GOBIERNO DE PUERTO RICO

Negociado de la Policía de Puerto Rico

ORDEN GENERAL

Capítulo: 600	**Sección:** 613	**Fecha de Efectividad:** 25 de marzo de 2022
Título: Ocupación de Computadoras, Celulares y Equipos Electrónicos y Solicitud de Servicios de la División de Crímenes Cibernéticos		
Fecha de Revisión: Octubre/2021	**Revisión: Bienal**	**Número de Páginas: 14**

I. Propósito

Esta Orden General tiene el propósito de establecer en el Negociado de la Policía de Puerto Rico (en adelante NPPR), las normas y procedimientos que deberán cumplir con los Miembros del Negociado de la Policía de Puerto Rico (en adelante MNPPR), para solicitar, intervenir y procesar las actividades y equipos electrónicos relacionados con la comisión de delitos.

El tiempo que transcurre desde que se comete un delito utilizando un medio cibernético, hasta que la persona se querella y se recopila la información mediante un *subpoena* o se solicita una preservación de datos, es un factor importante y decisivo para evitar que se elimine, dañe o se altere la evidencia digital. Es de suma importancia que cada MNPPR conozca el procedimiento a seguir ante una querella de una víctima de crimen cibernético, o cuando ocupe algún equipo electrónico para que, de esta manera, la evidencia que se recopile pueda prevalecer en los foros judiciales.

II. Definiciones

1. **Analista de Evidencia Digital o Examinador**: Profesional que adquiere, recupera, gestiona, analiza y presenta las evidencias digitales contenidas en sistemas informáticos y dispositivos de tecnología digital.

2. **Bolsa Antiestática**: es una bolsa que previene daños a dispositivos electrónicos sensitivos como lo son discos duros, "Motherboard", tarjetas SD, XD, micro SD, flash drive, tarjetas de memoria, entre otros, de pequeñas cargas eléctricas acumuladas en el cuerpo u objetos (electricidad estática), que puede liberarse al entrar en contacto con dicho objeto, dañando su funcionamiento interno. La bolsa antiestática no impide que un equipo electrónico inalámbrico reciba señal.

3. **Bolsa Faraday**: se utiliza para prevenir el borrado o la modificación remota de dispositivos electrónicos inalámbricos incautados en investigaciones criminales. La bolsa Faraday tiene el efecto de proteger el equipo electrónico de señal externa. Una vez el equipo es embalado, queda protegido de interferencia de radiofrecuencia externa, bloqueando así señales celulares, bluetooth, RFID, NFC y Wi-Fi. La caja faraday se utiliza como otro método para preservar evidencia digital, similar a la bolsa faraday. Se utiliza mayormente si se va a realizar una extracción de datos del equipo electrónico móvil en la escena o fuera del laboratorio.

4. **Casillero Provisional de Depósito de Evidencia**: Armario seleccionado para el depósito de evidencia recopilada, que tendrá controles de acceso y cumplirá con las garantías mínimas de seguridad para guardar la propiedad incautada o recuperada por los MNPPR.

5. **Comunicación Telemática**: Aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada.

6. **Dirección de IP (IP Address)**: Es la identificación numérica de un nodo o servidor en Internet. Consta de cuatro octetos del 0 al 255, separado por puntos o de ocho cifras hexadecimales, separadas por puntos.

7. **Estera Antiestática con Cable Disipador de Tierra (*"grouding strap and elestrostatic mat"*)**: Son alfombras usadas para descargar la electricidad estática que llevan las personas, por lo general colocadas en lugares de manipulación de equipo electrónico delicado, ya que la estática acumulada en el cuerpo, puede dañar dicho equipo.

8. **Equipo Electrónico**: Combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas, que mediante determinados programas, permite almacenar, tratar información, y resolver problemas de diversa índole.

9. **Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés)**: Organismo autorizado en proporcionar servicios de apoyo y catalogación de estándares, incluyendo servicios de calibración, para organizaciones o personas en los Estados Unidos.

10. **Proveedor de Servicios de Internet (ISP por sus siglas en inglés)**: Organización o compañía que provee servicio de Internet por paga a individuos o negocios.

11. **Servicio de Informática en la Nube (Cloud Services)**: Proporciona tecnología de la información (TI) como un servicio a través de Internet o una red dedicada, con entrega según demanda y pago, según el uso.

12. **Servicio de Mensajes Cortos (SMS por sus siglas en inglés)**: Mensaje corto de texto que se pueden enviar entre teléfonos celulares y equipos móviles, utilizando la red de telefonía celular.

13. **Servicio de Mensajería Multimedia (MMS por sus siglas en inglés):** es un servicio de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video o fotos, utilizando la red de telefonía celular.

14. **Voz sobre Protocolo de Internet, también llamado Voz sobre IP (VoIP por sus siglas en inglés):** Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). El tráfico de Voz sobre IP puede circular por cualquier red IP, ya sea sólo en una red de área local (LAN) o aquellas conectadas a internet.

III. Normas y Procedimiento

A. Equipos electrónicos

Se considerarán como equipos electrónicos aquellas computadoras desktop, laptop, torres, tabletas, teléfonos celulares, teléfonos celulares inteligentes, *PDA*, dispositivos de almacenamiento portátiles "flash drives", disco duros externos, discos compactos (cd's y dvd's), "blue ray", consolas de juegos de video, *GPS*, drones, "smart watch", cualquier otro dispositivo que tenga capacidad de procesar y almacenar información digital, dispositivo de almacenamiento inalámbrico, "small single-board computers (SBCs)" "Raspberry Pi", entre otros.

B. Principios generales para la ocupación de equipos electrónicos

1. Si se tiene motivos fundados para creer que el equipo electrónico fue o será utilizado en un crimen, se tomarán las medidas correspondientes de forma inmediata para preservar la evidencia.

2. Sólo un MNPPR adiestrado podrá extraer la evidencia digital de equipos electrónicos ocupados.

3. La ocupación del equipo electrónico debe haberse realizado de forma legal para poder acceder a la información que éste contiene mediante orden judicial.

4. Si el equipo está apagado, dejarlo apagado y seguir el protocolo aquí establecido.

5. Si el equipo está prendido, seguir el protocolo aquí establecido para equipos prendidos.

6. Si se tiene la creencia razonable de que equipo electrónico está eliminando o destruyendo evidencia, se desconectará el cable del tomacorriente.

7. Documentar la localización en donde fue ocupado el equipo y el estado del mismo.

8. Tomar fotografías del equipo, equipos y cables conectados, monitor, teclado, ratón, entre otros.

C. Reglas Aplicables a la Ocupación de Equipo Electrónicos

Todo MNPPR observará y seguirá las siguientes normas cuando respondan a cualquier escena del crimen, que implique o haya equipos electrónicos como parte de la evidencia:

1. En las circunstancias excepcionales en que se ocupe un equipo electrónico sin orden judicial o consentimiento firmado por el dueño del equipo, el MNPPR tendrá la autoridad legal sólo para incautar u ocupar los equipos electrónicos, pero no la autoridad legal para llevar a cabo una búsqueda en los mismos. Esto aplica a todos los medios electrónicos, "hardware" y "software".

2. Para poder acceder a la información que guarda el equipo, se obtendrá una orden judicial antes de realizar la búsqueda.

3. Asegurará la escena. De tener motivos fundados para creer que el equipo tecnológico está involucrado en el crimen que está investigando, tomará la medida inmediata para preservar la evidencia, incluyendo la ocupación del equipo. El MNPPR asegurará tener un documento judicial (orden de registro y allanamiento) o consentimiento oficial para ello. Para el Consentimiento a Registro de un equipo electrónico el MNPPR utilizará el formulario PPR 612.1 y el 612.2 debidamente firmado por el dueño del equipo.

4. Si una persona a quien se le incauta un equipo electrónico móvil o telefónico; ya sea sospechoso o algún testigo, y este está dispuesto a consentir a un registro, alega ser quien utiliza dicho equipo pero no es el dueño o titular de la cuenta; para que un consentimiento a registro sea válido bajo dichas circunstancias, la persona debe demostrar que tiene uso mutuo con el dueño o titular de la cuenta; para ello pudiera ser válido que demuestre que puede desbloquear la pantalla "screen lock" del equipo ya se mediante la contraseña en dicho equipo y/o poder desbloquear dicho equipo utilizando su huella dactilar, patrón o el ID de rostro. En dicho caso el MNPPR instruirá a la persona para que anote la contraseña en la hoja de consentimiento el formulario 612.1 y el PPR- 612.2. Si el teléfono utiliza ID de rostro instruirá a la persona a que deshabilite la función de desbloquear pantalla con el rostro (Face ID recognition) y que anote la contraseña o patrón en el formulario de

consentimiento PPR-612.1 y el PPR- 612.2.

5. En los casos que se ocupe un equipo electrónico en posesión de un menor de edad por la comisión de una falta al amparo de la Ley 88 del 1986 *"Ley de Menores de Puerto Rico"*, para que sea válido un registro a dicho equipo incautado, tiene que mediar el consentimiento del encargado mayor de edad del menor. Si el padre consciente al registro y la madre no, o viceversa, o si uno de los encargados del menor si consciente al registro y el otro no, el MNPPR deberá consultar con un procurador de menores para obtener un Orden de Registro y allanamiento. Si el equipo no es reconocido por los padres o encargados del menor se deberá consultar con un procurador de menores para obtener una orden de registro y allanamiento para que el equipo pueda ser registrado.

6. Para la toma de fotografías de los equipos electrónicos a ser incautados en una escena o lugar allanado se solicitará un Técnico de la División de Servicios de Servicios Técnicos del CIC.

7. Si la computadora, teléfono celular o equipo está apagado, lo dejará apagado. Si está encendido, no iniciará ninguna búsqueda a través de la computadora.

8. No accederá a ningún documento ni archivo de la computadora, teléfono celular o equipo.

9. Si es un servidor, no lo tocará, ni lo desconectará, ya que puede causar daños severos al sistema. Deberá consultar con un especialista o personal adiestrado para manejar los sistemas de redes. Para ello, deberá comunicarse con un supervisor de la DCC al (787)793-1234 ext. 2487, 2488.

10. Un Técnico de Fotografía o de la División de Servicios Técnicos tomará fotos del equipo y de la imagen en pantalla y área circundante antes de mover cualquier evidencia.

11. En el caso de teléfonos celulares o de equipos electrónicos móviles, se fotografiará la localización del equipo y su ubicación en la escena, así como las condiciones del mismo. Si fotografiara el teléfono en su parte frontal (pantalla) y la parte trasera.

12. Si la computadora está encendida y el monitor está en blanco o se fue a modo "screen saver", luego de tomarle foto, moverá el "mouse", o podrá oprimir la tecla de barra de espacio "spacebar". Esto activará el monitor y mostrará lo que tiene en pantalla, después que la imagen aparezca, volverá a fotografiar.

13. Si razonablemente cree que la computadora está borrando o destruyendo evidencia, desconectará inmediatamente la misma de la toma de corriente,

halando el cable principal de corriente de la torre. Si es una computadora tipo "laptop" en adición al cable de corriente, retirará la batería y en este caso no realizará el "shutdown". Las computadoras tipo "laptop" comúnmente tienen la batería en la parte de abajo. Usualmente un botón o un "switch" liberan la batería para que pueda ser retirada. No volverá a poner la batería en el compartimiento de la batería. **Si tiene batería interna** tendrá que apagarla presionando el botón de "power" por unos segundos hasta que apague el equipo.

14. En los demás casos, antes de desconectar cualquier cable de la computadora, haga el "shutdown" y realice un diagrama de los cables conectado e identificará los mismos con letras. Tomará fotos para luego identificar el orden de estos y los dispositivos conectados.

15. Identificará los cables con letras y/o números.

16. Se tomará fotografía del equipo "front & back", tal como están conectados los cables y los dispositivos a la computadora. Se fotografiarán todos los cables debidamente identificados, y se asegurarán de las letras puedan distinguirse en la fotografía.

17. Desconectará el "router" o "modem" de la toma de corriente "power".

18. Desconectará todos los cables y dispositivos conectados a la computadora.

19. Empacará todos los componentes, incluyendo "router" y "modem".

20. Transportará y almacenará con cuidado, como "carga frágil".

21. De igual forma, incautará medios de almacenamiento en la escena incluyendo, pero no limitándose a: "pendrive" o "thumb drives", "storage devices", tarjetas de cámaras, CD, DVD, BD, disco duro externo, y/o reproductores de MP3. Se incautará además los manuales de instrucciones, de estar disponibles.

22. Mantendrá los equipos retirados de magnetos, radios transmisores y otros dispositivos potencialmente dañinos. Se recomienda utilizar material antiestático y envoltura de burbuja rosada.

23. Si se trata de un teléfono celular, teléfono inteligente o un "PDA" (agenda electrónica), no lo apagará, esto podría habilitar algún "password" o clave que impida después acceder al equipo. Si está apagado, no lo prenderá.

24. Si está encendido, deberá ser fotografiado de manera que cubra lo que muestra en pantalla. Si está conectado a la computadora, rotulará y fotografiará todos los cables conectados al teléfono celular o PDA, y colectará

todos los cables, incluyendo el suplidor de corriente ("power supply" o cargador). Se aconseja que puede envolverlo en papel de aluminio cinco (5) capas para bloquear la señal o usar lata "arson pack", caja Faraday, bolsa Faraday, si esta desbloqueado ponerlo en modo "avión", siempre que el equipo lo permita, puede usar bolsas faraday para bloquear cualquier señal de comunicación, ya sea de la red de telefonía o de señal Wifi, Bluetooth, NFC.

25. Siempre que haya disponible en la escena un examinador o analista de evidencia digital, este podrá realizar una captura de la memoria volátil de la computadora (RAM) en las computadoras a incautarse que estén encendidas en la escena para preservar alguna data que se pierde al apagar la computadora. Para ello, el analista de evidencia digital o examinador utilizará aquellas herramientas recomendadas en NIST para el "Triage".

26. Cuando un MNPPR incaute un equipo electrónico, se llevará al cuarto de evidencia del CIC en un término no mayor de tres (3) días laborables, salvo justa causa, conforme a la Orden General Capítulo 600 Sección 612, titulada "Registros y Allanamientos". No se entenderá por justa causa para la dilación, la carga de trabajo.

27. En caso de que el equipo electrónico incautado objeto de evidencia esté averiado y sea necesario el cambio de alguna pieza para la obtención de la evidencia digital, el MNPPR tendrá que obtener una orden del Tribunal para poder obtener la evidencia y justificar el reemplazo, ya que siempre existe la posibilidad de que el equipo quede inservible. El dueño del equipo podrá proveer la pieza. No obstante, esto no supondrá ni garantizará la pieza y su funcionamiento, y en todos los casos no garantizará la obtención de la evidencia ni el funcionamiento del equipo. Esta disposición aplica también en los casos donde sea necesario realizar un JTAG a un equipo electrónico para poder extraer la evidencia.

D. En el caso que se ocupe el equipo móvil de Apple, el MNPPR deberá tomar las siguientes medidas:

1. Si el equipo móvil de Apple se incautó encendido, no lo apague, en la medida que sea posible mantendrá el equipo móvil de Apple con carga la batería y traerlo a la brevedad posible con la documentación correspondiente a la División de Crímenes Cibernético.

2. De no poder colocarlo en *modo avión,* insertar el mismo en una bolsa *Faraday*, de no contar que dichas bolsas envolver con cinco capas de papel aluminio.

3. Si va a utilizar una batería portable (power bank) para mantener con carga el equipo tome en cuenta que quepa en la bolsa Faraday con el equipo ocupado. Cualquier cable que sobre salga de la bolsa Faraday puede servir de antena y el equipo no estará aislado, lo cual pondría en riesgo la información contenida

en el equipo, como la posibilidad de que borren el equipo remotamente, borren mensajería de aplicaciones que sincronizan en la nube entre otras situaciones

4. De no contar con papel de aluminio ni bolsa Faraday, el agente procederá a remover la tarjeta SIM, asegurará la misma la cual deberá adherir a la parte posterior del equipo utilizando cinta adhesiva. Para retirar la tarjeta SIM de la bahía de SIM del teléfono podrá utilizar un "paper clip" metálico (sin revestimiento de goma) para presionar adentro del agujero donde se encuentra el pin expulsor como también podrá utilizar la herramienta "SIM Card Tray Ejector"

5. Recordar siempre que el MNPPR deberá consultar con la Fiscalía para obtener una Orden de Registro y Allanamiento o salvo que en casos de que el equipo sea de uso de una víctima menor de edad y los encargados del menor consientan a un registro del equipo electrónico se confeccionará la PPR 612.1 y 612.2 la que deberá firmar la persona que consienta para que el equipo sea llevado donde un examinador de evidencia digital de la División de Crímenes Cibernéticos o del Instituto de Ciencias Forenses o de alguna agencia federal, para que le realice un análisis forense al equipo.

6. En los casos de Homicidios donde el equipo móvil Apple está en posesión del occiso y/o fue incautado en la escena del asesinato no será necesario la orden para realizar el análisis, pero si la documentación de Inventario de Propiedad ocupada.

7. Todo caso que por consentimiento se autorice la examinación forense digital de un equipo electrónico; la persona que tiene autoridad para consentir deberá proveer y anotar en el formulario PPR 612.2 la contraseña de dicho equipo.

E. Procedimiento para Solicitar los Servicios de la División de Crímenes Cibernéticos (Crímenes en línea)

1. El agente del Distrito, Precinto o Unidad Especializada, investigará preliminarmente recopilando la información necesaria para consultar a la DCC y ultimar detalles sobre las circunstancias del caso en lo que respecta a la evidencia digital y solicitar preservación de la información según aplique.

2. No se referirán querellas ni querellantes directamente a la DCC.

3. En un término de quince (15) días laborables, el agente del Distrito, Precinto o Unidad Especializada obtendrá una cita en la DCC, para presentarse con la persona a la DCC con la parte querellante, con el número de querella y la información que haya suministrado la víctima en relación al caso. Si el agente investigador del caso está próximo a ausentarse por razón de disfrute de licencia regular o militar, por lo cual le imposibilite asistir a la DCC dentro del

mencionado término, deberá notificarlo a su supervisor inmediato para que éste evalúe y determine si tiene que asignar el caso a otro agente investigador. Los supervisores de cada Distrito, Precinto, o Unidad Especializada velarán por su estricto cumplimiento.

4. Una vez se presente a la DCC un MNPPR para solicitar servicio, proveerá el número de querella para que se abra un expediente de su caso.

5. Como norma general, en los casos de secuestro a menores de edad, seducción de menores a través de la Internet, venganza pornográfica, pornografía infantil, explotación sexual infantil, o trata humana, donde surja de la investigación preliminar que existe un nexo causal entre el delito investigado y el medio de comunicación telemática usado por la persona sospechosa, ya sea cuentas en redes sociales, correo electrónico o cualquier otro medio de comunicación telemática, el agente investigador se comunicará con la DCC lo más pronto posible, para obtener una cita.

6. En los casos que impliquen redes sociales, la parte querellante identificará las cuentas (Facebook, Twitter, Kik, WhatsApp, entre otros) involucradas en la comisión del delito. Para ello, es necesario que el agente le solicite a la parte querellante la dirección web de las cuentas implicadas. Dentro de la dirección web, se encuentra una cifra de números o combinación de números, letras y caracteres que identifican la cuenta en particular. Eso se le conoce como el identificador de la cuenta. Cuando se acceda la página principal del perfil a investigar, se copiará dicha dirección.

   Ejemplo #1:

   En las cuentas de Facebook el nombre de la cuenta puede ser cambiado a discreción del usuario, como también se pueden crear más de una cuenta con el mismo nombre. Es por ello, que siempre se requiere que se identifique de manera específica cuál es la cuenta utilizada en la comisión de delito. Los creadores de Facebook establecieron un identificador único para cada cuenta existente. Este ID puede ser tanto numérico como personalizado por el usuario, pero una vez se establece no puede ser alterado y siempre le pertenecerá a la misma cuenta. En el siguiente ejemplo se muestra el nombre de la página de Facebook de la DCC y el URL o dirección web donde se puede observar la porción de la dirección que representa el ID (identificador).

   Nombre de la cuenta:
   División de Crímenes Cibernéticos

   ID de la cuenta:
   ID de la cuenta - https://www.Facebook.com/crimenesciberneticospr

ID numérico de la cuenta-
https://www.Facebook.com/profile.php?id=105305989521746

ID de la cuenta usando browser versión móvil:
https://m.facebook.com/crimenesciberneticospr

Ejemplo #2:

En las cuentas de Twitter el usuario también puede cambiar el nombre de la cuenta, pero no así el identificador.

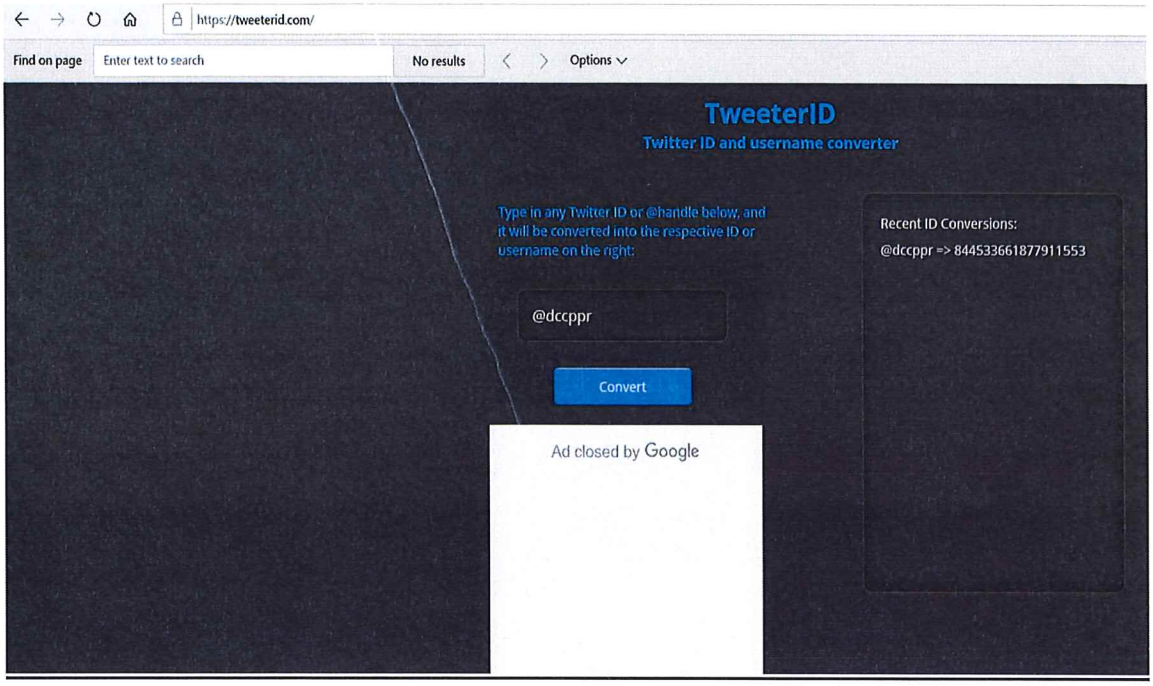
Nombre de la Cuenta:
DCC PPR

ID de cuenta en twitter: @dccppr
ID de cuenta en Twitter desde una sesión web en una computadora:
https://twitter.com/**dccppr**

Para obtener el identificador numérico de una cuenta de twitter
Deberá acceder a:

https://twitterid.com y en la casilla del identificador va a escribir el @twitter id que muestre la página bajo investigación:

Como ejemplo; la página de la DCC en Twitter tiene el @twitter id: @DCCPPR. Luego de colocar la información en el portal, el MNPPR marcará "convert" para convertir el ID a numérico como se muestra en la ilustración.
El ID numérico de la cuenta de twitter de la DCC:
@dccppr => 844533661877911553



7. Ante la gran cantidad de aplicaciones móviles existentes en el mercado, existen otros métodos o mecanismos de identificación y de validación de cuentas, por lo que se recalca a los agentes de Distrito, Precinto y/o Unidades Especializadas, que siempre se comuniquen con la DCC de existir alguna duda con la identificación de la cuenta.

8. Los agentes deberán instruir las víctimas para que no borren la evidencia que tengan sobre el incidente delictivo y la citarán para trabajar el caso en la DCC bajo el término dispuesto en el inciso (3) de esta Sección. Además, instruirán a las víctimas que no pongan sobreaviso al ciberdelincuente de que va a ser reportado a las autoridades.

F. Procedimiento para la Recopilación de Información de Actividades Delictivas Cibernéticas

La DCC evaluará toda información recibida sobre actividad delictiva en las redes sociales, foros, blogs, IRC Chats, App Messenger, páginas de anuncios clasificados, entre otros. Cuando, de la información recibida se identifique actividad sospechosa relacionada a pornografía infantil, trata humana o cualquier otra actividad delictiva, ya sea información recibida directamente de una persona o por cualquier otro medio, los agentes investigadores cibernéticos tomarán las siguientes medidas de acción:

1. El agente investigador cibernético asegurará la información mostrada en la página web, realizando una captura de pantalla marcando las teclas (Ctrl + PrtScn) en el teclado y luego importar dicha captura en un documento Word

(.doc). Podrá, además, utilizar la herramienta "snipping tool", snagit o Camtasia en la cual se realiza una captura de la imagen completa que cubra la dirección web (URL) que mostraba el navegador al momento de identificar el contenido. También puede utilizar la herramienta "Snagit" o "Camtasia" para realizar un "scroll down capture" o "record screen".

2. Además, se asegurará que se vea fecha y hora si es una conversación o mensaje. Luego guardará en formato JPEG o PDF e incluirá el "hash" para cada file, ya sea foto, audio, video, conversación, imagen, un "log" de sesión o algún código HTML.

3. Asignará un número de control y creará un archivo digital con la información. Notificará a la unidad o división correspondiente, para que un supervisor de la unidad especializada asigne a un agente para trabajar la investigación en conjunto al agente investigador cibernético. Será responsabilidad del agente investigador, ya sea de Precinto, Distrito o División Especializada, el curso general del caso. Si el caso es de jurisdicción federal, el agente investigador cibernético se comunicará con la agencia federal correspondiente, según sea el caso para notificarle sobre el status del caso.

4. Dicha notificación se realizará por los medios previamente acordados con la agencia federal.

5. Una vez se documente el caso, solicitará una preservación de datos a la compañía de servicios web o red social que ofrece tales servicios. (Stored Communication Act 18 US Code 2701-12).

6. Verificará el tipo de información que recopila la compañía a la cual se le pedirá la información, los términos y condiciones, y las políticas de privacidad de dicha compañía.

7. La solicitud de preservación de datos no deberá realizarse a un término de más de noventa (90) días de la ocurrencia de los hechos.

8. La DCC investigará y asesorará en lo referente a evidencia digital y las posibles leyes aplicables. No obstante, el agente investigador cibernético se pondrá en contacto con el fiscal o procurador enlace de la UICC del Departamento de Justicia para que asista en el caso, tanto en casos *subpoena* como en órdenes de registro correspondientes, según aplique.

9. Tramitará el *subpoena* y/o la orden de registro, recibirá, y analizará la información enviada por parte de la compañía de servicios de comunicación electrónica. Se le notificará al agente investigador que sometió la querella, una vez se culmine la investigación de la DCC o se requiera información adicional sobre el caso.

10. Una vez el agente investigador de Distrito, Precinto o División Especializada, sea notificado, será responsable de recoger los documentos y del curso general de la investigación.

11. El MNPPR adscrito a la División de Crímenes Cibernético citará de forma oficial al agente investigador. Para esto utilizará el formulario PPR-613.8 titulado: "Citación a la División de Crímenes Cibernéticos", el cual deberá ser tramitado por el correo electrónico oficial del agente con copia al supervisor del investigador.

IV. Disposiciones Generales

A. Interpretación

1. Las palabras y frases utilizadas en esta Orden General se interpretarán según el contexto y el significado sancionado por el uso común y corriente.

2. Los términos usados en esta Orden en el tiempo futuro incluyen también el presente; los usados en el género masculino incluyen el femenino y el neutro, salvo los casos en que tal interpretación resulte absurda; el número singular incluye el plural y el plural incluye el singular.

3. Si el lenguaje empleado es susceptible de dos o más interpretaciones, debe ser interpretado para adelantar los propósitos de esta Orden General y de la parte sección o inciso particular objeto de interpretación.

B. Cumplimiento

1. Todo agente o persona que visite la División, se registrará en el Registro de Visitantes (formulario PPR-204) bajo custodia del Retén. El Retén le indicará que dicha información es para fines estadísticos. Las comparecencias sólo se entregarán basadas en el Registro de Visitantes.

2. Será responsabilidad del agente del Distrito, Precinto o División Especializada, darle el seguimiento a la información solicitada, una vez se crea un expediente en la DCC.

3. Se prohíbe a todo MNPPR que, sin un fin legítimo, levante, mantenga, preserve, recopile información personal de individuos, organizaciones, agrupaciones, si dichos individuos, organizaciones y agrupaciones no están vinculadas con la comisión o intento de cometer un delito.

4. Todo MNPPR tendrá la obligación de cumplir con las disposiciones de esta Orden General y de informar a su supervisor inmediato o superior del sistema de rango, sobre cualquier violación a estas normas. Cualquier acto u omisión

que viole las disposiciones de esta Orden General será referido e investigado por la SARP a tenor con las normas aplicables.

5. Los supervisores asegurarán el cumplimiento de esta Orden General, así como de que el personal a su cargo sea debidamente adiestrado en la misma. Aquel MNPPR que incumpla con cualquier disposición de esta Orden General estará sujeto a medidas disciplinarias, posibles cargos criminales y/o acciones civiles, según corresponda.

C. Derogación

1. Esta Orden General deroga la Orden General Capítulo 600, Sección 613, titulada: "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos".

2. Esta Orden General deroga cualquier otra Orden, Normas, comunicación verbal o escrita o partes de las mismas que entren en conflictos con ésta.

D. Cláusula de Separabilidad

Si cualquier disposición de esta Orden General fuese declarada nula o inconstitucional por un Tribunal competente, tal declaración no afectará o invalidará las restantes disposiciones o partes de la misma, las cuales continuarán vigentes.

E. Aprobación

Aprobada hoy 17 de MARZO de 2022, en San Juan, Puerto Rico.

F. Vigencia

Esta Orden General entrará en vigor el día 25 de marzo de 2022.

Cnel. Antonio López Figueroa
Comisionado