEI de donde se generaron las transacciones fraudulentas.
  - Detalles sobre el estado de cuenta y movimientos de los beneficiarios (cuentas receptoras), así como registro de sus datos personales, líneas telefónicas y correos electrónicos vinculados.

- Al identificar al presunto autor, se procede a notificar, conforme a ley, para la toma de su declaración y demás diligencias, entre ellas verificaciones domiciliarias (de ser el caso), sus antecedentes policiales, así como las informaciones proporcionadas por las plataformas *web*.

e. Elaboración del informe policial

V°B°
S. DE LA CRUZ Q.

Elaborar el documento policial, de acuerdo a lo establecido en el artículo 332 del D. Leg. Nº 957 – Nuevo Código Procesal Penal y la Manual de Documentación Policial (Utilizar el FORMATO 46).

CAPÍTULO II

TRATAMIENTO DE INFORMACIÓN DE PERFILES DE USUARIOS DE REDES SOCIALES

2.1. Procedimiento de identificación e individualización de perfiles de usuarios de redes sociales

El personal policial que realice este procedimiento debe contar con un correo electrónico institucional activo y/o utilizar la figura procesal de agente encubierto de delitos informáticos (previa autorización fiscal)[14], de ser el caso, para poder acceder a estas plataformas que las redes sociales nos ofrecen.

S. DE LA CRUZ Q.

Antes de realizar la preservación de un perfil es importante poder ***identificar e individualizar*** un perfil en la red social de ***Facebook, Instagram, WhatsApp y TikTok***, para lo cual corresponde extraer su **identificador del perfil**. El identificador de un perfil es único dentro de la plataforma de la red social, es como el documento de identidad de una persona; para poder extraer el identificador de cada red social, se realizan los siguientes pasos:

2.1.1. Identificando e individualizando un perfil de Facebook

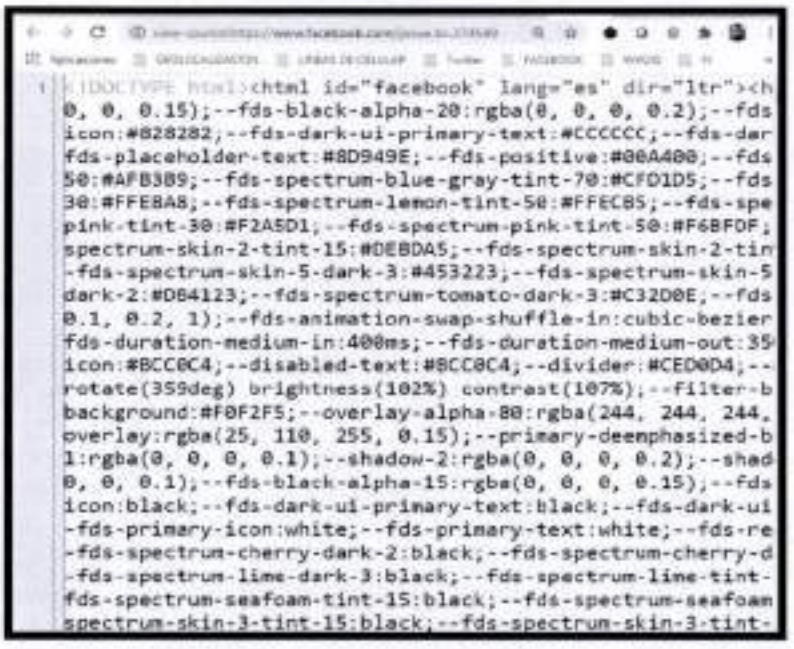
a. Al tomar conocimiento de un perfil en *Facebook* vinculado a una noticia criminal se visualiza en el navegador *Google Chrome* u otro similar.

[14] Ley de delitos informáticos Nº 30096, DISPOSICIONES COMPLEMENTARIAS FINALES; SEGUNDA.- Agente encubierto en delitos informáticos. El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F988B554E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf



b. Visualizando el perfil de *Facebook*, hacer *click* derecho en el perfil y se muestra una lista desplegable de la cual se elige la opción *"ver código fuente de la página"* abriéndose una nueva pestaña que muestra el código fuente del perfil investigado.



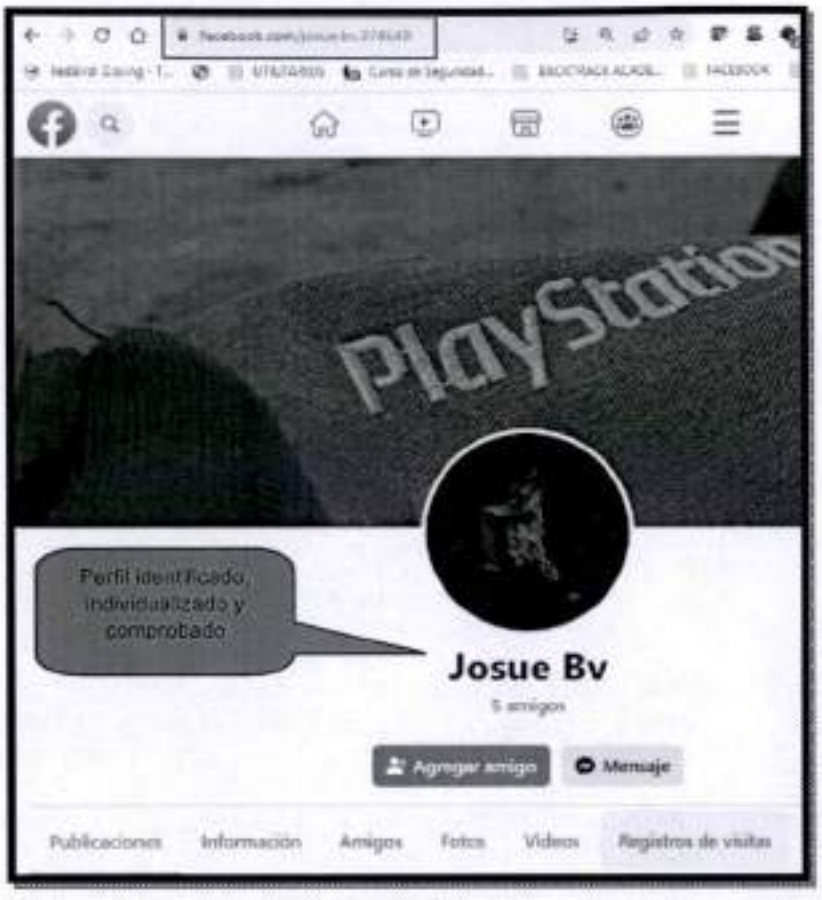


V°B°
S. DE LA CRUZ Q.

c. En la nueva pestaña donde se muestra el código fuente del perfil investigado, presionar las teclas "CTRL + F", para realizar la búsqueda de la palabra clave "*userID*" y de esta manera extraer el identificador del perfil de *Facebook*.

d. Luego de identificado el perfil se procede a realizar la comprobación del mismo. Se abre una nueva pestaña en el navegador, se digita www.facebook.com/digitamosElUserID y se debe presionar el botón ENTER, ejemplo: www.facebook.com/100045787740767, inmediatamente se muestra el perfil de *Facebook* investigado.





e. De la identificación e individualización de un perfil de *Facebook* investigado, se extrae la **URL del perfil** y el **identificador del perfil**, para poder preservarlo en la Plataforma de Aplicación de la Ley de *Facebook*.

Del ejemplo:

URL: www.facebook.com/josue.bv.374549
Identificador:100045787740767
Nombre del perfil: Josue Bv

2.1.2. Identificando e individualizando un perfil de Instagram

Existe distintas herramientas *online* que ayudan a identificar e individualizar un perfil de Instagram, en esta Guía se usa la herramienta "***Find Instagram User ID***".

a. Para identificar e individualizar un perfil de *Instagram* vinculado a una noticia criminal, se utiliza la herramienta online "***Find Instagram User ID***[15]" de la siguiente URL https://www.codeofaninja.com/tools/, para conocer el identificador de usuario del perfil la palabra clave es "***profilePage***":

[15] Herramienta online gratuita, que permite visualizar el identificador de usuario de un perfil de Instagram, se encuentra en el sitio web https://www.codeofaninja.com/tools/



b. En la herramienta "*Find Instagram User ID*", digitar el nombre de usuario del perfil incriminado y hacer click en el botón "*Find Instagram User ID*":

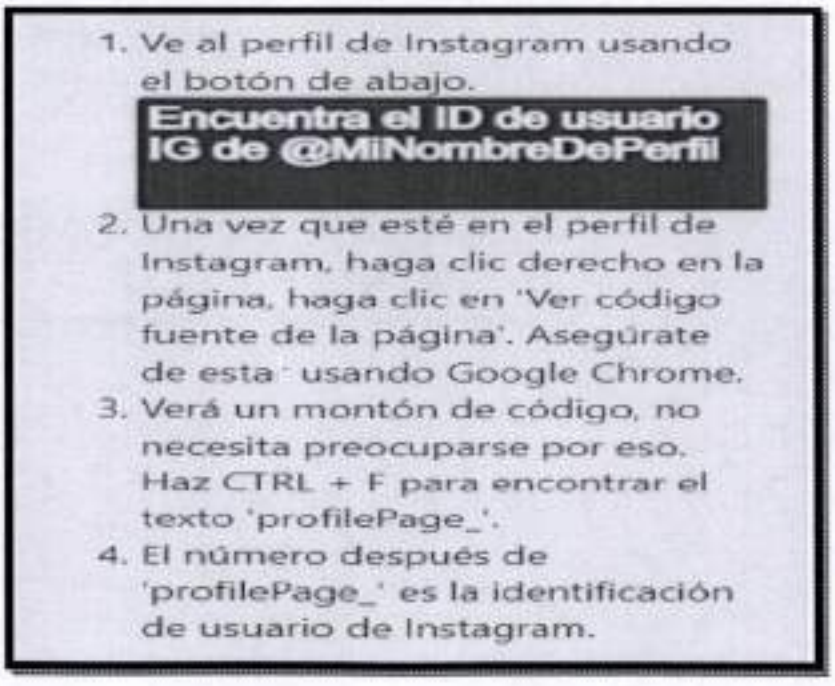
PERFIL DE INSTAGRAM





c. Para ubicar el ID de usuario de *Instagram* se deben seguir los pasos que señala la herramienta online:

Pasos a seguir:



d. En el perfil de *Instagram* que direcciona la herramienta *online* se debe buscar el ID del usuario, visualizando el perfil de *Instagram*, hacer *click* derecho y se muestra una lista desplegable de la cual se debe elegir la opción "ver código fuente de la página" y se abre una nueva pestaña que muestra el código fuente del perfil investigado:

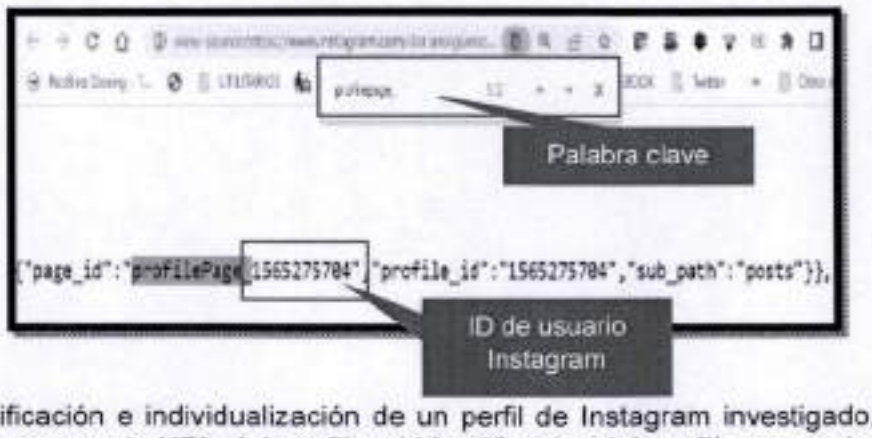
PERFIL DE INSTAGRAM



MINISTERIO DEL INTERIOR
V°B°
S. DE LA CRUZ Q.



e. En la nueva pestaña donde se muestra el código fuente del perfil investigado, se debe presionar las teclas "*CTRL + F*", para realizar la búsqueda de la palabra clave "***profilepage_***" y de esta manera extraer el identificador del perfil.



f. De la identificación e individualización de un perfil de Instagram investigado, se tiene que extraer la **URL del perfil** y el **identificador del perfil**, para poder preservarlo en la Plataforma de Aplicación de la Ley de *Facebook*.
Del ejemplo:
URL: www.instagram.com/dariansiguenzaa

S. DE LA CRUZ Q.
JURISPOL

Identificador: 1565275704
Nombre del perfil: dariansiguenzaa

2.1.3. Identificando e individualizando un perfil de WhatsApp

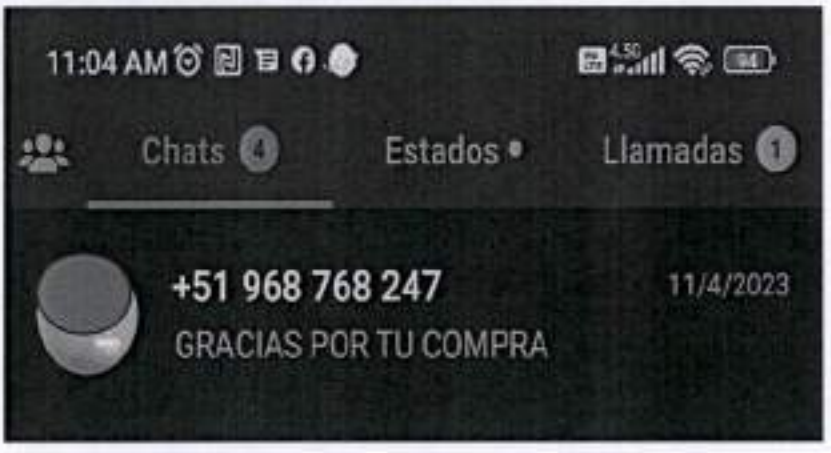
El ID de usuario de *WhatsApp* está estructurado con el símbolo (+), el código de país y el número de teléfono investigado, conforme a la siguiente gráfica:

+	Código de país	Número de teléfono

Ejemplo:

+	51	987654321

a. En el aplicativo de *WhatsApp*, ubicar el contacto incriminado:



b. Ingresar al perfil del contacto incriminado para visualizar el ID del usuario:



V°B°
S. DE LA CRUZ Q.

c. De la identificación e individualización de un perfil de WhatsApp investigado, se tiene que extraer el **identificador del perfil**, para poder preservarlo en la Plataforma de Aplicación de la Ley de *WhatsApp*.

Del ejemplo:
Identificador: +51968768247

2.1.4. Identificando e individualizando un perfil de TikTok

Para identificar e individualizar un perfil de *TikTok* se tiene que distinguir el nombre de usuario de la cuenta investigada.

a. En la red social *TikTok*, el nombre de usuario se ubica debajo de la imagen del perfil, conforme al siguiente detalle:



b. De la identificación e individualización de un perfil de *TikTok* investigado, se tiene que extraer el **Nombre de usuario y el identificador de usuario**, para poder preservarlo en la Plataforma de Cumplimiento de la Ley de *TikTok*.

Del ejemplo:
Nombre de usuario: Ericklaflojita
Identificador: @ericklaflojita

2.2. Procedimiento para preservación de información en redes sociales

Existen las plataformas de aplicación de la ley de *Facebook*, *Instagram*, *WhatsApp* y *TikTok*, los cuales ofrecen básicamente **TRES (03) procedimientos** en apoyo a las investigaciones de usuarios de redes sociales: preservación de un perfil, solicitud de registro de un perfil con resolución judicial y solicitud de registro en caso de emergencia.

A continuación, se detallan los procedimientos para la preservación de perfiles de redes sociales.

La preservación de perfiles permite guardar en el tiempo, hasta por **NOVENTA (90) días** y prorrogables por el mismo periodo, un perfil de *Facebook*, *Instagram*, *WhatsApp* o *TikTok* relacionado a la investigación de un delito, evitando que por

más que el usuario del perfil lo elimine y/o suspenda, se conserven los datos técnicos generados, como el registro de direcciones IP de inicio de sesión, IP primigenio de registro, número de teléfonos vinculados, correos electrónicos vinculados, entre otros.

En el tiempo de **CIENTO OCHENTA (180) días** aproximadamente, brinda la oportunidad al instructor de la investigación de solicitar la medida limitativa del levantamiento del secreto de las comunicaciones y documentos privados de "el" o "los" perfiles de redes sociales investigados.

Una vez identificado e individualizado el perfil investigado, corresponde realizar los siguientes pasos para la preservación, según perfil:

2.2.1. Preservación para perfiles de Facebook e Instagram

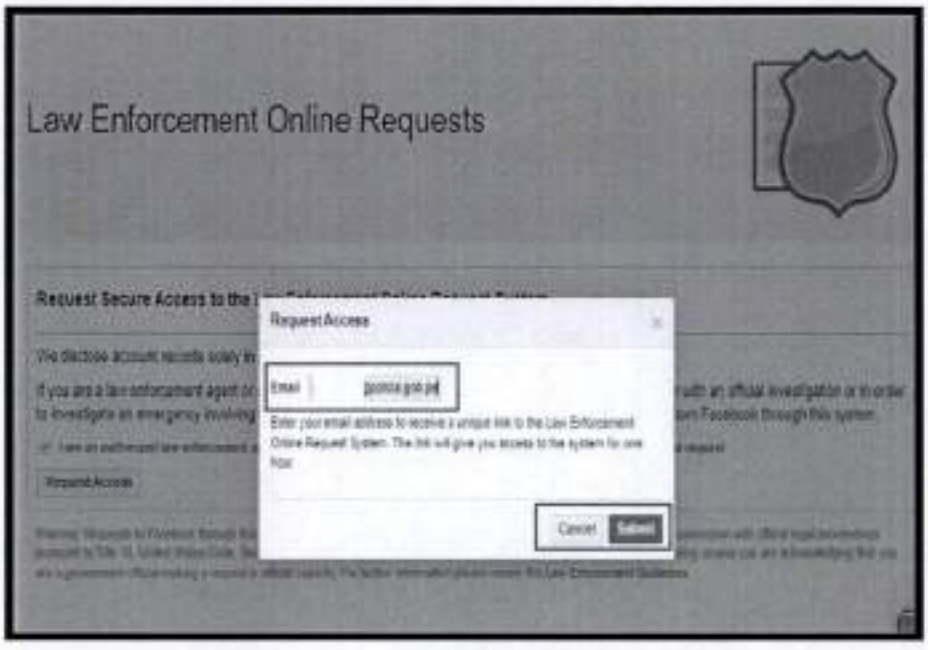
Los procedimientos descritos a continuación se utilizan para perfiles de *Facebook* como para los perfiles de *Instagram*.

a. Se ingresa a la Plataforma de Aplicación de la Ley de *Facebook*[16] con la siguiente URL www.facebook.com/records. Luego se marca con un *check* en la opción *"I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request"* y seguidamente se hace click en el botón *"Request Acces"*.

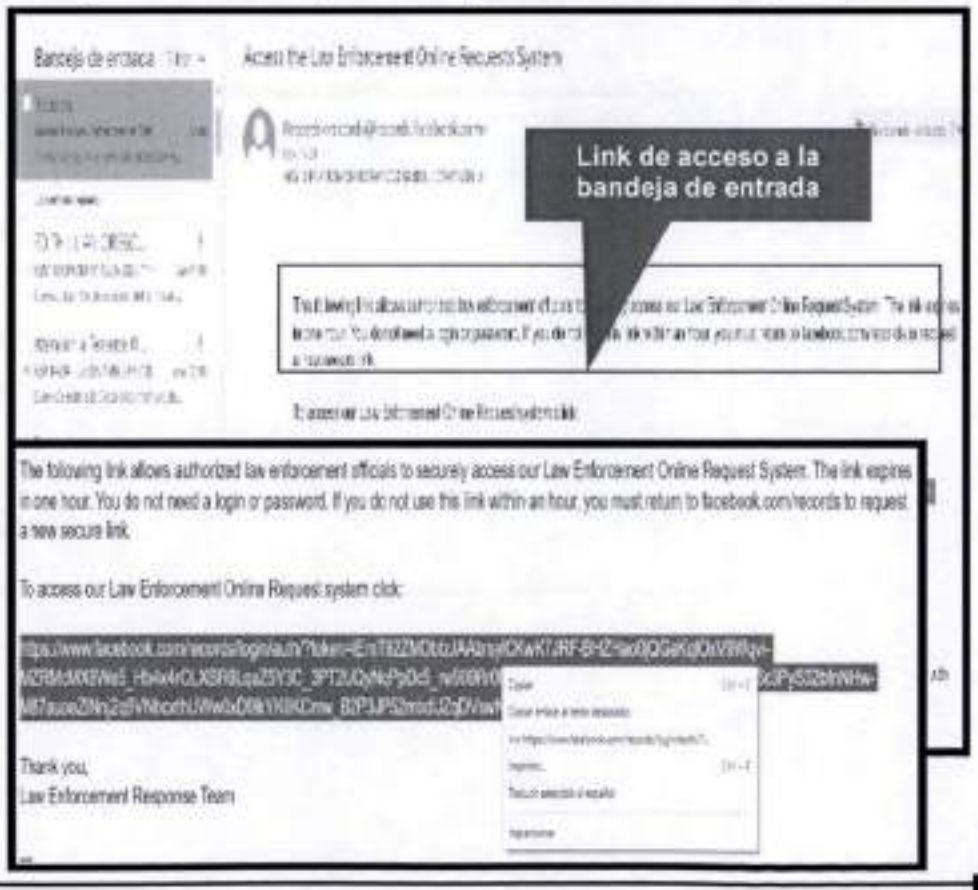


[16] Plataforma informática habilitada por la empresa Meta, empresa que administra las redes sociales Facebook, Instagram y WhatsApp, esta plataforma ayuda a los operadores de justicia a preservar información, solicitar registro con resolución judicial o por emergencia de perfiles de Facebook o Instagram que se encuentren vinculados a la comisión de un ilícito penal.

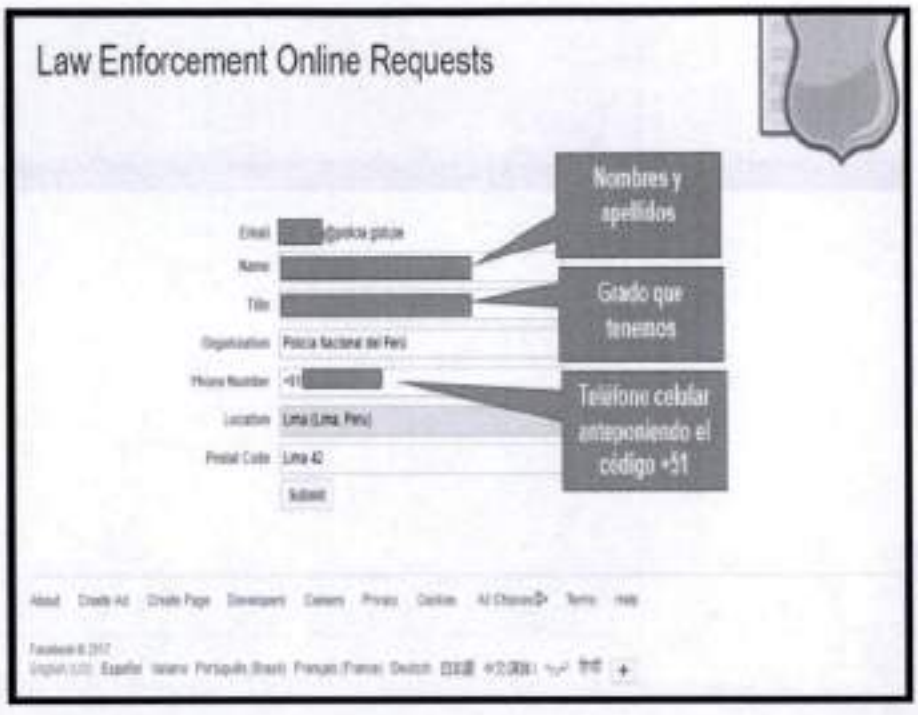
b. Luego la plataforma solicita que se ingrese el correo electrónico institucional, para enviar el *link* de acceso al sistema de aplicación de la ley como mensaje a la bandeja de entrada del correo electrónico institucional.



c. Posteriormente se verifica el mensaje de confirmación que envía la plataforma de aplicación de la Ley y se selecciona el *link* remitido, luego hacer *click* derecho y seleccionar la opción *"Ir a."* para tener acceso a la plataforma.



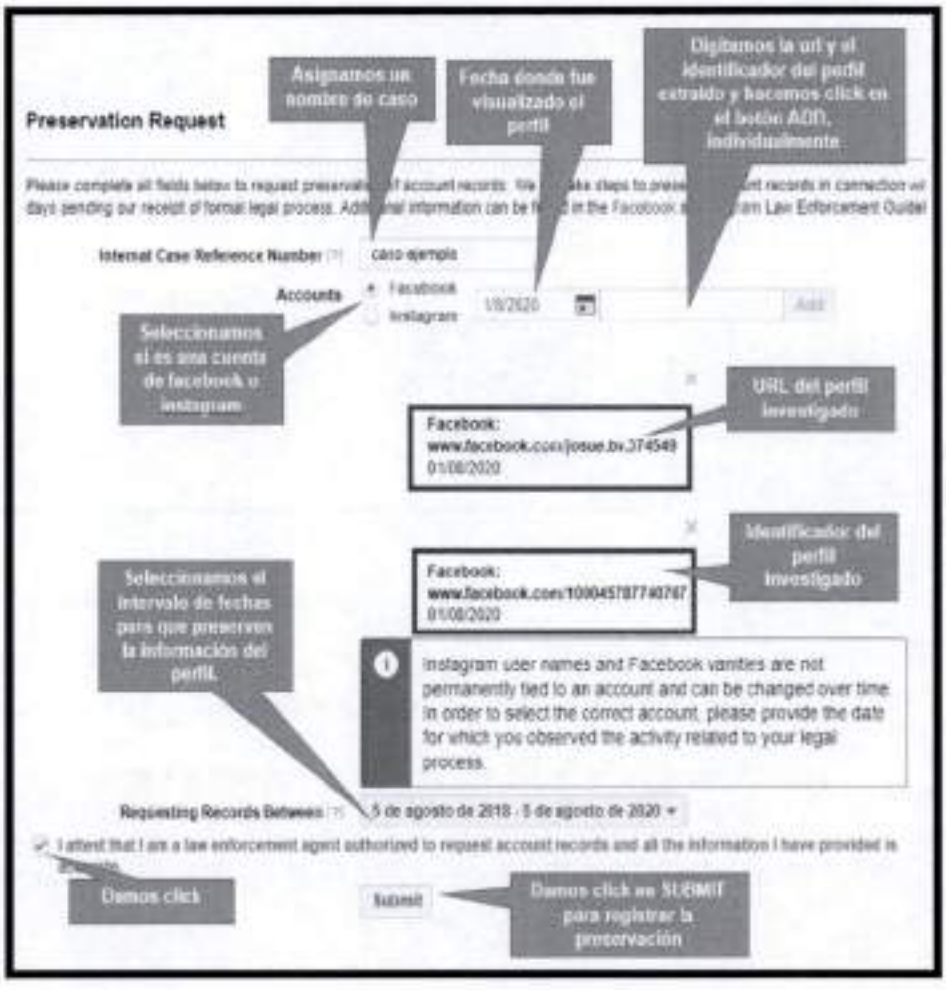
d. Cuando se accede por primera vez a la plataforma de aplicación de la Ley, se solicita el registro de los datos personales por única vez.



e. Una vez registrados los datos, se muestra una bandeja de casos y en la parte superior se aprecian unas pestañas de acceso a los procedimientos que se necesitan.

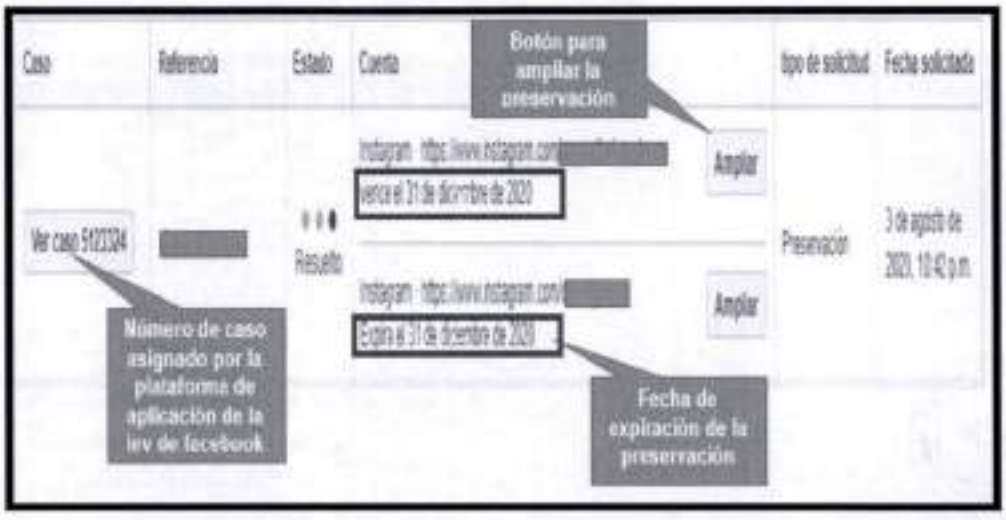


f. Se selecciona la pestaña "*Preservation Request*" y se digitan los datos que solicita el formulario y por último se hace click en el botón "*Submit*".



MINISTERIO DEL INTERIOR
V°B°
S. DE LA CRUZ Q.

g. Por último, se verifica el registro del caso en la bandeja de casos de la plataforma.



h. Los procedimientos descritos anteriormente son aplicables también para los perfiles de la red social de *Instagram*.

2.2.2. Preservación para perfiles de WhatsApp

a. Se ingresa a la plataforma de aplicación de la Ley de *WhatsApp*[17] con la siguiente URL www.whatsapp.com/records. Luego, se marca con un *check* la opción *"I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request"* y se hace *click* en el botón *"Request Access"*.

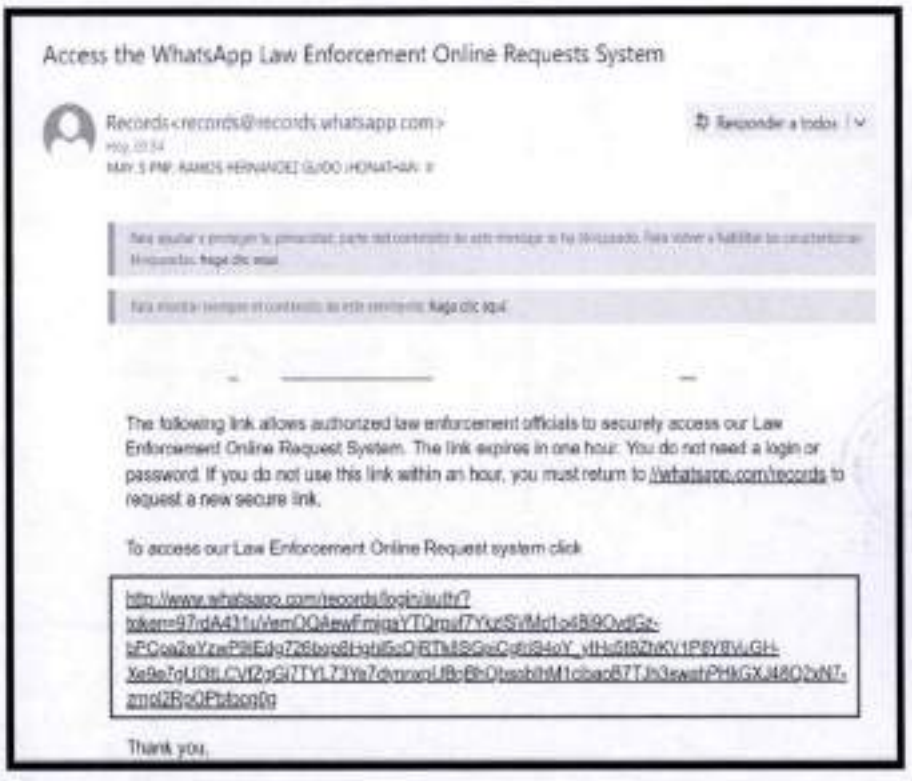
[17] Plataforma informática habilitada por la empresa Meta, empresa que administra las redes sociales Facebook, Instagram y WhatsApp, esta plataforma ayuda a los operadores de justicia a preservar información, solicitar registro con resolución judicial o por emergencia de perfiles de WhatsApp que se encuentren vinculados a la comisión de un ilícito penal.



b. Luego la plataforma indica que ingrese su correo electrónico institucional y/o el autorizado a nivel fiscal, para poder solicitar el acceso al sistema mediante un *link* que llega como mensaje a la bandeja de entrada del correo.



c. Posteriormente se verifica el mensaje de confirmación que envía la plataforma de aplicación de la Ley y se da *click* al *link* mostrado para tener acceso a la plataforma.



Access the WhatsApp Law Enforcement Online Requests System

Records<records@records.whatsapp.com>

Responder a todos

The following link allows authorized law enforcement officials to securely access our Law Enforcement Online Request System. The link expires in one hour. You do not need a login or password. If you do not use this link within an hour, you must return to /whatsapp.com/records to request a new secure link.

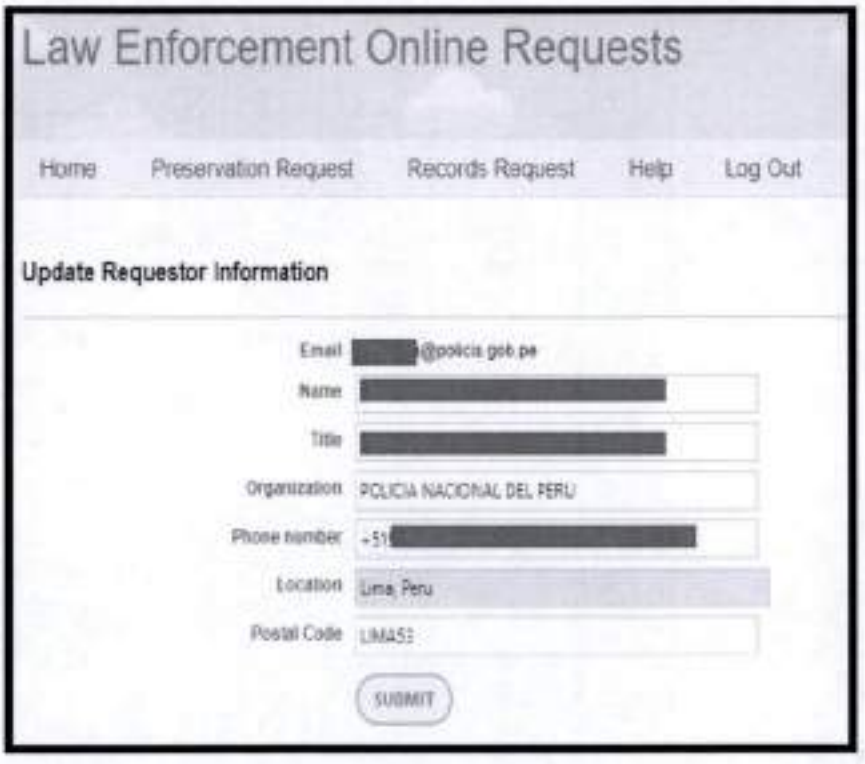
To access our Law Enforcement Online Request system click

http://www.whatsapp.com/records/login/auth?token=97dA431uVemOQAewFmjqaYTQmuf7YucSvMd1o4Bi9OvdGz-kPCoaZeYzwP9iEdg726bog8t+gtd5cOfBTbBSGpCg6i94oY_yHuSIBZhKV1P8YBVuGH-Xe9e7gUI0tLCVfZpGi7TY173Ye7dynnxnUBpBhOtwshthM1cibao877Jh3ewstPHkGXJ48O2vN7-zmol2RoOPbbon0g

Thank you.

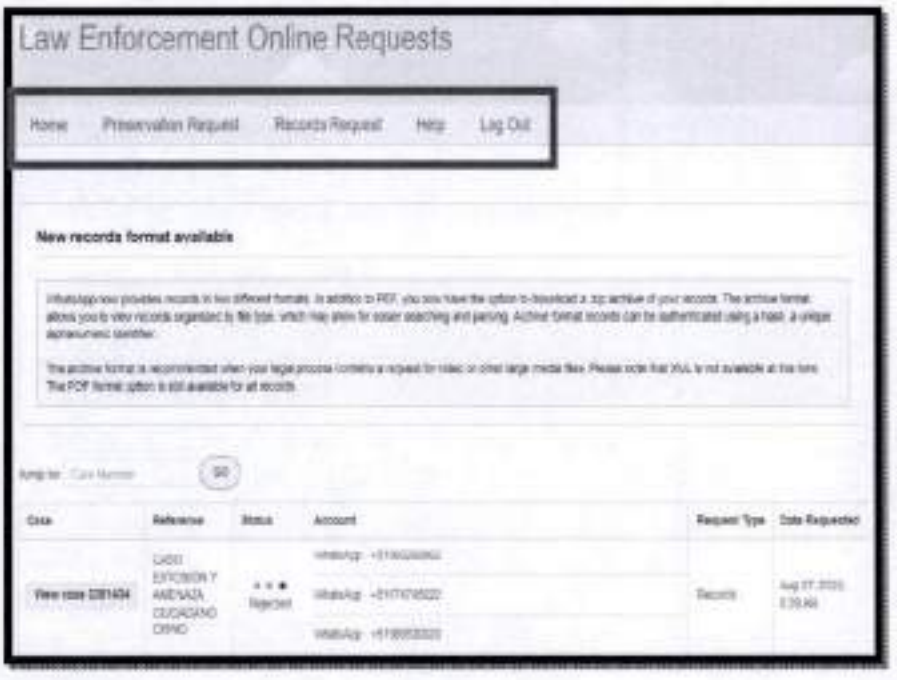
V°B°
S. DE LA CRUZ Q.

d. Cuando se accede por primera vez a la plataforma de aplicación de la Ley, se deben registrar los datos personales por única vez.



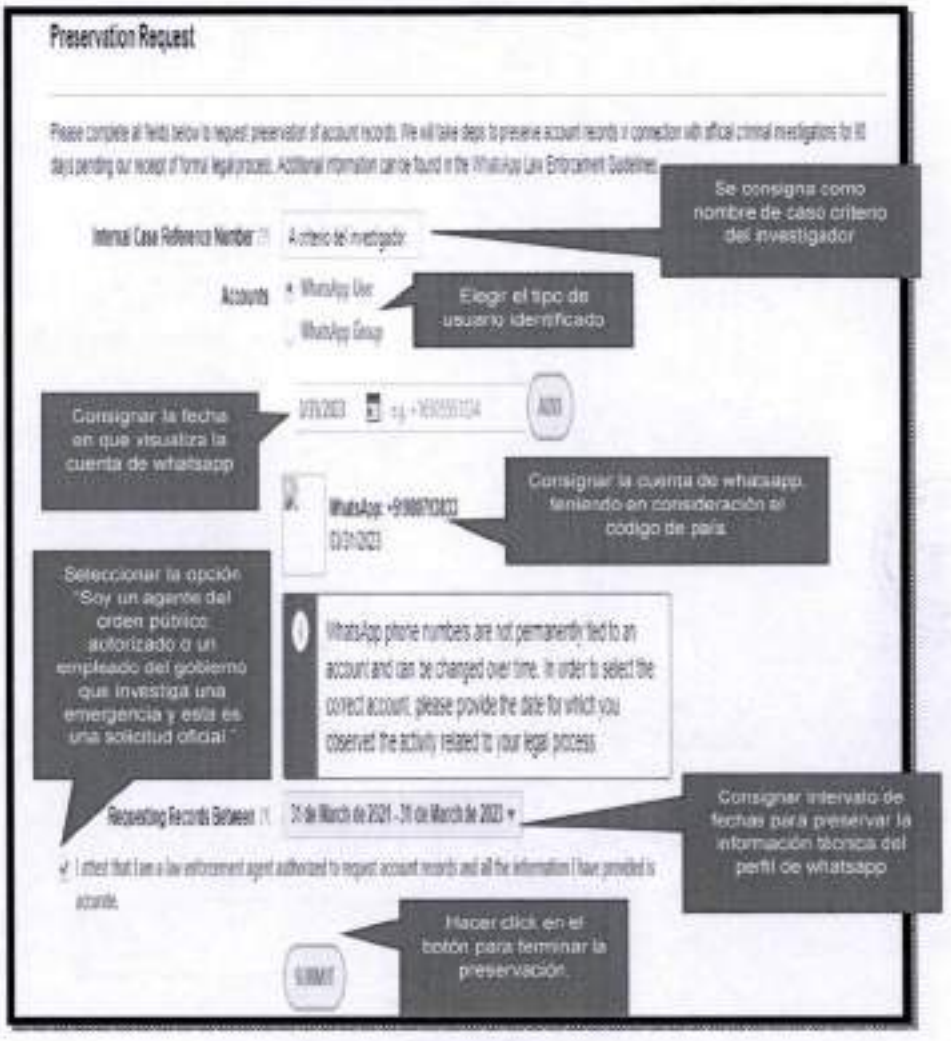
MINISTERIO DEL INTERIOR
V°B°
S. DE LA CRUZ Q.

e. Una vez registrados los datos, se muestra una bandeja de casos y en la parte superior, se aprecian unas pestañas de acceso a los procedimientos que se necesitan.

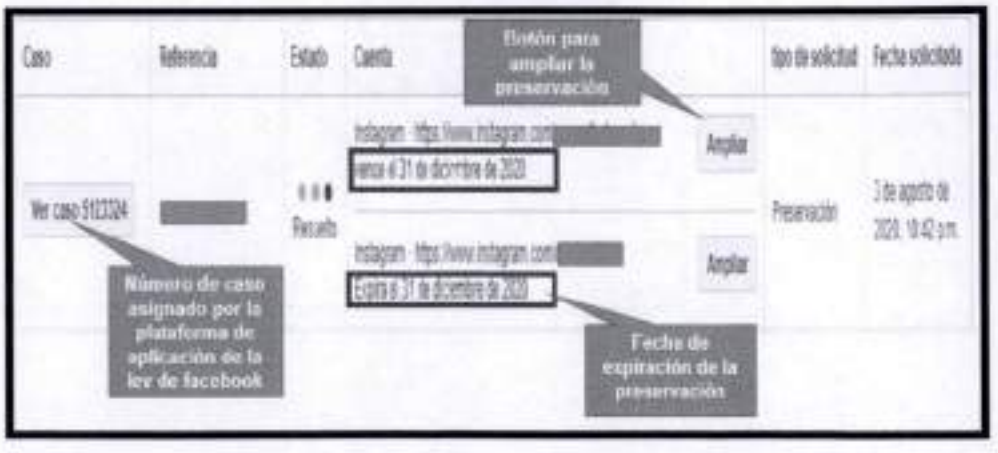


JURISPOL

f. Se selecciona la pestaña *"Preservation Request"* y se digitan los datos que solicita el formulario y por último se hace *click* en el botón *"Submit"*.



g. Por último, se verifica el registro del caso en la bandeja de casos de la plataforma.

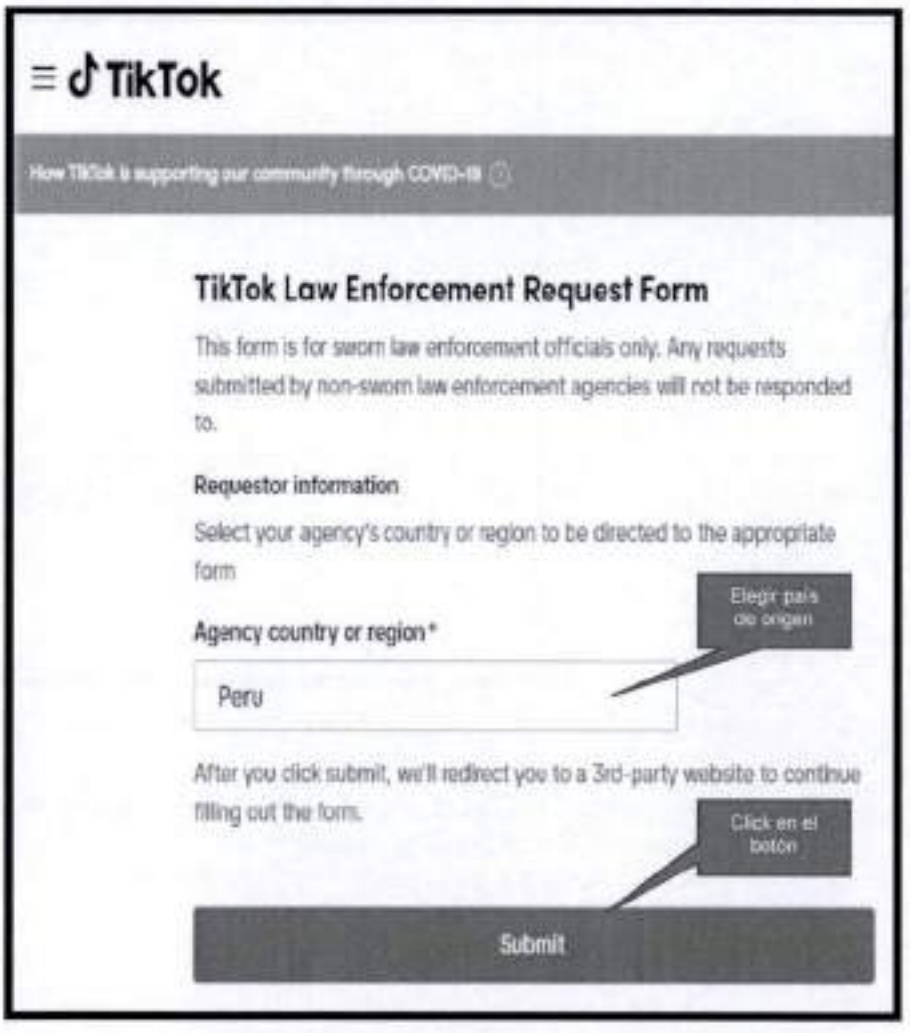


S. DE LA CRUZ Q.

2.2.3. Preservación para perfiles de TikTok

a. Se ingresa al Formulario de solicitud de cumplimiento de la Ley de TikTok[18] con la siguiente URL www.tiktok.com/legal/report/lawenforcementrequest.

Luego se elige el país al cual se pertenece y dar click en el botón *submit*:



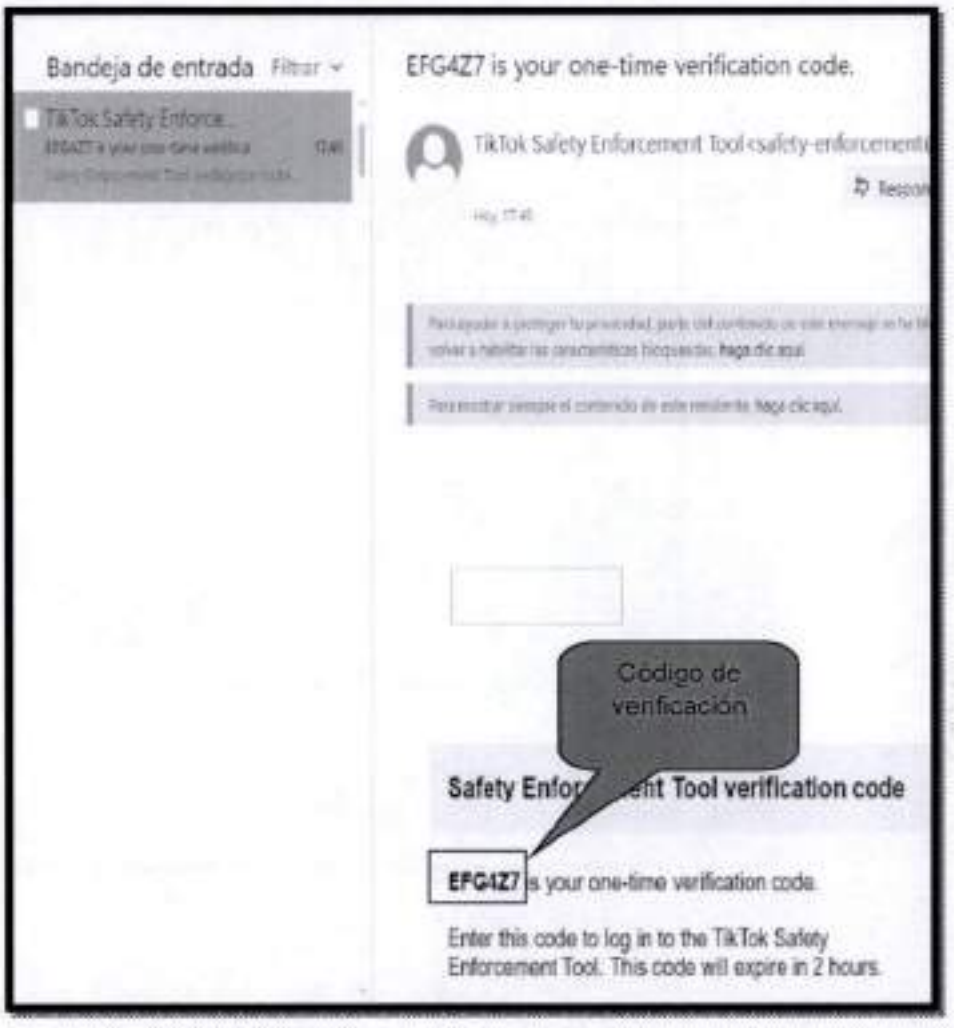
b. Luego la plataforma solicita el correo electrónico institucional, se debe seleccionar la opción *"An authorized GOVERNMENT OFFICIAL or acting on behalf of a government-approved entity"*, por último, dar *click* en el botón *"Log in"*, conforme a la siguiente captura de imagen:

[18] Plataforma informática habilitada por la empresa ByteDance, empresa que administra la red social TikTok, esta plataforma ayuda a los operadores de justicia a preservar información, solicitar registro con resolución judicial o por emergencia de perfiles de TikTok que se encuentren vinculados a la comisión de un ilícito penal.



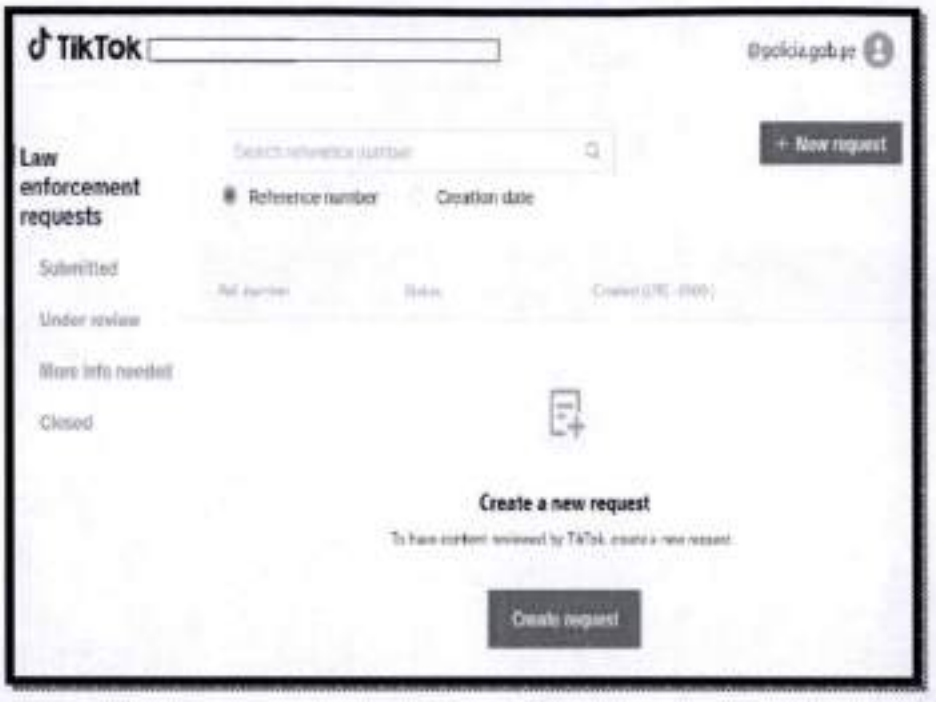
S. DE LA CRUZ Q.

c. La plataforma envía un código de verificación al correo electrónico institucional consignado previamente, dicho código debe ser consignado en dicha plataforma para poder ingresar, conforme a las siguientes imágenes:



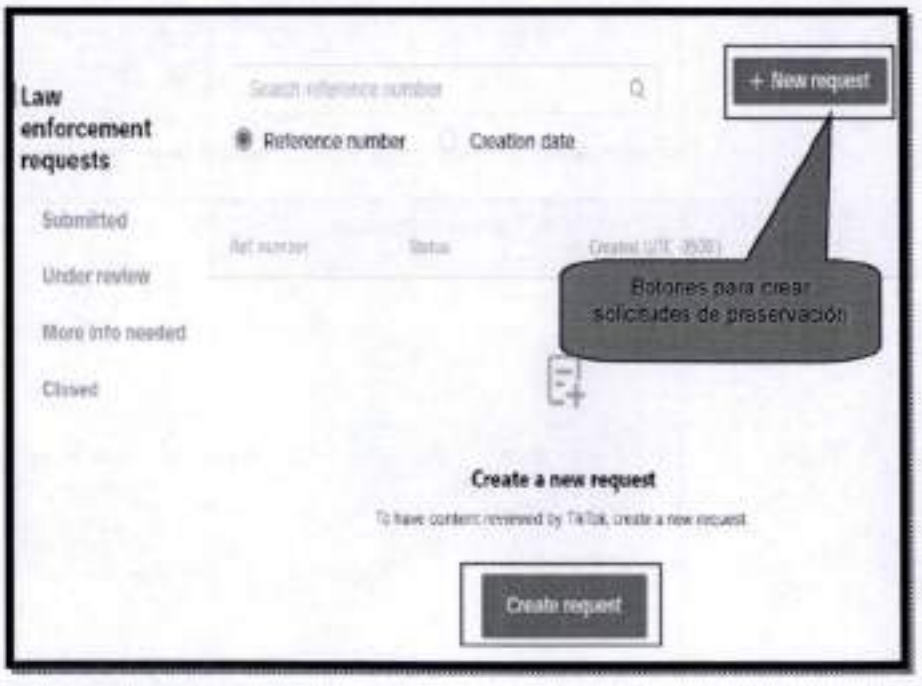


V°B°
S. DE LA CRUZ Q.



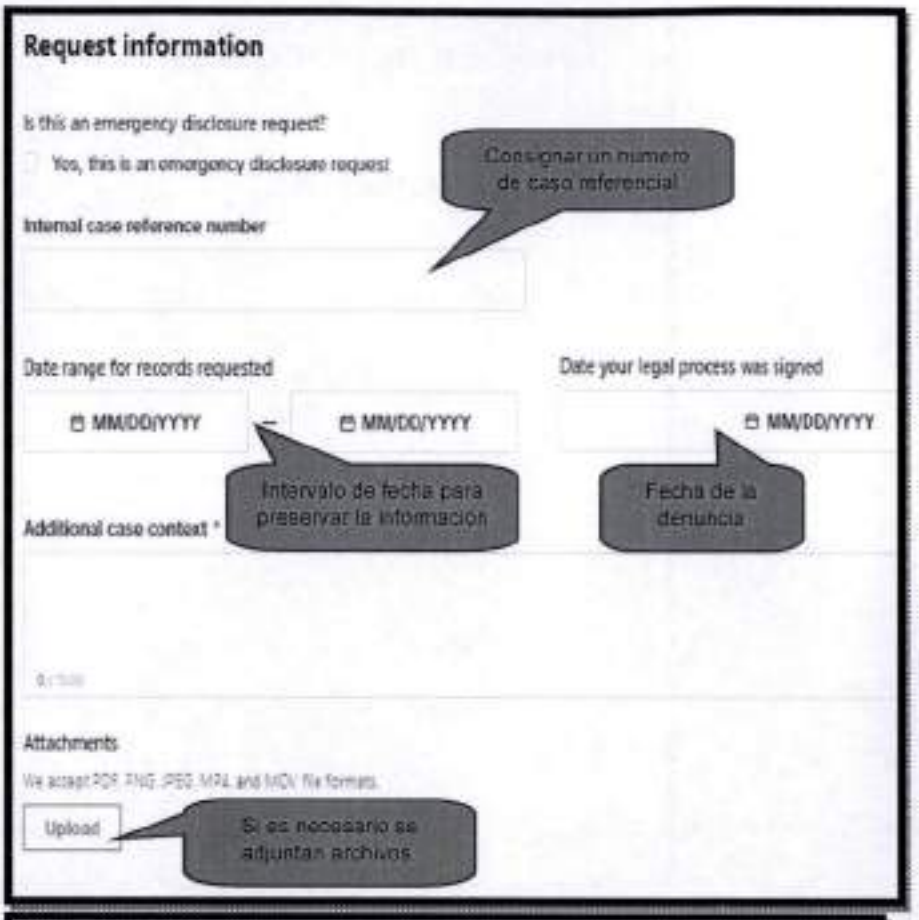
V°B°
S. DE LA CRUZ Q.

d. Para crear una solicitud de preservación, hacer *click* en el botón "*New request*" o "*Create request*" y proceder a consignar la información del solicitante, conforme a las siguientes imágenes:

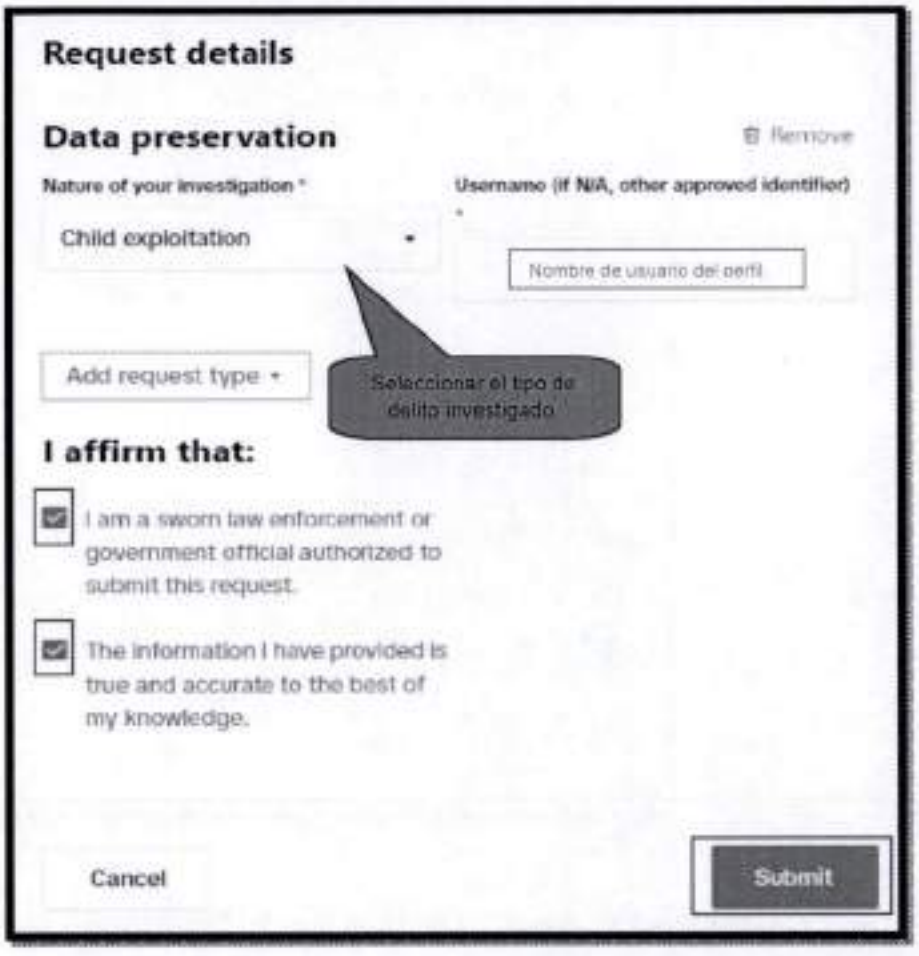




e. Asimismo, en la sección del detalle de la solicitud se elige la opción *"Data Preservation"*, luego consignar los datos solicitados, seguidamente hacer *click* en las opciones múltiples y finalmente hacer click en el botón *"Submit"*, conforme a las siguientes imágenes:

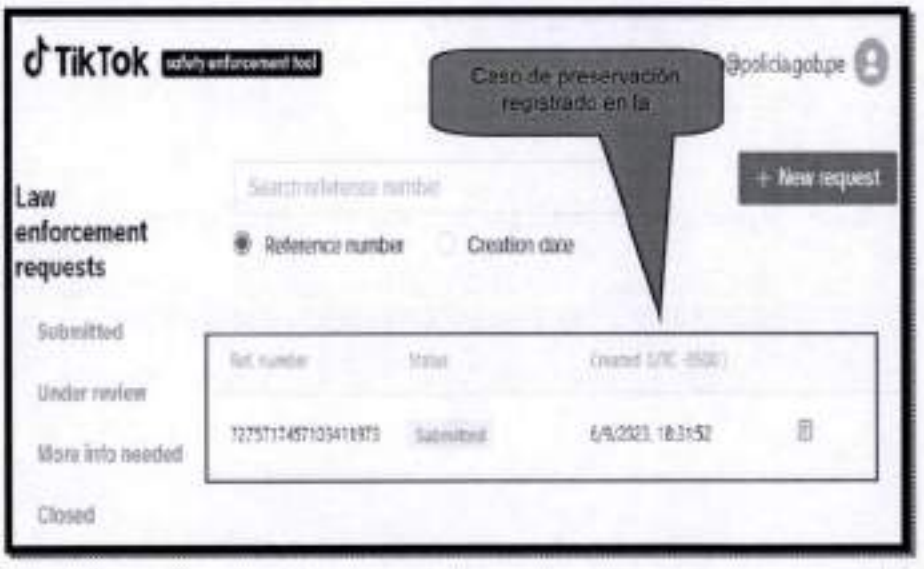

Request information
Is this an emergency disclosure request?
Yes, this is an emergency disclosure request
Internal case reference number
Consignar un numero de caso referencial
Date range for records requested
MM/DD/YYYY
MM/DD/YYYY
Intervalo de fecha para preservar la información
Date your legal process was signed
MM/DD/YYYY
Fecha de la denuncia
Additional case context *
Attachments
Upload
Si es necesario se adjuntan archivos


Request details
Add request type
Data preservation
Data disclosure
I affirm that:
I am a sworn law enforcement or government official authorized to submit this request.
The information I have provided is true and accurate to the best of my knowledge.
Cancel
Submit



S. DE LA CRUZ Q.

f. El caso de preservación se registra en la bandeja de casos, conforme a la siguiente imagen:





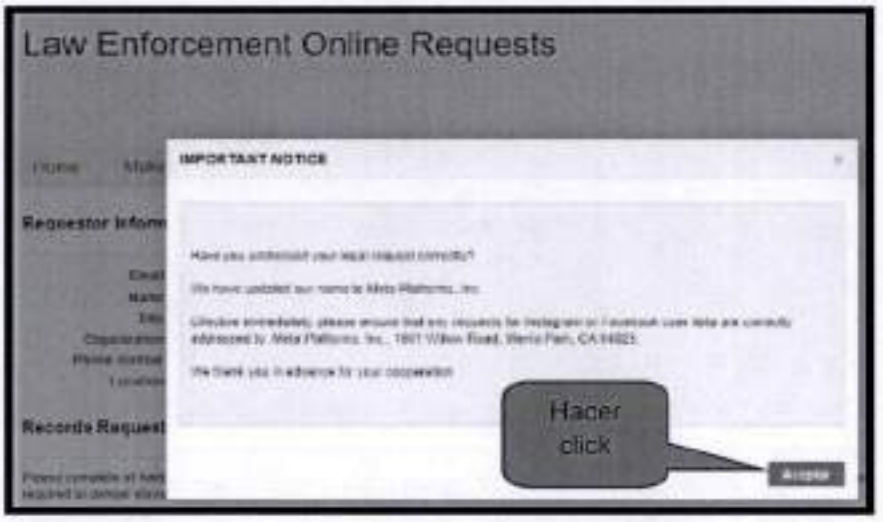
S. DE LA CRUZ Q.

2.3. Procedimiento de solicitud de registros de información en redes sociales

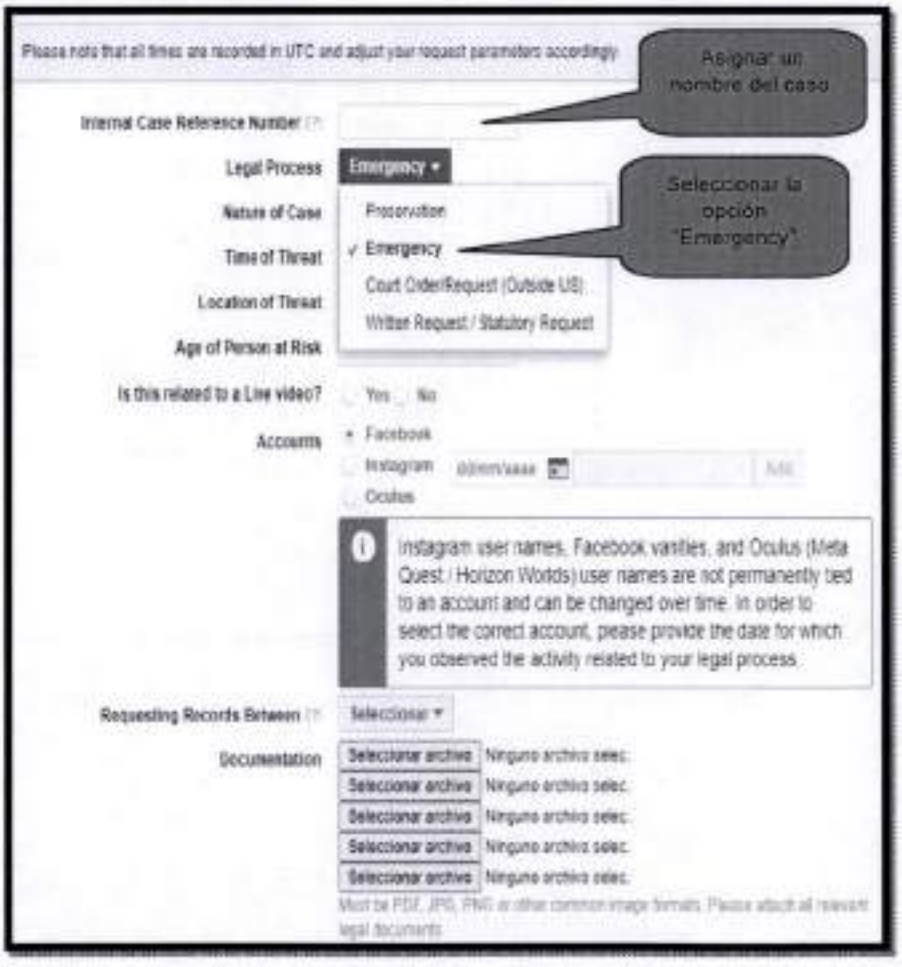
La solicitud de registro en casos de emergencia permite solicitar información técnica de perfiles de las redes sociales de Facebook, Instagram, WhatsApp y TikTok, relacionados a los registros de direcciones IP de inicio de sesión, el IP primigenio de registro, números de teléfonos vinculados, correos electrónicos vinculados, entre otros. Esto se lleva a cabo siempre que **exista riesgo inminente de muerte o daños corporales graves (a una persona o grupo de personas)**, sobre todo cuando se trata de casos donde menores de edad sean las víctimas.

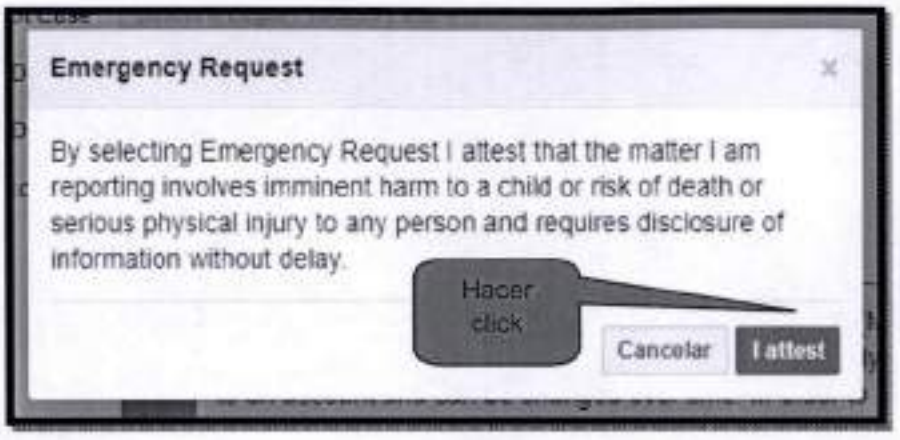
2.3.1. Procedimientos para *Facebook* e *Instagram*

a. Una vez dentro de la Plataforma de Aplicación de la Ley, se selecciona la pestaña ***"Make a Records Request"*** y se elige la naturaleza del caso.

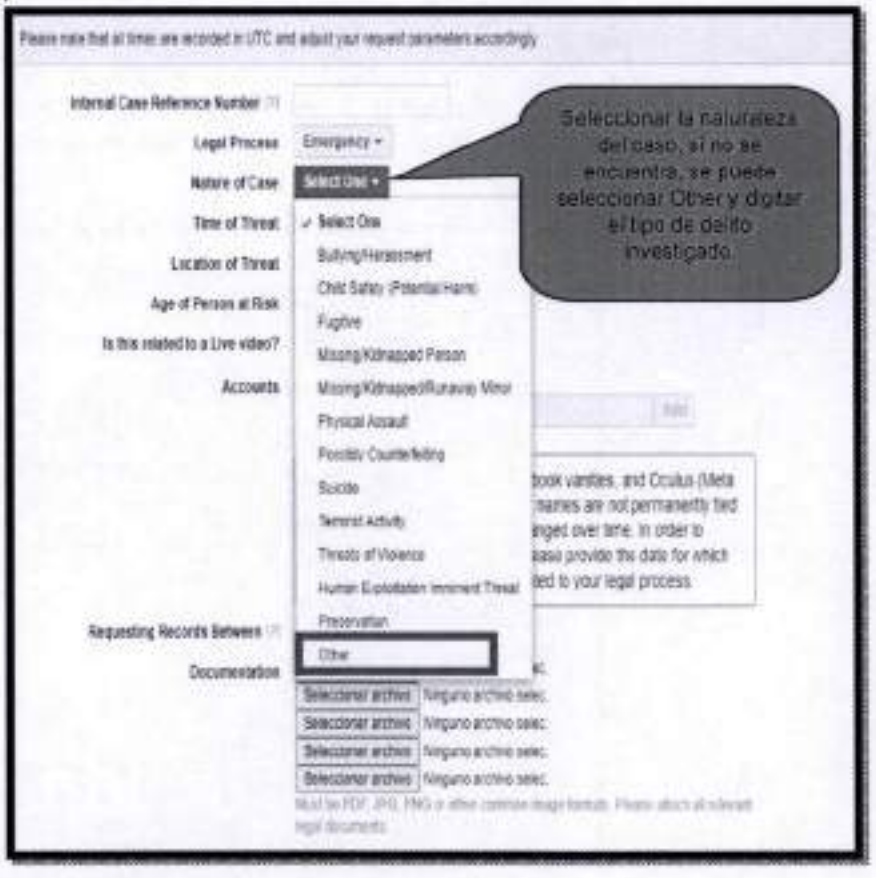


b. Al seleccionar la opción "*Emergency*", se muestra el siguiente aviso "*By selecting Emergency Request I attest that the matter I am reporting involves imminent harm to a child or risk of death or serious physical injury to any person and requires disclosure of information without delay*". Y proseguir en hacer click en el botón "*I attest*":





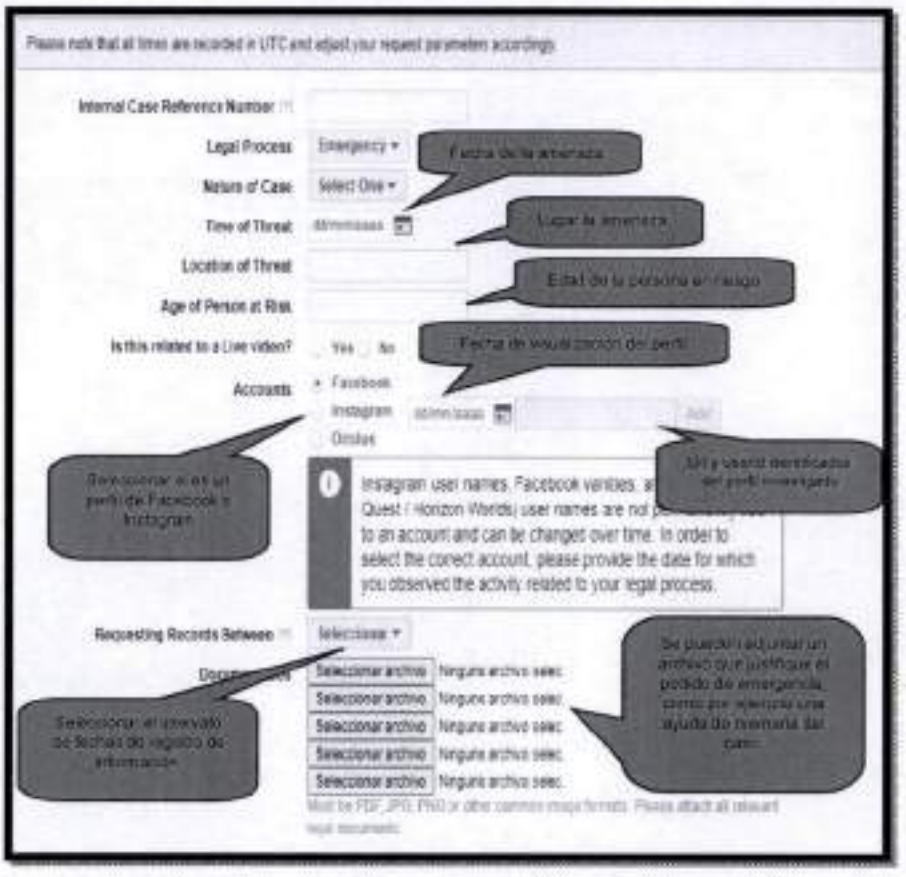
c. Se selecciona *"Nature of case"* que hace referencia al tipo de delito investigado.



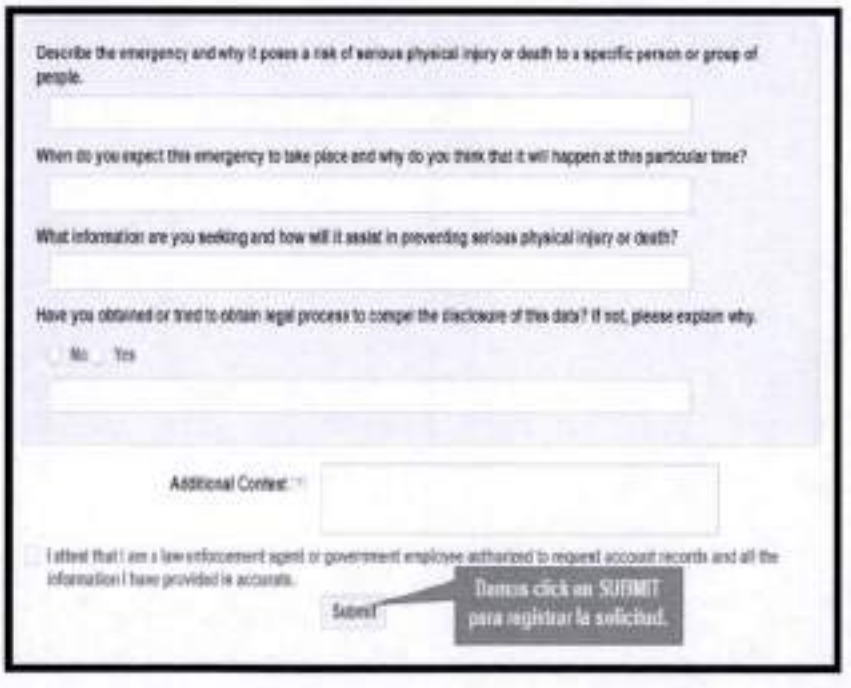
d. Se procede a consignar todos los datos que nos solicitan. Es importante que en la sección de documentación se realice una ayuda de memoria donde se narren los hechos investigados.

V°B°
S. DE LA CRUZ Q.

JURISPOL



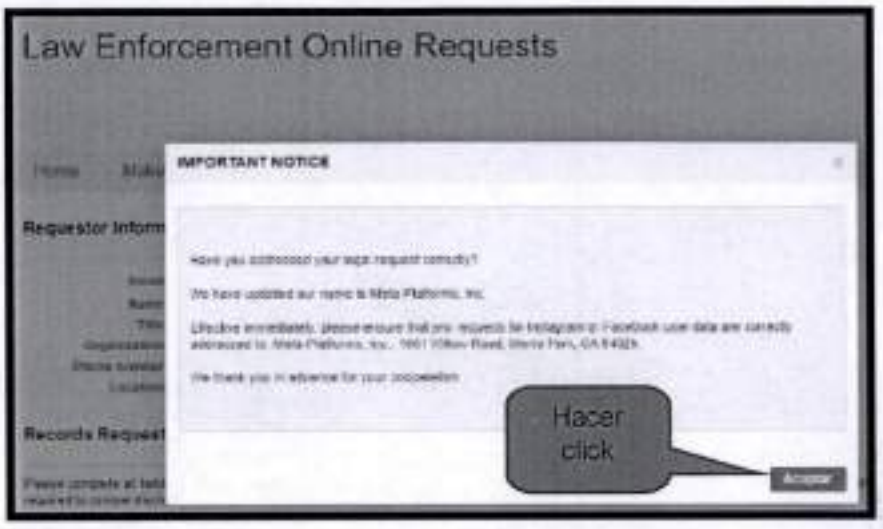
e. Por último, se debe justificar la solicitud respondiendo las preguntas mostradas en el formulario.



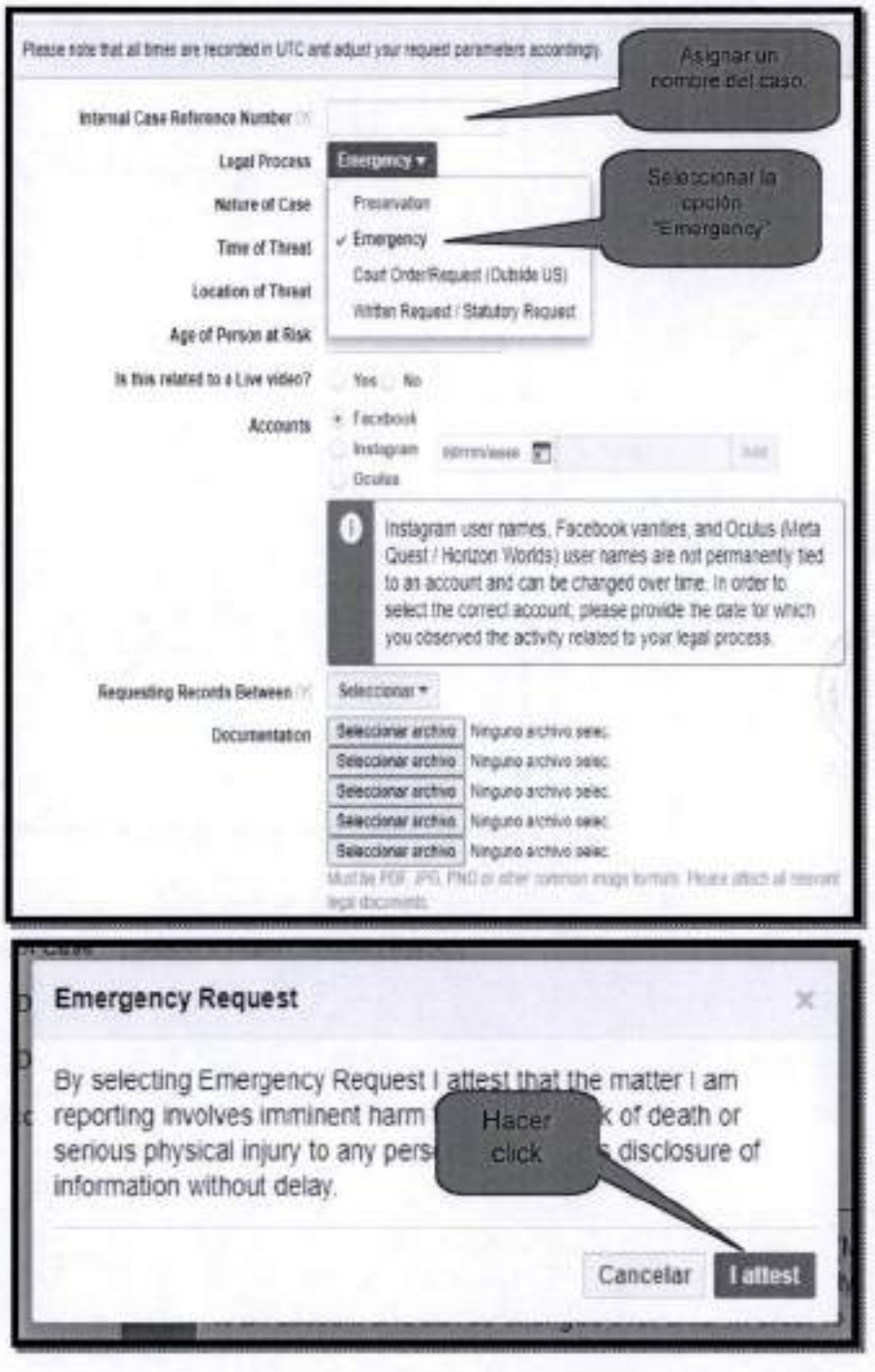
V°B°
S. DE LA CRUZ Q.

2.3.2. Procedimientos para *WhatsApp*

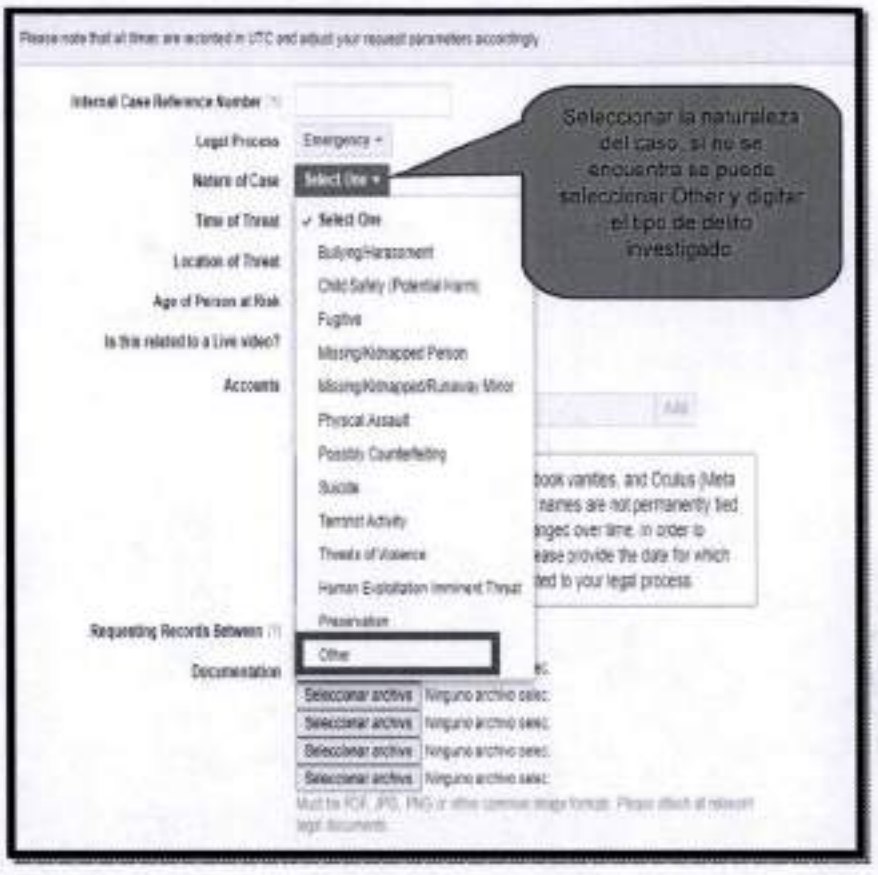
a. Una vez dentro de la Plataforma de Aplicación de la Ley, se selecciona la pestaña ***"Records Request"*** y se elige la naturaleza del caso.



b. Al seleccionar la opción *"Emergency"*, se muestra el siguiente aviso: *"By selecting Emergency Request I attest that the matter I am reporting involves imminent harm to a child or risk of death or serious physical injury to any person and requires disclosure of information without delay"*. Y proseguir en hacer click en el botón *"I attest"*:

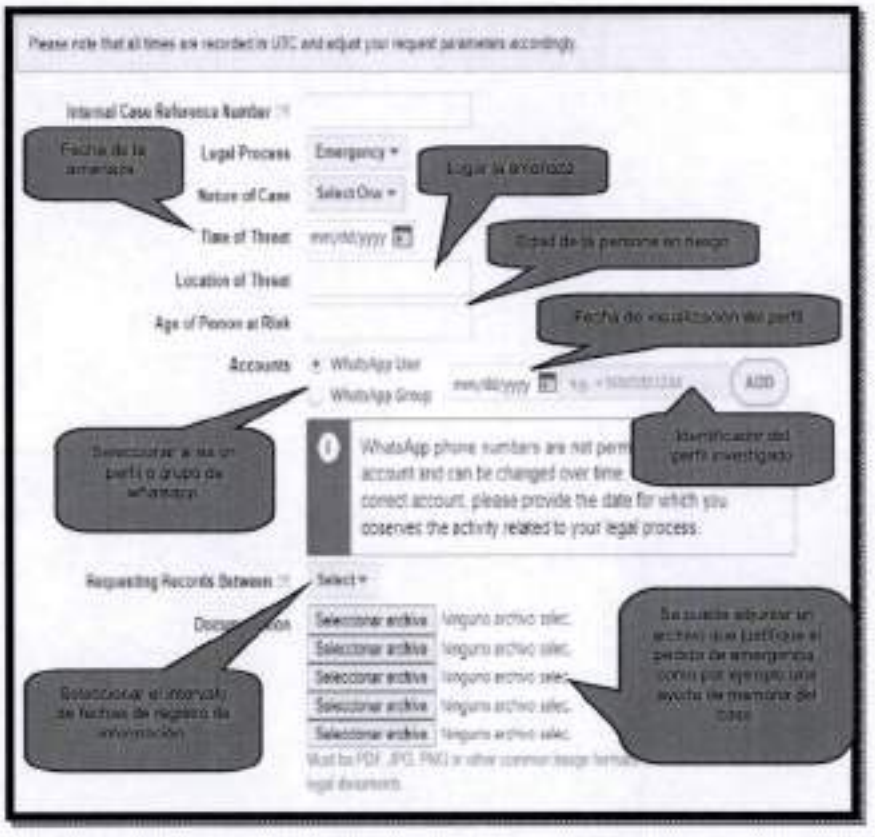


c. Se selecciona *"Nature of case"* que hace referencia al tipo de delito investigado.

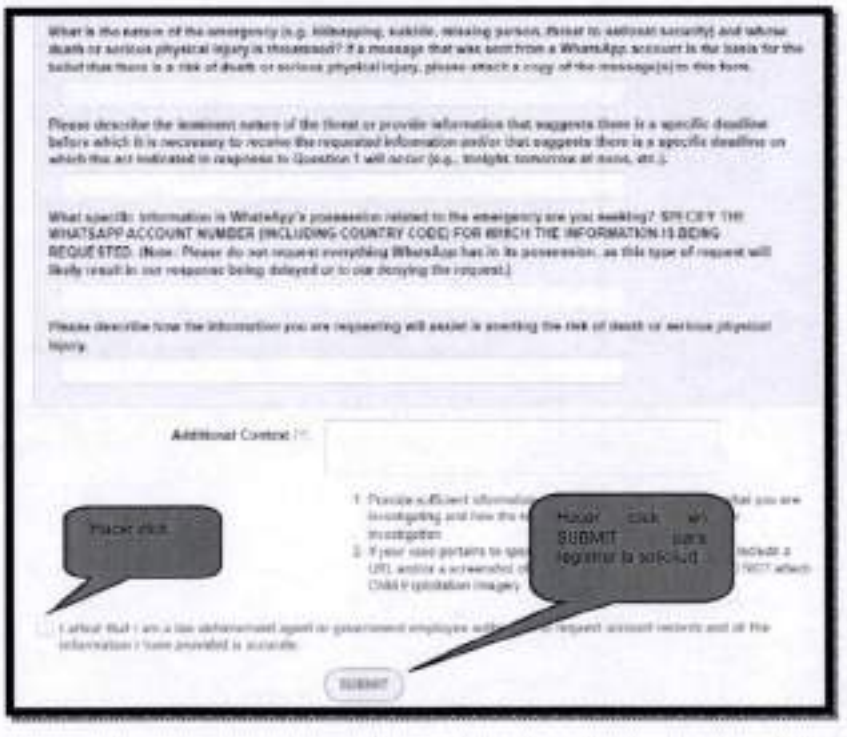


V°B°
S. DE LA CRUZ Q.

d. Se procede a consignar todos los datos que nos solicitan. Es importante que en la sección de documentación se realice una ayuda de memoria donde se narren los hechos investigados.

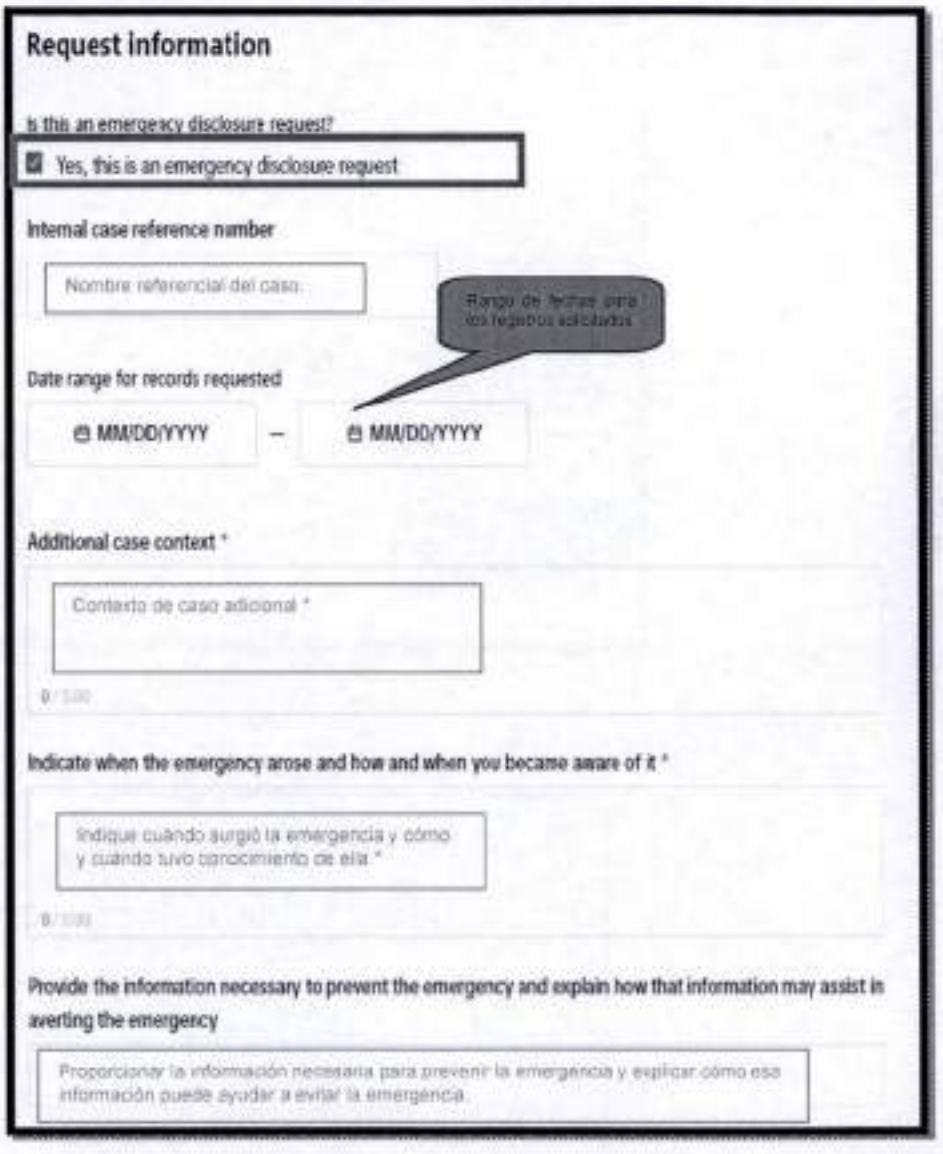


e. Por último, se debe justificar la solicitud respondiendo las preguntas mostradas en el formulario.



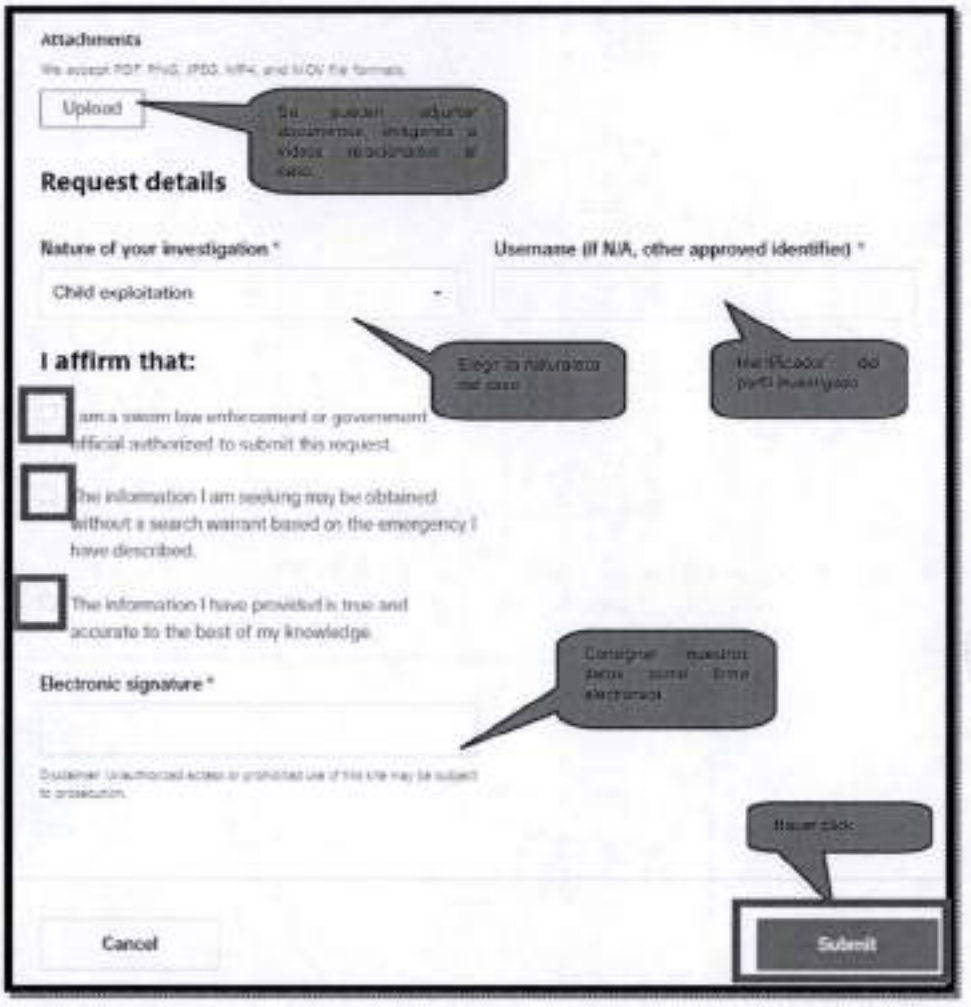
2.3.3. Procedimientos para *TikTok*

a. En la sección de *"Request information"*, se debe elegir la opción *"Yes, this is an emergency disclosure request"*, y consignar los datos solicitados:



b. Se consignan los datos solicitados, se elige la naturaleza de la investigación, se seleccionan las opciones de afirmación solicitadas y se procede a guardar con el botón *"Submit"*:

S. DE LA CRUZ Q.

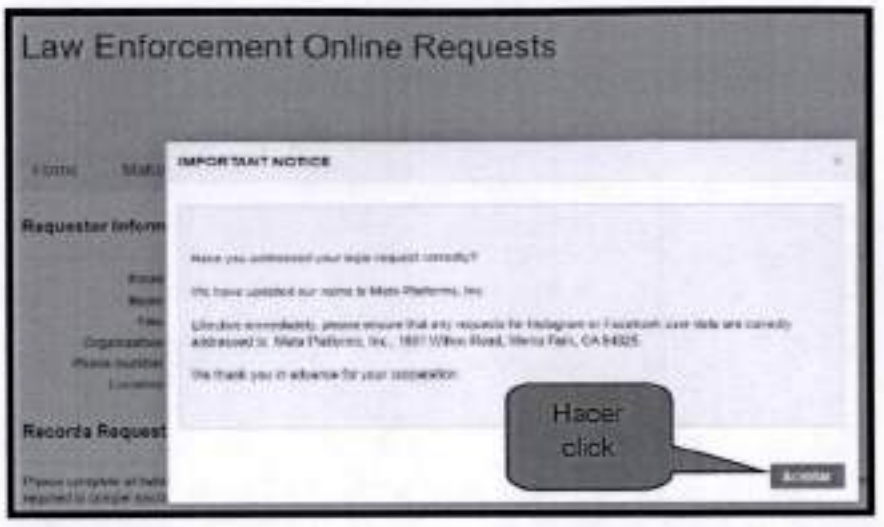


2.4. Solicitud de registro con Resolución Judicial

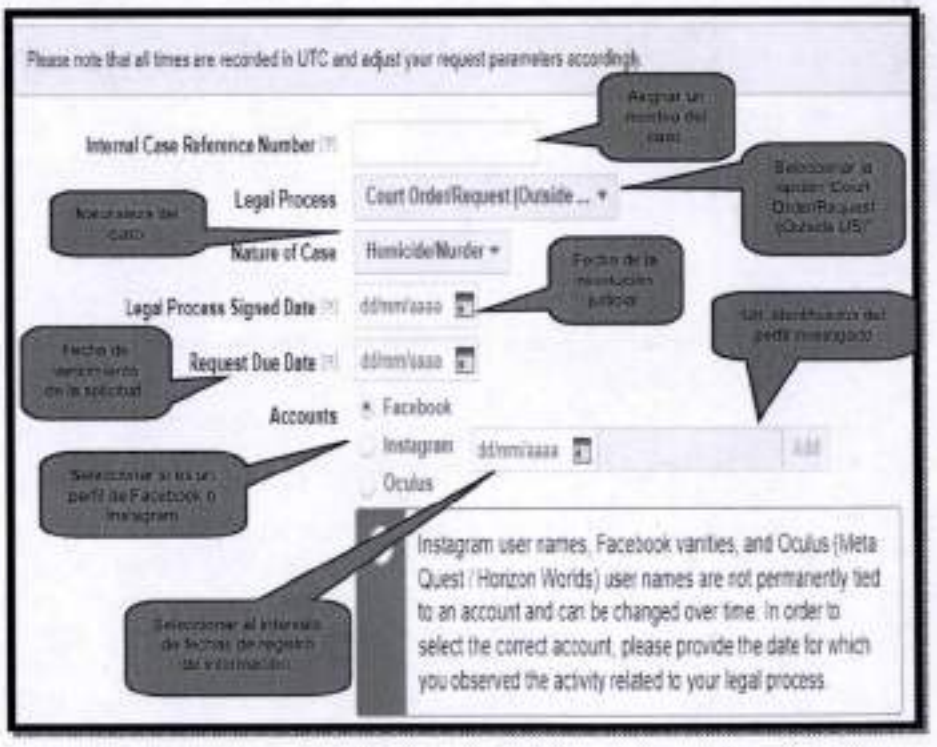
Permite solicitar información técnica de perfiles de las redes sociales de *Facebook*, *Instagram*, *WhatsApp* y *TikTok*, relacionados a los registros de direcciones IP de inicio de sesión, el IP primigenio de registro, número de teléfonos vinculados, correos electrónicos vinculados, entre otros. Esto se lleva a cabo siempre que se tenga la resolución judicial del Levantamiento del Secreto de las Comunicaciones y documentos privados de los perfiles de redes sociales investigados.

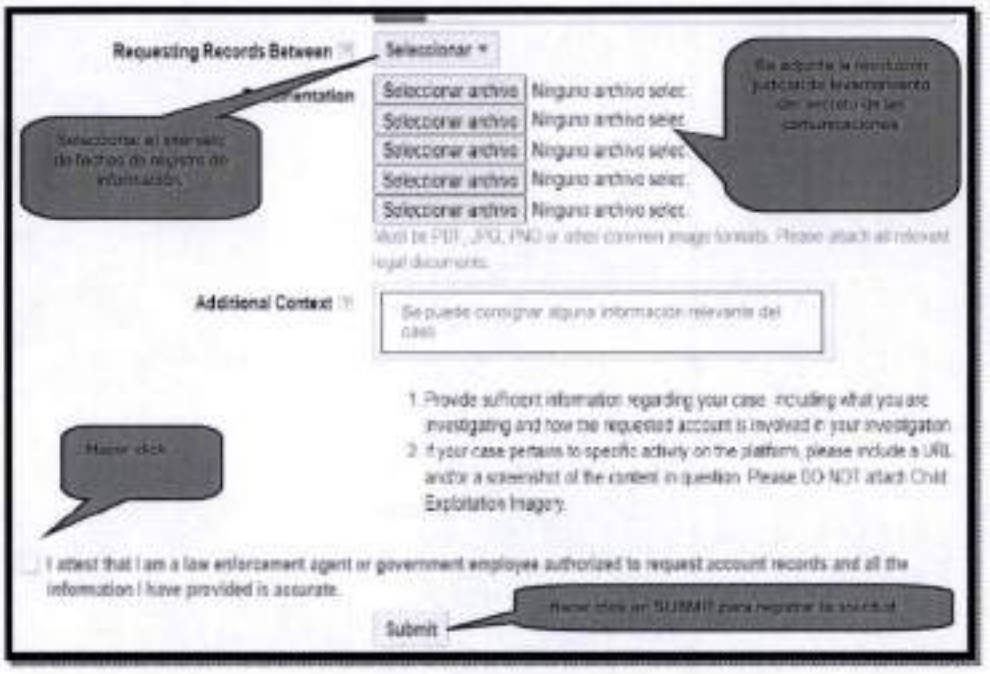
2.4.1. Procedimientos para Facebook e Instagram

a. Una vez dentro de la Plataforma de Aplicación de la Ley, se selecciona la pestaña ***"Make a Records Request"*** y se elige la naturaleza del caso.



b. Al seleccionar la opción *"Court Order/Request (Outside US)"* se procede a consignar los datos solicitados:

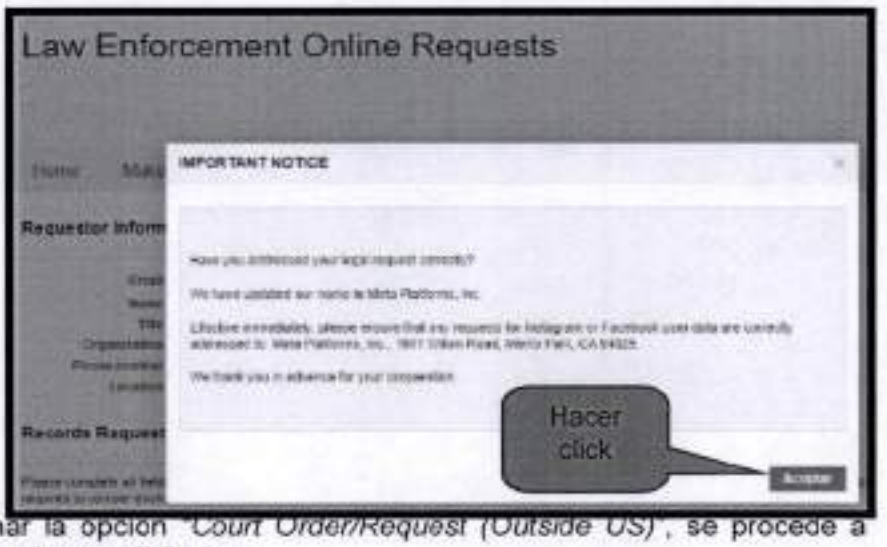




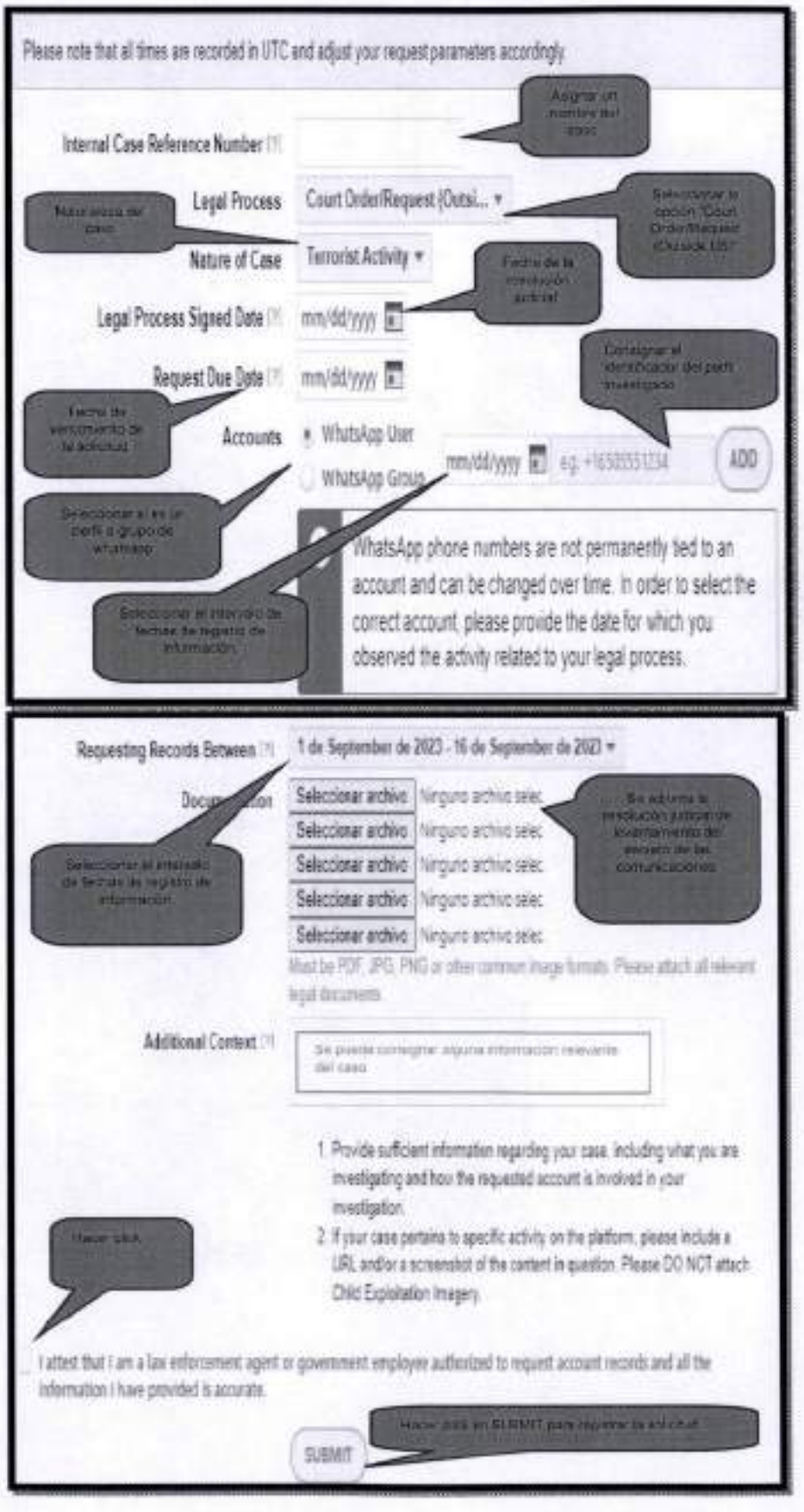
S. DE LA CRUZ Q.

2.4.2. Procedimientos para *WhatsApp*

a. Una vez dentro de la Plataforma de Aplicación de la Ley, se selecciona la pestaña ***"Records Request"*** y se elige la naturaleza del caso.



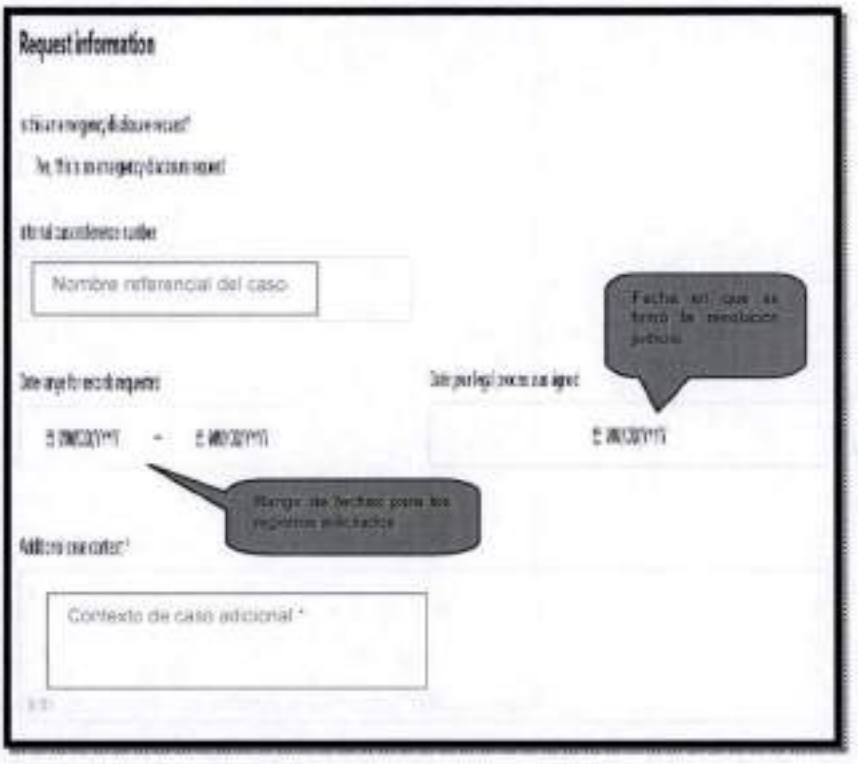
b. Al seleccionar la opción *"Court Order/Request (Outside US)"*, se procede a consignar los datos solicitados.


Please note that all times are recorded in UTC and adjust your request parameters accordingly
Internal Case Reference Number (?)
Legal Process
Court Order/Request (Outsi...
Nature of Case
Terrorist Activity
Legal Process Signed Date (?)
mm/dd/yyyy
Request Due Date (?)
mm/dd/yyyy
Accounts
WhatsApp User
WhatsApp Group
mm/dd/yyyy
e.g. +16505551234
ADD
WhatsApp phone numbers are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.
Requesting Records Between (?)
1 de September de 2023 - 16 de September de 2023
Seleccionar archivo
Ningún archivo selec
Must be PDF, JPG, PNG or other common image formats. Please attach all relevant legal documents
Additional Context (?)
1. Provide sufficient information regarding your case, including what you are investigating and how the requested account is involved in your investigation.
2. If your case pertains to specific activity on the platform, please include a URL and/or a screenshot of the content in question. Please DO NOT attach Child Exploitation Imagery.
I attest that I am a law enforcement agent or government employee authorized to request account records and all the information I have provided is accurate.
SUBMIT

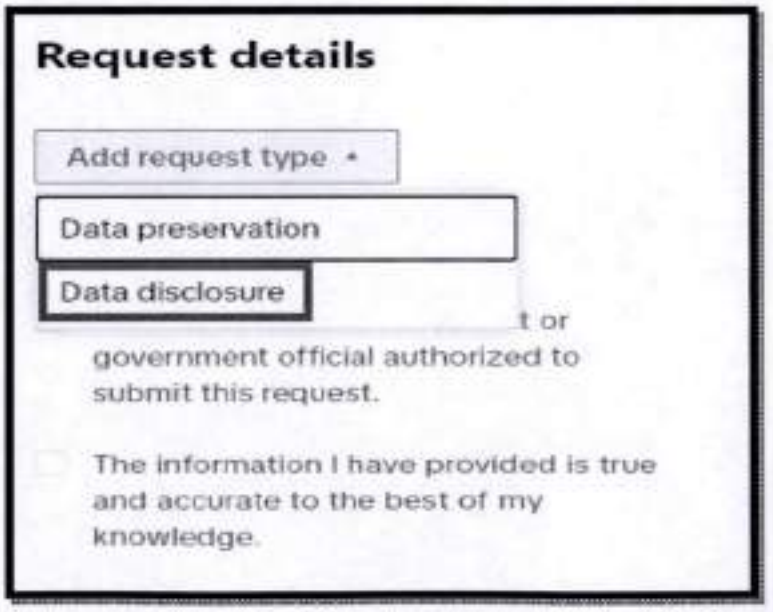
S. DE LA CRUZ Q.

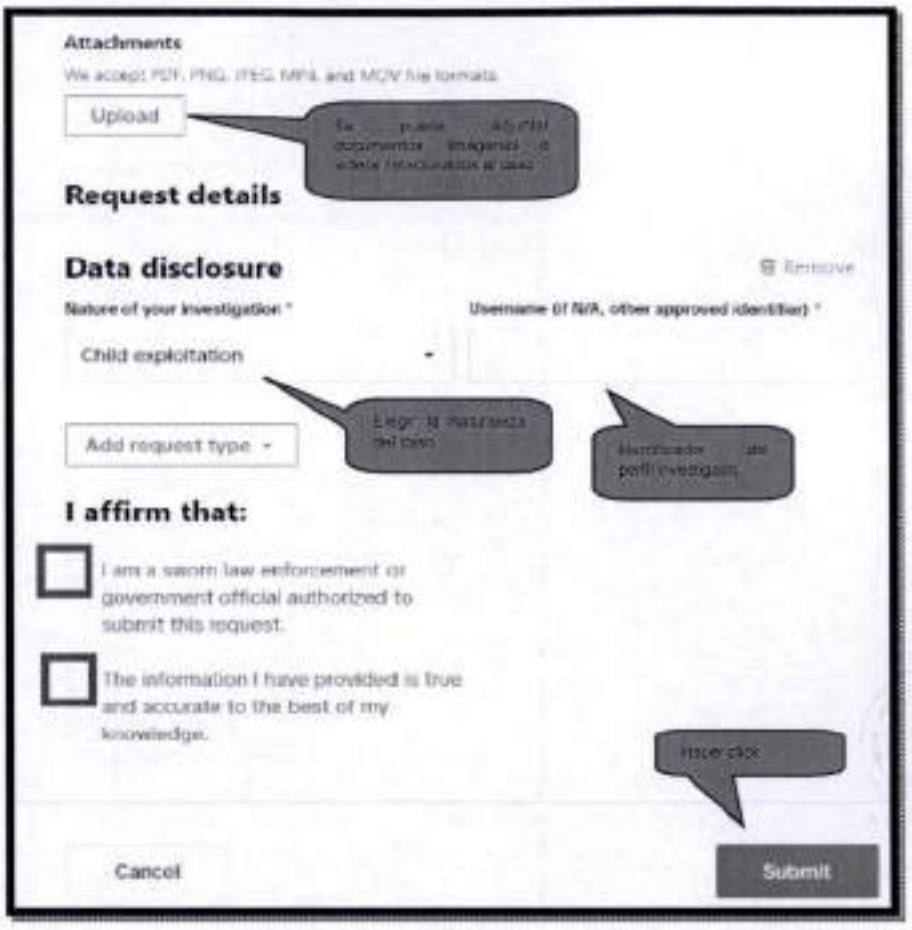
2.4.3. Procedimientos para *TikTok*

a. En la sección de "*Request information*" *se consignan* los datos solicitados:



b. En la sección de "*Request details*" se selecciona la opción "*Data disclosure*". Asimismo, se adjunta la resolución judicial en formato PDF y se consignan los siguientes datos:





V°B°
S. DE LA CRUZ Q.

CAPÍTULO III

PROCEDIMIENTOS PARA PRESERVAR UNA PÁGINA WEB Y/O DOMINIO WEB

La descarga de páginas *web* o dominios *web* mediante herramientas *software open source* (libres) o licenciadas como *HTTrack Website Copy, Cyotek WebCopy, Getleft*, entre otras, constituye una práctica esencial para la preservación digital responsable frente a la volatilidad inherente de internet.

Los contenidos digitales que se encuentran publicados en el internet, son útiles para investigaciones criminales, no obstante, desaparecen diariamente por cambios tecnológicos o porque siguen administrados por los autores de los hechos criminales. El uso de *software* de descarga de páginas *web* o sitios *web* y generando la respectiva cadena de custodia garantiza transparencia en el proceso técnico de preservación de este tipo de evidencia digital. La recopilación de evidencia digital publicada en el internet puede usarse para:



- Preservar sitios *web* sospechosos (por ejemplo, foros ilegales, páginas de venta de drogas, *phishing*, entre otros) antes de que sean modificados o eliminados.
- Crear copias *off line* de páginas relevantes para análisis forense posterior sin depender de la conexión a internet o la disponibilidad del sitio original.
- Documentar contenido público como parte de una investigación preliminar.

Para mejor ilustración se detallan los siguientes procedimientos utilizando el *software HTTRACK Website Copier*, que permite descargar una página *web* y/o sitio *web*, sin embargo, existen diferentes herramientas *open source* y/o licenciadas que pueden ser utilizadas.

3.1. Uso del software HTTRACK Website Copier

3.1.1. Descarga e Instalación del software HTTRACK Website Copier

a. Se descarga el software *HTTRACK Website Copier* del sitio web https://www.httrack.com/page/2/en/index.html y se elige la mejor opción de descarga de acuerdo a las características de la computadora donde se trabaja la preservación.

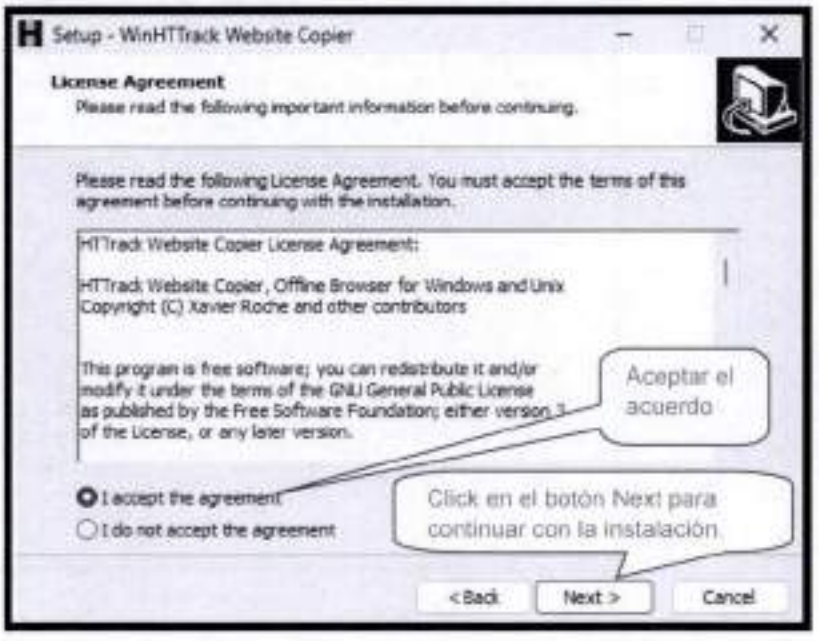




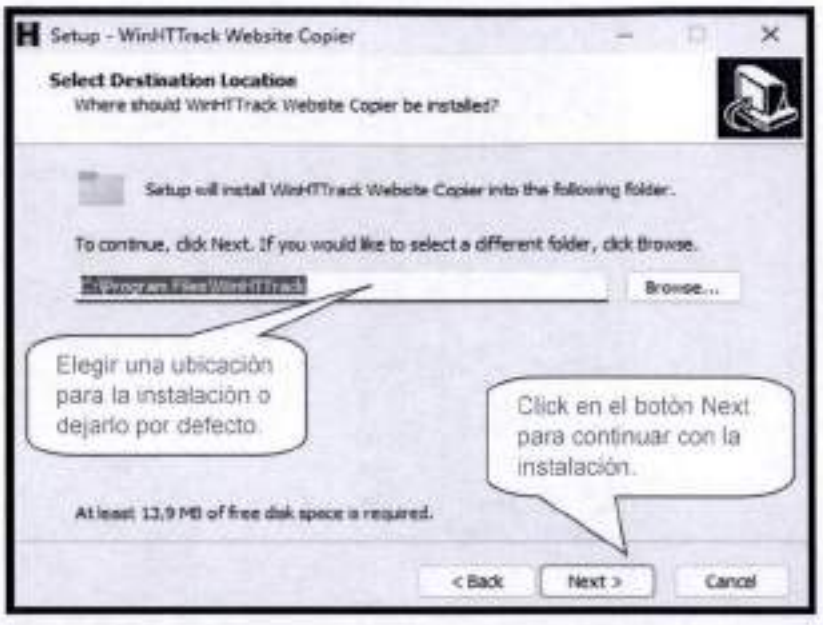
b. Instalar el *software HTTRACK Website Copier* descargado, conforme a las siguientes capturas de pantalla:

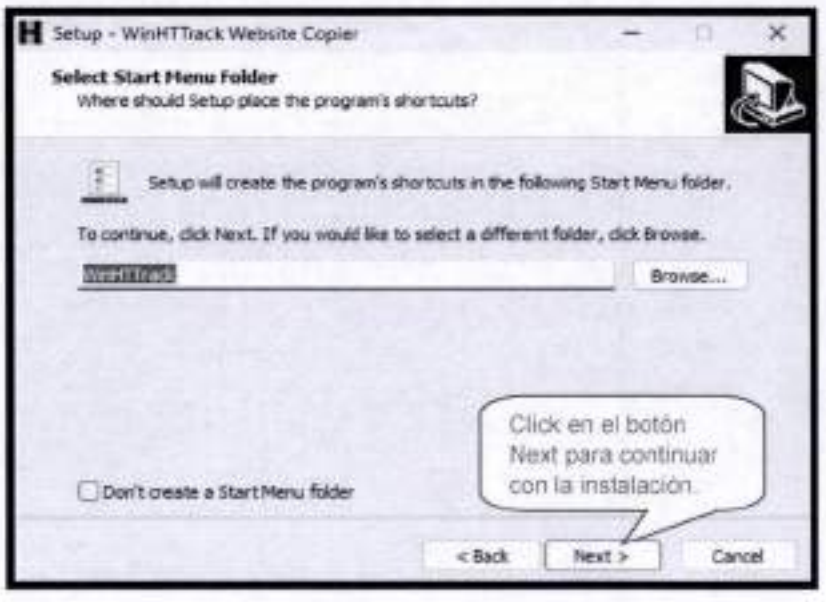




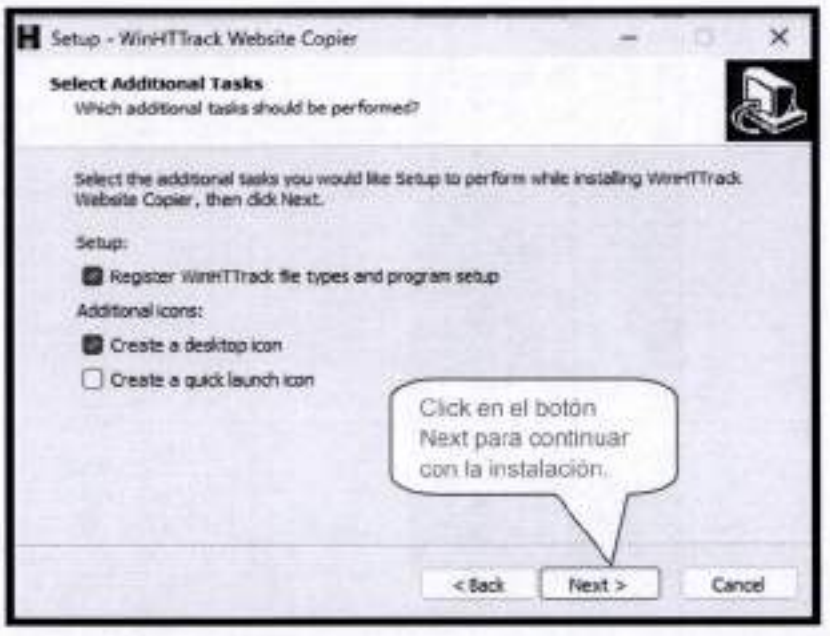


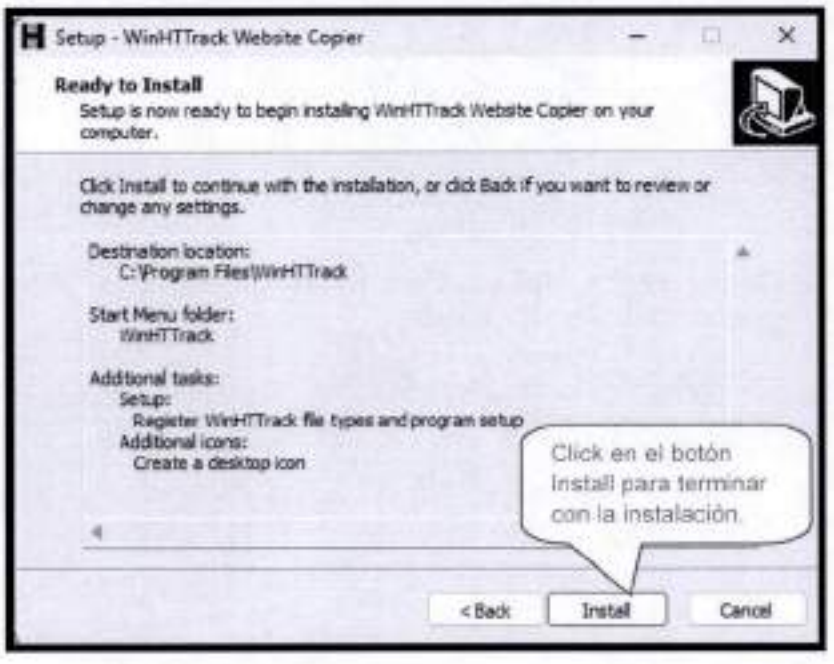
V°B°
S. DE LA CRUZ Q.

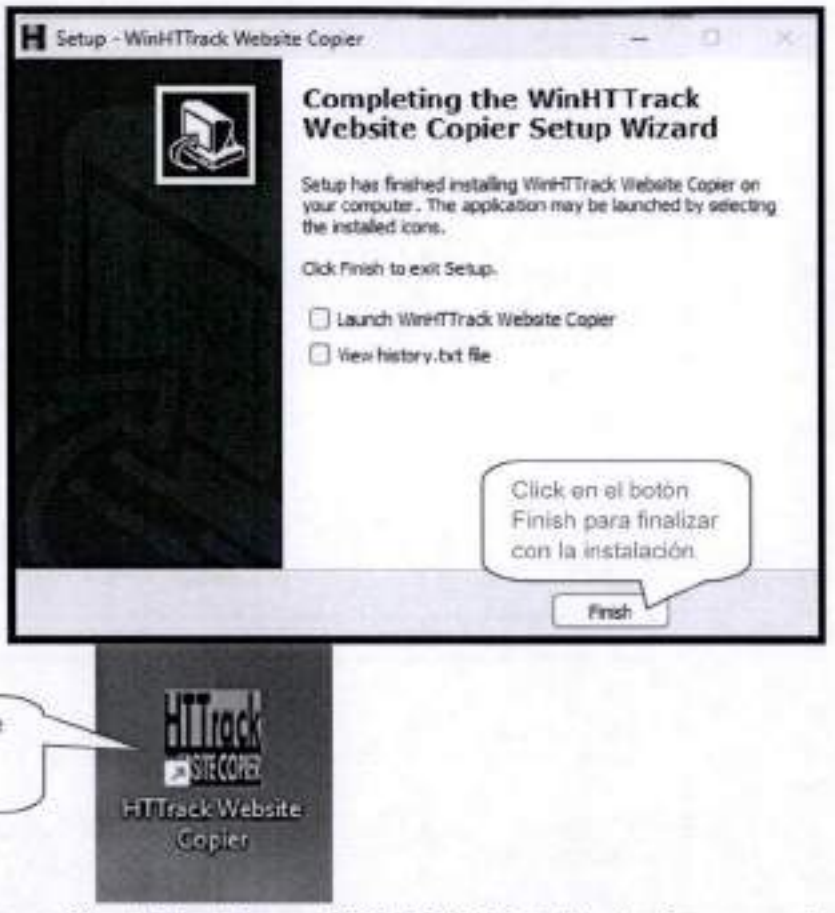

Setup - WinHTTrack Website Copier
Select Destination Location
Where should WinHTTrack Website Copier be installed?
Setup will install WinHTTrack Website Copier into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Browse...
Elegir una ubicación para la instalación o dejarlo por defecto.
Click en el botón Next para continuar con la instalación.
At least 13,9 MB of free disk space is required.
< Back
Next >
Cancel


Setup - WinHTTrack Website Copier
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Browse...
Don't create a Start Menu folder
Click en el botón Next para continuar con la instalación.
< Back
Next >
Cancel

S. DE LA CRUZ Q.


Setup - WinHTTrack Website Copier
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing WinHTTrack Website Copier, then click Next.
Setup:
Register WinHTTrack file types and program setup
Additional icons:
Create a desktop icon
Create a quick launch icon
Click en el botón Next para continuar con la instalación.
< Back
Next >
Cancel


Setup - WinHTTrack Website Copier
Ready to Install
Setup is now ready to begin installing WinHTTrack Website Copier on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\WinHTTrack
Start Menu folder:
WinHTTrack
Additional tasks:
Setup:
Register WinHTTrack file types and program setup
Additional icons:
Create a desktop icon
Click en el botón Install para terminar con la instalación.
< Back
Install
Cancel

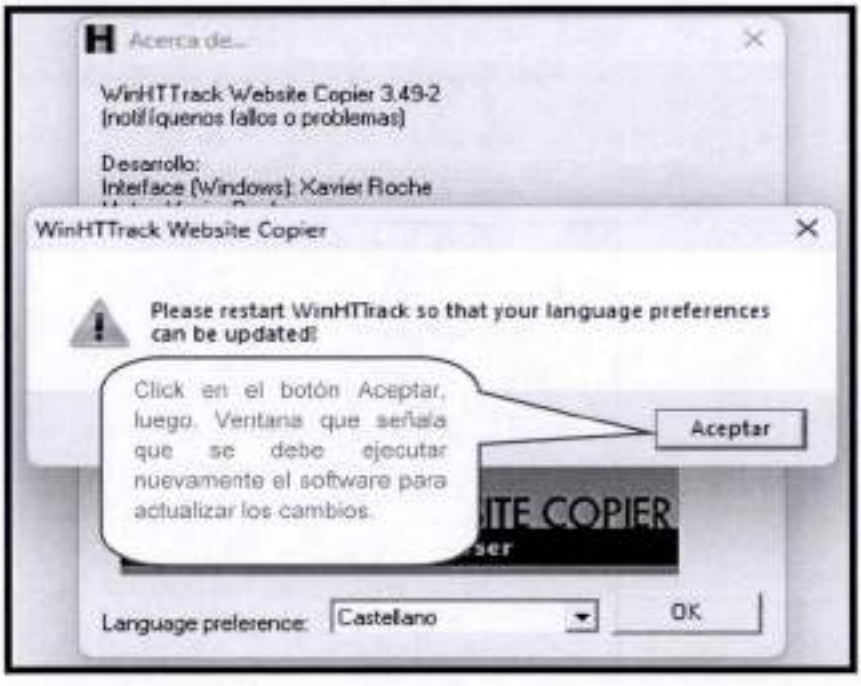


3.1.2. Configuración del software HTTRACK Website Copier para descargar página web y/o sitios web.

Previamente el instructor del caso debe haber identificado la página web o sitio web vinculado a la investigación realizada.

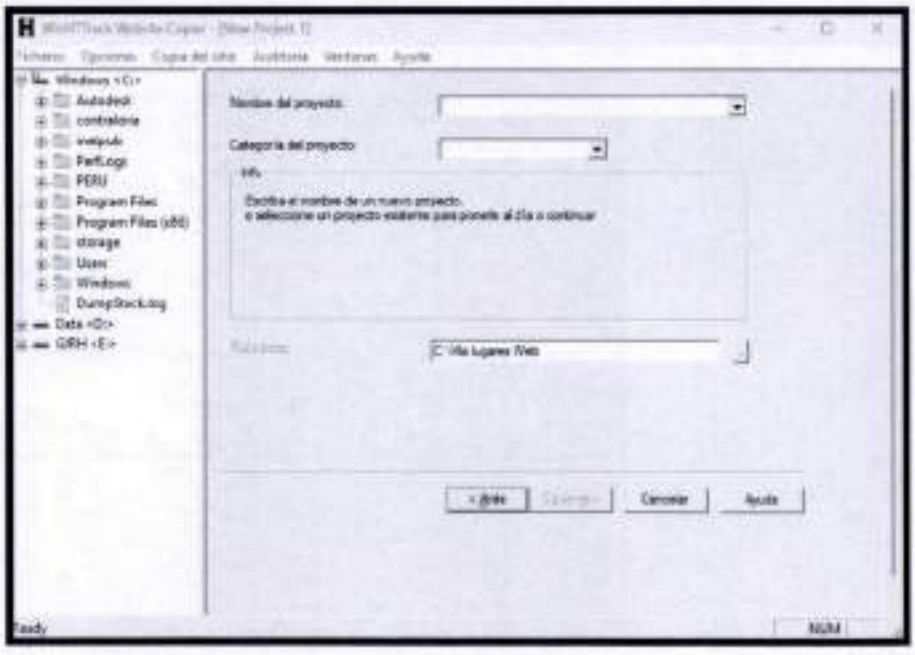
a. Ejecutar el *software HTTRACK Website Copier*, para una mejor comodidad configurar el mencionado software a lenguaje español:


About WinHTTrack Website Copier
WinHTTrack Website Copier 3.49-2
(Please notify us of any bug or problem)
Development:
Interface (Windows): Xavier Roche
Spider: Xavier Roche
JavaParserClasses: Yann Philippot
(C)1998-2003 Xavier Roche and other
MANY THANKS for translation tips to:
Robert Lagadec (rlagadec@yahoo.fr)
Please visit our Web page :
http://www.httrack.com
Seleccionar lenguaje Castellano y luego el botón OK.
HTTrack WEBSITE COPIER
Open Source offline browser
Language preference:
English
OK

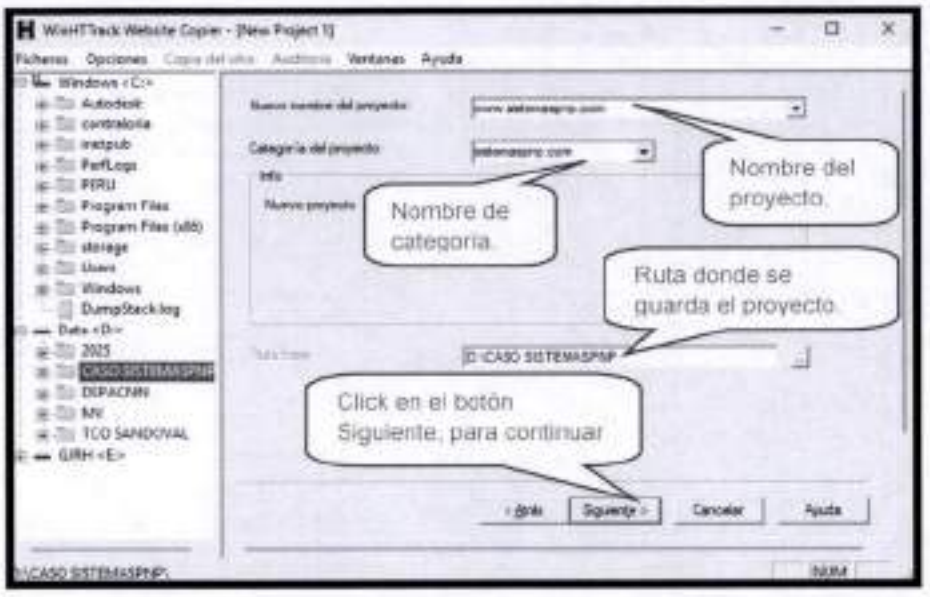

Acerca de...
WinHTTrack Website Copier 3.49-2
(notifíquenos fallos o problemas)
Desarrollo:
Interface (Windows): Xavier Roche
WinHTTrack Website Copier
Please restart WinHTTrack so that your language preferences can be updated!
Click en el botón Aceptar, luego. Ventana que señala que se debe ejecutar nuevamente el software para actualizar los cambios.
Aceptar
Language preference:
Castellano
OK



b. Ejecutar y configurar el *software HTTRACK Website Copier* para descargar el sitio *web* "www.sistemaspnp.com" (como ejemplo):

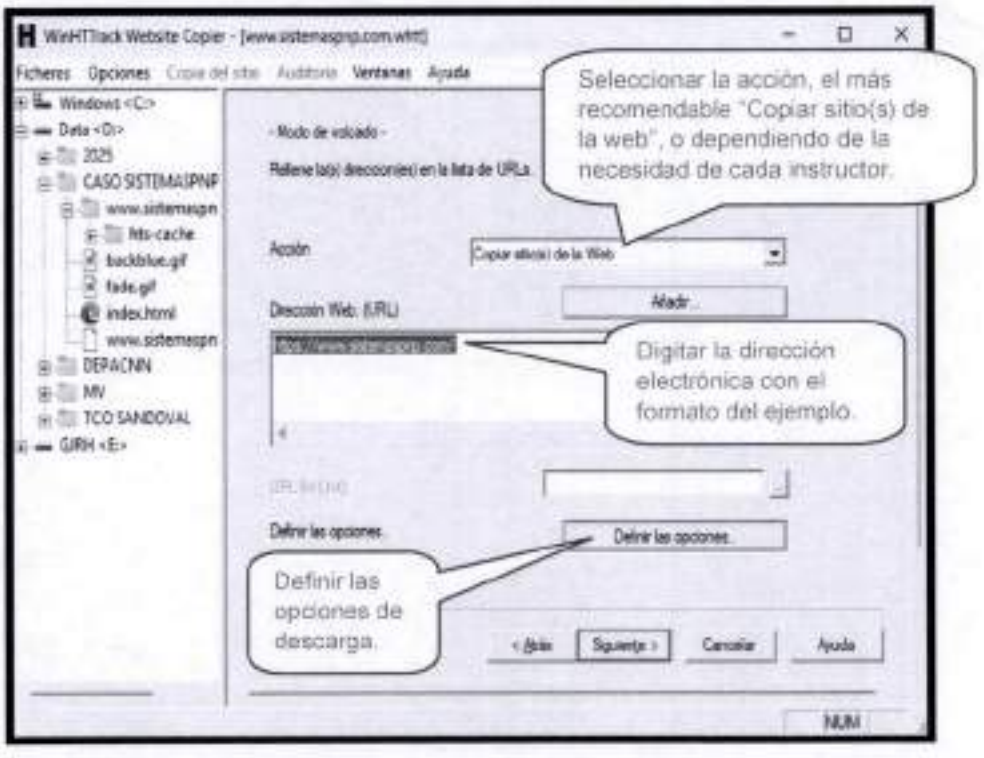


c. Consignar el nombre del proyecto, nombre de la categoría, la ruta electrónica donde se guarda el proyecto, se sugiere colocar datos que puedan relacionarse al caso investigado para tener un mejor orden, conforme a la siguiente imagen:

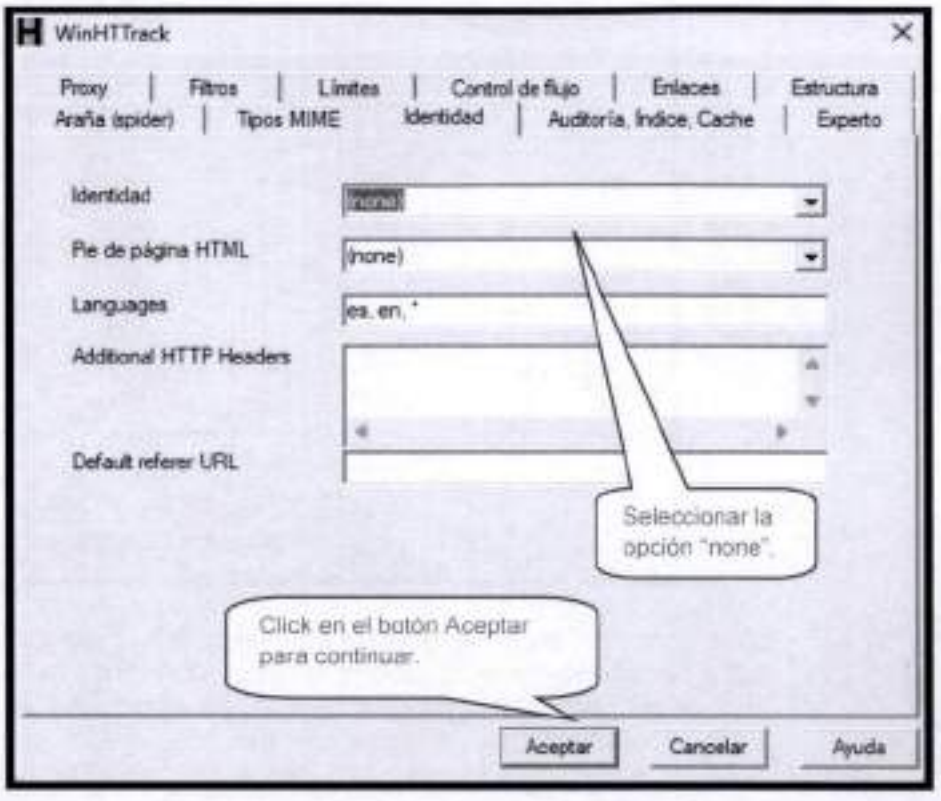


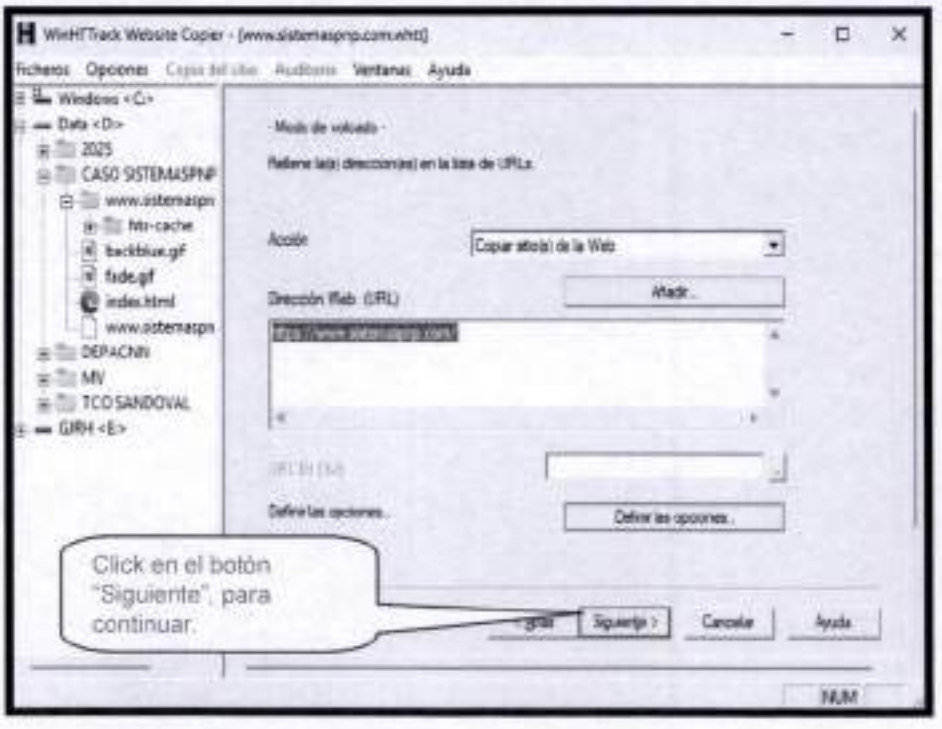
S. DE LA CRUZ Q.

d. Seleccionar el tipo de acción para el volcado o copia del sitio *web*, depende de la necesidad del instructor del caso; consignar la dirección electrónica (URL) de la página *web* y/o sitio *web*; definir opciones y continuar, conforme a la siguiente imagen:

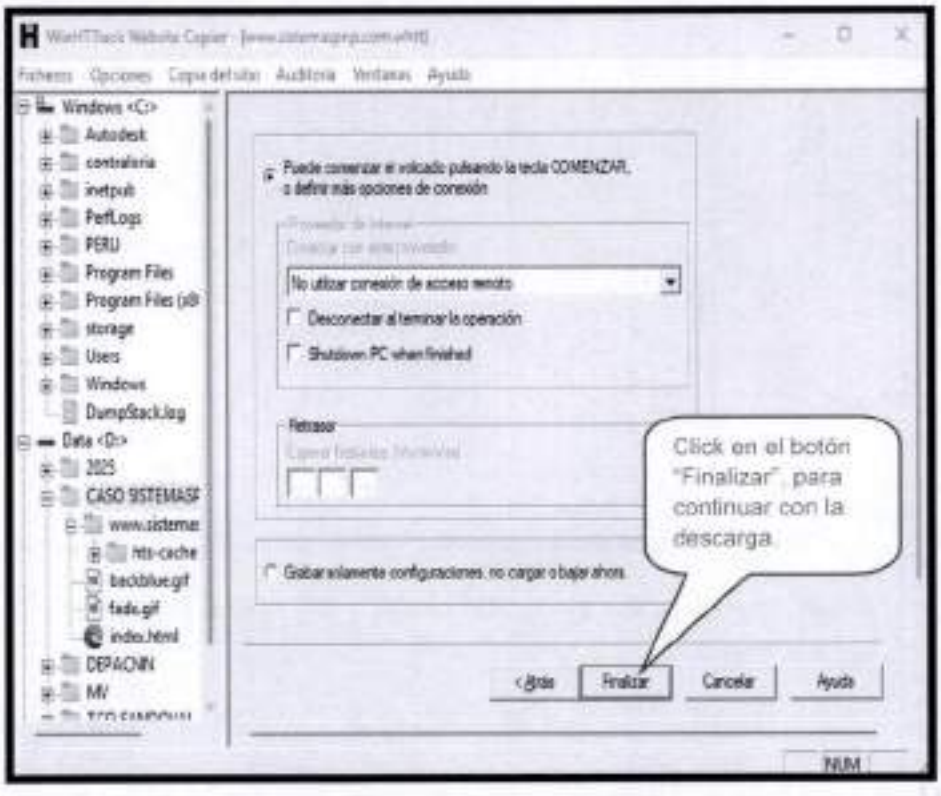


e. En el botón "Definir las opciones...", en la ficha "Identidad", en las listas Identidad y Pie de página HTML, seleccionar la opción "*(none)*", para no registrar la descarga de la información en el servidor, por último, continuar presionando el botón "Siguiente".





f. Para empezar la descarga, después de la configuración recomendada, hacer click en el botón "Finalizar".



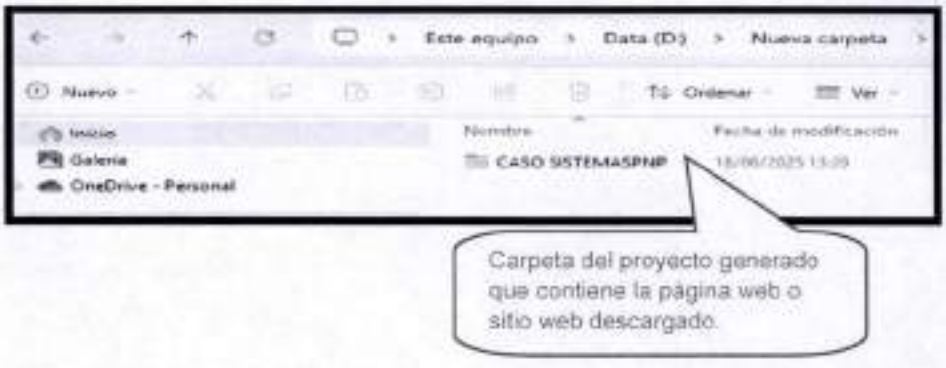


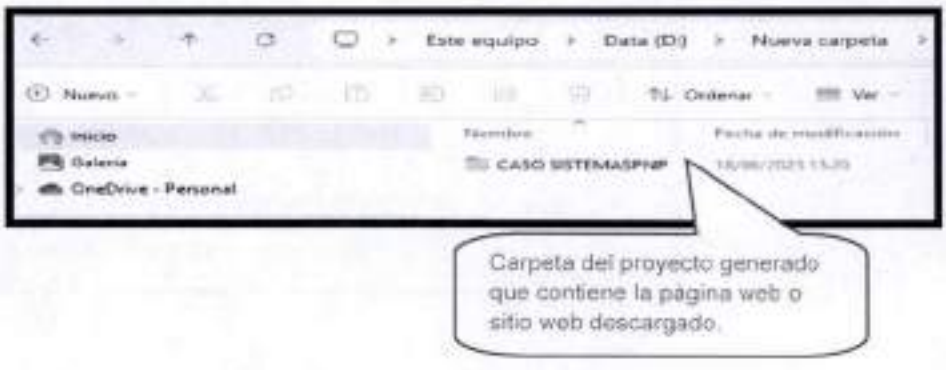
g. Luego de terminado la descarga, hacer click en el botón "Finalizar", para terminar el procedimiento y posteriormente verificar la descarga.



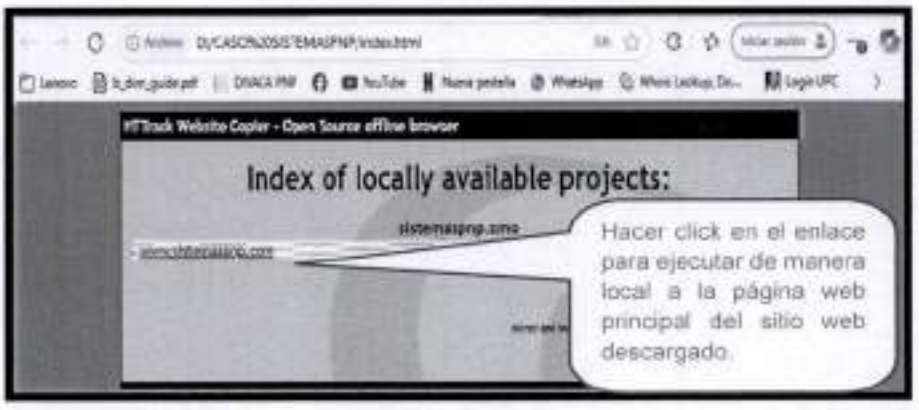
3.1.3. Verificación de la descarga y preservación de la página web y/o sitio *web*

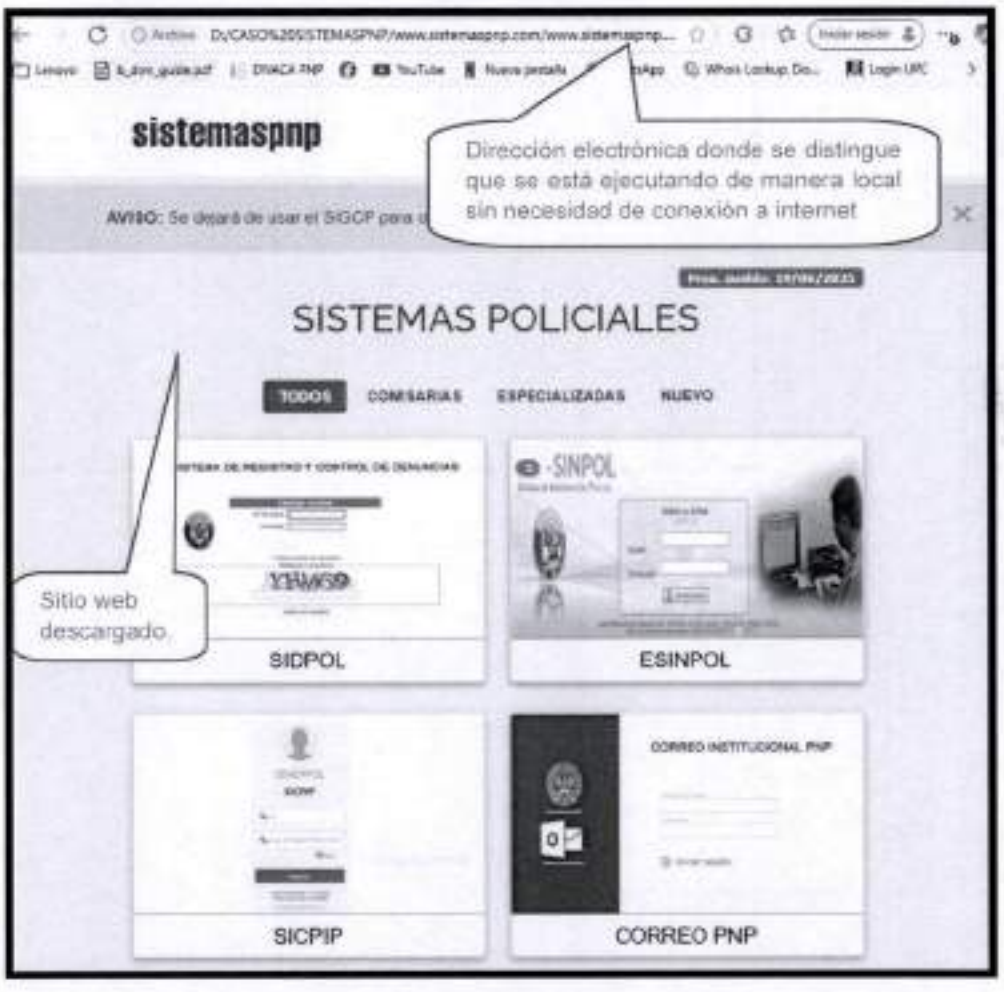
a. Proceder con la verificación de la descarga de la página *web* o sitio *web*.





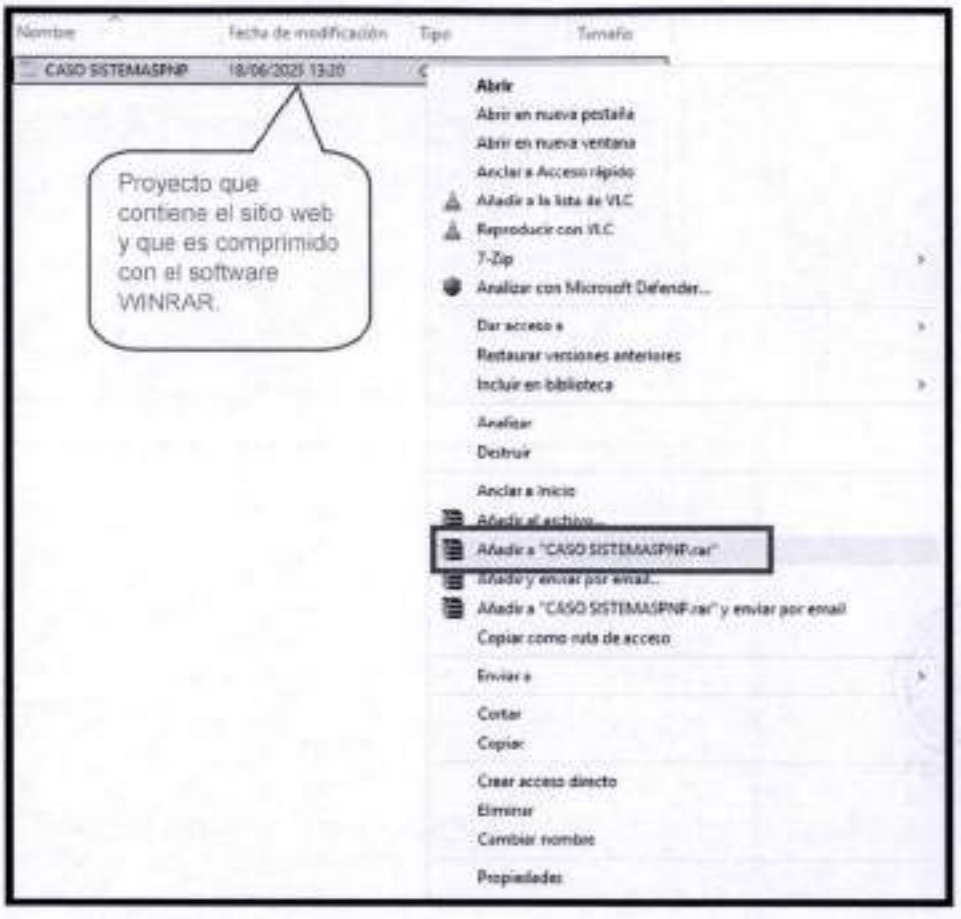
S. DE LA CRUZ Q.



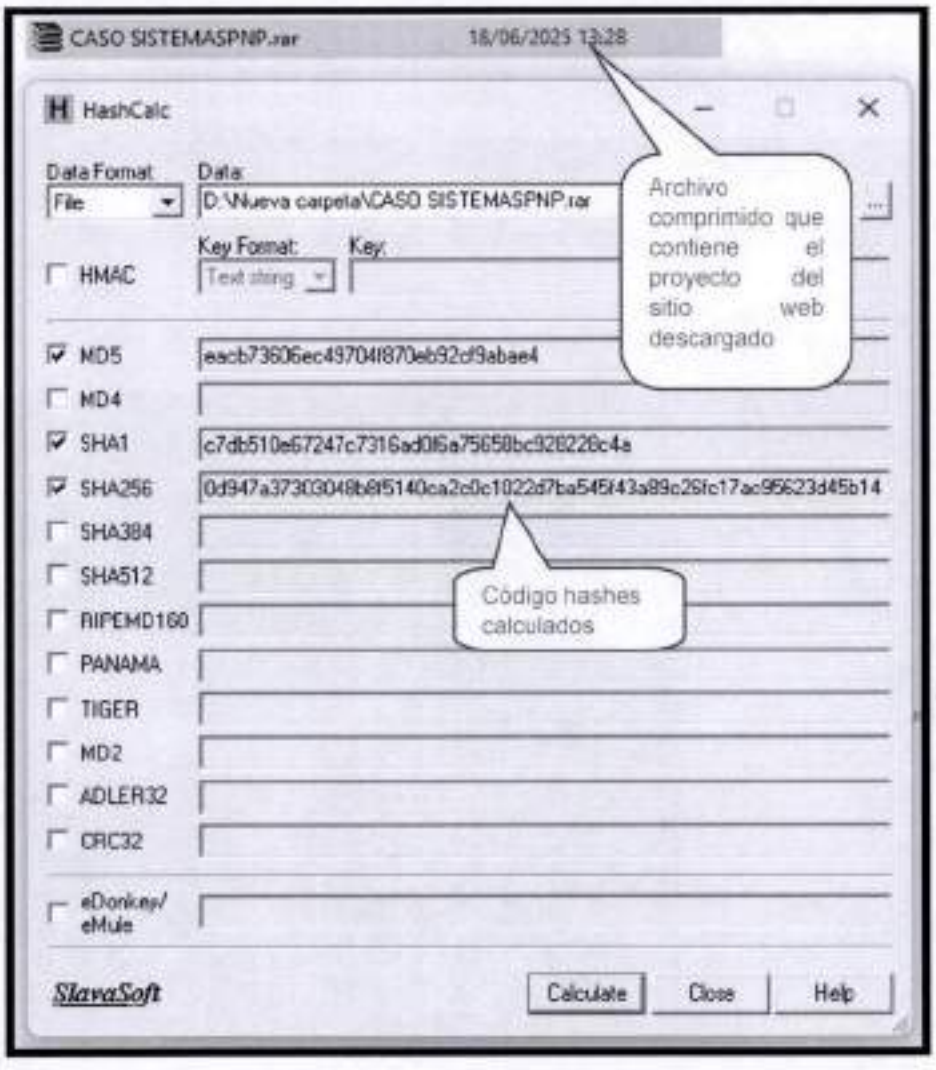


V°B°
S. DE LA CRUZ Q.

b. Proceder a comprimir el sitio *web* descargado y posteriormente salvaguardar la integridad del archivo digital calculando el respectivo código hash del archivo comprimido. En el ejemplo se utiliza el software WINRAR para la compresión.


Nombre
Fecha de modificación
Tipo
Tamaño
CASO SISTEMASPNP
18/06/2025 13:20
Proyecto que contiene el sitio web y que es comprimido con el software WINRAR.
Abrir
Abrir en nueva pestaña
Abrir en nueva ventana
Anclar a Acceso rápido
Añadir a la lista de VLC
Reproducir con VLC
7-Zip
Analizar con Microsoft Defender...
Dar acceso a
Restaurar versiones anteriores
Incluir en biblioteca
Analizar
Destruir
Anclar a Inicio
Añadir al archivo...
Añadir a "CASO SISTEMASPNP.rar"
Añadir y enviar por email...
Añadir a "CASO SISTEMASPNP.rar" y enviar por email
Copiar como ruta de acceso
Enviar a
Cortar
Copiar
Crear acceso directo
Eliminar
Cambiar nombre
Propiedades

c. Proceder a salvaguardar la integridad del archivo digital calculando el respectivo código *hash* del archivo comprimido con el *software* respectivo. En el ejemplo se utiliza el *software HashCalc* para el cálculo respectivo.



d. El archivo comprimido es guardado en un dispositivo de almacenamiento óptico o electrónico de acuerdo al peso del archivo, posteriormente se formula la respectiva acta de descarga de página *web* o sitio *web*, preservación y lacrado de dispositivo de almacenamiento donde se consigne el código hash generado, con su respectivo rotulo y continuidad de cadena de custodia.

3.2. Procedimiento para obtener información sobre dominios web y direcciones IP

El nombre de dominio *web* es la denominación por medio del cual los visitantes acceden a una página *web*. Por otra parte, es importante mencionar que, tras colocar el nombre de **dominio** en un navegador, se obtiene una determinada dirección que nos dirige hacia un servidor DNS (Sistema de Nombres de Dominio, por sus siglas en inglés), que nos enlaza hacia la **dirección IP** del servidor *web* que contiene las páginas *web* componentes de un **sitio web**. De acuerdo a lo

S. DE LA CRUZ Q.

anteriormente mencionado, puede decirse, entonces, que un nombre de dominio es la herramienta que facilita el acceso a las páginas *web*.

Para mejor entendimiento se realizan los siguientes procedimientos utilizando el servicio WHOIS, que permite obtener información técnica y los datos de registro de los titulares que administran un nombre de dominio de un sitio *web* o dirección IP, para lo cual se usa la herramienta "*Whois Lookup*[19]" del sitio *web* whois.domaintools.com, sin embargo, existen diferentes herramientas online que pueden ser utilizadas.

3.2.1. Obtención de información técnica de sitios *web*

a. Se ingresa a la dirección *web* whois.domaintools.com y se procede a consultar la información registrada del sitio web investigado:



b. Proceder a visualizar y analizar la información técnica del sitio *web* como, por ejemplo: nombres de servidores, direcciones IP vinculados al nombre del dominio, dato del proveedor de servicios de internet, localización de la dirección IP, administradores, correos electrónicos. Es preciso mencionar que la información mostrada no es uniforme para todos los casos, conforme a las siguientes imágenes:

[19] whois.domaintools.com, sitio web que tiene una variedad de herramientas online gratuitas y de pago, cuya utilización ayuda a la investigación del delito vinculados a sitios web o direcciones IP.

Home › Whois Lookup › BuscadorPoliciaSur.xyz

Whois Record for BuscadorPoliciaSur.xyz

— Domain Profile

Registrar	Namecheap IANA ID: 1068 URL: https://namecheap.com Whois Server: whois.namecheap.com abuse@namecheap.com (p) +1.9854014545
Registrar Status	clientTransferProhibited

Datos de la empresa que registró el nombre de dominio.

DomainTools

Fecha de creación, expiración del dominio y antigüedad en línea del dominio.

Dates	293 days old Created on 2023-01-17 Expires on 2024-01-17 Updated on 2023-08-31
Name Servers	DNS1.REGISTRAR-SERVERS.COM (has 8,905,598 domains) DNS2.REGISTRAR-SERVERS.COM (has 8,905,598 domains)
IP Address	212.32.248.107 is hosted on a dedicated server
IP Location	- Noord-holland - Amsterdam - Leaseweb Netherlands B.v.
ASN	AS60781 LEASEWEB-NL-AMS-01 LeaseWeb Netherlands B.V., NL
IP History	4 changes on 4 unique IP addresses ov
Hosting History	1 change on 2 unique name servers ov

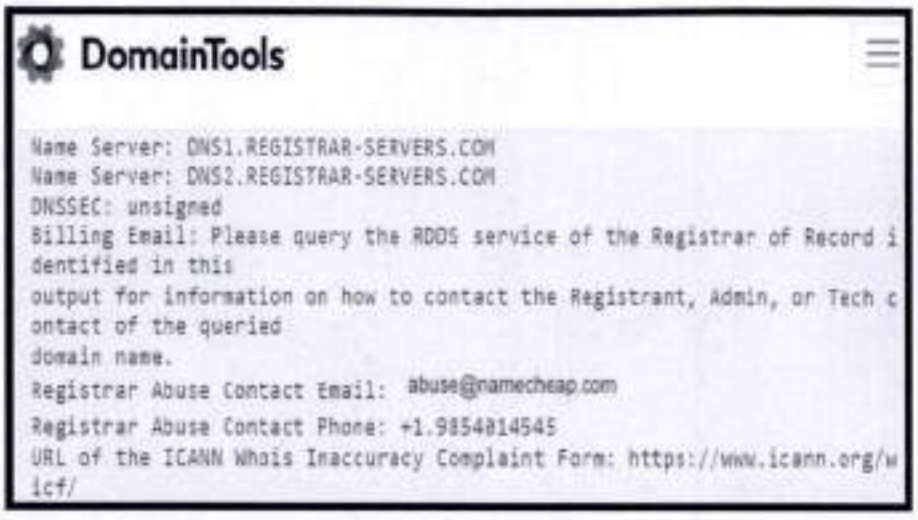
Nombre de los servidores.

Dirección IP

Proveedor del servicio de internet y su localización

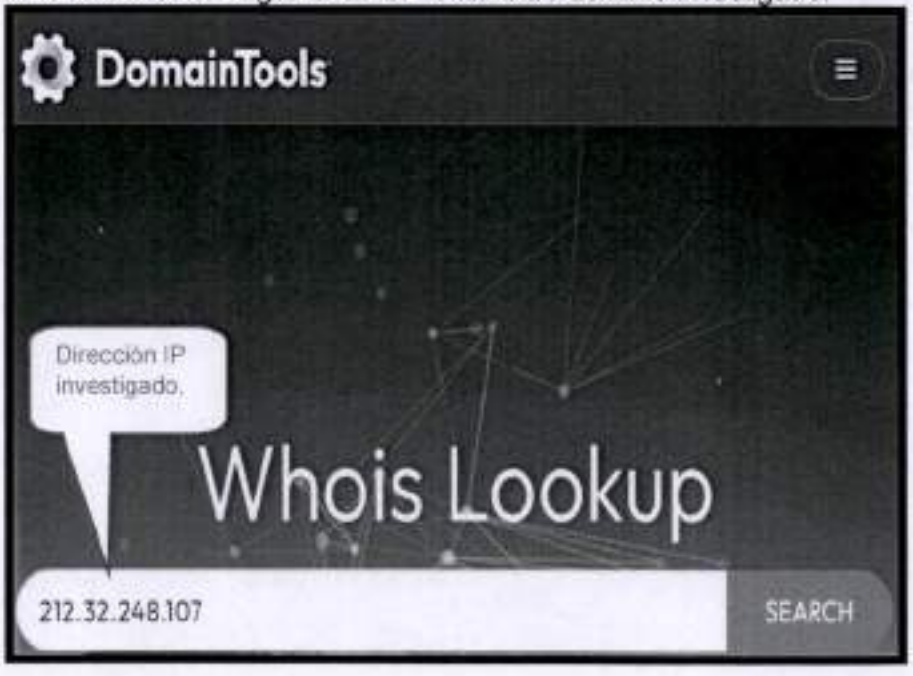
```
Registry Domain ID: D344036460-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Updated Date: 2023-08-31T17:04:21.0Z
Creation Date: 2023-01-17T00:17:47.0Z
Registry Expiry Date: 2024-01-17T23:59:59.0Z
Registrar: Namecheap
Registrar IANA ID: 1068
```

S. DE LA CRUZ C.



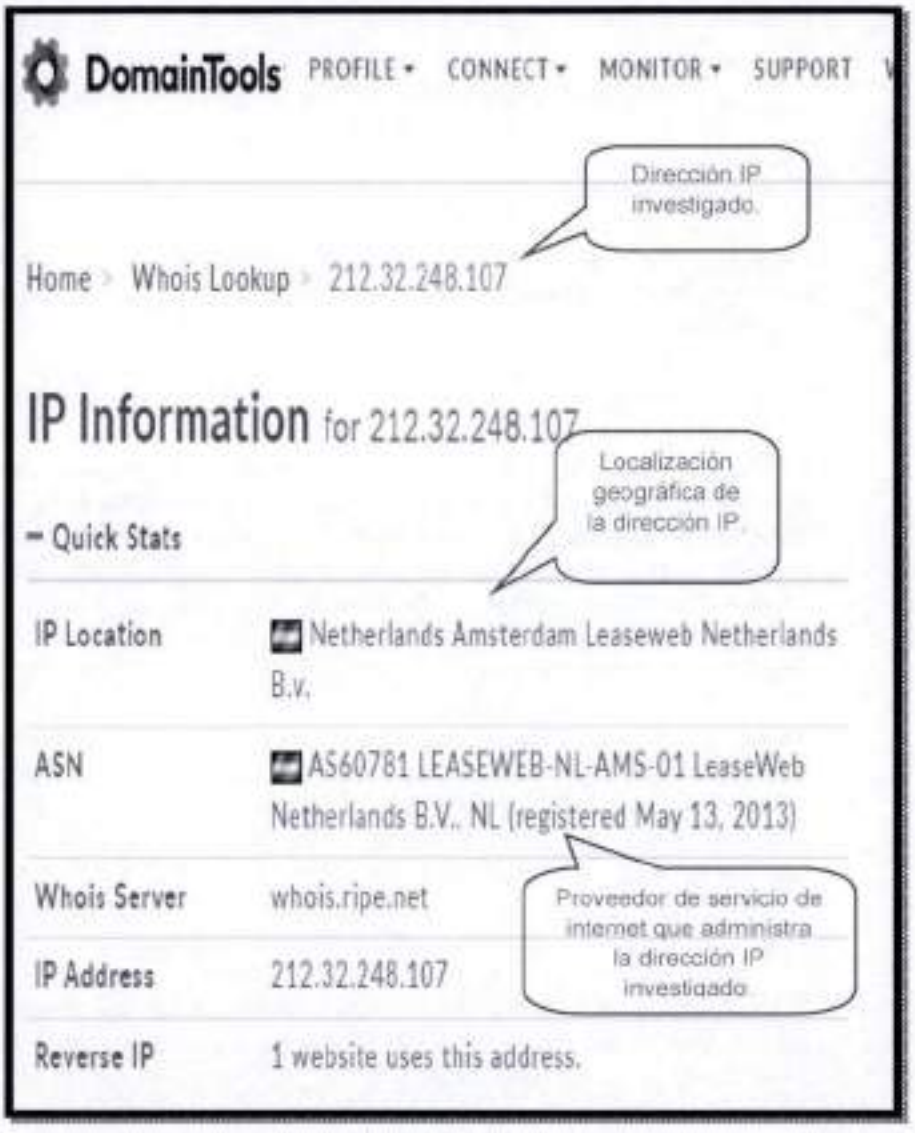
3.2.2. Obtención de información técnica de direcciones IP

a. Se ingresa a la dirección *web* whois.domaintools.com y se procede a consultar la información registrada del nombre de dominio investigado:



b. Proceder a visualizar y analizar la información técnica del nombre de la dirección IP investigada como, por ejemplo: dato del proveedor de servicios de internet, localización de la dirección IP, correos electrónicos, entre otros. Es preciso mencionar que la información mostrada no es uniforme para todos los casos, conforme a las siguientes imágenes:

S. DE LA CRUZ Q.



Una vez obtenida la información técnica del sitio *web* o dirección IP, se elabora el respectivo informe policial justificando la necesidad de contar con la titularidad del número telefónico, dirección IP, correo electrónico o cualquier dato identificatorio, con el que se adjudicó dicho registro de acceso a la red; sin embargo, en el mencionado requerimiento se debe considerar la fecha, hora y huso horario del momento que registre la operación y/o acceso.

Este requerimiento es expuesto al fiscal titular de la investigación para que éste lo extienda al juzgado correspondiente y se obtenga el levantamiento secreto de las comunicaciones y documentos privados. De esta manera, el instructor puede recibir la resolución emitida por el juez y posteriormente es remitida a las entidades prestadoras de servicios (ISP) y otros para la ejecución de la disposición respectiva, la cual contribuye a la investigación policial.

CAPÍTULO IV
ASEGURAMIENTO DE LA EVIDENCIA DIGITAL

4.1. Aspectos legales

El Perú cuenta con documentos normativos que regulan la incautación, recojo y preservación de dispositivos informáticos en la escena del crimen, los cuales se detallan a continuación:

4.1.1. Resolución N° 729-2006-MP-FN del 15 junio del 2006

Reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados, aprobado con Resolución N° 729-2006-MP-FN del 15 junio del 2006, el objetivo de este documento normativo es *"regular el procedimiento de la cadena de custodia de los elementos materiales y evidencias incorporados a la investigación de un hecho punible. Asimismo, regula los procedimientos de seguridad y conservación de los bienes incautados, según su naturaleza."*

Tiene como finalidad: *"establecer y unificar procedimientos básicos y responsabilidades de los representantes del Ministerio Público y funcionarios, a efecto de garantizar la autenticidad y conservación de los elementos materiales y evidencias incorporados en toda investigación de un hecho punible, auxiliados por las ciencias forenses, la criminalística, entre otras disciplinas y técnicas que sirvan a la investigación criminal. Además, unificar los lineamientos generales de seguridad y conservación de los bienes incautados."*

Y su ámbito y alcance es *"...de aplicación progresiva en todo el territorio nacional y de obligatorio cumplimiento para los señores Fiscales, funcionarios y servidores del Ministerio Público."*

4.1.2. Decreto Supremo N° 010-2018-JUS del 25 de agosto del 2018

a. **Protocolo de Actuación Interinstitucional N° 6 de Protección e Investigación de la Escena del Crimen, aprobado con Decreto Supremo N° 010-2018-JUS del 25 de agosto del 2018,** el objetivo de este documento normativo es *"...fortalecer la actuación policial y fiscal, para garantizar una adecuada protección e investigación de la escena del crimen virtual e incrementar de manera potencial las probabilidades del esclarecimiento del hecho delictivo. Y como segundo objetivo estaría dirigido a evitar errores que dificulten la investigación y que determinen negativamente el caso".*

Y tiene como alcance: *"establecer un conjunto de procedimientos destinados a generar actividades predecibles en cuanto a la protección e investigación de la escena del crimen en el marco de las actuaciones urgentes de investigación realizadas por el/la Policía y el/la Fiscal".*

b. **Protocolo de Actuación Interinstitucional N° 12 para la aplicación de la incautación, comiso, hallazgo y cadena de custodia, aprobado con**

V°B° S. DE LA CRUZ O.

JURISPOL

Decreto Supremo N° 010-2019-JUS del 25 de agosto del 2018, el objetivo de este documento normativo es *"...fortalecer la actuación interinstitucional de los operadores del Sistema de Administración de Justicia Penal durante los procedimientos de incautación, comiso, hallazgo y cadena de custodia."*

Y tiene como alcance: *"...para todos los delitos comunes que se conocen en el Código Procesal Penal."*

4.2. Fases para el aseguramiento de la evidencia digital

4.2.1. Fase inicial

En esta fase, la unidad policial que toma conocimiento de la noticia criminal, debe evaluar si se encuentra en situación de flagrancia o de lo contrario, impulsar por medio del Ministerio Público la solicitud de medidas de coerción correspondientes, propias del proceso común (de detención preliminar, allanamiento y/o incautación).

S. DE LA CRUZ Q.

4.2.1.1. En flagrancia ante la comprobación de una noticia criminal:

a. Utilizar la Directiva N° 03-04-2016-DIRGEN-PNP/EMG-DIRASOPE-B "Directiva para la Intervención Policial en Flagrante Delito" aprobado con Resolución Directoral N° 135-2016-DIRGEN/EMG-PNP.

b. Estando en sede policial, el personal policial debe de tomar conocimiento a detalle de lo sucedido a efectos de esclarecer la presunta comisión de un delito informático.

c. El personal policial, debe explicar los detalles de la noticia criminal al personal de apoyo asignado en la ejecución del operativo, para que en conjunto determinen las evidencias digitales que deben recoger de la escena del crimen.

d. Si la noticia criminal se encuentra vinculada a una página *web* o dirección de correo electrónico, puede realizar un patrullaje virtual para perennizar las evidencias digitales relacionadas al delito denunciado y **tener en consideración lo señalado en el punto 2.2** de la presente Guía, sobre los procedimientos para la identificación e individualización de perfiles de usuarios de redes sociales (*Facebook, Instagram, WhatsApp y TikTok*) o del procedimiento para obtener información sobre dominios web, direcciones IP y en el caso de puertos IP a Meta.

e. El efectivo policial encargado de la recolección de evidencia digital volátil y/o activa, lleva el *software* portable y/o el *hardware* según sea el caso, para poder recolectar evidencia digital; como por ejemplo un *pendrive* (memoria USB) con *software* portable necesario, discos duros externos para guardar copias *bit* a *bit*, de ser el caso y otros que se requieran, según la presente Guía, para el Recojo de Evidencia Digital.

JURISPOL

f. Si la noticia criminal se encuentra vinculada a un Sistema y/o infraestructura de información, necesariamente debe concurrir a las diligencias con personal policial especializado, quien evalúa la forma correcta de recolectar evidencia digital relacionada a la noticia criminal. Caso contrario, pueden seguir los procedimientos recomendados en el Manual para el Recojo de la Evidencia Digital, en caso identifiquen dispositivos informáticos en la escena del crimen.

4.2.1.2. Fuera de flagrancia, para la ejecución de una Resolución Judicial de detención preliminar, allanamiento y/o incautación:

a. Utilizar el protocolo específico N° 1 de *"Articulación, trabajo y coordinación entre el Ministerio Público y la Policía Nacional del Perú"* aprobado con Decreto Supremo N° 010-2018-JUS.

b. Formular la orden de operación para la ejecución cuando se presente mandato judicial.

c. El instructor debe intercambiar información con el grupo de investigación y el personal especializado, facilitando detalles del caso, así como de la Resolución Judicial, respecto a los dispositivos tecnológicos que se pretenden incautar y el destino de los mismos, a efectos de salvaguardar la información correspondiente.

d. Tener en cuenta, que a mayor información recabada y dependiendo del delito informático el especialista en recojo de evidencias digitales se encuentra en mejores condiciones para cumplir su función.

e. Para ello, se debe prever con anticipación, toda la información posible sobre el caso, para poder preparar los medios digitales y procedimientos técnicos correspondientes, conforme resuelva el juzgado en la Resolución Judicial del Levantamiento del Secreto de las Comunicaciones y/o Documentos Privados.

4.2.2. Fase de ejecución

Debido a las diversas modalidades y complejidad de los delitos informáticos, se realiza una descripción en forma general, con los siguientes pasos detallados a continuación:

4.2.2.1. Asegurar la escena:

Considerar la seguridad del personal policial, previa coordinación con las Unidades Policiales comprometidas, para proteger y custodiar físicamente la escena del crimen.

Luego, se debe de asegurar la escena desde el punto de vista informático, para evitar cualquier modificación, adulteración o pérdida de evidencia digital, para lo cual se debe tener en cuenta el Manual para el Recojo de la Evidencia Digital.

S. DE LA CRUZ Q.

JURISPOL

a. Realizar una evaluación general

En este punto se debe focalizar el orden y prioridades para el procesamiento del material informático. Esto es relevante si se pretende obtener las imágenes forenses durante la realización del registro.

Durante el desarrollo de la diligencia y de ser factible, el personal especializado debe realizar *in situ*, la creación de las copias forenses de los soportes digitales (discos duros, usb's, entre otros) con las herramientas necesarias (bloqueadores, duplicadores, entre otros) teniendo en cuenta el Mandato Judicial emitido por el Juez correspondiente; en caso no pueda realizarse, dichos soportes deben ser precintados y asegurados, según la normativa vigente, para que luego sean sometidos al proceso técnico en el Laboratorio Digital Forense.

b. Documentar la escena

Al momento de la incautación del material informático, se debe considerar los datos del fabricante, modelo, número de serie y otros datos que identifiquen el soporte informático, así como a las personas involucradas, la fecha y hora y la constancia de la copia forense con su respectivo *hash* (si es factible realizarlo *in situ*).

Es relevante que, durante todas las diligencias, las muestras debidamente documentadas, al ser trasladadas mantengan la respectiva cadena de custodia, para poder controlar y monitorear el estado de las mismas, y evitar incurrir en vicios procesales que anulen los esfuerzos policiales.

Es preciso y necesario documentar el estado original, en que los dispositivos hallados se encuentran, para ello se debe realizar las tomas fotográficas y/o grabación de video respectivamente.



Siempre es necesaria la identificación de los dispositivos que almacenen

la evidencia digital, para lo cual, se debe tener como referencia el Manual **para el Recojo de la Evidencia Digital.**



c. Procesar evidencia.

Durante la ejecución, para recabar la mayor cantidad de información que pueda servir en la investigación, se debe tener en cuenta los procedimientos indicados en el Capítulo II: Tratamiento de información de perfiles de usuarios de redes sociales, sobre procedimientos (de investigación, identificación e individualización, preservación y solicitud de información de redes sociales, sitios *web*, así como su aseguramiento) durante la entrevista con el agraviado en la toma de denuncia.

Así como, considerar las diligencias a solicitar según la naturaleza de la investigación, las mismas que están establecidas en el capítulo II de la presente Guía, según corresponda:

- Incautación: se asegura e inmoviliza la evidencia[20] documenta el dispositivo del lugar de los hechos y se procede al elaborar el acta lacrado respectivo[21]. No se realizan más acciones con el dispositivo incautado, hasta que sea puesto a disposición del Laboratorio Digital Forense.

- Realización de la copia forense: para cada uno de los tipos de evidencia se aplican los procedimientos técnicos, de forma directa o indirecta.

[20] Ministerio Público – Fiscalía de la Nación, (2006). Reglamento de Cadena de Custodia de elementos, art. 8° Del Procedimiento de la cadena de custodia. - La Cadena de Custodia se inicia con el aseguramiento, inmovilización o recojo de los elementos materiales y evidencias en el lugar de los hechos, durante las primeras diligencias o incorporados en el curso de la Investigación preparatoria; y, concluye con la disposición o resolución que establezca su destino final.
[21] Ministerio del Interior. (2020). Manual para el recojo de la evidencia digital. Acta de lacrado (Pág. 57).

4.2.2.2. Procedimientos específicos

Para realizar los procedimientos detallados a continuación, se debe evaluar el escenario en que se encuentran las evidencias identificadas en la escena del crimen y la relevancia de la obtención y su preservación.

Todo procedimiento especifico a realizarse debe ser coordinado previamente con el fiscal a cargo de la investigación para brindar la validez legal según lo establecido, en el Código Penal, Código Procesal Penal, así como la jurisdicción donde se realice la intervención.

Por su parte, se recomienda usar un pendrive (USB) donde se encuentren guardadas las herramientas portables a utilizar (bloqueadores de escritura, para copia forense, calculadoras *hash*, entre otros), con la finalidad de no alterar los registros del dispositivo informático a incautarse.



1. Verificación de archivo host

La visualización de archivo de sistema "*host*", resulta relevante para cuando se investiga delitos informáticos relacionados al *phishing* o *pharming*, toda vez que la configuración del archivo *host* permite relacionar las direcciones IP de los servidores o sitios *web* con sus nombres de dominio.

Cada sistema operativo tiene una ruta especifica donde ubicar el archivo *host*. En el siguiente cuadro se observa la ruta del archivo *host* por el tipo de sistema operativo;

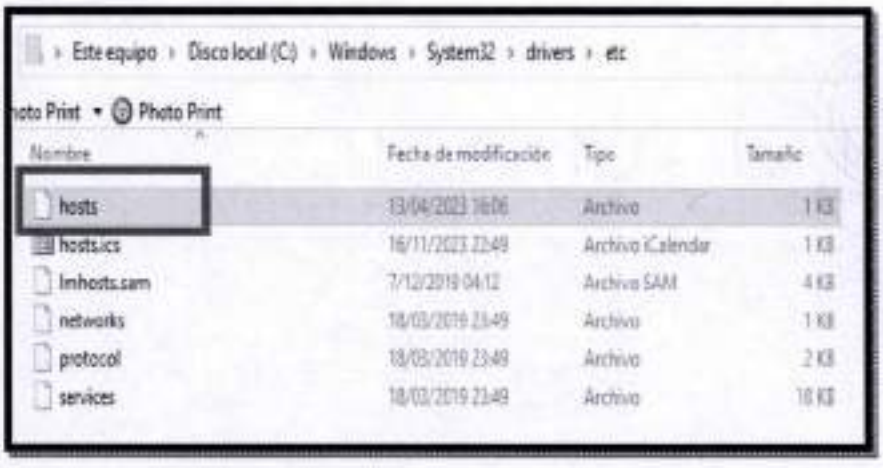
Sistema Operativo	Ruta
Windows 95 / 98 / Me	C:\Windows\hosts
Windows NT / 2000	C:\WINNT\System32\drivers\etc\hosts
Windows XP / 2003 / Vista / 7 / 8 / 8.1 / 10	C:\Windows\System32\drivers\etc\hosts
Mac OS / iPhone OS	/private/etc/hosts
Unix / Linux / BSD	/etc/hosts
Novell NetWare	SYS:etc\hosts
OS/2 / eComStation	"bootdrive":\mptn\etc\
BeOS	/boot/beos/etc/hosts
Symbian OS 6.1-9.0	C:\system\data\hosts
Symbian OS 9.1+	C:\private\10000882\hosts
Android	/system/etc/hosts

Se debe tener en cuenta que la ubicación del archivo *host* puede variar según la versión y actualización de los sistemas operativos.

A continuación, se muestra un ejemplo para ubicar y visualizar el archivo *host* del sistema operativo *WINDOWS*, conforme a los siguientes procedimientos:

a. **Ubicación del archivo *host* en los sistemas operativos *Windows* *(explicar el proceso por cada sistema operativo del cuadro – SOLICITAR ÁREA TÉCNICA)*.** En la computadora personal o de escritorio, ingresar a la ruta **C:\Windows\System32\drivers\etc**, según los siguientes pasos:

- Presionar en el teclado (⊞+E) o de lo contrario ubicar la carpeta "Este equipo" en el computador.
- Ingresar a la carpeta C, luego dirigirse a la carpeta Windows, posteriormente abrir la carpeta "*System 32*".
- Ingresar a la carpeta "*drivers*".
- Ubicar el archivo *host*.



b. **Visualización del archivo *host* en los sistemas operativos *Windows*.**

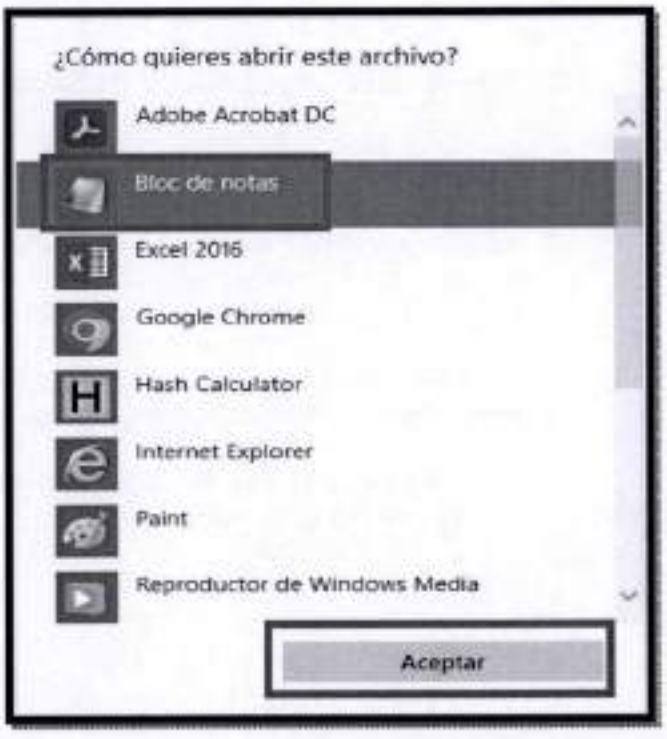
En la computadora personal o de escritorio:

- Hacer click derecho al archivo "*host*" y seleccionar la opción "*Abrir con*", luego seleccionar la opción "*bloc de notas*" y por último click en el botón "*Aceptar*" o "*solo una vez*", para poder visualizar el contenido del archivo.

S. DE LA CRUZ Q.

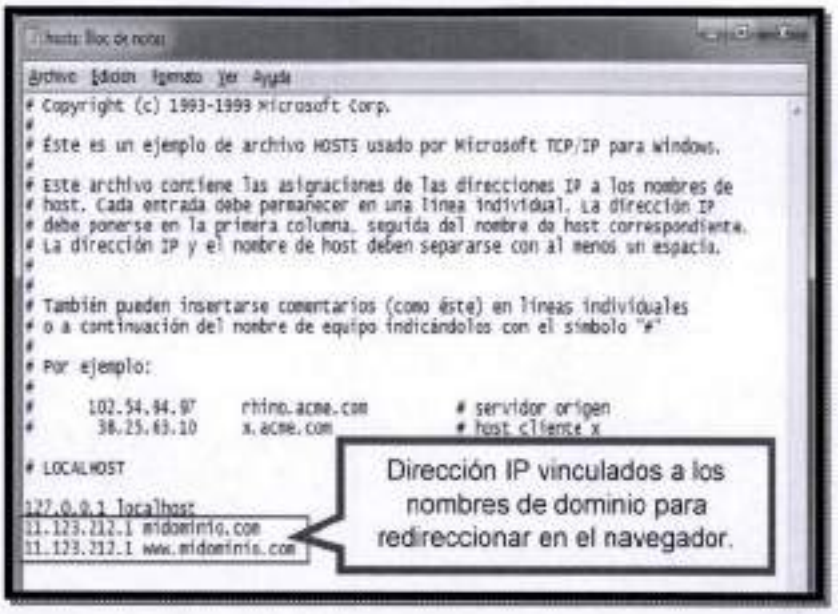


Opción *"Abrir con"*, para seleccionar el programa que ayuda a visualizar el contenido del archivo.



La opción "Bloc de notas", permite visualizar y modificar el contenido del archivo "*host*".

- Visualizar el archivo *host*, para identificar el direccionamiento de las direcciones IP a los sitios *web*.



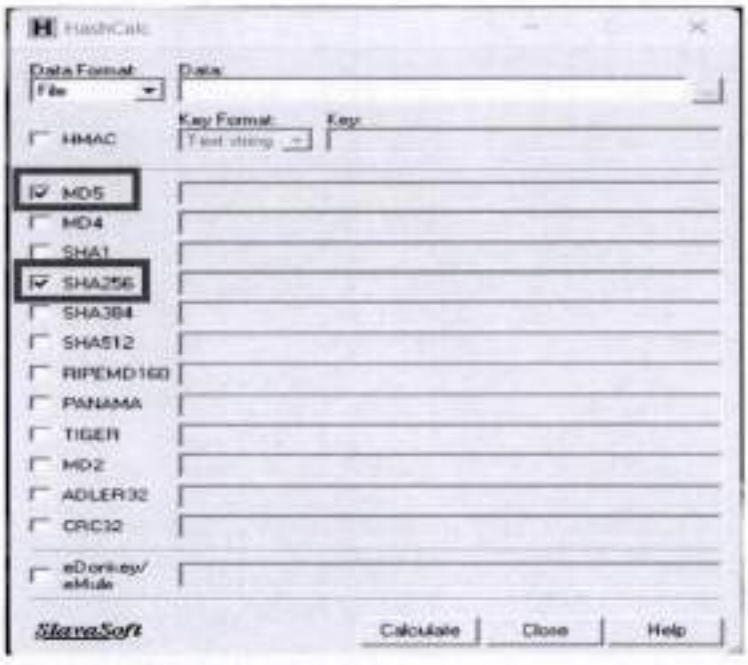
De ser necesario se tiene que hacer una copia del archivo *host*, asegurando la integridad del mismo, con el cálculo de su respectivo código *hash*.

2. Cálculo del código hash de archivos digitales:

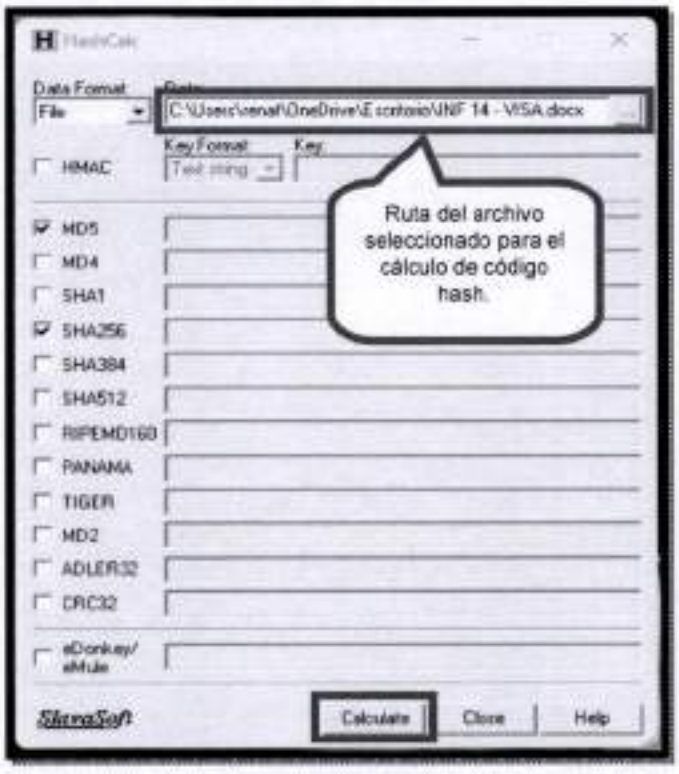
Este procedimiento debe ser realizado para asegurar la integridad de un archivo digital, para ello se utilizan herramientas *software* portables que ayudan al cálculo del código *hash*; asimismo, se calcula y utiliza como mínimo dos tipos de códigos *hash* para un archivo digital, como por ejemplo los códigos *hash* del tipo MD5 y SHA-256.

Para ello, se puede utilizar el *software* portable *HashCalc*, *HashMyFiles*, entre otros. A continuación, se detallan los procedimientos:

a. Ejecutar el *software HashCalc* y seleccionar el tipo de código *hash* que se debe calcular.



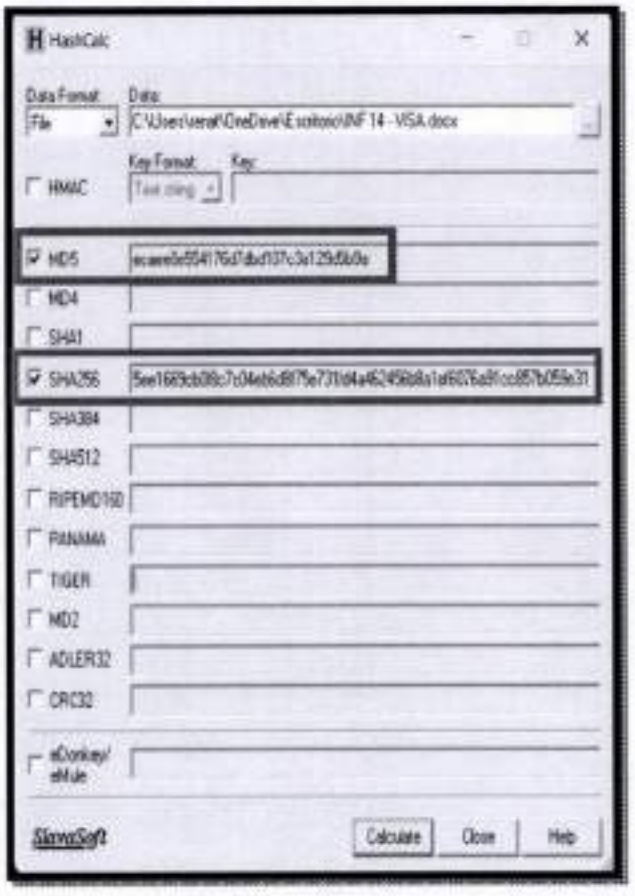
b. Ubicar y seleccionar en la opción "data" el archivo digital al cual se le calcula el código *hash* del tipo MD5 y SHA-256 y luego hacer click en el botón "*Calculate*".





S. DE LA CRUZ Q.

c. Consignar en el acta respectiva los códigos *hash* calculados de los archivos digitales, con la finalidad de asegurar la integridad de los archivos digitales.



3. Adquisición de memoria volátil:

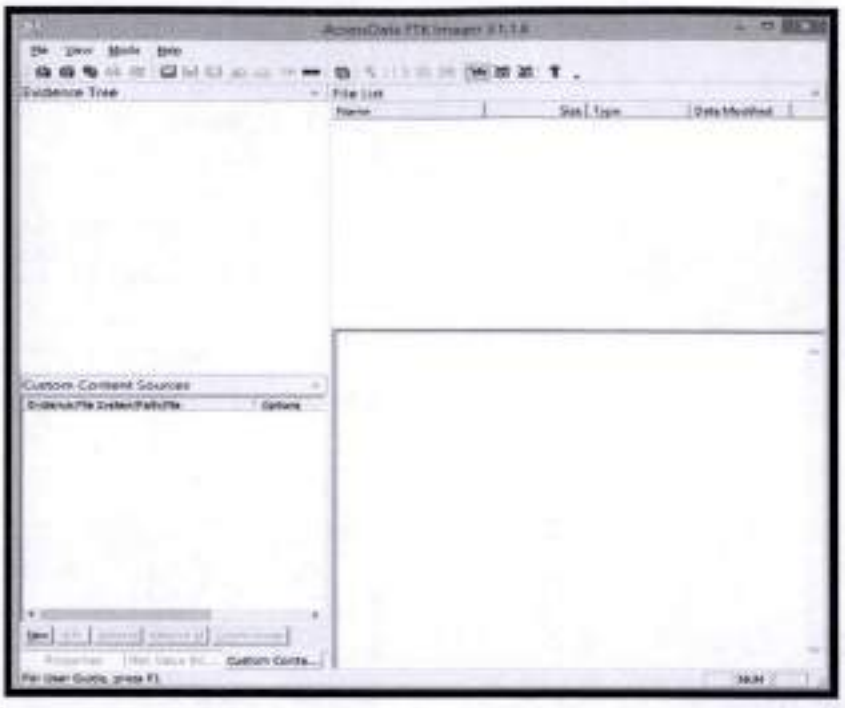
Este procedimiento debe ser realizado *in situ* en la escena del crimen y con participación del fiscal, el usuario de la evidencia y/o el abogado defensor.

La bondad de utilizar este procedimiento es obtener información de los procesos que se están ejecutando en la memoria RAM del computador personal o portátil al momento de la intervención, para posteriormente poder analizarlos en laboratorio identificando al/los proceso(s) vinculado(s) a la investigación del ilícito penal.

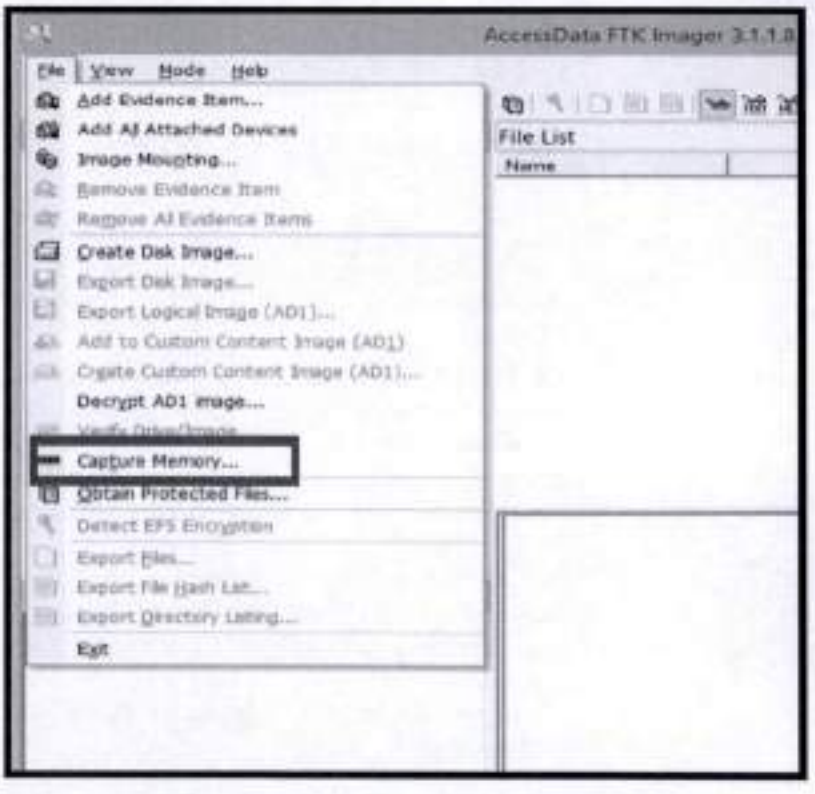
Se pueden utilizar herramientas para recolectar la evidencia volátil como por ejemplo *FTK Imager*, *RamCapturer* o similares. A continuación, se detallan los procedimientos para la herramienta *FTK Imager*:

a. Tener una memoria pendrive (USB) con la herramienta *FTK IMAGER* portable.

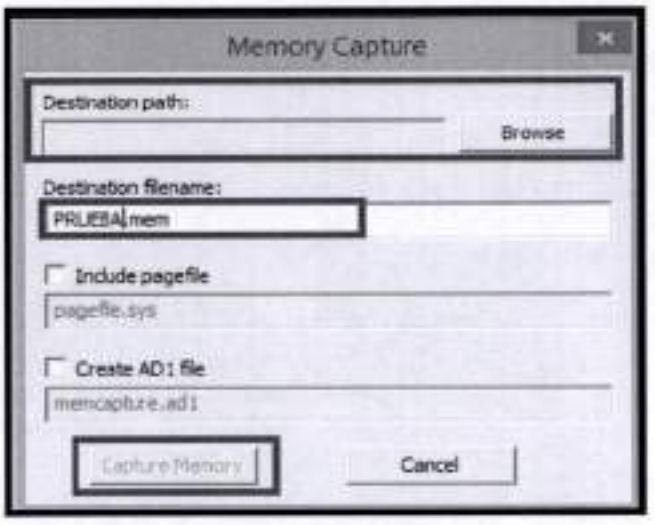
b. Ejecutar en la computadora la herramienta *FTK IMAGER* portable, dando doble click sobre el mismo.



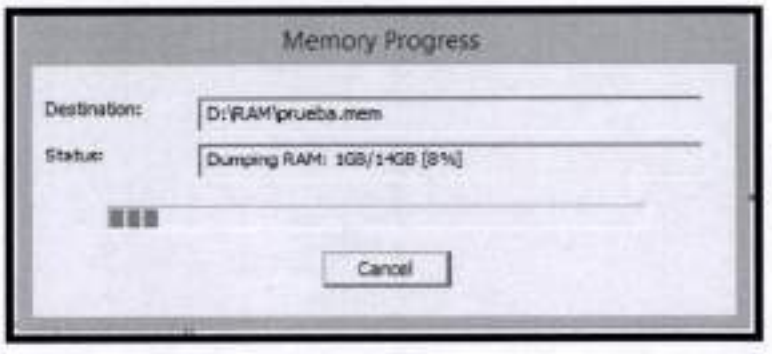
c. Elegir la opción file – Capture Memory.



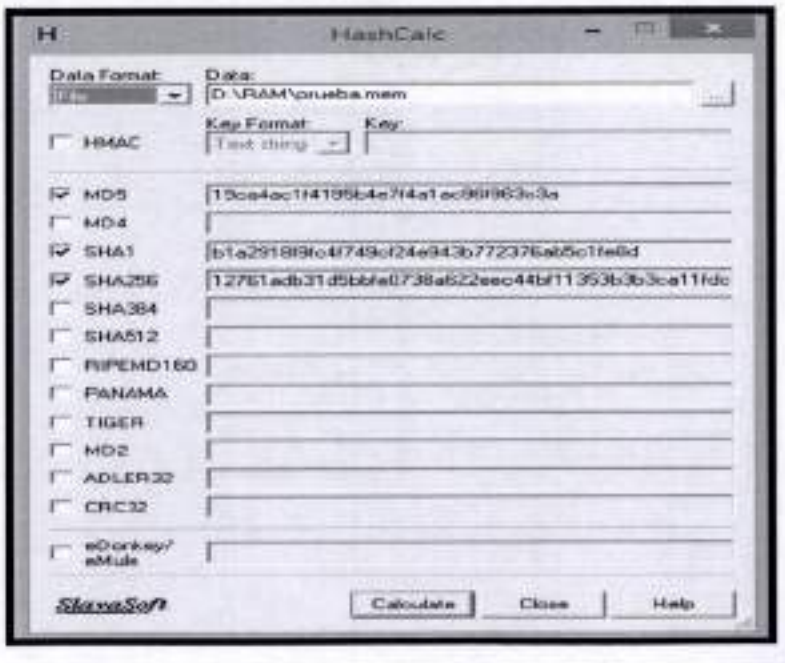
d. Escoger el lugar donde se guarda la memoria volátil adquirida, preferentemente guardarlo en otro dispositivo de almacenamiento y colocar un nombre al archivo creado de la memoria volátil y dar click en *"Capture Memory"*.



e. Ejecutar la adquisición de la memoria RAM.



f. Generar el respectivo código *hash* (MD5, SHA256, entre otros) del archivo de la memoria RAM adquirida y consignarla en el acta respectiva.



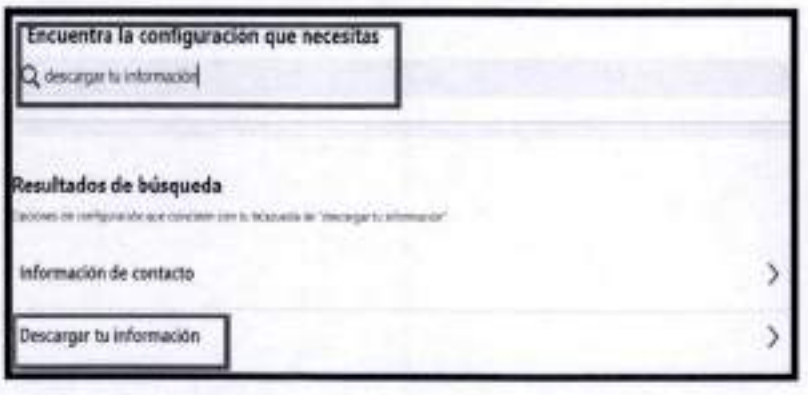
4. Descarga de información de perfil de Facebook:

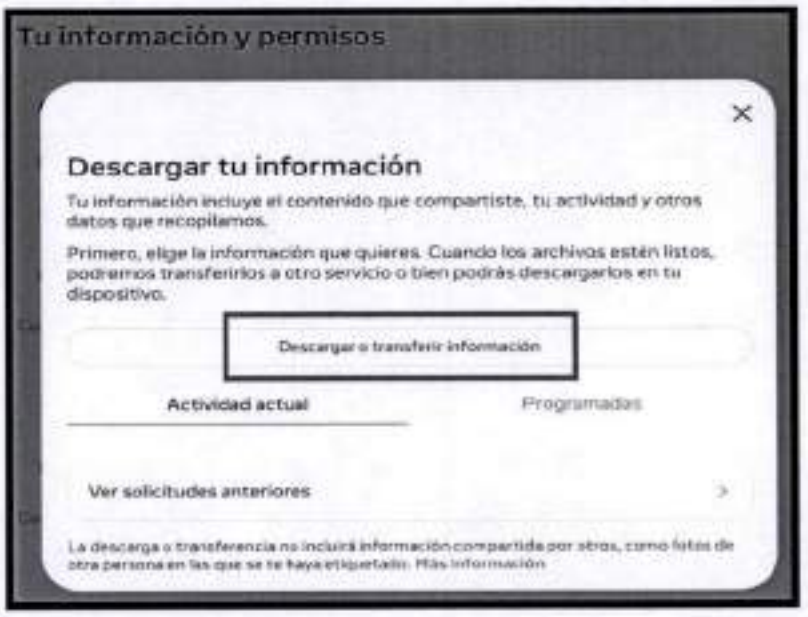
Este procedimiento se utiliza cuando **se encuentra una sesión iniciada de *Facebook*** y se encuentre vinculado a la investigación; en este proceso, deben participar el fiscal, el usuario de la evidencia y/o el abogado defensor.

a. En el navegador donde se encuentra activo el perfil de *Facebook* se debe digitar la siguiente URL https://www.facebook.com/settings?tab=your_facebook_information y en la sección "Encuentra la configuración que necesitas" digitar y buscar "Descargar tu información de *Facebook*".

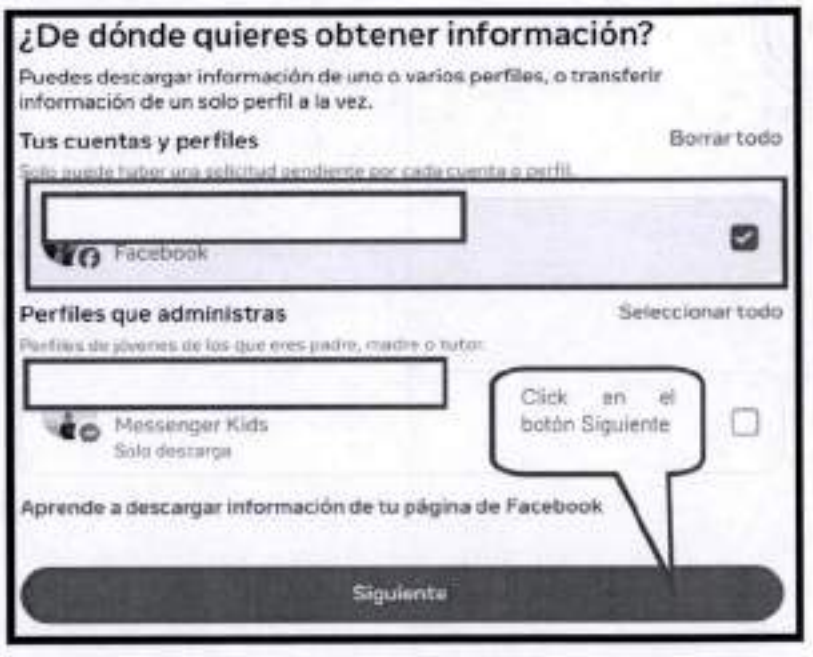


b. Elegir la opción de "Descargar o transferir información".

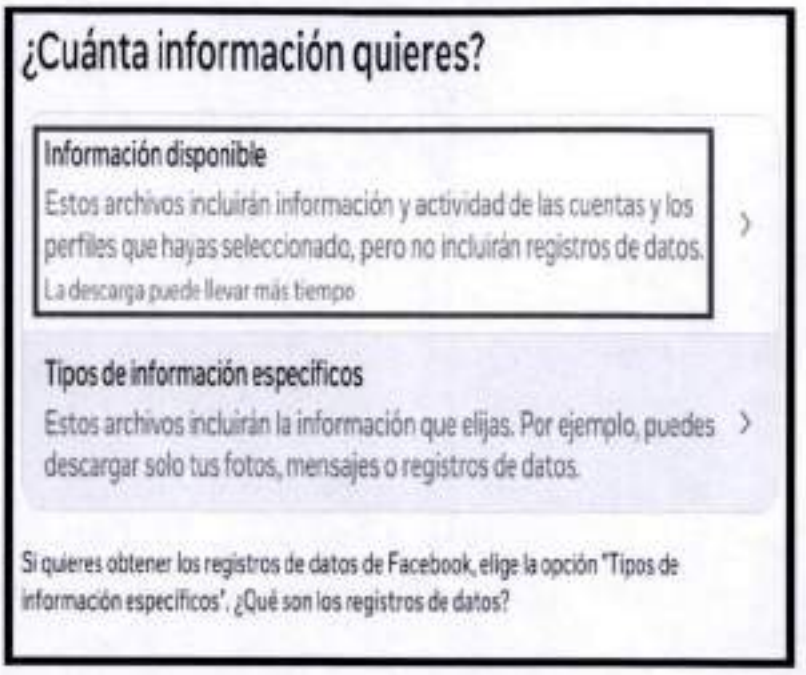




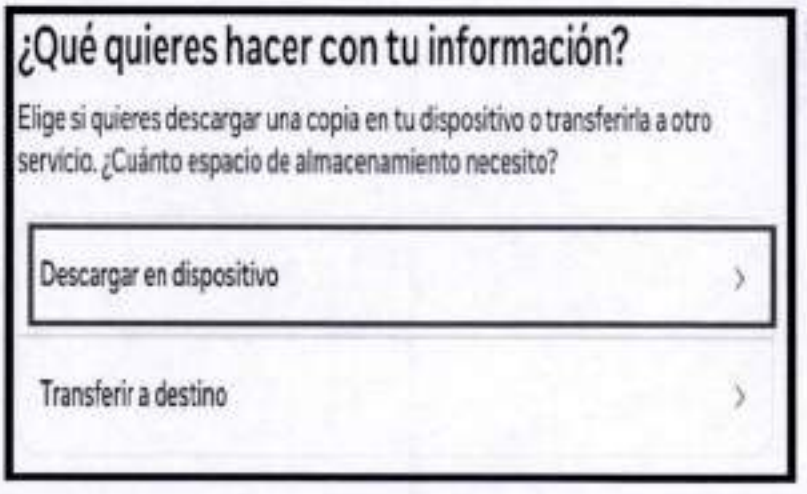
c. Elegir el perfil de donde se quiere descargar la información y dar click en el botón siguiente.



d. Elegir la mejor opción de acuerdo a la necesidad de la investigación, para el ejemplo se selecciona la opción "información disponible".



e. Elegir la opción "Descargar en dispositivo".



f. Elegir las opciones de "Intervalo de fechas" se recomienda que sea según la necesidad de la investigación; "Calidad del contenido multimedia" y hacer click en el botón "Crear archivos". La creación de la descarga tomara un tiempo según la cantidad de información solicitada.

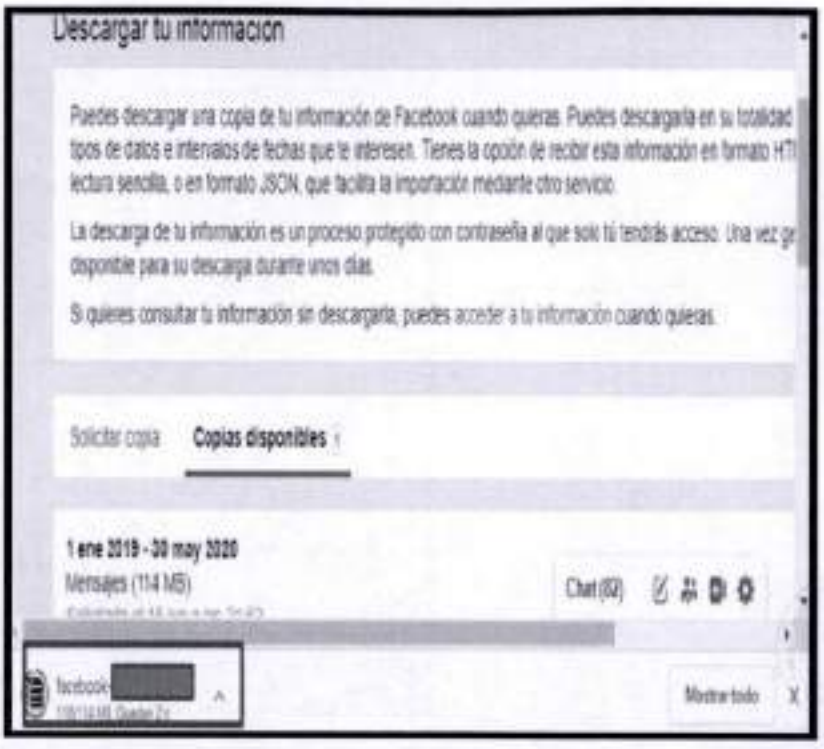
S. DE LA CRUZ Q.







g. Para continuar la descarga de la información se debe de solicitar al usuario del perfil que proporcione la clave de inicio de sesión del perfil.



S. DE LA CRUZ O.

h. Luego de descargado el archivo puede ser visualizado, asimismo, a la información descargada se le debe de generar su respectivo código hash y ser almacenado en un pendrive (USB) u otro dispositivo de almacenamiento y realizar el acta respectiva y, rotulo y continuidad de cadena de custodia.

5. Descarga de correo de GMAIL:

Este procedimiento se utiliza cuando se encuentra activo el correo de GMAIL, se logra recuperar el usuario y contraseña y/o con la cooperación del usuario y se encuentre vinculado a la investigación, con la finalidad de extraer y guardar los mensajes de correo electrónico vinculados a la investigación; asimismo, deben participar el fiscal, el usuario de la evidencia y/o el abogado defensor.

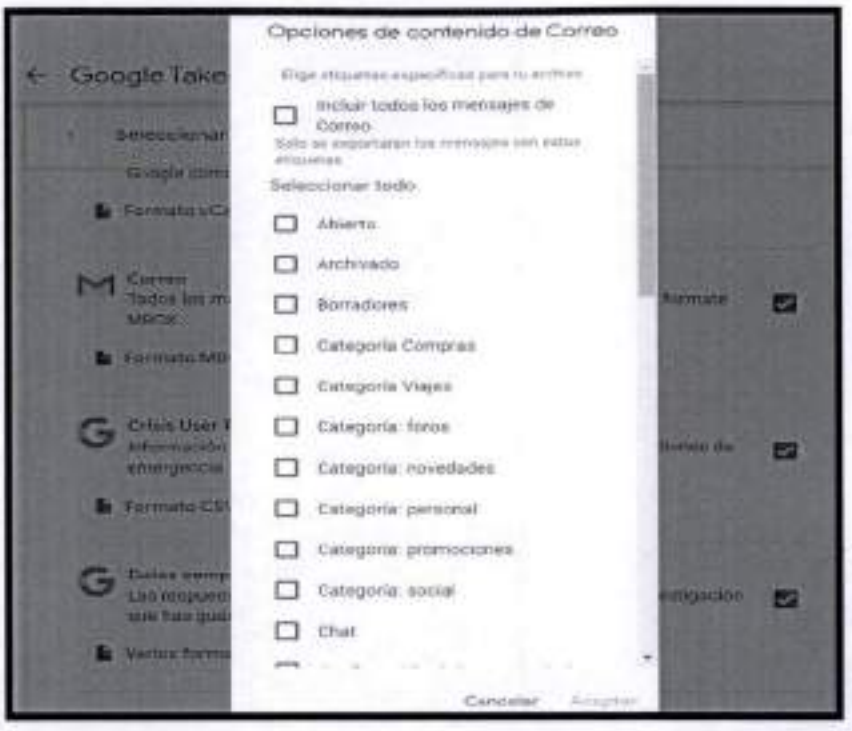
a. En el navegador donde se encuentra el correo GMAIL con sesión iniciada, abrir una nueva pestaña y digitar la siguiente URL https://takeout.google.com y se puede exportar el contenido de la cuenta de GOOGLE y elegir las opciones necesarias para exportar información, como por ejemplo el calendario, historial de Chrome, correo de GMAIL, entre otras.



Elegir el formato para descargar los mensajes y archivos adjuntos:



Se seleccionan las etiquetas de los mensajes para la exportación:



b. Luego de seleccionar el tipo de información a descargar, se debe elegir el tipo, la frecuencia y el destino del archivo.



c. Descargar la información solicitada ingresando la contraseña de la cuenta de GOOGLE.

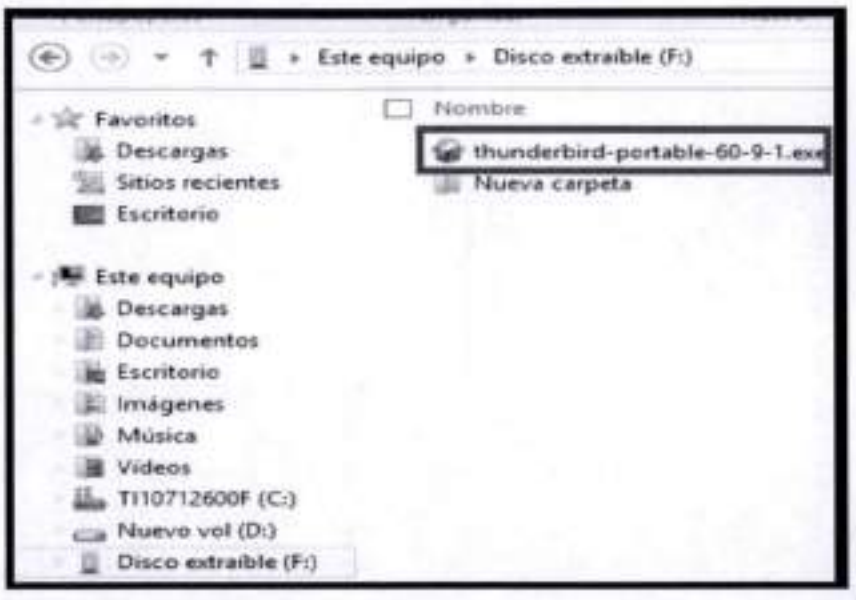


d. Luego de descargar el archivo, este puede ser visualizado, y se debe generar su respectivo código *hash* y almacenarlo en un pendrive (USB) u otro dispositivo de almacenamiento y realizar el acta respectiva.

6. Descarga de correo de Hotmail y otros:

Para este procedimiento se utiliza la herramienta *Thunderbird* portable y se requiere la cooperación del investigado para que entregue sus credenciales de acceso (correo y contraseña), con la finalidad de extraer y guardar los mensajes de correo electrónico vinculados a la investigación; asimismo, debe participar el fiscal y/o el abogado defensor.

a. Descargado el programa thunderbird-portable.exe, se ejecuta dándole doble click.

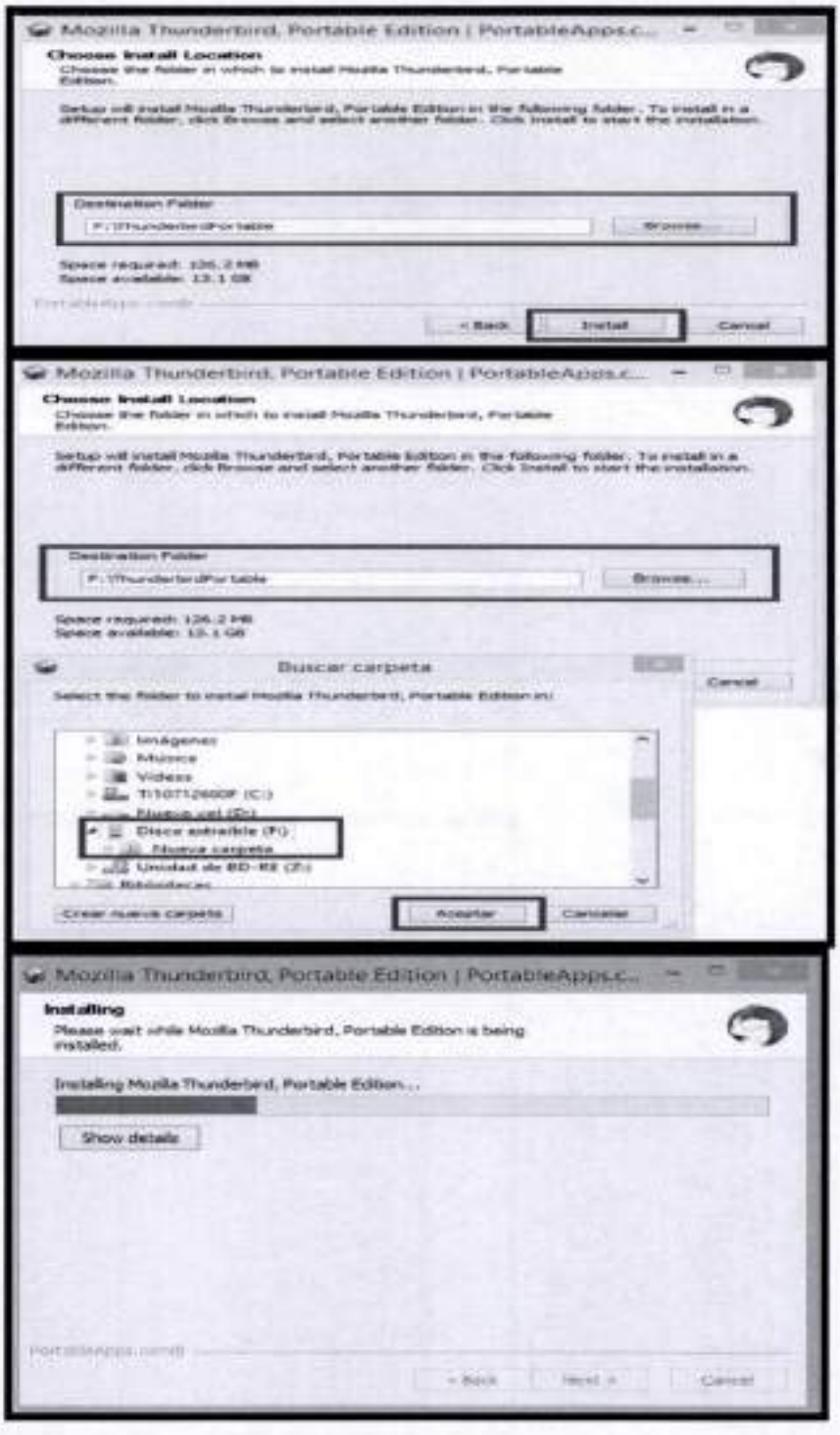


b. En esta pantalla de inicio se indica que se instala el *thunderbird* en su edición portable y se hace click en "*Next*".

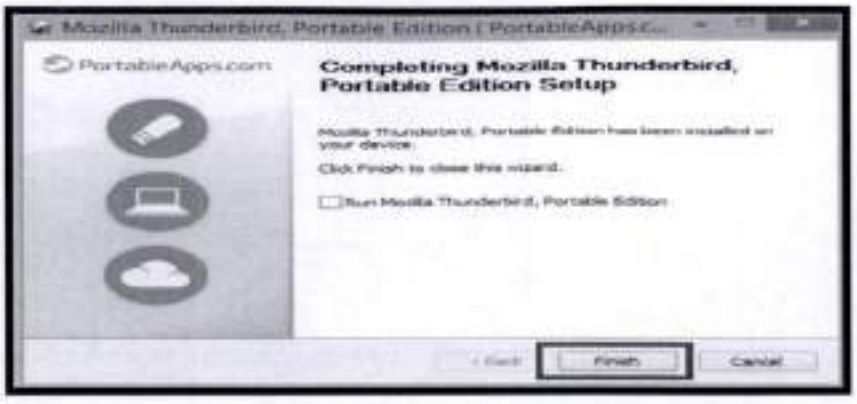


c. En esta pantalla seleccionar el lugar donde se instala el programa, se recomienda instalarlo en un pendrive (USB), se puede cambiar el nombre según lo deseado, ejemplo nombre del investigado, y hacer click en "*Install*".

S. DE LA CRUZ Q.



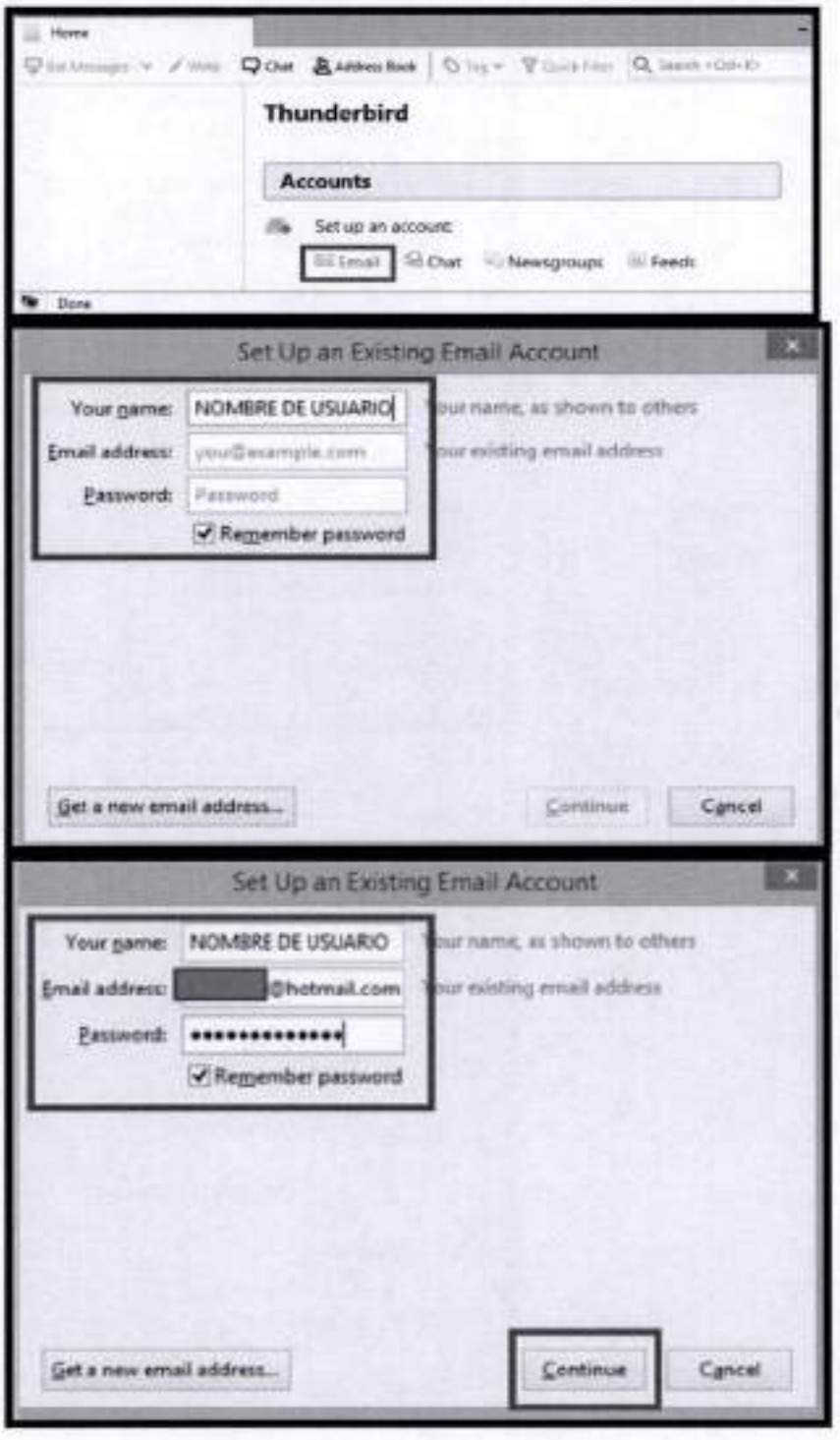
d. En esta pantalla se indica que la instalación ha sido completada y dar click en "Finish".

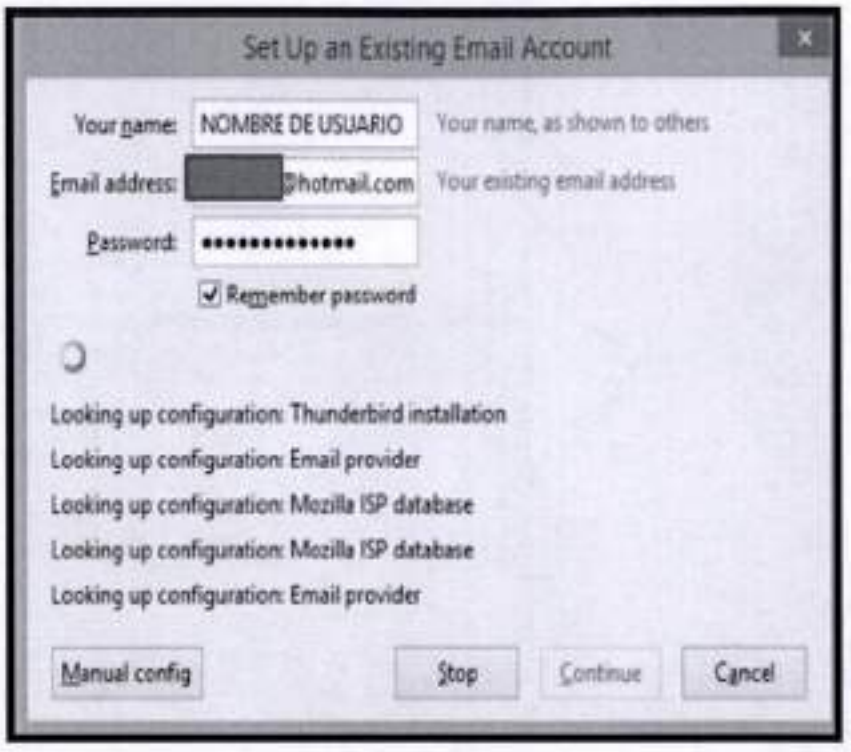


e. Dirigirse al pendrive (USB) donde se instaló el programa *Thunderbird* portable e ingresar a la carpeta creada y ejecutar el programa ThunderbirdPortable.exe, para que el programa inicie.

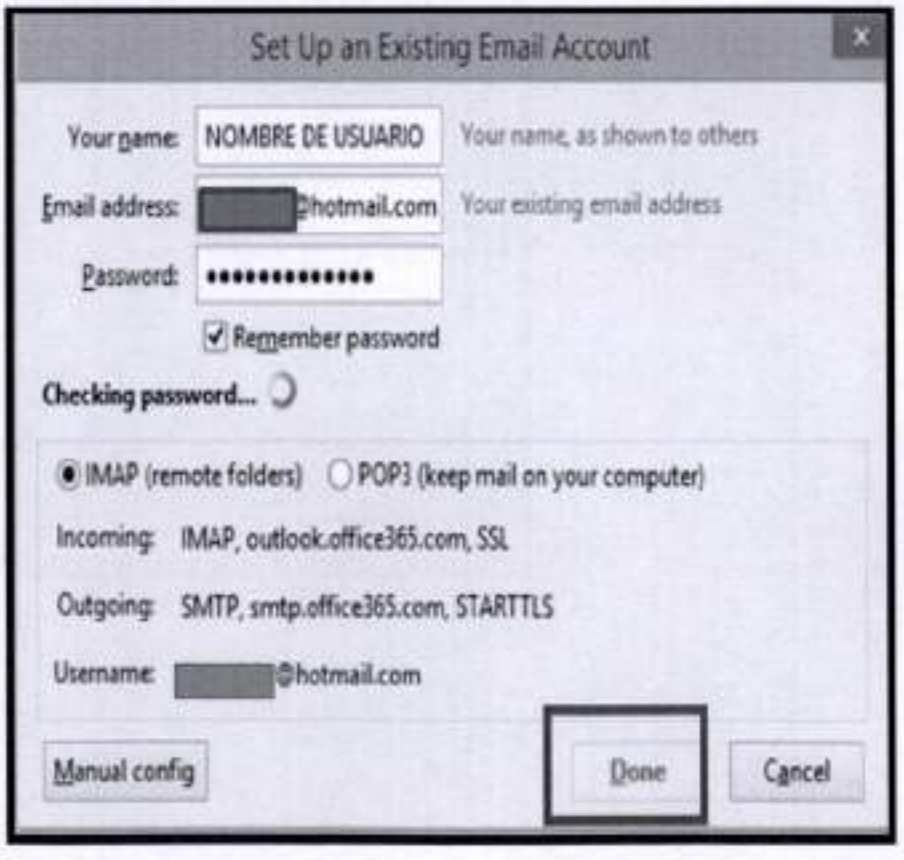


f. En esta pantalla seleccionar la opción "Email" e ingresar los datos solicitados como nombre, correo electrónico y contraseña; y, dar click en continuar. Como se indicó anteriormente, se necesita la colaboración del investigado para poder acceder y descargar los correos electrónicos.

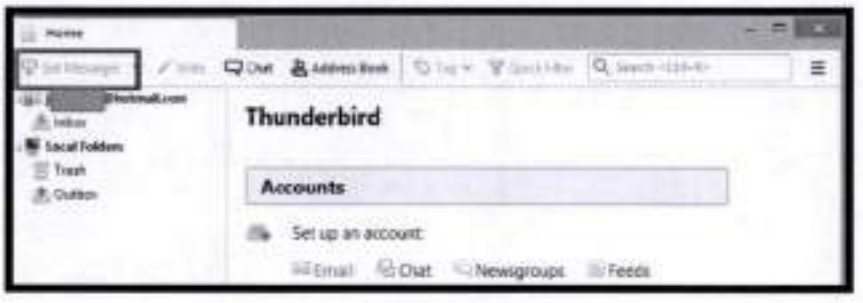

Thunderbird
Accounts
Set up an account:
Email
Chat
Newsgroups
Feeds
Done
Set Up an Existing Email Account
Your name:
NOMBRE DE USUARIO
Email address:
Password:
Remember password
Get a new email address...
Continue
Cancel
Set Up an Existing Email Account
Your name:
NOMBRE DE USUARIO
Email address:
@hotmail.com
Password:
Remember password
Get a new email address...
Continue
Cancel



g. En esta pantalla se indica que la configuración es correcta y se da click en "*Done*".



h. En esta pantalla se puede observar que el correo electrónico vinculado a la investigación se encuentra configurado y solo queda hacer click en el botón "*Get Messages*".

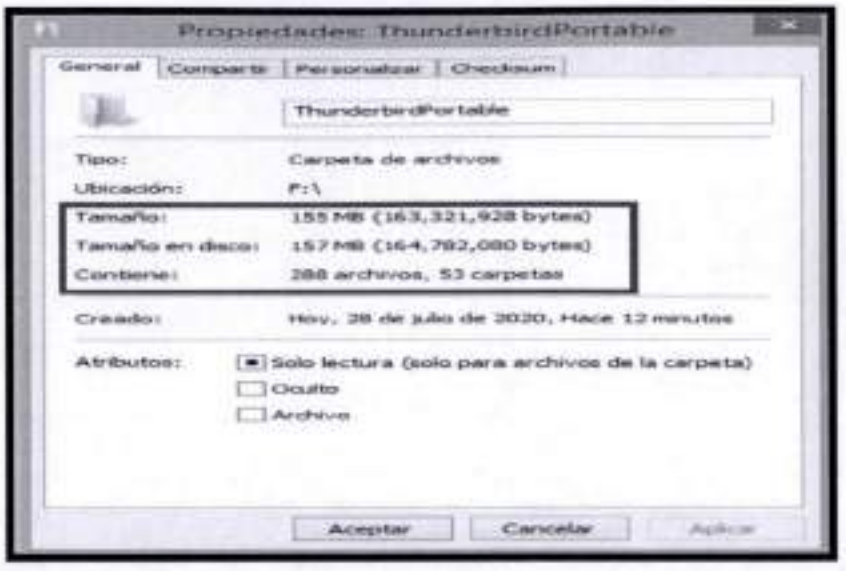


i. En esta pantalla se indica que se inició la descarga de todos los mensajes de correo, esto puede tardar unos minutos dependiendo de la velocidad del internet.

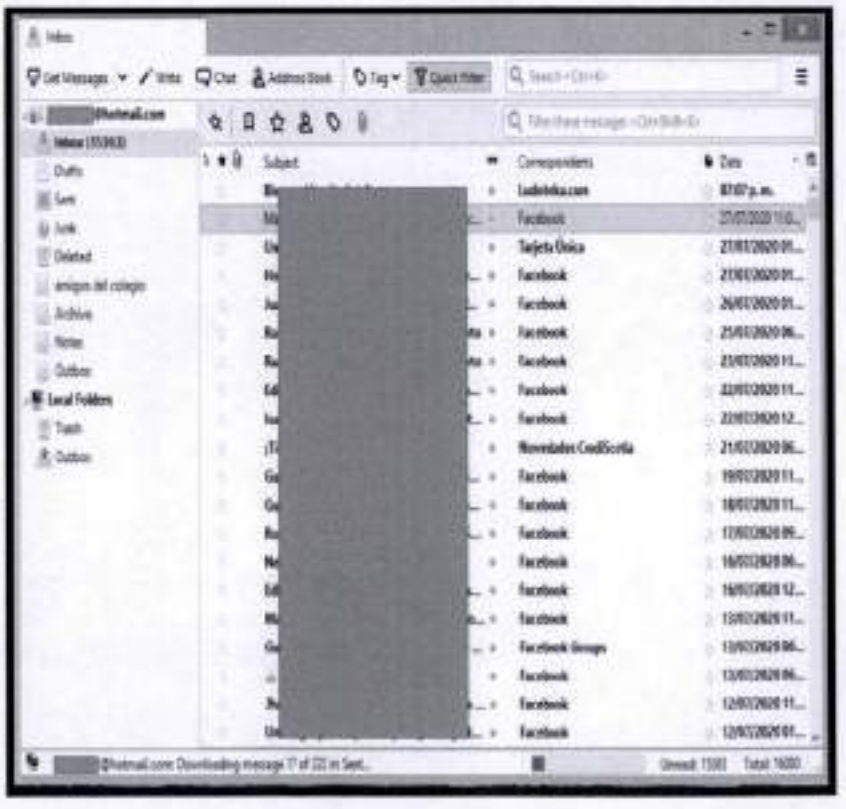


j. Se puede comprobar que al iniciar la descarga de los mensajes de correo la carpeta destino donde se configuró el correo electrónico tiene un peso y una cantidad de archivos determinados, cuyos valores cambian luego de finalizar la descarga de todos los correos.

S. DE LA CRUZ Q.



k. En esta pantalla se pueden ver los mensajes descargados del correo electrónico vinculado a la investigación.



l. En esta pantalla se pueden ver uno de los mensajes descargados del correo electrónico vinculado a la investigación y en la siguiente pantalla se puede observar la diferencia de peso y cantidad de archivos de la carpeta de destino donde se descargaron los mensajes.

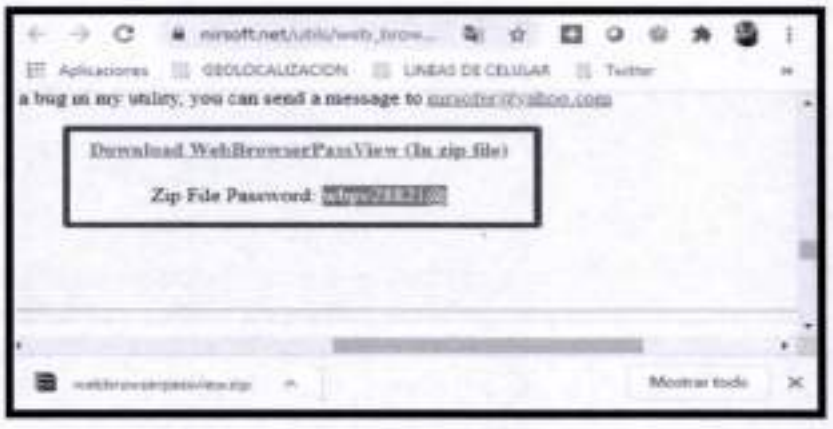


m. Luego de descargar los mensajes de correo se debe de comprimir la carpeta destino donde se descargaron los mensajes, generar su respectivo código hash y ser almacenado en un pendrive (USB) u otro dispositivo de almacenamiento y realizar el acta respectiva.

7. Obteniendo contraseñas con WebBrowserPassView:

La herramienta *WebBrowserPassView* permite ver las contraseñas almacenadas en su navegador web (admite Internet Explorer, Firefox, Chrome, Safari y Opera), esta herramienta puede ser descargada de la página web www.nirsoft.net que ofrece una colección única de utilidades gratuitas pequeñas y útiles.

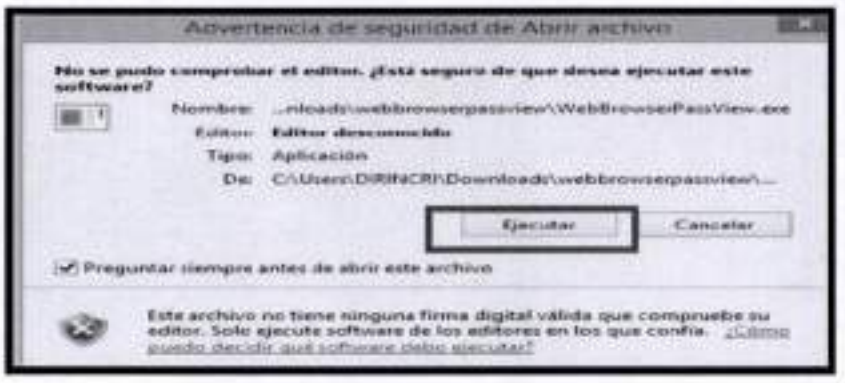
a. Descargar la herramienta *WebBrowserPassView*, haciendo click en "*Download WebBrowserPassView (In zip file)*" y después de la descarga descomprimir el archivo comprimido, para lo cual solicita una contraseña, la misma que se encuentra en "*Zip File Password*".



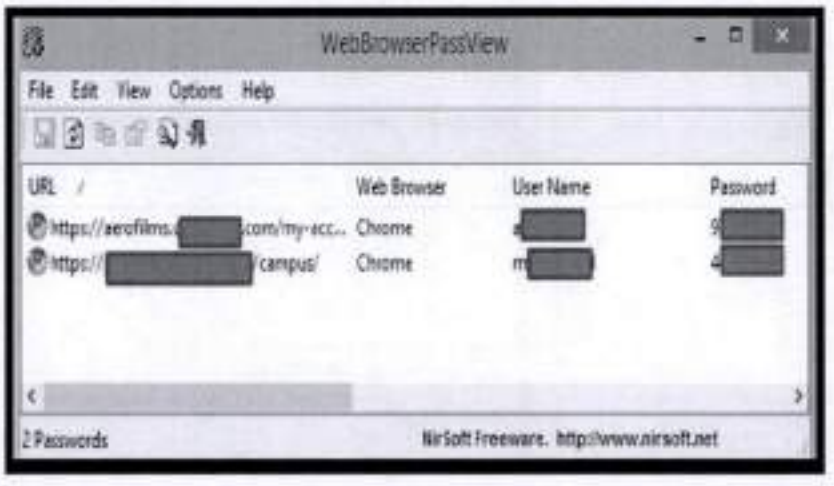
b. Ingresar a la carpeta descomprimida y ejecutar el programa "*WebBrowserPassView.exe*"



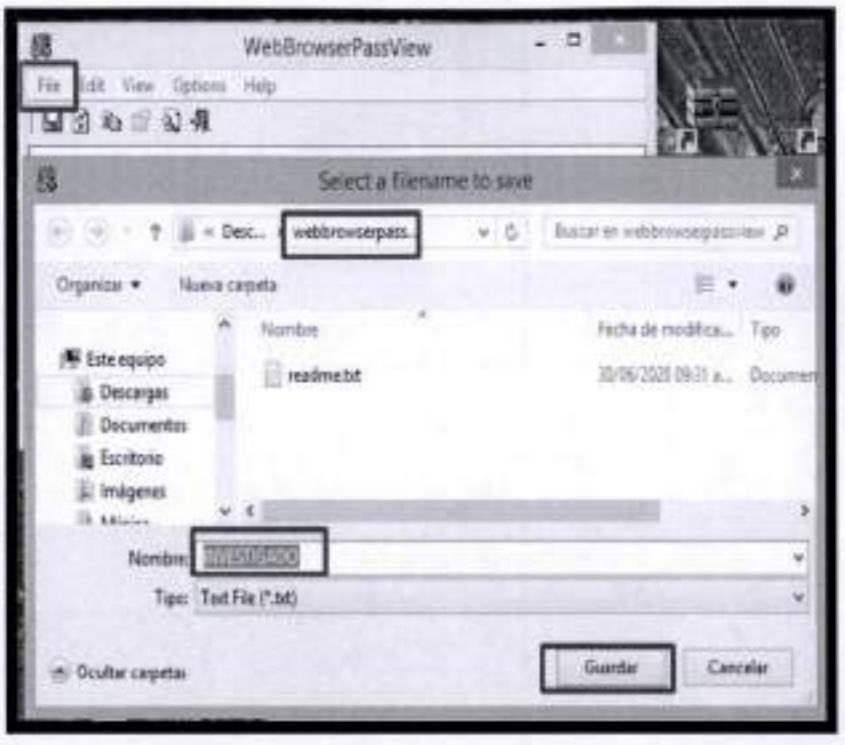
S. DE LA CRUZ Q.

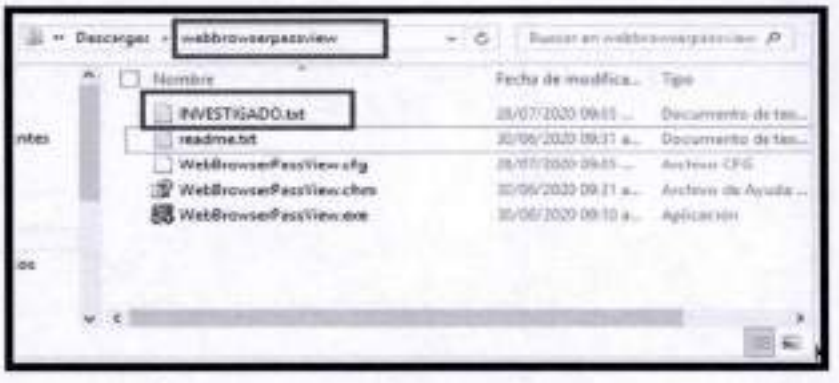


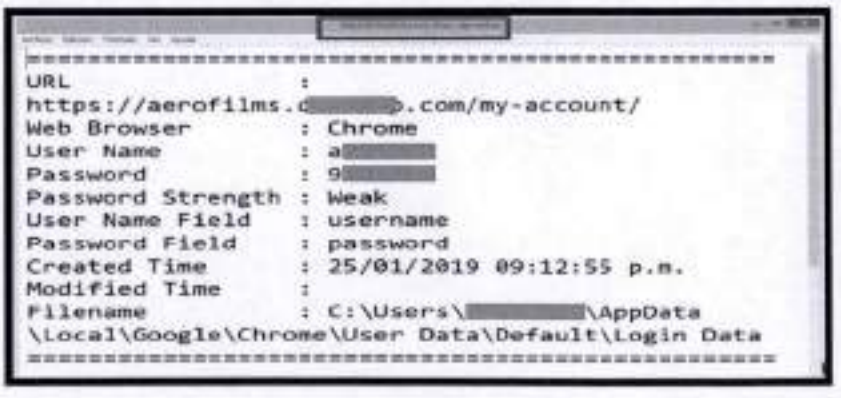
c. Al ejecutar el programa "*WebBrowserPassView.exe*", automáticamente busca los datos de usuario y contraseña en los navegadores instalados en el equipo de cómputo y muestra la URL, el navegador, el nombre de usuario, la contraseña, la fecha creada, entre otros datos.



d. Se puede guardar la información extraída en un *bloc* de notas, seleccionando los registros, hacer click en "*File*", se coloca un nombre al archivo y se puede seleccionar una ubicación para guardar el archivo. Por defecto se guarda en la carpeta descomprimida donde se ejecutó el programa.





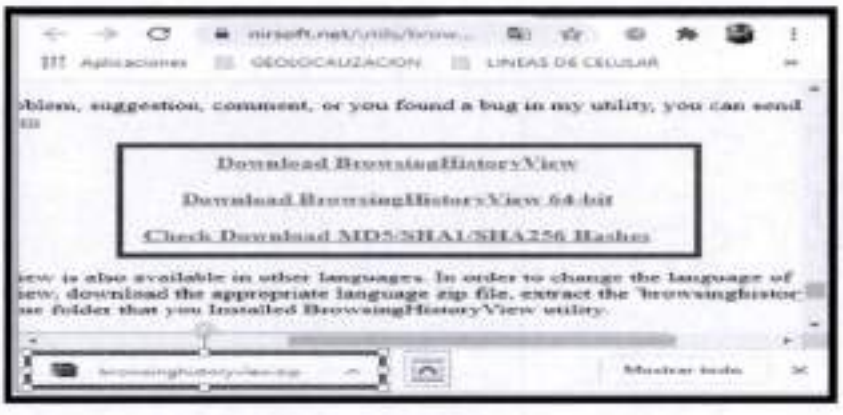


e. Luego de guardar el resultado se debe de generar su respectivo código hash y ser almacenado en un pendrive (USB) u otro dispositivo de almacenamiento y realizar el acta respectiva.

8. Obteniendo historial de navegación con BrowsingHistoryView:

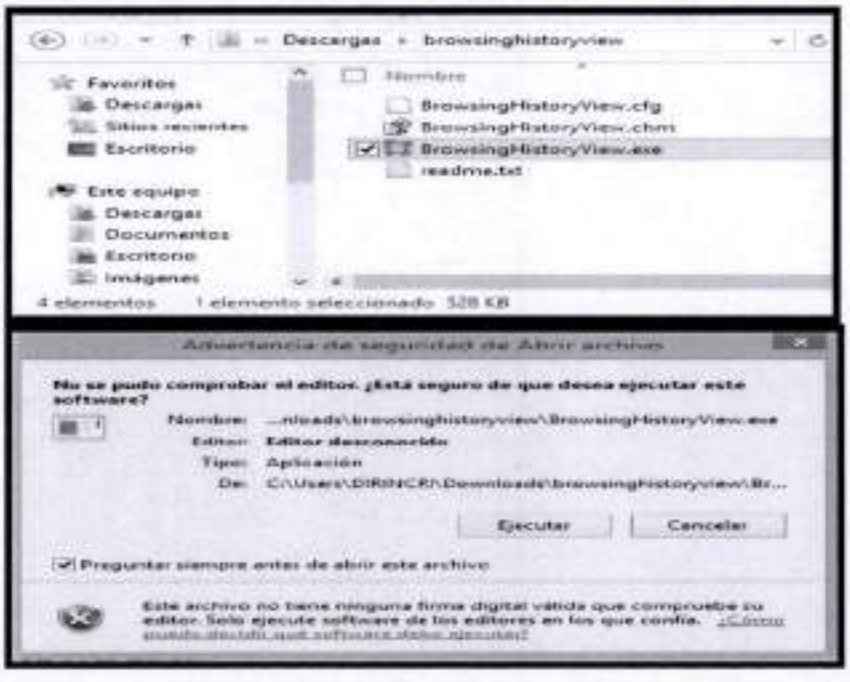
La herramienta *BrowsingHistoryView* nos permite ver historial de navegación de los navegadores web (admite Internet Explorer, Firefox, Chrome, Edge), esta herramienta puede ser descargada de la página web www.nirsoft.net que ofrece una colección única de utilidades gratuitas pequeñas y útiles.

a. Descargar la herramienta *BrowsingHistoryView*, haciendo click en "*Download BrowsingHistoryView*" y después de la descarga descomprimir el archivo comprimido.



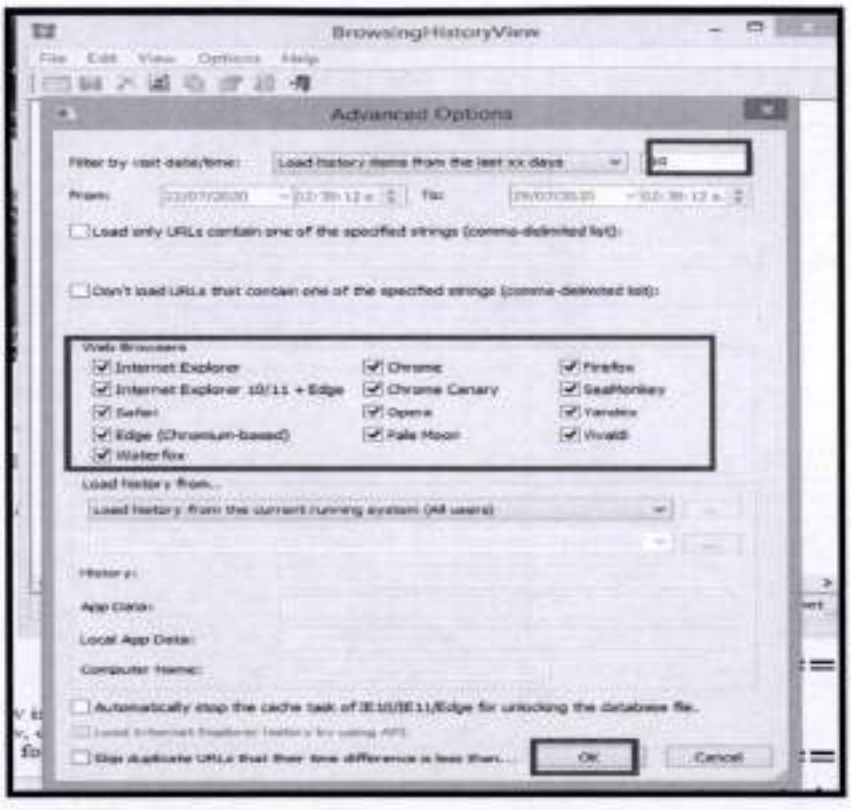
V°B°
S. DE LA CRUZ ©

b. Ingresar a la carpeta descomprimida y ejecutar el programa "*BrowsingHistoryView.exe*"

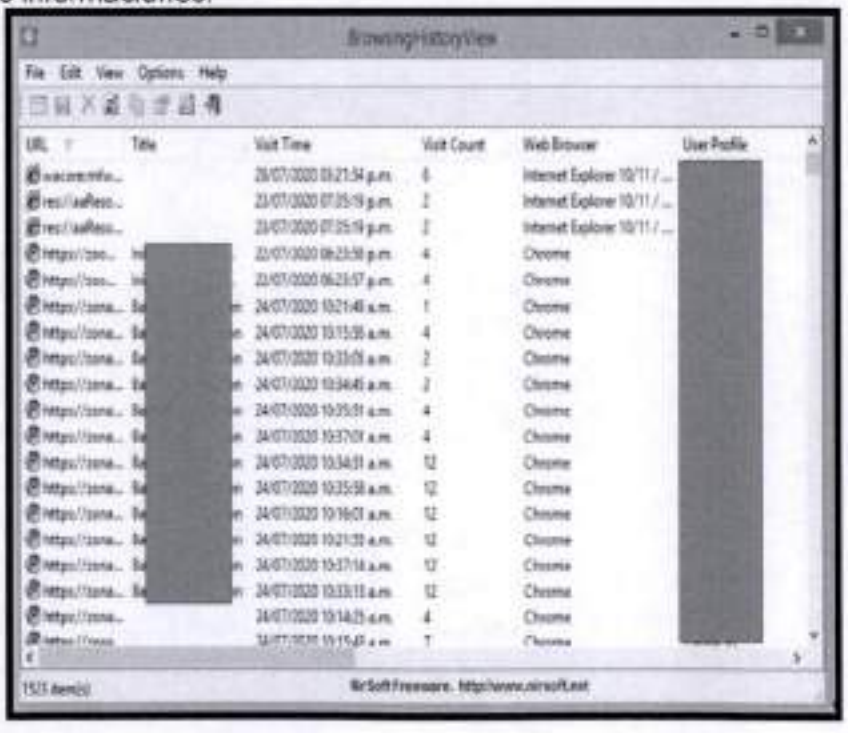


c. Al ejecutar el programa "*BrowsingHistoryView.exe*", se puede configurar la extracción de información detallando la cantidad de días, de que navegadores web se desea extraer información y luego

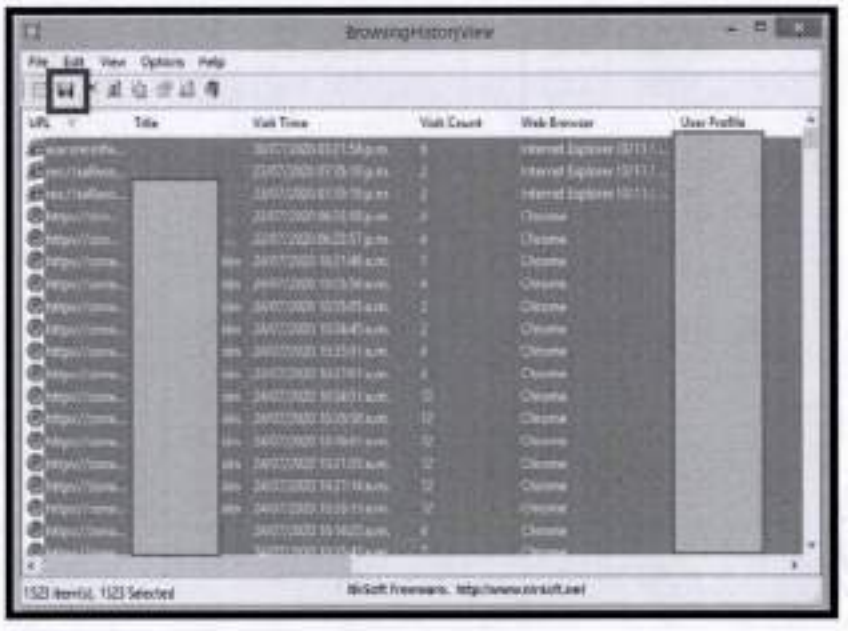
se ejecuta el programa.

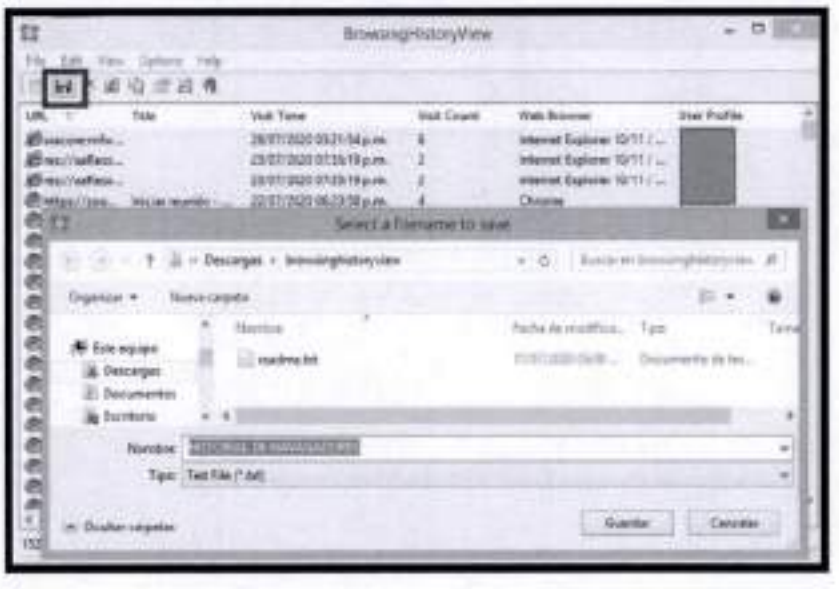


d. El resultado del historial muestra la URL, el título de la página *web*, fecha de visita, contador de visitas, navegador web, usuario, entre otras informaciones.



e. Se puede guardar la información extraída en un bloc de notas, seleccionando los registros, hacer click en "el icono del *diskette*", se poner pone un nombre al archivo y se puede seleccionar una ubicación para guardar el archivo. Por defecto se guarda en la carpeta descomprimida donde se ejecutó el programa.







f. Luego de guardar el resultado se debe de generar su respectivo código hash y ser almacenado en un pendrive (USB) u otro dispositivo de almacenamiento y realizar el acta respectiva.

S. DE LA CRUZ Q.

BIBLIOGRAFÍA

1. Bustamante Rúa, M. M. (2023). *Cibercriminalidad e investigación penal tecnológica: Una mirada desde la experiencia de la cooperación internacional para la persecución de la cibercriminalidad en Latinoamérica*. Palestra.
2. Comisión Económica para América Latina y el Caribe. (2021). *Digitalización de las mujeres en América Latina y el Caribe: Acción urgente para una recuperación transformadora y con igualdad* (LC/TS.2021/18). CEPAL.
3. Foro Económico Mundial. (2021). *Informe sobre gobernanza tecnológica*. Foro Económico Mundial.
4. Unión Internacional de Telecomunicaciones. (2023). *Medición del desarrollo digital*: datos y cifras 2023.UIT
5. Policía Nacional del Perú (2016). *Manual de documentación policial (R.D. N° 776-2016-DIRGEN/EMG-PNP, 27 de julio de 2016)*. Lima, Perú. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/7716945/6529039-manual-de-documentacion-policial.pdf

ANEXOS

Anexo I Definición de Términos

1. ***Adware***: Se trata de un software que secuestra el navegador u otras partes del sistema para inundarlo con anuncios no deseados.

2. ***Backup***: Un backup no es más que una copia de seguridad a mayor o menor escala de la información de un sistema informático. Puede ser una versión reciente de la información contenida en todos los equipos de nuestra compañía, o puede tratarse de servidores completos con ingentes cantidades de datos, este término se enfoca al respaldo de información que se puede obtener durante la investigación.

3. **Bloqueador de escritura:** Es una herramienta hardware y/o software que permite realizar una copia forense en modo de bloqueo de escritura, es decir sin poder modificar el dispositivo de almacenamiento original. Es una herramienta fundamental para procedimientos periciales.

4. ***Carding:*** Uso no autorizado de los datos de las tarjetas de débito o crédito, cuentas bancarias o cualquier otra información de una persona sin su consentimiento.

5. **Código *hash*:** Es un algoritmo matemático aplicado a un archivo digital y nos brinda como resultado una cadena de caracteres alfanuméricos de una longitud fija, nos garantiza la integridad de un archivo digital, existen varios tipos de algoritmos hash como, por ejemplo: MD5, SHA1, SHA256, entre otros.

6. **Copia forense:** también conocido como imagen forense o copia bit a bit, es la copia exacta de un dispositivo de almacenamiento (disco duro, pendrive (USB), disco duro externo, memoria microSD, entre otros) a otro dispositivo de almacenamiento de mayor capacidad de almacenamiento. Este procedimiento es realizado para poder aplicar procedimientos de la informática forense a la copia forense realizada.

7. **Criptografía:** Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet, siendo utilizado en determinadas circunstancias por los ciberdelincuentes para ocultar su información y no se pueda acceder.

8. **Criptomonedas:** Son monedas virtuales, independientes y descentralizadas, puesto que no están controladas por ningún Estado, institución financiera, banco o empresa. Se trata de monedas intangibles, que pueden ser utilizadas como medio de pago igual que el dinero físico.

9. ***Cyberbullying***: Es el uso de medios digitales con la intención de acosar psicológicamente (insultos, hostigamientos, mensajes ofensivos, y/o amenazadores, chantajes entre otros) a una persona pudiendo generar consecuencias fatales.

MINISTERIO DEL INTERIOR V°B° S. DE LA CRUZ Q.

JURISPOL

10. ***Dark Web:*** Es la parte no regulada de Internet. Ninguna organización, empresa o gobierno está a cargo de ella o es capaz de aplicar reglas. Esta es exactamente la razón por la que la dark web se asocia comúnmente con prácticas ilegales. Para acceder a los contenidos de la Dark Web es necesario utilizar navegadores web no convencionales (Tor, I2P o Freenet).

11. ***Deep web:*** Es la parte de Internet a la que los principales metabuscadores (Google, Bing, entre otros) no son capaces de acceder e indexar su contenido, ya sea porque no es público el contenido o porque se necesita algún requisito o credencial para acceder.

12. **Dirección IP:** IP por sus siglas en ingles "Internet Protocol" que traducido al español, significa "Protocolo de Internet". Este protocolo, al igual que otros muchos como HTTP, TCP, UDP entre otros, se encarga de establecer conectividad en las redes.

13. **Dominio *web*:** Es el nombre único y exclusivo asociado a una dirección IP que nos permite acceder a un sitio web.

14. **Duplicador forense:** Es una herramienta de hardware y/o software que permite realizar una copia forense de un dispositivo de almacenamiento, existen duplicadores forenses con sus respectivos bloqueadores de escritura.

15. **Firma electrónica:** Es una herramienta digital que utilice mecanismos de autenticación para sustituir la firma manuscrita en el papel, generalmente consta de códigos numéricos.

16. **Grooming:** Es una técnica de engaño de un adulto que simula ser un menor de edad, para abordar a menores de edad mediante el uso del internet con el objetivo de obtener una ventaja sexual o material de abuso sexual de niños, niñas y adolescentes (MASI), que pueden acabar en violencia sexual.

17. **Historial de navegación:** Es un registro de todas las páginas web visitadas o visualizadas en un navegador web de una computadora.

18. **Hosting:** Es un servicio en línea que te permite alojar una página web en Internet. Consiste en alquilar un espacio en un servidor donde puedes almacenar todos los archivos y datos necesarios para que tu sitio web funcione correctamente y pueda ser visualizado en internet.

19. **HTTP**: (Hypertext Transfer Protocol), se trata de un protocolo de transferencia de texto que opera a través de solicitudes entre un cliente y un servidor. HTTP es el término utilizado para describir este sencillo lenguaje basado en texto.

20. **HTTPS:** Es el acrónimo de Hypertext Transfer Protocol (en español protocolo de transferencia de hipertexto). HTTPS es igual que HTTP pero añadiéndole "Seguro", puesto que, usa una conexión segura mediante

MINISTERIO DEL INTERIOR V°B° S. DE LA CRUZ Q.

JURISPOL

un cifrado SSL (Capas de Sockets Seguros) y por tanto los datos viajan de un modo seguro de un lugar a otro. Este término referencia sobre la seguridad de las conexiones en las distintas plataformas informática.

21. **Huso horario:** Es cada una de las 24 zonas horarias en que se divide la Tierra, tiempo que le toma al planeta girar sobre su propio eje, y que determina la hora de una zona geográfica a partir del meridiano de Greenwich, desde donde se deben sumar o restar horas según corresponda. Durante las diligencias en la investigación, este término asociado a la dirección IP permite conocer la ubicación referencial de donde se ejecutaron las actividades criminales es una determinada fecha, hora y huso horario.

22. **IMEI**: Por sus siglas en inglés *International Mobile Equipment Identity* (identidad internacional de equipo móvil) es un código de quince dígitos pregrabado en los teléfonos móviles. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta. El IMEI permite contrastar las características técnicas de equipos móviles, que pueden coadyuvar en la investigación.

23. **ISP:** Siglas en inglés de Internet Service Provider (Proveedor de Servicios de Internet), empresa que facilita a los usuarios la conexión a Internet.

24. **LAN**: Es la abreviatura de Local Area Network. Denominadas redes con extensión física limitada. La mayoría de las redes LAN se usan en hogares privados o en empresas, configurando una red de equipos en esa área reducida. De este modo, distintos dispositivos pueden comunicarse entre ellos.

25. **Memoria RAM:** (acrónimo de *Random Access Memory*, o Memoria de Acceso Aleatorio) es un tipo de memoria operativa de alta velocidad de los computadores y sistemas informáticos, donde se ejecuta la mayor parte del software: el propio sistema

26. **Memoria volátil:** Es aquella memoria cuya información se pierde al desconectarse de un flujo de energía, como por ejemplo la memoria RAM.

27. ***Malware*:** También llamado "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. La intención del malware es sacarle dinero al usuario ilícitamente.

28. **Navegador *Web*:** Es un programa que interpreta código de programación web y permite visualizar la información de páginas web y permite al usuario interactuar con su contenido, entre los principales navegadores web se encuentran Internet Explorer, Firefox, Chrome, Safari, Opera, entre otros.

29. **Nube/*Cloud*:** Es una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema. Estos servidores están diseñados para almacenar y administrar datos,

ejecutar aplicaciones o entregar contenido o servicios, como streaming de videos, correo web, software de ofimática o medios sociales con disponibilidad 24/7.

30. **OSINT:** Open Source Inteligence es la investigación en fuentes abiertas para recopilar o generar inteligencia de internet.

31. **Patrullaje virtual:** Utilizar las tecnologías de la información aplicando técnicas de OSINT para ubicar información libre en internet que ayude a la investigación de una noticia criminal.

32. ***Pharming*:** Es una modalidad delictiva que utiliza el ciberdelincuente para alterar el archivo host de un computador, redireccionado a un sitio web falso, que tienen como propósito capturar información confidencial de la víctima, como: nombres de usuario, contraseñas y datos de tarjetas electrónicas bancarias o bien pueden instalar malware en el computador.

33. ***Phishing*:** Es una modalidad delictiva que consiste en suplantar sitios web de personas, entidades públicas y privadas con la finalidad de obtener información confidencial como: contraseñas, números de tarjetas electrónicas bancarias, entre otros.

V°B°
S. DE LA CRUZ Q.

34. **Programa portable:** Es un programa que no necesita instalarse en una computadora, por lo cual no realiza ningún cambio en el registro del sistema y se utiliza con un archivo ejecutable.

35. ***Proxy*:** Es una herramienta que hace de intermediario entre las conexiones de un cliente y un servidor de destino. Esta herramienta es utilizada por los ciberdelincuentes para ocultar su verdadera identidad en internet y cometer actos ilícitos.

36. ***Ransomware*:** Es el secuestro o cifrado de la información o del equipo informático, que consiste en solicitar un rescate con el fin de devolver el contenido de la información a su estado original.

37. ***Spyware*:** Es un software malicioso que infecta ordenadores y otros dispositivos conectados a internet, y graba secretamente sus datos de navegación, compras online, entre otra información.

38. **Troyano:** Software malicioso que al instalarse en un sistema informático puede realizar diversas tareas con el objetivo de controlar el equipo de un usuario, robar datos e introducir software malicioso en el equipo de la víctima.

39. **URL:** Por sus en siglas en inglés "Universal Resource Locator" (localizador de recurso universal) es una dirección web completa que se utiliza para encontrar una página web o recurso específico en internet.

40. **VPN:** (*Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Mediante una conexión cifrada se consigue que un equipo pueda trabajar como si físicamente estuviera dentro de la red privada.

JURISPOL

41. ***Vishing***: Es una modalidad delictiva que pretende suplantar la identidad a través de llamadas telefónicas, recreando una voz automatizada semejante a las oficiales con el fin de solicitar información confidencial del cliente (clave token, datos personales, entre otros).

S. DE LA CRUZ Q.

Anexo II

MEMBRETE CONFORME A LOS DATOS DE LA UNIDAD Y AÑO EN VIGENCIA

Lugar, fecha del año en curso

OFICIO N.º .....-2023-....(siglas de la unidad).....

SEÑOR : Representante Legal.
(Nombre de Entidad Bancaria).

ASUNTO : Solicita información por motivo que se indica.

REF. : ----(registro de denuncia o Carpeta fiscal).

Es grato dirigirme a Usted, con la finalidad de comunicarle que en esta DIVINDAT – DIRINCRI PNP, se viene llevando a cabo diligencias preliminares contra ---(NOMBRE DEL DENUNCIADO o los que resulten responsables) por la presunta comisión de delito informático contra el patrimonio - Fraude informático, en agravio de (**nombre de la víctima**), al haberse realizado (Breve reseña de los hechos ocurridos), motivo por el cual se solicita con carácter de **MUY URGENTE**, la siguiente información:

1. Se remita información detallada respecto a los procesos realizados desde la cuenta bancaria N°.....~~~~, especificando el medio utilizado (banca móvil o aplicativo), asimismo el detalle de los registros de fecha, hora al momento de efectuarse la operación inusual, debiendo especificar desde que dispositivo electrónico, dirección IP o número IMEI y de ser el caso, el número telefónico que efectuó la llamada para realizar la solicitud. ----------
2. Informar el detalle de las operaciones ilícitas, especificando los números de cuenta donde se abonó el dinero de la víctima, así como también sobre los consumos y operaciones realizadas desde la cuenta N°....., especificando el comercio donde se efectuó la compra o disposición de dinero. ----------
3. Remitir una copia de la resolución sobre las investigaciones internas realizadas en su representada por los suscitados en agravio de (nombre del denunciante) y de ser el caso, que medidas se adoptaron posterior a ella. ----------

Lo solicitado se requiere con carácter de **"MUY URGENTE"**, con la finalidad de continuar con las investigaciones que se lleva a cabo en esta Unidad Especializada, para el esclarecimiento de la presunta comisión del Delito informático contra el Patrimonio – Fraude Informático, adjuntando la autorización respectiva del titular de la cuenta agraviada a fin de que su representada brinde toda la información solicitada.

Es propicia la oportunidad para expresarle las muestras de mi consideración y estima personal.

Dios guarde a Ud.

SIGLAS ( )*

V°B°
S. DE LA CRUZ Q.

MEMBRETE DEL JEFE DE LA UNIDAD CON SELLO REDONDO

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORRE ELECTRÓNICO)

Anexo III

MEMBRETE CONFORME A LOS DATOS DE LA UNIDAD Y AÑO EN VIGENCIA

Lugar, fecha del año en curso

OFICIO N.º .....-2023-....(siglas de la unidad).....

SEÑOR : Representante Legal.
(Nombre de Comercio So tienda virtual).

ASUNTO : Solicita información por motivo que se indica.

REF. : ----(registro de denuncia o Carpeta fiscal).

Es grato dirigirme a Usted, con la finalidad de comunicarle que en esta DIVINDAT – DIRINCRI PNP, se viene llevando a cabo diligencias preliminares contra ---(NOMBRE DEL DENUNCIADO o los que resulten responsables) por la presunta comisión de delito informático contra el patrimonio - Fraude informático, en agravio de (**nombre de la víctima**), al haberse realizado (Breve reseña de los hechos ocurridos), motivo por el cual se solicita con carácter de **MUY URGENTE**, la siguiente información:

1. Se remita información detallada respecto a los procesos de pagos y/o compras realizadas desde la cuenta bancaria N°....., especificando el detalle de los registros de fecha, hora al momento de efectuarse la operación inusual, debiendo especificar desde que dispositivo electrónico con indicación de la dirección IP o código IMEI y de ser el caso, el número telefónico que efectuó la llamada para realizar la solicitud. ----------
2. Informar al detalle sobre el tipo de servicio o compra adquirido desde la tarjeta o cuenta bancarias N°....., detallando el motivo del pago, los beneficiarios del servicio, líneas telefónicas asociadas al momento del registro del pago, correos utilizados como verificados de la compra, lugar donde se hizo él envió del producto especificando la fecha y hora de entrega, adjuntándose copia de los comprobantes de pago generados al momento de la recepción, señalar el nombre de la persona encarga en la entrega del producto y demás información que guarde relación a la operaciones ilicita antes detallada. ----------
3. Remitir al detalle información sobre posibles compras y/o pagos de servicios realizadas en la misma o anteriormente desde los mismos puntos de conexión IP o correos electrónicos que son materia de investigación. ----------

Lo solicitado se requiere con carácter de **"MUY URGENTE"**, con la finalidad de continuar con las investigaciones que se lleva a cabo en esta Unidad Especializada, para el esclarecimiento de la presunta comisión del Delito informático contra el Patrimonio – Fraude Informático, adjuntando la autorización respectiva del titular de la cuenta agraviada a fin de que su representada brinde toda la información solicitada.

Es propicia la oportunidad para expresarle las muestras de mi consideración y estima personal.

Dios guarde a Ud.

SIGLAS ( )*

V°B°
S. DE LA CRUZ Q.

MEMBRETE DEL JEFE DE LA UNIDAD CON SELLO REDONDO

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORRE ELECTRONICO)

Anexo IV

MENBRETE CONFORME A LOS DATOS DE LA UNIDAD Y AÑO EN VIGENCIA

Lugar, fecha del año en curso

OFICIO N.º .....-2023-.....(siglas de la unidad).....

SEÑOR : Representante Legal.
(Nombre de Comercio S|p tienda virtual).

ASUNTO : Solicita información por motivo que se indica.

REF. : ----(registro de denuncia o Carpeta fiscal)

Es grato dirigirme a Usted, con la finalidad de comunicarle que en esta DIVINDAT – DIRINCRI PNP, se viene llevando a cabo diligencias preliminares contra ---(NOMBRE DEL DENUNCIADO o los que resulten responsables) por la presunta comisión de delito informático contra el patrimonio - Fraude informático, en agravio de (**nombre de la víctima**), al haberse realizado (Breve reseña de los hechos ocurridos), motivo por el cual se solicita con carácter de **MUY URGENTE**, la siguiente información:

1. Se remita información detallada respecto a los procesos de pagos y/o compras realizadas desde la cuenta bancaria N°....., especificando el detalle de los registros de fecha, hora al momento de efectuarse la operación inusual, debiendo especificar desde que dispositivo electrónico con indicación de la dirección IP o código IMEI y de ser el caso, el número telefónico que efectuó la llamada para realizar la solicitud. ----------
2. Informar al detalle sobre el tipo de servicio o compra adquirido desde la tarjeta o cuenta bancarias N°....., detallando el motivo del pago, los beneficiarios del servicio, líneas telefónicas asociadas al momento del registro del pago, correos utilizados como verificados de la compra, lugar donde se hizo él envió del producto especificando la fecha y hora de entrega, adjuntándose copia de los comprobantes de pago generados al momento de la recepción, señalar el nombre de la persona encarga en la entrega del producto y demás información que guarde relación a la operaciones ilícita antes detallada. ----------
3. Remitir al detalle información sobre posibles compras y/o pagos de servicios realizadas en la misma o anteriormente desde los mismos puntos de conexión IP o correos electrónicos que son materia de investigación. ----------

Lo solicitado se requiere con carácter de **"MUY URGENTE"**, con la finalidad de continuar con las investigaciones que se lleva a cabo en esta Unidad Especializada, para el esclarecimiento de la presunta comisión del Delito informático contra el Patrimonio – Fraude Informático, adjuntando la autorización respectiva del titular de la cuenta agraviada a fin de que su representada brinde toda la información solicitada.

Es propicia la oportunidad para expresarle las muestras de mi consideración y estima personal.

Dios guarde a Ud.

SIGLAS ( )*

V°B°
S. DE LA CRUZ O

MENBRETE DEL JEFE DE LA UNIDAD CON SELLO REDONDO

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORRE ELECTRONICO)

Anexo V

MEMBRETE CONFORME A LOS DATOS DE LA UNIDAD Y AÑO EN VIGENCIA

(ANEXO 3)

Lima, ...(fecha de redacción).....

OFICIO Nº -2020- SIGLAS DE DEPENDENCIA POLICIAL

SEÑOR : **Representante Legal**
(EMPRESA RESPONSABLE DE AREA DE SISTEMAS)

ASUNTO : Información por motivo que se indica. -**SOLICITA**

REF. : ..... **Documentación de referencia a la denuncia**.....

Tengo el agrado de dirigirme a Ud. a fin de informar que en esta .....(Unidad y/o Dependencia Policial)....., se viene llevando a cabo una investigación con relación a la denuncia presentada por **(NOMBRE DEL DENUNCIANTE)** contra **(NOMBRE DE DENUNCIADOS)** y los que resulten responsables, al haberse realizado de manera ilícita intromisiones a su sistema informático con el propósito de capturar información relacionada a ..... (Tipo de archivos capturados)..... el... (fecha de ocurrido el hecho)....., por lo que se solicita información de acuerdo al siguiente detalle:

1. Información sobre las funciones de su representada en sistema informático agraviado.
2. Sobre las acciones realizadas una vez tomado conocimiento de los hechos denunciados.
3. Remitir el Informe Técnico elaborado sobre los hechos ocurridos en perjuicio de la empresa.
4. Nombres y cargos del personal responsable del sistema perteneciente a la empresa agraviada.
5. Otros.

En tal sentido y estando de conformidad a lo previsto en el Art. VI del D. Leg.1267 **"Las autoridades, entidades públicas y privadas, así como las personas naturales y jurídicas que están obligadas a prestar apoyo a la Policía Nacional del Perú, cuando las circunstancia así lo requieran, en el cumplimiento de sus funciones"**, por tal motivo lo solicitado se requiere con el carácter de **MUY URGENTE**, de su incumplimiento se accionara de acuerdo a ley.

Aprovecho la oportunidad para expresarle las muestras de mi consideración y estima personal.

Dios guarde a Ud.

SIGLAS DE REDACCION

FDO.

NOMBRE DEL JEFE DE UNIDAD

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORREO

V°B°
S. DE LA CRUZ G.

Anexo VI

ACTA DE VISUALIZACION DE CONTENIDO DE CORREO ELECTRONICO Y REDES SOCIALES (CASOS DE SUPLANTACIÓN DE IDENTIDAD)

En la ciudad de Lima, siendo las .....: horas del ....., en una de las oficinas de la .....(NOMBRE DE DEPENDENCIA POLICIAL)....., en presencia del ....(NOMBRES DEL REPRESENTANTE DEL MINISTERIO PUBLICO Y ABOGADO DEFENSOR)....., presente ..... (NOMBRE DEL AGRAVIADO), (EDAD), (ESTADO CIVIL), (OCUPACION), con DNI N°....., con domicilio en ....., con número telefónico ..... y correo electrónico....., a quien se le solicita bajo su consentimiento realizar la visualización del contenido de sus cuentas de correo electrónico y redes sociales, procediendo a levantar la presente acta con el siguiente resultado: ----------

V°B° S. DE LA CRUZ Q.

PRIMERO.- Se procedió a realizar el ingreso a la plataforma de mensajería instantánea de la empresa (RED SOCIAL) teniendo en el portal la opción de ingresar al registro de usuario y contraseña, siendo esta ingresada por parte de la mencionada titular de la cuenta para poder acceder a la bandeja principal de mensajes, teniendo como resultado .....(DETALLES SOBRE LO VISUALIZADO)....., por lo que se procede a realizar las capturas correspondientes que continuación se muestran:----------

CAPTURAS DE PANTALLAS

--- En el Distrito de Cercado de Lima, siendo las .:.. horas del día de la fecha, se procede a cerrar la presente acta, para lo cual los participantes de la misma firman de conformidad a continuación. ----------

EL INSTRUCTOR **AGRAVIADA**

RMP | **ABOGADO DEFENSOR**

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORREO

Anexo VII

ACTA DE VISUALIZACION DE CONTENIDO DE CORREO ELECTRONICO (CASOS DE FRAUDE O TRANSFERENCIAS BANCARIAS)

En la ciudad de Lima, siendo las ..... horas del ....., en una de las oficinas de la .....(NOMBRE DE DEPENDENCIA POLICIAL)....., en presencia del ....(NOMBRES DEL REPRESENTANTE DEL MINISTERIO PUBLICO Y ABOGADO DEFENSOR)....., presente ..... (NOMBRE DEL AGRAVIADO (EDAD), (ESTADO CIVIL), (OCUPACION), con DNI N°....., con domicilio en ....., con número telefónico ..... y correo electrónico....., a quien se le solicita bajo su consentimiento realizar la visualización del contenido de sus cuentas de correo electrónico y redes sociales, procediendo a levantar la presente acta con el siguiente resultado: ----------

PRIMERO.- Se procedió a realizar el ingreso a la plataforma de mensajería instantánea de la empresa (CORREO ELECTRONICO) teniendo en el portal la opción de ingresar al registro de usuario y contraseña, siendo esta ingresada por parte de la mencionada titular de la cuenta para poder acceder a la bandeja principal de mensajes, teniendo como resultado .....(DETALLES SOBRE LO VISUALIZADO "LOS CORREOS ENVIADOS DENOMINADOS SPAMS Y DIRECCIONES URL DONDE LA VICTIMA INGRESO)....., por lo que se procede a realizar las capturas correspondientes que continuación se muestran:----------

CAPTURAS DE PANTALLAS

--- En el distrito de Cercado de Lima, siendo las ..... horas del día de la fecha, se procede a cerrar la presente acta, para lo cual los participantes de la misma firman de conformidad a continuación. ----------

EL INSTRUCTOR **AGRAVIADA**

RMP **ABOGADO DEFENSOR**

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORREO

S. DE LA CRUZ Q.

Anexo VIII

ACTA DE LACRADO (casos de allanamiento y/o flagrancia)

---En la distrito de ..... en el departamento del ....., siendo las ___:___ horas del ....., en el interior del inmueble ubicado en ....., presente el instructor la persona de .....(NOMBRE DE INTERVENIDO)..... (sus generales de ley)..... en su calidad de DETENIDO, se procede al lacrado de lo siguiente:

- CARACTERISTICAS DEL DISPOSITIVO INCAUTADO.

---Dicho dispositivo magnético es introducido en una bolsa de plástico, y ésta dentro de un sobre color amarillo, para su LACRADO con cinta adhesiva transparente y su posterior envío para el análisis correspondiente.

---Siendo las ..... hora de la fecha, se da por concluida con la presente diligencia, firmando a continuación en señal de conformidad el instructor PNP y el personal policial antes señalado.

EL INSTRUCTOR

INTERVENIDO

RMP

ABOGADO DEFENSOR

DATOS DE LA UNIDAD Y/O DEPENDENCIA POLICIAL (DIRECCIÓN, NÚMERO TELEFÓNICO, CORREO

Anexo IX

MANUAL DE DOCUMENTACION POLICIAL

FORMATO 46

MEMBRETE

INFORME POLICIAL N° - SIGLAS

ASUNTO : Detalle de lo que se está informando sobre la investigación preliminar.

REF. : Si lo hubiera

I. ANTECEDENTE

Transcripción de la denuncia, ocurrencia, carpeta fiscal o documento que da origen a la investigación.

II. DILIGENCIAS POLICIALES EFECTUADÁS

A. Comunicación a la autoridad competente (Fiscal o Juez de la investigación preparatoria).
B. Actas (Lectura de derecho del imputado, registro domiciliario, registro personal, inspección policial, incautación, comiso, allanamiento, recojo, levantamiento de cadáver).
C. Manifestaciones (agraviado, imputado, testigo)
D. Información obtenida de entidades públicas y privadas.
E. Pericias (Balística, Físico-Químico, Grafotécnica, Psicología Forense, Medicina Forense, otros)
F. Reconocimiento médico legal, protocolo de necropsia.
G. Fotografías de especies incautadas o comisadas.
H. Planos, croquis, otros
I. Todas las diligencias Policiales realizadas por el pesquisa, estando al delito o delitos que se investigó, considerando todo lo indispensable para el esclarecimiento de la imputación.

III. ANÁLISIS Y EVALUACIÓN DE LOS HECHOS

IV. ANEXOS

Lugar y Fecha

ES CONFORME

EL INSTRUCTOR

FIRMA
POST FIRMA DEL JEFE DE LA DEPENDENCIA

JURISPOL