



ORDEN GENERAL

Capítulo: 600	Sección: 613	Fecha de Efectividad: 25 de abril de 2018	Núm. Págs: 29
Título: División de Crímenes Cibernéticos			
Reglamentación que Deroga: Orden General Capítulo 600, Sección 613, titulada "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos" (29 de agosto de 2014)			

I. Propósito

Esta Orden General tiene el propósito de establecer la estructura organizacional y funcional de la División de Crímenes Cibernéticos (en adelante "DCC"), además de establecer los deberes, normas y procedimientos a seguir por todos los Miembros del Negociado de la Policía de Puerto Rico (en adelante "MNPPR") adscritos a ésta y detallar los servicios de apoyo y las herramientas tecnológicas para que todo MNPPR pueda identificar y realizar una búsqueda de información que permita identificar al sospechoso y agilizar las investigaciones criminales en curso. Se establecen además, las normas y procedimientos 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. **"Child Grooming":** Constituye una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de una persona menor de edad, creando una conexión emocional con la misma, con el fin de disminuir las inhibiciones del infante y poder abusar sexualmente de ella.
6. **Comunicación Telemática:** Aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada.
7. **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.
8. **Esteras Antiestática con Cable Disipador de Tierra ("grounding strap and electrostatic 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.
9. **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.

10. **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.
11. **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.
12. **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.
13. **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.
14. **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.
15. **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. División de Crímenes Cibernéticos

A. Organización

HER
La División de Crímenes Cibernéticos estará adscrita a la Superintendencia Auxiliar en Investigaciones Criminales (en adelante "SAIC"). Esta División ofrecerá sus servicios a las trece (13) Áreas Policiacas, a los Cuerpos de Investigaciones Criminales (tanto en el área investigativa criminal como administrativa), incluyendo, pero sin limitarse a la División de Homicidios, Propiedad y Fraudes, Delitos Sexuales, Robos, Inteligencia, Arrestos, Violencia Domestica, Vehículos Hurtados, Superintendencia Auxiliar en Responsabilidad Profesional (en adelante "SARP"), Policías Municipales, entre otras. Establecerá además coordinación y comunicación con Agencias Federales tales como el FBI, ICE, Servicio Secreto, entre otros.

La División estará representada en tres (3) Áreas Policiacas, pero su principal sede estará ubicada en el Cuartel General del Negociado de la Policía de Puerto Rico.

1. Área Policiaca de San Juan (Oficinas Centrales)
2. Área Policiaca de Mayagüez
3. Área Policiaca de Ponce

B. Deberes y Responsabilidades del Personal Adscrito a la División

El personal adscrito a la División tendrá, entre otros, las siguientes funciones y responsabilidades:

1. Orientar a los MNPPR, funcionarios del Departamento de Justicia, la Rama Judicial y al público en general, sobre el proceso para solicitar información y asistencia tecnológica en una investigación criminal, sea esta mediante teléfono o visita a dicha unidad de trabajo.
2. Documentar, redactar y reproducir los documentos necesarios para dar apoyo a cualquier investigación, y documentar cada solicitud de asistencia. Documentar los hallazgos obtenidos en el formulario PPR-613.5, titulado "Informe y Certificación de Evidencia Digital", y en el PPR-613.4, titulado "Informe Forenses de Equipos Móviles".
3. Cumplimentar el formulario PPR-613.1, titulado "Planilla Informativa de Investigaciones de Crímenes Cibernéticos".
4. Archivar cada expediente de caso para futuras referencias.
5. Asistir a charlas, seminarios, adiestramientos, academias locales mensuales, y seminarios vía web ("Webinars") que se le requieran para capacitarse y ampliar sus conocimientos, en aquellas áreas que estén relacionadas con sus funciones en dicha unidad de trabajo.
6. Investigar y dar seguimiento a los casos trabajados para su posterior notificación al Agente del Precinto, Distrito o División Especializada sobre los hallazgos.
7. Mantenerse informado sobre las comunicaciones, directrices o política pública emitidas por el Secretario y/o Comisionado.
8. Una vez la DCC haya culminado el análisis del equipo, lo entregará al Agente Investigador del caso mediante el formulario PPR-613.6, titulado "Recibo de Entrega de Evidencia de Crímenes Cibernéticos".
9. Tomar todos aquellos adiestramientos que le sean requeridos para pertenecer a ésta División, al igual que aquellos ofrecidos por agencias federales.

C. Director de la División

Será dirigida por un MNPPR con Rango no menor de Sargento que será designado por el Comisionado Auxiliar en Investigaciones Criminales con previa autorización del Comisionado. Este responderá administrativa y operacionalmente al Director de la Oficina de Asuntos Estratégicos de la SAIC y sus responsabilidades serán las siguientes:

1. Dirigir, planificar, organizar, administrar y coordinar todas las actividades propias de la DCC.
2. Informar al Comisionado Auxiliar en Investigaciones Criminales sobre toda investigación, modalidades delictivas y asuntos de interés público, dentro las funciones propias de la División.
3. Implementar, a tenor con las leyes y reglamentos vigentes, métodos adecuados de investigación dirigidos a prevenir y detener los delitos relacionados a crímenes cibernéticos.
4. Implementar programas de orientación a la ciudadanía, y colaborar con las agencias estatales y federales en la disseminación de información para la prevención de crímenes cibernéticos.
5. Coordinar los adiestramientos que sean necesarios para los MNPPR adscritos a la División.
6. Recopilar, clasificar, organizar y evaluar la información referente a los delitos reportados e investigados relacionados con los crímenes cibernéticos.
7. Coordinar con el Director del Negociado de Tecnología y Comunicaciones, todo lo relacionado al uso de la tecnología en su División.
8. Se asegurará de que todo personal adscrito en su División tenga todos los adiestramientos requeridos para pertenecer en la misma, y todos aquellos otros requeridos por las autoridades federales.

D. Supervisor

Cada División tendrá un supervisor, quien será un MNPPR con rango no menor de Sargento, el cual será designado por el Comisionado Auxiliar en Investigaciones Criminales. Tendrán los siguientes deberes y responsabilidades:

1. La sede central de la División contará con un supervisor que fungirá como interino en ausencia del Director. Las demás divisiones contarán con un supervisor quien supervisará las operaciones en sus respectivas dependencias.
2. Coordinar y evaluar la labor de las secciones que integran la División, identificando y atendiendo los aspectos administrativos y operacionales.
3. Supervisar y coordinar la labor administrativa que se realice en las secciones.
4. Ejercer supervisión directa sobre los procesos de evaluación e inspección de las secciones investigativas y del personal del sistema de rango, a través del monitoreo continuo de la productividad de los mismos.
5. Se asegurará del buen uso y mantenimiento de los vehículos y equipo asignado a las secciones de la División.
6. Tendrá la obligación continua de informar al Director sobre la actividad delictiva relacionada con las investigaciones en curso y las estadísticas diarias del crimen.
7. Mantendrá un registro de todos los adiestramientos y/o readiestramientos del personal asignado a la División y llevará un registro, desglosado por materia de enseñanza.
8. Coordinará, a través del Coordinador de Adiestramientos de la SAIC, el adiestramiento o readiestramiento de los MNPPR asignados a División.
9. Se asegurará de que los MNPPR de las Divisiones cumplan con los adiestramientos y readiestramientos requeridos por la Superintendencia Auxiliar en Educación y Adiestramiento, o cualquier otro que mediante acuerdo que sea autorizado con otra agencia estatal o federal.
10. Rendirá un informe mensual al Coordinador de la SAIC, a través de la cadena mando, que contendrá como mínimo:
 - a. Cantidad de MNPPR que asistieron a adiestramientos y/o readiestramientos, según aplique.
 - b. Cantidad de MNPPR que no comparecieron a adiestramientos y/o readiestramientos, según aplique, y las razones para no hacerlo.
11. Llevará un registro de las conferencias realizadas por cada Sección adscrita y documentará las mismas en el formulario "Informe Mensual de Conferencia".

12. Coordinará todas las solicitudes de conferencias y solicitará mediante requisición equipos como proyectores, computadoras y/o cualquier otro equipo necesario para que los instructores impartan sus charlas y/o conferencias.
13. Realizará cualquier otra función que le sea encomendada por el Director.

E. MNPPR designado en el Retén

Tendrá los siguientes deberes y responsabilidades:

1. Atenderá las llamadas telefónicas de conformidad a lo establecido en el protocolo titulado "Protocolo de la Agencia para Responder las Llamadas Telefónicas", del 16 de septiembre de 2010.
2. Anotará toda información confidencial que se reciba en el formulario PPR-785, titulado "Hoja de Recibo de Confidencias", conforme a la Orden Especial 2003-35, titulada "Normas y Procedimientos para el Recibo y Disseminación de Llamadas Confidenciales". Dicho formulario será tramitado inmediatamente al supervisor.
3. Cumplimentará el formulario PPR-887, titulado "Registro Visitantes Personas con Impedimentos", conforme a la comunicación OS-1-10-15-mm.
4. No permitirá tertulias en el área de retén.
5. Estará debidamente ataviado en vestimenta, identificación visible en todo momento, de conformidad con la Orden General 2010-11, titulada "Normas y Procedimientos para la Expedición y Uso de Tarjetas de Identificación para Empleados de la Policía de Puerto Rico".
6. Tendrá todo el equipo reglamentario entregado por el NPPR.
7. Recibir las quejas de las personas contra cualquier MNPPR o empleado de la Agencia, y/o reconocimientos por la labor de éstos, y seguirá el procedimiento establecido en la Orden Administrativa 2015-2, titulada "Programa de Información Pública sobre Querellas y Reconocimientos".
8. No permitirá ni autorizará a ningún MNPPR o agente perteneciente a otra agencia, a verificar, examinar, fotocopiar o copiar información de documentos o libros de control, sin antes estar debidamente autorizado por el Comisionado,

Comisionado Auxiliar de la SAIC, o por el Director.

9. No realizará ni permitirá que se realicen llamadas de larga distancia o llamadas a servicios prestados por compañías telefónicas, tales como 4-1-1, 5-1-1 o cualquier otro, excepto que las mismas sean de carácter oficial.
10. Notificará inmediatamente al supervisor cuando un MNPPR se reporte por licencia de enfermedad mediante llamada telefónica.
11. No brindará datos personales por teléfono a ninguna persona, excepto al Supervisor o Director de la División.
12. Mantendrá un inventario perpetuo de la propiedad que hay en su área de trabajo y lo documentará en el formulario PPR-952, titulado "Inventario Área de Retén", el cual incluye:
 - a. casilleros de depósito de evidencia;
 - b. sobres de evidencia;
 - c. radios portátiles;
 - d. llaves de vehículos oficiales;
 - e. libros de registros; y
 - f. cualquier otro artículo que le sea asignado para su custodia.
13. Custodiará y certificará el Libro de Entrada y Salida, de conformidad con la Orden General 80-11, titulada "Normas y Procedimiento para el Uso y Conservación del Libro de Entrada y Salida de los Miembros de la PPR".
14. Registrará la información para asignar la querrela, ya sea de manera electrónica o física (libro de querrela o, de estar disponible, Registro Electrónico de Querellas de Crímenes Cibernéticos (JOB)).
15. No abandonará su área de trabajo sin la autorización del supervisor inmediato. Además, será el custodio y encargado de toda la propiedad y evidencia depositada o asignada a su área de trabajo.
16. Verificará que los Agentes Investigadores Cibernéticos de todas las secciones de la DCC completen las novedades.
17. Cuando surjan novedades que involucren a un Agente Investigador de la DCC, notificará inmediatamente al supervisor y al Director de la División.

F. Coordinador de la Propiedad

1. Será un MNPPR designado por el Director de la División.
2. Cumplirá con las responsabilidades establecidas en la Orden General Capítulo 600, Sección 637, titulada "Centro de Bienes Advenidos" y la Orden General 2008-4, titulada "Reorganización de los Procedimientos Fiscales para el Control y Contabilidad de la Propiedad Publica en Uso por la Agencia".
3. Realizará cualquier otra función que le encomiende el Director de la División.

G. Encargado del Sistema de Asistencia y su Alterno

1. Serán MNPPR o personal del sistema clasificado designados por el Director de la División.
2. Tendrán las responsabilidades establecidas en la Orden General Capítulo 200, Sección 203, titulada "Normas y Procedimientos para el Registro de Horas Trabajadas, Disfrutadas, Disfrute y Pago de Horas Extras Trabajadas".
3. Realizarán cualquier otra función que le designe el Director de la División.

H. Encargado de Estadísticas/Informes Mensuales

1. Será un empleado del NPPR designado por el Director de la División.
2. Preparará los datos estadísticos que se generen en la División, así como los informes semanales, quincenales y mensuales, incluyendo, pero sin limitarse a cada orden de registro y allanamiento, al expediente del caso donde se mantenga copia de la misma, al MNPPR que solicitó la orden y a cada supervisor que revisa la solicitud de la orden. La División de Inspección de la SARP realizará inspecciones sin previo aviso para velar por el cumplimiento de las órdenes promulgadas por la Agencia.
3. Realizará cualquier otra función que le sea encomendada por el Director de la División.

I. Sección de Requerimientos Legales "Legal Request"

En esta Sección, el personal asignado orienta y asiste sobre los procedimientos

establecidos que dispone esta Orden General, el curso de acción del NPPR para atender casos de Crímenes Cibernéticos y los servicios que ofrece la División. Tendrá los siguientes deberes y responsabilidades:

1. Ofrecerá orientación a los agentes investigadores y público general sobre el procedimiento a seguir para solicitar los servicios de la División de Crímenes Cibernéticos. Además, ofrecerá asistencia en la investigación de cualquier otro delito en donde en alguna parte de la investigación se descubre que el sospechoso utilizó algún medio cibernético.
 - i. Ejemplo: Amenazar, para atraer a su víctima comunicándose por correo electrónico, aplicación móvil, vía red social u otro sitio en la Internet.
2. Realizará análisis de mensajes de correos electrónicos implicados en la comisión de delitos; y analizará direcciones web (URL) dominios, "websites", o cualquier medio de emisión y difusión de información en Internet como "blogs", "fóruns", "webcast", "podcast", "RSS", redes sociales, entre otros.

Nota: Cada caso será analizado teniendo como base la legislación vigente relacionada al uso de la tecnología y la comunicación electrónica para la comisión de los crímenes cibernéticos.
3. Recopilará, preservará y analizará toda evidencia suministrada que provenga de algún medio social o servicio en línea como correo electrónico, sitio web o cualquier cuenta o servicio de alguna compañía proveedora de servicio de comunicación electrónica, a través del cual se haya identificado la comisión de un delito.
4. Orientará y asistirá a diferentes agentes y funcionarios de ley y orden en el desarrollo de requerimientos de *subpoenas* u órdenes de registro ("search warrant") para la obtención de información digital de diferentes compañías de servicios de comunicación electrónica.
5. Cuando se detecte la comisión de un delito en la Internet es necesario que se solicite la preservación y/o retención de datos de evidencia reservada o mantenida en posesión de cualquier proveedor de servicios de comunicación electrónica (Stored Communication Act 2703f:1,2) por noventa (90) días, pudiendo solicitar una extensión de hasta noventa (90) días adicionales, según sea solicitado por la entidad gubernamental conforme a lo dispuesto en la ley federal (SCA 2703F2).

6. Toda información basada en contenido, entiéndase mensajes privados, imágenes, información de ubicación, que se desee obtener de cualquier compañía de servicios de comunicación electrónica como parte de un proceso de investigación de delito, será solicitada a través de una orden de registro o "search warrant". En la misma, se debe establecer una relación o nexo causal entre el delito investigado y la información solicitada, estableciendo así una causa probable que deberá aparecer en la Orden. Para ello, el agente investigador del caso consultará el caso con un fiscal o procurador enlace de la Unidad Investigativa de Crímenes Cibernéticos (en adelante "UICC") del Departamento de Justicia.
7. La Sección de Legal Request confeccionará el documento siguiendo las recomendaciones del fiscal o procurador enlace de la UICC del Departamento de Justicia. Para obtener la información actualizada de contacto de cualquier fiscal y/o procurador enlace de la UICC de cualquier distrito judicial, podrá comunicarse con la Sección de Legal Request de la DCC.
8. El agente investigador deberá traer copia de las declaraciones juradas para que se le prepare el documento de Orden de Registro. Cuando el agente investigador obtenga una Orden de Registro la traerá a la Sección de Legal Request de la DCC para que sea tramitada con la compañía proveedora de servicios de comunicación electrónica. Una vez se obtenga la respuesta con la información, se valida, se preserva, se analiza y reporta, garantizando siempre la cadena de custodia, la confidencialidad y el debido proceso de ley de las personas. Luego se le entregará al agente investigador, quien seguirá el curso general de la investigación.
9. Toda solicitud de información básica de registro, no basada en contenido, será solicitada a través de un *subpoena*. Para ello, el agente investigador primero consultará el caso con un agente de la Sección de Legal Request de la DCC, quien le proveerá la orientación adecuada y la información de contacto del fiscal o procurador enlace de la UICC del Departamento de Justicia. El agente cibernético de la Sección de Legal Request preparará el *subpoena* siguiendo las recomendaciones del fiscal o procurador enlace de la UICC del Departamento de Justicia.
10. Con un *subpoena* del fiscal, el proveedor de servicios de comunicación electrónica o de servicios informáticos remotos revelará a la entidad gubernamental solicitante lo siguiente:

- a. Nombre.
- b. Dirección.
- c. Registros de conexión telefónica y duración de llamada para un número telefónico específico.
- d. Duración del servicio (incluida la fecha de inicio) y tipos de servicios utilizados.
- e. Número de teléfono o de instrumento, u otro número o identidad de abonado, incluyendo cualquier dirección de red temporalmente asignada (dirección de IP, o dirección de correo electrónico).
- f. Medios y/o fuente de pago para dicho servicio (incluyendo cualquier tarjeta de crédito o número de cuenta bancaria) de un abonado o cliente de tal servicio.
- g. La ley federal establece que aunque la entidad gubernamental que recibe la información solicitada mediante *subpoena*, no está obligada a proporcionar aviso a un suscriptor o cliente. Dicho esto, internamente las compañías proveedoras de comunicación electrónica podrían notificar a su cliente sobre la petición de información de registro. En circunstancias exigentes, donde el agente investigador entienda que el sospechoso podría destruir evidencia si entra en conocimiento de la solicitud de información, solicitará la información mediante orden del Tribunal y notificará al agente de la Sección de Legal Request de DCC para que solicite una preservación de datos a la compañía proveedora de comunicación electrónica.

11. Una vez recibida la información por parte de la compañía de servicios de comunicación electrónica, la misma será analizada con el fin de determinar la persona que utilizó el medio de comunicación electrónica para la comisión del delito. Luego de esto, se le notificará al agente investigador para que recoja la información y continúe la investigación.

J. Sección de Crímenes en Línea

La Sección de Crímenes en Línea tendrá los siguientes deberes y responsabilidades:

1. Dará apoyo en las investigaciones de menores desaparecidos, a través de un acuerdo interno con el Coordinador de Personas Desaparecidas de la SAIC.
2. Recibirá información y dará seguimiento a todo aquello que represente un delito cometido, o próximo a cometerse, dentro de las principales redes sociales, así como también chats y aplicaciones móviles, con el propósito de

ayudar en la investigación de crímenes contra menores, explotación sexual infantil, pornografía infantil y seducción de menores a través de la Internet.

3. En los casos de seducción de menores a través de la Internet, se utilizará el formulario PPR-936, titulado "Consentimiento para Asumir Identidad de Cuentas de Internet", con el fin de obtener consentimiento de los padres y/o encargados del menor para entrar a la cuenta de la red social del menor de edad donde se ha recibido evidencia, ya sea mensajes de texto, conversaciones de aplicaciones de chats o fotos que indiquen el acercamiento de naturaleza sexual o "child grooming" por parte de una persona adulta.
4. En casos de pornografía infantil y/o seducción de menores a través de la Internet, una vez se valida la información y se identifica al sospechoso, se notifica el caso a ICE-HSI para coordinar la detención del mismo.
5. La notificación se hará mediante llamada telefónica interna a la persona encargada de la División de Explotación Sexual Infantil de ICE-HSI.
6. Proveerá al Comisionado o al Comisionado Auxiliar de la SAIC cualquier información sobre la comisión de un crimen que haya ocurrido o que exista una alta probabilidad de que vaya a ocurrir.

K. Sección de Evidencia Digital

La evidencia digital es cualquier información en forma digital que pueda establecer una relación entre un delito y su autor. La labor que se realiza en esta Sección es materia de cómputo forense, ya que la evidencia que se extrae es prueba científica en un foro judicial. Esta Sección tendrá los siguientes deberes y responsabilidades:

1. Estará a cargo de la extracción de la evidencia digital en diferentes dispositivos electrónicos, así como la recuperación y análisis de la información que ha sido eliminada de los mismos.
2. Se documentará el equipo a ser analizado utilizando el formulario PPR-613.1, y el PPR-613.3, titulado "Plantilla para Fotografía Forense". El formulario PPR-613.3 también se podrá utilizar cuando se solicite foto del equipo analizado.
3. Custodiará la información que se considere evidencia digital y la entregará al agente investigador que esté a cargo de la investigación.

4. Analizará y evaluará nuevas tecnologías, tanto de software como de hardware, que pudieran estar siendo utilizadas para la comisión de delitos.
5. Los servicios de esta Sección serán solicitados por el MNPPR investigador del caso mediante el formulario PPR-613.2, titulado "Solicitud de Examen Digital".

a. Analista de Evidencia Digital o Examinador

- i. Utilizará el equipo asignado por el NPPR o aquél otro suministrado por una agencia federal o estatal a través de un memorando de entendimiento o acuerdo colaborativo, para lo cual fue debidamente adiestrado.
- ii. Todo proceso de extracción de evidencia digital y de cómputo forense que se lleve a cabo, será realizado conforme a las prácticas generalmente aceptadas y conforme a los estándares y guías establecidas por la National Institute of Standards and Technology (en adelante "NIST"), NIST 800 o el más reciente, y los Manuales (SOP) que se promulguen a esos fines.
- iii. Utilizará sólo programas y herramientas de versión comercial completa y aquellas registradas en el portal del NIST.
- iv. Será responsable del mantenimiento adecuado del equipo asignado. Esto incluye instalar las actualizaciones que requiera el equipo o sus programas, sistema operativo, como también será responsable del mantenimiento físico del equipo, conservándolo y haciendo buen uso del mismo, manteniéndolo limpio, libre de polvo y humedad.
- v. Será responsable del equipo asignado y de cada uno de sus componentes, el cual se mantendrá en su área de trabajo, salvo circunstancias excepcionales que ameriten utilizar aquellos equipos que sean portátiles fuera de la oficina, previa autorización del Director.
- vi. No modificará ni alterará el funcionamiento del equipo asignado.
- vii. Informará cualquier defecto o mal funcionamiento del equipo al supervisor inmediato.

- viii. Ningún MNPPR adscrito a la DCC está autorizado a realizar reparaciones al equipo asignado, ya que si el equipo tiene alguna garantía podría invalidarla. Las reparaciones livianas o "troubleshooting" se podrán realizar, previa consulta con el Director de la DCC.
- ix. Cuando un MNPPR incaute un equipo electrónico, se llevará a la DCC en un **término tres (3) días**, conforme a la Orden General Capítulo 600 Sección 612, titulada "Autoridad de la Policía de Puerto Rico para Llevar a Cabo Registros y Allanamientos".
- x. 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.
- xi. Trabajará de forma organizada y tomará las medidas de protección personal utilizando equipo como: guantes, gafas y cualquier otro equipo de protección que sea necesario y provisto por la División de Prevención de Accidentes. No colocará bebidas ni recipientes abiertos con líquido en las mesas de trabajo ni sobre los equipos.
- xii. Utilizará una estera antiestática con cable disipador de tierra y "*grounding strap and electrostatic mat*" cuando maneje cualquier equipo de computadora, equipos electrónicos o piezas internas de computadoras como el "motherboard", circuitos, procesador o tarjetas de memoria, ya que estos son susceptibles a electricidad estática que produce el cuerpo y la data contenida en ellos pudiera perderse o dañarse si surge una descarga.
- xiii. Para crear cualquier tipo de imagen forense de cualquier medio, *siempre se utilizará el equipo adecuado para proteger de escritura "write blocker"* el dispositivo fuente. Entre los equipos adquiridos por

la DCC se encuentra el "Tableau 3D y 4D", los cuales están integrados al Forensic Recovery of Evidence Device (FRED SR). También se podrán utilizar el "Forensic Bridge", "Ultrakit" y "TD2". Esto garantizará que la imagen se capturó bit por bit y que no sea alterada o rescrita.

- xiv. Siempre que el Analista de Evidencia Digital o Examinador vaya a utilizar un dispositivo de almacenamiento para colocar evidencia en el mismo, primero deberá realizar un "wipe" o escritura con cero al dispositivo, para garantizar que no haya ningún tipo de datos que alteren la información que será grabada en el mismo.
- xv. Toda imagen y reporte creado de un equipo móvil utilizando el "UFED4PC" o el "UFED Touch Ultimate" de Cellebrite, será colocado en el RAID del Forensic Recovery of Evidence Device (FRED SR), luego de ser analizado. En el caso de una imagen de una computadora(s) también se depositará en el RAID de la FRED o en el RAID de la Talino Forensic Workstation, desde donde será analizada con las herramientas que haya adquirido el NPPR para dichos fines.
- xvi. Mantendrá un expediente digital con los formularios digitales usados para el desarrollo de reportes y documentación pertinente sobre los dispositivos examinados y aquellos reportes generados usando herramientas como el UFED Logical y Physical Analyzer, Encase, Forensic Explorer, Internet Evidence Finder, PALADIN de Sumuri, entre otros, recomendados por NIST. Los expedientes se clasificarán por nombre del analista o examinador y número de querrela.

L. Encargado de los Casilleros Provisionales de Depósito de Evidencia

Los casilleros provisionales de evidencia, se utilizan con el fin de mantener una cadena de custodia de la evidencia que permita su admisibilidad en los foros judiciales y/o administrativos, así como la protección de la misma. Cumplirá con las siguientes disposiciones, conforme a la Orden General Capítulo 600, Sección 636, titulada "Normas y Procedimientos para el Recibo, Custodia, Entrega y Disposición de Propiedad que Forma Parte de Evidencia".

1. Como garantías mínimas de seguridad, se utilizará la Hoja de Control para registrar la entrada y salida de la evidencia por parte del supervisor de turno y el depositante.
2. El encargado será un MNPPR designado por escrito por el Director de la DCC y tendrá los siguientes deberes y responsabilidades:
 - a. Asegurará que la propiedad almacenada en estos casilleros sea exclusivamente propiedad considerada evidencia digital, por estar envuelta en la comisión de delito o falta.
 - b. Mantendrá un registro por cada evidencia depositada, el cual contendrá los siguientes documentos:
 - i. PPR-240 "Registro de Evidencia".
 - ii. PPR-126 "Inventario de Propiedad Ocupada".
 - iii. PPR-879 "Consentimiento".
 - iv. *Subpoena* y/u orden de allanamiento.
3. A los fines de mantener la cadena de evidencia, el encargado del casillero de evidencia exigirá que le firmen el recibo, formulario PPR-240, cada vez que la evidencia salga del casillero provisional de evidencia.
4. Solicitará mediante requisición SC-1001, titulada "Requisición de Materiales, Equipo y Servicios", a la División de Compras de la Superintendencia Auxiliar en Servicios Gerenciales (SASG), las envolturas especializadas y materiales adecuados. Además, solicitará guantes y aquel equipo de protección que sea necesario a la División de Prevención de Accidentes.
5. Cada casillero tendrá dos (2) llaves, la que posee el agente investigador cibernético de la Sección de Evidencia Digital y la que posee el Encargado de Casilleros.
6. Tomará posesión del casillero cuando se pierda una llave o candado, asegurando que nadie tenga acceso al mismo, hasta que se asigne un nuevo candado.

M. Asignación de Casilleros Provisionales de Evidencia

1. Todo casillero provisional de evidencia, se entregará mediante recibo y con las disposiciones generales, antes señaladas.
2. Cada casillero provisional de evidencia contará con un candado enumerado y con llave asignada.
3. El encargado de custodia certificará que las llaves asignadas se encuentren completas.
4. Los casilleros estarán sujetos a inspección con o sin aviso previo.
5. En caso de pérdida de llave o candado, el poseedor redactará un informe en donde indique dicha pérdida. El poseedor de la llave o candado extraviado será responsable de costear para la adquisición de un candado nuevo. Inmediatamente, el encargado de los casilleros hará un inventario del contenido del casillero a la hora de la pérdida. Inmediatamente tomará posesión del casillero hasta tanto se cambie el candado.
6. El candado se reemplazará, aunque éste no se haya extraviado, si faltara una de las llaves. Dicho reemplazo se realizará antes de que el agente investigador cibernético al que se le asignó dicho casillero termine su turno de trabajo.
7. No se sacará copia de llave alguna.
8. En las siguientes circunstancias se inspeccionará el casillero en ausencia del agente asignado:
 - a. Si luego de ser citado, se negara a comparecer.
 - b. Si se encontrase disfrutando de licencia regular.
 - c. Si fue trasladado.
 - d. Si fuese suspendido administrativamente.
 - e. Si es expulsado.
 - f. Si se encuentra en licencia militar.
 - g. Si se ausenta prolongadamente por razones de salud o muerte.
9. Cada vez que se asigne un casillero provisional de evidencia a un agente investigador cibernético, se le asignará un candado nuevo.

N. Proceso a Llevarse a Cabo para el Inventario en Ausencia del Agente Investigador

1. Al agente investigador se le citará para la entrega de la propiedad. Si el agente investigador no comparece para la entrega, se levantará un acta donde estará presente el Director de la División, un supervisor o el personal que el Director designe (Encargado de Custodia), quien fungirá como testigo.
2. En dicha acta se hará constar lo siguiente:
 - a. Nombre y placa de los MNPPR presentes en ese momento.
 - b. Nombre y placa del agente investigador a quien corresponde el casillero.
 - c. Si es posible las razones por las cuales el agente investigador no compareció para abrir el casillero.
 - d. Se tomará fotografía a la hora de abrirse el casillero.
 - e. Se hará un inventario o lista de todo lo que haya dentro del casillero.
 - f. De encontrarse alguna propiedad de índole ilegal, se procederá a notificarse inmediatamente a la SAIC y a la SARP.

**O. Procedimiento para Solicitar los Servicios de la División de Crímenes Cibernéticos**

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.
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 se personará 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, 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 presentará a la DCC lo más pronto posible.
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:

[https://www.facebook.com/profile.php?id=crimenesciberneticospr](https://www.facebook.com/profile.php?id=<u>crimenesciberneticospr</u>)

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>

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.

P. 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" 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 querrela, 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.

Q. 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. 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.
2. El MNPPR asegurará tener un documento judicial (orden de registro o allanamiento) o consentimiento escrito oficial y debidamente firmado, para incautar la computadora o equipo electrónico.
3. En las circunstancias excepcionales en que se ocupe un equipo electrónico sin orden judicial o consentimiento firmado, 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". Se obtendrá una orden judicial antes de realizar una búsqueda en el equipo.

4. No accederá a ningún documento ni archivo de la computadora o equipo.
5. Si la computadora o equipo está apagada, la dejará apagada. Si está encendida, no iniciará ninguna búsqueda a través de la computadora.
6. 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.
7. Un Técnico de Fotografía o de la División de Servicios Técnicos tomará fotos del área circundante antes de mover cualquier evidencia.
8. 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. 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. Si tiene batería interna tendrá que apagarla presionando el botón de "power" hasta que apague el equipo.
9. Desconectará el "router" o "modem" de la toma de corriente "power".
10. Si la computadora está apagada, tomará fotografía del equipo "front & back", tal como están conectados los cables y los dispositivos a la computadora.
11. Si la computadora está encendida, además, se tomará foto del monitor de forma que cubra todo lo que se muestra en él.
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. Antes de desconectar cualquier cable de la computadora, hará un diagrama e identificará los mismos con letras. Tomará fotos para luego identificar el orden de los mismos y los dispositivos conectados.

14. Luego de retratar, hará "shut down" al equipo y desconectará el cable de corriente de la parte de atrás de la torre. Si es una computadora tipo "laptop" y está conectada a la toma de corriente, desconectará el cable de corriente y retirará la batería. No volverá a poner la batería en el compartimiento de la batería.
15. Desconectará todos los cables y dispositivos conectados a la computadora.
16. Empacará todos los componentes, incluyendo "router" y "modem".
17. Transportará y almacenará con cuidado, como "carga frágil".
18. 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.
19. Mantendrá los equipos retirados de magnetos, radios transmisores y otros dispositivos potencialmente dañinos. Se recomienda utilizar material antiestático y envoltura de burbuja rosada.
20. 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.**
21. Si esta 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 coleccionará todos los cables, incluyendo el suplidor de corriente ("power supply" o cargador). Se aconseja que puede envolverlo en papel de aluminio 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 o Bluetooth.
22. 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.

R. Controles Administrativos

1. La DCC redactará mensualmente un informe sobre la información estadística recopilada. En éste, se detallará la cantidad de servicios prestados a las investigaciones, tipos de orientaciones e información reportada sobre crimen cibernético y aquellos delitos establecidos en el Código Penal de Puerto Rico que contemplan la comunicación telemática o Internet.
2. 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.
3. Las comparecencias sólo se entregarán basadas en el Registro de Visitantes.
4. Asimismo, cada vez que un MNPPR o una persona se comunique por cualquiera de las extensiones de la DCC, el MNPPR que atienda la llamada, completará una hoja de Solicitud de Asistencia. En la misma anotará el nombre, fecha, lugar de origen de la querrela (pueblo), número de teléfono del MNPPR o parte querellante. Además, detallará de forma resumida los hechos y el curso de acción. Entrará la información al registro electrónico con detalles del servicio solicitado y un breve resumen del caso.
5. Cada vez que sea revisado un caso, el agente investigador cibernético suplementará la actividad en el registro electrónico y hará la anotación en el expediente.
6. Cada expediente será archivado por nombre del agente investigador cibernético del caso y número de querrela. El agente que solicita asistencia será responsable de darle seguimiento y proveer toda información solicitada.
7. Cada agente investigador cibernético será responsable de sus expedientes y de la información que se solicite.
8. Si cualquier agente investigador cibernético fuese trasladado a otra unidad del NPPR, estuviese reportado por cualquier tipo de licencias que excediera los quince (15) días, renunciare a su puesto o fuese destituido del mismo, realizará una transición de los casos con toda información pendiente de recibir, si alguna, al Director de la DCC. De no cumplir con tal disposición, pudiera ser objeto de una investigación administrativa realizada por la SARP, así como a la imposición de medidas disciplinarias.
9. Toda solicitud de charlas, conferencias o actividades, serán dirigidas al Comisionado Auxiliar de la SAIC. Las solicitudes se realizarán con no menos de treinta (30) días laborables de antelación a la fecha en que se desea el servicio.

La misma se ofrecerá de acuerdo a la disponibilidad de los recursos humanos, sin que se afecten los servicios en la unidad de trabajo, y cumpliendo con los requerimientos del "Acuerdo para la Reforma Sostenible de la Policía de Puerto Rico".

10. 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.
11. La DCC tramitará el envío de *subpoenas* y órdenes de registro dirigidas a entidades, corporaciones, compañías de comunicación electrónica, ISP, entre otras, que proveen servicios web incluyendo, pero sin limitarse a servicios de correo electrónico, servicios virtuales, "cloud services", "domain hosting", redes sociales, servicios de comunicación VOIP, entre otros.
12. Aquellos *subpoenas* u órdenes del Tribunal que vayan dirigidas hacia alguna entidad o corporación fuera de Puerto Rico, una vez el fiscal provea la misma, el agente investigador cibernético realizará las gestiones a través de División de Administración de Documentos, su envío mediante correo certificado con acuse de recibo, o a través de cualquier otro medio que disponga la compañía a la cual se le va a solicitar dicha información.
13. Todo equipo "hardware" y "software" asignados a la DCC, ya sea adquirido con fondos estatales o federales, será operado sólo por el personal adiestrado de la DCC y será para el uso oficial de esta División y además, permanecerán en las facilidades de la DCC. En el caso de los programas que se adquieran, sólo serán instalados y operados en los equipos asignados a la DCC.

S. Designación del Personal y Equipo

1. Previa autorización del Comisionado Auxiliar en Investigaciones Criminales, se asignará el equipo, materiales y vehículos necesarios para las operaciones de la División y se adiestrará al personal para realizar de manera eficiente las tareas que se le designen.
2. Todo MNPPR que solicite traslado para la División, cumplirá con las normas establecidas en la Orden General Capítulo 300, Sección 305, titulada "Normas y Procedimientos para las Transacciones de Traslados del Personal del Sistema de Rango"
3. El MNPPR no podrá tener querellas administrativas pendientes de adjudicación, o que hayan sido sostenidas en los últimos cinco (5) años por las siguientes causales:
 - a. Uso de fuerza.

- b. Arrestos o detenciones ilegales o irrazonables.
 - c. Registros, allanamientos e incautaciones ilegales o irrazonables.
 - d. Acometimiento y/o agresiones injustificadas o excesivas.
 - e. Uso de violencia injustificada, coacción física o psicológica contra un arrestado.
 - f. Conducta inmoral.
 - g. Agresión física.
 - h. Maltrato verbal.
 - i. Uso indebido de sustancias controladas.
 - j. Violencia doméstica.
 - k. Violación de derechos civiles.
 - l. Hostigamiento sexual.
4. Mínimo de cinco (5) años de experiencia como MNPPR.
 5. Someterse a una investigación de campo y pasar favorablemente la misma.
 6. Someterse a evaluaciones psicológicas y pasar favorablemente las mismas, según la reglamentación vigente de la Agencia.
 7. Conocimiento y Manejo de Sistemas Operativos.
 8. Manejo de Sistemas Operativos de equipos móviles: Android, iOS y Windows Phone.
 9. Conocimiento en programas de MS Office.
 10. Grado técnico o bachillerato en Sistemas de Información, Ciencias en Computadoras, o Justicia Criminal, con concentración en Crímenes Cibernéticos o cualquier otro relacionado.
 11. Cualquier otro requisito que mediante convocatoria el Comisionado establezca.

IV. Jurisdicción

La jurisdicción operacional de la DCC será el espacio terrestre, marítimo y aéreo que comprende el Gobierno de Puerto Rico, según lo dispuesto en nuestro ordenamiento jurídico.

V. 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. 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.
2. 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.
3. El traslado de personal será de conformidad con la Orden General Capítulo 300, Sección 305, titulada "Normas y Procedimientos para las Transacciones de Traslados del Personal de Sistema de Rango".
4. Mantendrán un ambiente de trabajo libre de hostigamiento, según lo dispone el *"Reglamento Interno para la Prevención de Hostigamiento, Discrimen y Represalias de la Policía de Puerto Rico"* y cualquier otra norma legal aplicable.
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.

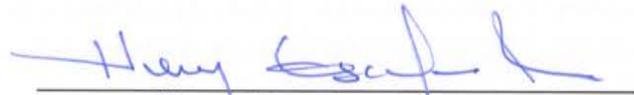
C. Derogación

Esta Orden General deroga cualquier otra Orden, Reglamento, 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.

Esta Orden entrará en vigor el 25 de abril de 2018.



Henry Escalera Rivera
Comisionado Interino