



ORDEN GENERAL

Capítulo: 400	Sección: 408	Fecha de Efectividad: 15 de enero de 2019
Título: Acceso y Manejo a los Sistemas de Información de Justicia Criminal		
Fecha de Revisión: Septiembre/2021	Revisión: Bial	Número de Páginas: 19

I. Propósito

Esta Orden General tiene el propósito de establecer las directrices para los empleados y/o contratistas del Negociado de la Policía de Puerto Rico (en adelante, "NPPR"), para el acceso y manejo de los Sistemas de Información de Justicia Criminal provistos por la División de Servicios de Información de los Sistemas de Justicia Criminal del FBI (CJIS, por sus siglas en inglés) y por la División de los Sistemas de Información de Justicia Criminal del Departamento de Justicia de Puerto Rico (SIJC, por sus siglas en español).

II. Definiciones

Las palabras y conceptos mencionados en esta Orden tendrán el siguiente significado.

AHP

- 1. Agencia de Sistemas de CJIS (CSA, por sus siglas en inglés):** Agencia de Justicia Criminal de un estado o territorio que lleve a cabo la responsabilidad administrativa, por el mantenimiento del Sistema de Justicia Criminal que haga vínculo con el sistema NCIC para proveer servicio estatal a sus usuarios con respecto a los datos del NCIC. En Puerto Rico, el Departamento de Justicia.
- 2. Centro Nacional de Información Criminal (NCIC por sus siglas en inglés):** Es un sistema nacional de información computarizado establecido para servir a todas las agencias locales, estatales y federales de Justicia Criminal.
- 3. Confirmación de Acierto:** Es una respuesta positiva del NCIC sobre la persona o propiedad solicitada que aparece igual que la contenida en la respuesta. En estos casos se requiere contactar la unidad que hizo la entrada para validar la información antes de tomar acción oficial.
- 4. Coordinador Agencial de Terminales (TAC, por sus siglas en inglés):** Persona designada por el Comisionado, quien es responsable por asegurarse que se cumpla con las políticas y regulaciones del NCIC y el estado, incluyendo los requisitos de validación.
- 5. Coordinador del Área de los Sistemas de Información (POC, por sus siglas en inglés):** Persona designada por el Comandante de Área, quien es responsable de asegurarse que se cumpla con las políticas y regulaciones del NCIC y el estado, incluyendo los requisitos de validación.

6. **Identificador de la Agencia (ORI, por sus siglas en inglés):** Identificador que asigna el FBI a cada agencia para ser usado en cada transacción. El mismo se compone de nueve (9) caracteres; los primeros dos (2) significan estado o país, los siguientes tres (3) son la agencia y los últimos cuatro (4) es la ubicación del mismo dentro de la agencia. Ej. PRPPR1800
7. **Oficial de Sistema de Información de Justicia Criminal (CSO, por sus siglas en inglés):** Persona designada por el administrador del CSA que es el responsable de la supervisión del uso de los sistemas, haciendo cumplir la disciplina del sistema y asegurándose que los procedimientos del funcionamiento del NCIC sean seguidos por los usuarios autorizados según estipulado por el acuerdo de usuarios del NCIC.
8. **Operadores de Sistemas de Información Criminal:** Persona designada por el director de la unidad de trabajo para hacer búsqueda, entrada, suplementar, modificar, eliminar y cancelar en los casos de acceso completo (Full), y en los casos búsqueda (Inquiry) en los Sistemas de Información de Justicia Criminal.
9. **Servicios de Información de Justicia Criminal del FBI:** La División del FBI que es responsable de la recopilación, almacenamiento y difusión oportuna de la información de justicia criminal relevante al FBI, a las agencias calificadas de ley y orden, justicia criminal, civil, académica, empleo y licencias.
10. **Sistema de Información para el Registro Criminal Integrado (RCI, por sus siglas en inglés):** Sistema que integrará las bases de datos de las agencias de Justicia Criminal.

### III. Normas y Procedimientos

#### A. Asignación y cancelación de cuentas

1. El Director de la unidad de trabajo solicitará mediante comunicación al TAC, el personal que será adiestrado en los Sistemas NCIC, RCI y DAVID Plus.
2. El personal seleccionado una vez completado el adiestramiento se tomará las huellas dactilares en la División de Servicios Técnicos del Área o la División de Identificación Criminal del Cuartel General, según corresponda.
3. El Director de la unidad de trabajo solicitará al TAC la cancelación inmediata del acceso a los sistemas NCIC, RCI y DAVID Plus en los siguientes casos:
  - a. Uso ilegal de los sistemas
  - b. Traslados
  - c. Renuncia
  - d. Suspensión de días
  - e. Muerte

- f. Expulsión
  - g. Arresto por delito grave
  - h. Suspensión sumaria de empleo
  - i. Suspensión sumaria de empleo y sueldo
4. La cancelación de la contraseña del sistema NCIC y RCI será sometida por correo electrónico al TAC. En el caso de DAVID Plus deberá cumplimentar el formulario DTOP-140f, titulado: "Solicitud para Desactivar Cuentas o Cambiar Accesos al Sistema David+".
5. No se dará acceso al NCIC, RCI o al David Plus a ningún MNPPR que no haya aprobado el adiestramiento para el uso y manejo de estos sistemas.

#### **B. Acceso a los datos e información**

1. El acceso a los terminales de información de Justicia Criminal está limitado a los empleados adiestrados por el TAC, CSA o FBI.
2. El empleado del NPPR no certificado que realice investigaciones cumplimentará el formulario PPR-135.4, titulado: "Solicitud de Información Expediente Criminal Computarizado" (PPR-135.4) para solicitar información de los sistemas.
3. Esta solicitud será cumplimentada por el investigador y será enviada al Operador del Sistema del área policiaca correspondiente.

#### **C. Operador de Sistema**

1. El operador de los sistemas cumplirá con los siguientes requisitos:
- a. Ser empleado del NPPR y certificado por el TAC.
  - b. Completar y aprobar adiestramiento de Operador de Sistema y de seguridad básica (Security Awareness).
  - c. Cumplimentar el formulario titulado "Addendum de Seguridad".
  - d. Cumplimentar el documento con las "Reglas de Comportamiento de los Usuarios".
  - e. Aprobar certificación adiestramiento NCIC y RCI.
  - f. Recertificarse cada dos (2) años. Además, deberá renovar las Reglas de Comportamiento de Usuarios.

#### **D. Procedimiento de Investigación para acceso al Área de Información de Justicia Criminal (CJI)**

**Todo empleado que vaya a acceder al área donde se encuentran los terminales de Información Criminal, cumplirá con lo siguiente:**

1. Personal con acceso sin escolta o contratista, aprobará una investigación de antecedentes de huellas dactilares por agencias federales y estatales.
2. Completar el registro de huellas digitales para contratistas y proveedores.
3. Aprobar investigación realizada por la Oficina de Seguridad y Protección.

#### **E. Disponibilidad de los Sistemas de Información**

1. Los Sistemas están diseñados para dar servicio veinticuatro (24) horas al día, siete (7) día a la semana.
2. Las unidades de trabajo que realizan entradas al sistema tendrán disponibles operadores 24/7 para proporcionar una respuesta de confirmación en el momento de ser solicitada. Además, tendrán dos (2) operadores por turno.
3. Las unidades de trabajo con el sistema, que no realizan entradas, tendrán como mínimo un operador por cada turno de trabajo.

#### **F. Medidas de Seguridad**

1. Los Sistemas de Información de Justicia Criminal son para uso oficial exclusivamente.
2. Todo empleado o contratista del NPPR cumplirá con las políticas y procedimientos establecidos por el NPPR y el CJIS.
3. Normas de Seguridad Física
  - a. Bloquear su computadora y utilizar una contraseña segura según dispone la Orden General 400-403 titulada: "Uso y Manejo de los Sistemas Computadorizados" (OG 400-403).
  - b. Asegurar la computadora, dispositivo móvil y/o laptop en todo momento.
  - c. Formatear tres (3) veces antes de decomisar computadoras o dispositivos móviles.
  - d. Posicionar la computadora de manera que el personal no autorizado o transeúnte no pueda observar información sensible.
  - e. Asegurar el área donde están ubicados los terminales antes de abandonar el lugar.
  - f. Las puertas que dan acceso a los terminales deberán ser controladas por clave o tarjeta.
  - g. La información confidencial no será tirada o abandonada por los alrededores, esto incluye facsímil, impresora o fotocopidora.
  - h. La disposición de información sensible en papel o CD será triturada. En el caso de los discos duros se deberán destruir lógica y físicamente según dispone la OG 400-403.

#### 4. Seguridad Personal

Todo contratista o proveedor de servicios del NPPR aprobará una investigación realizada por la Oficina de Seguridad y Protección antes de tener acceso a los Sistemas de Información de Justicia Criminal.

#### 5. Seguridad de Escritorio (Computadoras Desktop)

- a. Apagar o bloquear el terminal cuando este lejos de su escritorio.
- b. Deshabilitar (Lock) la computadora cuando no esté en uso.

#### 6. Seguridad Información Tecnológica

Este término se refiere a la protección de información de acceso no autorizado, uso, divulgación, alteración, modificación o destrucción mediante el uso de los siguientes conceptos:

- a. **Confidencialidad:** la información será utilizada para asuntos estrictamente oficiales y no será divulgada a personas no autorizadas.
- b. **Integridad:** garantizar que los sistemas de información no se modifiquen maliciosa o accidentalmente.
- c. **Disponibilidad:** fiabilidad de acceso oportuno a los datos y recursos por parte de personas no autorizadas.

#### 7. Visitantes

- a. El operador o supervisor acompañará al visitante en todo momento y supervisará la actividad de estos.
- b. El visitante cumplimentará el formulario PPR-408.1, titulado: "Registro de Visitantes" (PPR-408.1).

#### 8. Contraseña

Los parámetros de la contraseña serán los siguientes:

- a. Mínimo de ocho (8) caracteres;
- b. No usar palabra de diccionario o su nombre;
- c. No usar el nombre de usuario;
- d. No usar las diez (10) contraseñas anteriores;
- e. Cambiar la contraseña cada sesenta (60) días;
- f. No publicar o transmitir la contraseña; y
- g. No mostrar la contraseña cuando la escribe.

### 9. Número Personal de Identificación (PIN)

- a. El número personal de identificación deberá tener un mínimo de seis (6) dígitos;
- b. No podrá repetir dígitos o usar patrones secuenciales. (ej. 11, 22, 33, o 12345);
- c. No usar el mismo id de usuario;
- d. No mostrar cuando se escribe; y
- e. No publicar o transmitir fuera de un lugar seguro.

### 10. Disposición de Datos

- a. La disposición autorizada de récords será realizada con una máquina trituradora.
- b. Toda unidad de trabajo con terminales de NCIC tendrá una máquina trituradora.

### 11. Encriptación

- a. Toda información que se envíe en un medio electrónico oficial del NPPR tendrá que ser mediante un mecanismo con capacidad de encriptación.
- b. La transmisión de información mediante facsímil se podrá realizar una vez la persona se asegure que la persona responsable de recibir la información se encuentre esperando frente a la máquina de facsímil.

### 12. Dispositivos Móviles

En el caso de los dispositivos móviles deberán tomar las siguientes medidas de seguridad:

- a. Desactivar cualquier acceso inalámbrico (Bluetooth, Wi-Fi, etc.).
- b. Configurar el dispositivo para que pregunte antes de conectarse a cualquier red inalámbrica.
- c. Desactivar la aplicaciones y complementos que no utilice frecuentemente.
- d. Eliminar listas de servicio inalámbrico que no sean necesarias.
- e. No almacenar documentos del sistema en computadoras de trabajo o personales.
- f. Mantener separados los dispositivos móviles del trabajo y los personales.

### 13. Dispositivos Personales

- a. El NPPR prohíbe el uso de equipo electrónico o computadorizado personal tales como unidades de almacenamiento secundario tales como: flash drives, teléfonos celulares, tabletas, entre otros.

## G. Controles

1. La consulta en el registro de los sistemas NCIC, RCI, DAVID Plus y demás sistemas que componen los Sistemas de Información de Justicia Criminal deberá realizarse para asuntos estrictamente oficiales.
2. El solicitante deberá cumplimentar el formulario PPR-135.4 "Solicitud Información Expediente Criminal Sistema Computadorizado".
3. La solicitud de información por radio de comunicaciones estará limitada a la siguiente información:
  - a. Marca, modelo, año, tablilla, número de registro y número de identificación impreso por el fabricante (VIN) del vehículo.
  - b. Número de licencia, nombre y apellidos, así como el estatus de la licencia de conducir.
4. El operador que realice una búsqueda de información por radio solicitará el número de placa del peticionario y la unidad de trabajo a la cual pertenece.
5. El miembro del NPPR (en adelante "MNPPR") que intervenga con un conductor de un vehículo de motor vendrá obligado a verificar la información de tablilla y VIN en el sistema NCIC.
6. Los datos almacenados en el NCIC, RCI y demás sistemas de Justicia Criminal es de carácter confidencial. Cualquier empleado del NPPR que disemine información en violación a las normas establecidas en esta orden general estará sujeto a acciones disciplinarias, penales o civiles. En estos casos será referido a la Superintendencia Auxiliar en Responsabilidad Profesional (en adelante "SARP") de conformidad con la reglamentación vigente.
7. La información obtenida mediante estos sistemas, incluyendo récord criminal, fotos, entre otros, no será publicada ni utilizada para otros propósitos que no sean los oficiales y autorizados por la legislación federal y estatal aplicable.

ANP

## IV. Entrada de Gravamen

### A. Hurto de Auto

El gravamen de hurto de auto solamente será ingresado en los sistemas por el personal autorizado de los Centros de Mando. El operador deberá cumplir con las disposiciones establecidas en la Orden General Capítulo 600 Sección 647 titulada "Investigación Preliminar Hurto de Vehículos". Además, tendrá los siguientes deberes y responsabilidades:

1. Impondrán el gravamen inmediatamente en el NCIC, RCI, DAVID Plus o cualquier otro medio que se establezca en el futuro.
2. El operador entrará como hurto de auto en el sistema NCIC los vehículos hurtados mediante apropiación ilegal, robo o escalamiento.
3. El operador verificará que el vehículo no tenga gravamen en el Sistema NCIC, DAVID Plus.
4. El operador ingresará el vehículo usando el formato (EV).
5. El operador imprimirá la transacción y procederá a cumplimentar y firmar el formulario PPR-408.2, titulado: "Doble Cotejo" (PPR-408.2).
6. Entregará a otro operador el documento para el doble cotejo y archivo.
7. En el caso de vehículos recuperados seguirá el siguiente proceso:
  - a. Si el vehículo es recuperado por otra área con número de ORI distinto al que realizó la entrada, deberá imponer un localizado (located) usando el formato (LV).
  - b. Imprimir la evidencia de notificación de located.
  - c. Archivar en el récord.
  - d. Eliminar el récord del sistema usando el formato (CV).

AHP

## B. Vehículo involucrado en la Comisión de un Delito Grave

El operador, a petición del investigador, deberá entrar en el sistema todo vehículo involucrado en la comisión de un delito grave que se desconozca su paradero. El investigador deberá proveer la siguiente información:

- a. El formulario PPR-621.1, titulado: "Informe de Incidente", según cumplimentado a través del sistema *GTE*, estableciendo la descripción del vehículo: marca, modelo, año, puertas, tablilla, VIN y las características particulares.
- b. Corroboración de la información del vehículo para evitar entradas incorrectas en el sistema NCIC.

## C. Persona Buscada (Most Wanted)

1. Orden de Arresto
  - a. La entrada al archivo de personas buscadas deberá ser entrado inmediatamente se obtengan los datos mínimos requeridos y la documentación del récord.
  - b. El operador verificará que la persona no aparezca como prófugo usando el formato (QW). Además, buscará en el sistema DAVID Plus y el Interstate



Identification Index (Triple III). Este último solamente será para casos de adultos.

- c. En el caso del Triple III el operador siempre cumplimentará el formulario PPR-135.4.
- d. Realizará la entrada de la persona buscada usando el formato (EW).
- e. Cuando exista información de vehículo que conduce la persona buscada se podrá entrar en el récord.
- f. Cuando se tenga conocimiento que la persona buscada tiene armas y es peligroso, tiene tendencias suicidas, es hemofílico, previamente ha escapado, es adicto a heroína o es diabético, se añadirá esta información en el récord usando el campo de precaución (CMC).
- g. De existir una orden de extradición, deberá asegurarse del alcance de la misma y si va a ser autorizada. Cuando la unidad que originó la entrada reciba una notificación definitiva que la persona no será extraditada deberá modificar el récord con el código apropiado en el campo (EXL). Esta norma aplica a delitos graves y menos grave.
- h. Culminado el proceso de entrada en el sistema deberá imprimir la copia de la transacción. Además, entregará a otro operador el documento. Éste último, cumplimentará el formulario PPR-408.2 y lo firmará.

## 2. Orden de Arresto Temporera

Este elemento de dato se podrá utilizar cuando el MNPPR necesite tomar acción inmediata para la aprehensión de una persona que ha cometido un delito o tiene motivos fundados para creer que cometió el delito y no tiene tiempo razonable para obtener la orden de arresto.

El MNPPR que tenga motivos fundados para arrestar se comunicará con el Centro de Mando para que se tramite esta orden de arresto temporera en el sistema, que tendrá una vigencia de cuarenta y ocho (48) horas.

## 3. Arresto (*detainer*)

Cuando un MNPPR diligencia una orden de arresto, el operador del sistema deberá cumplir con el siguiente proceso:

- a. Añadirá la información en el archivo de persona buscada en el estado de localizado (*located*).
- b. Si el MNPPR o la agencia que arresta va a radicar cargos criminales bajo las leyes de Puerto Rico, el operador del sistema en la transacción colocará el *located*.
- c. Cuando se recibe una confirmación de orden de arresto a través del sistema, el operador tendrá cinco (5) días a partir de la transacción de *located* para consultar con el Departamento de Justicia de Puerto Rico. Si se va a extraditar la persona, colocará el código de detención (DETN) en el campo de extradición (EXT).

#### D. Persona Desaparecida

1. El operador verificará que la persona no aparece en el sistema como desaparecido o prófugo usando el formato de búsqueda (QW). Además, buscará en el Sistema DAVID Plus y el Triple III.
2. En el caso de que la persona desaparecida que figura como desaparecidos en el sistema en un incidente anterior, la entrada anterior quedará anulada por la nueva querrela.
3. En el caso del Triple III el operador siempre cumplimentará el PPR-135.4.
4. Realizará la entrada utilizando el formato (EM).
5. Culminada la transacción deberá imprimir copia de la transacción y la firmará.
6. Firmada la transacción la entregará a otro operador para que haga el doble cotejo y archivo mediante el formulario PPR-408.2.
7. Cuando la persona sea localizada en un área distinta al ORI que realizó la entrada deberá imponer un *located* usando el formato (LM), imprimirá la evidencia de notificación y lo archivará en los récords.
8. Cuando la querrela sea infundada se cancelará en el sistema con el formato (XM).

ALF

#### E. Persona con Información en el Archivo de Personas Desaparecidas

1. El operador realizará esta entrada en las siguientes circunstancias:
  - a. Persona desaparecida fue vista por última vez en circunstancias que supone un riesgo para la seguridad de esa persona.
  - b. Posibilidad sustancial de que la persona tiene información relevante acerca de la persona desaparecida que podría resultar en la localización de la misma.

#### F. Archivo Orden de Protección

1. En este archivo se encuentra el récord de personas que están sujetas a una orden de protección expedida por un tribunal de un estado, tribu o territorio de los Estados Unidos. Esto para prevenir actos de violencia, hostigamiento, amenaza, comunicación o contacto físico con la otra persona.

2. La orden de protección deberá ser entrada en el sistema dentro de un periodo no mayor de ocho (8) horas de recibida en el NPPR.
3. El operador verificará que la persona no aparece en el archivo de órdenes de protección usando el formato de búsqueda (QW) o (QPO). Además, buscará en el sistema DAVID Plus y el Triple III.
4. En el caso del Triple III el operador siempre cumplimentará el PPR-135.4.
5. El operador realizará la entrada en el sistema utilizando el formato (EPO).
6. Imprimirá copia de la transacción, cumplimentará y firmará el formulario PPR-408.2.
7. Entregará a otro operador el documento para el doble cotejo y archivo.

#### **G. Archivo del Registro de Personas Convictas por Delitos Sexuales (NSOR)**

##### 1. Criterio de entrada

- ALP
- a. Aplica a toda persona que ha sido convicta por un delito sexual o su tentativa o conspiración. Las personas bajo esta condición son personas que han sido convictas por delitos contra menores de edad, convictos por delitos sexuales violentos, o se ha determinado que son depredadores sexuales violentos.

Personas que no han sido convictas por un delito que no reúne los criterios (escalamiento, incendio, etc.) no serán registrados bajo este archivo.

- b. Las personas catalogadas como ofensores sexuales, antes de entrarse al Registro NCIC, deben ser clasificados según lo establecido en la Ley Núm. 266 de 9 de septiembre de 2004, según enmendada Ley del Registro de Personas Convictas por Delitos Sexuales y Abuso Contra Menores. Las clasificaciones son las siguientes:
  - i. Ofensor Sexual Tipo I
  - ii. Ofensor Sexual Tipo II
  - iii. Ofensor Sexual Tipo III
- c. Los ofensores que han sido clasificados bajo Tipo I y Tipo II no podrán aparecer en el campo de *Fecha de Culminación en el Registro (Ending Registration Date, ERD)* como *NOEXP* (sin fecha de expiración). Deberán tener una fecha específica de acuerdo a su clasificación. Ese dato sólo puede cambiar si al momento de concluir su obligación con el Registro, la persona hace los trámites necesarios, de acuerdo a la ley, para ser excluido del mismo. En dicho caso se colocaría *NOEXP* en el campo de *ERD* hasta que

la persona cumpla con los requisitos para ser removido de acuerdo a la ley vigente.

d. La persona convicta y catalogada como ofensor sexual deberá mantenerse inscrito en el Registro y cumplir con los requisitos establecidos en esta Ley durante los siguientes términos:

- i. Quince (15) años, si el convicto es un Ofensor Sexual Tipo I;
- ii. Veinticinco (25) años, si el convicto es un Ofensor Sexual Tipo II; y
- iii. De por vida, si el convicto es un Ofensor Sexual Tipo III.

e. Los términos aquí dispuestos empezarán a contar desde que el ofensor sexual sea excarcelado, por haber cumplido la pena de reclusión impuesta y la Administración de Corrección notifique su inclusión en el Registro. En los casos del disfrute de los beneficios de libertad a prueba, libertad bajo palabra o participación de un programa de desvío, tratamiento o rehabilitación, el término de inclusión en el Registro comenzará a contar desde que se emite la sentencia, resolución o determinación para participar en dichos programas y se notifique su inclusión al Registro.

f. La validación será realizada según su clasificación:

- i. Tipo I – Anualmente
- ii. Tipo II – Cada seis (6) meses
- iii. Tipo III – Cada tres (3) meses

## 2. Búsqueda

- a. El Formato de QXS es usado para búsqueda en el *Archivo del Registro de Personas Convictas por Delitos Sexuales*.
- b. El formato QXS está restringido solamente a búsqueda del *Archivo del Registro de Personas Convictas por Delitos Sexuales* y debe traer récords activos o inactivos (eliminados o expirados) del *Archivo del Registro de Personas Convictas por Delitos Sexuales*.
- c. Una búsqueda realizada en *Personas Buscadas (QW)*, incluirá también el *Archivo del Registro de Personas Convictas por Delitos Sexuales*, además de otros archivos de personas y solamente contendrá los récords activos.

## 3. Entrada

- a. La puntualidad de entrada garantizará la máxima eficacia del sistema NCIC.
- b. Los récords del registro deben ser ingresados inmediatamente cuando se cumplan las condiciones de entrada sin exceder tres (3) días luego de recibido por la Agencia.
- c. Las únicas excepciones a la entrada inmediata son:

- i. cuando por estatuto federal se establezca lo contrario; o

- ii. cuando existe documentación para respaldar la entrada demorada en el registro NSOR.
- d. En la auditoría, CJIS revisará que los récords se ingresen dentro de los tres (3) días posteriores a la recepción de la información por parte de la Agencia.
- e. Toda entrada tendrá que ser verificada por parte de otro operador del sistema para corroborar la precisión de los datos del récord.
- f. Para los récords de NSOR, todos los campos ingresados deben ser verificados contra el documento de origen para garantizar que los datos del registro NSOR coincidan con los datos del récord.

## H. Validación

1. El POC de las Comandancias de Área y de las unidades de trabajo que realizan entradas al sistema, validará los récords para asegurarse que están completos, exactos y continúan vigentes. En caso de que el POC no se encuentre, el supervisor de la unidad designará un operador del sistema para realizar las validaciones.
2. El TAC enviará mensualmente a la unidad correspondiente las validaciones.
3. EL POC u operador asignado seguirá el siguiente procedimiento para validar los récords:
  - a. Localizar el récord.
  - b. Comparar las entradas con la información archivada. Deberá asegurarse que la información coincide y verificará si hay información adicional que añadir. La información incorrecta deberá ser eliminada o corregida y la información adicional deberá ser añadida en el récord. (ej. AKA's marcas, tatuajes o cicatrices entre otros).
  - c. La orden de arresto y orden de protección serán validadas con el tribunal que expidió la misma o el sistema RCI.
  - d. En los casos de personas desaparecidas y propiedad, se deberá verificar en partes policiacos si la querrela tiene un informe suplementario que valide o requiera que el récord sea ser removido. Además, se contactará a la persona querellante por teléfono o visita.
  - e. Remover todos los récords que no estén vigentes y exactos.
  - f. La hoja de validación deberá tener anejada el documento que sustenta la entrada. Además, deberá tener la firma con lo siguiente: rango, nombre, apellido y placa de la persona que realizó la misma.
  - g. La validación será realizada en un término no mayor de treinta (30) días de recibida.
  - h. Devolver al TAC la certificación que los récords están actualizados y exactos. En caso de que por alguna razón no se pudieran validar todos los récords, se certificará la validación parcial y se documentará la razón por la cual no se pudo validar todos los récords.
  - i. El TAC remitirá la información al CSA.

AHA

## I. Auditoría

1. Las auditorías en las unidades de trabajo que realizan entradas en el NCIC serán cada tres (3) años. Estas auditorías no son punitivas, sino para mejorar las operaciones del sistema.
2. Procedimiento de auditoría:
  - a. Un mes antes el director de la unidad recibirá un cuestionario de pre-auditoría y una carta estableciendo la fecha y los récords que serán auditados.
  - b. El cuestionario deberá ser completado y devuelto en un término de cuatro (4) a ocho (8) semanas, según establezca la unidad de auditoría de los Sistemas de Información de Justicia Criminal (CJIS Audit Unit).
  - c. De tener conflicto con la fecha de auditoría deberá programar una fecha con el auditor.
  - d. El TAC podrá realizar visitas a las unidades de trabajo sin notificar para velar que el personal cumpla con las políticas del NCIC y esta orden general.

## J. Mantenimiento de los Récords

### 1. Precisión

Los récords del NCIC deben mantenerse precisos y actualizados. Las Agencias con acceso a los récords en el Sistema NCIC son responsables de su exactitud, puntualidad e integridad. La exactitud de los récords del NCIC es una parte integral del sistema NCIC.

### 2. Integridad

Los récords completos incluyen toda la información crítica que se encuentra disponible sobre la persona o propiedad en el momento de la entrada. La validación debe incluir una revisión de información adicional, que no estuvo disponible en la entrada original, para su inclusión en el récord del Registro.

### 3. Remoción de récords

Cada Agencia es responsable de la eliminación de un récord de NCIC tan pronto adquiera conocimiento que el récord ya no es válido.

### 4. Expediente de Entrada

El TAC instruirá a los operadores del Sistema NCIC con relación a las normas y procedimientos para mantener los récords. El TAC y el POC deberán asegurarse que los operadores de terminales conozcan como mínimo lo siguiente:

- a. El deber de mantener un registro de los documentos de entrada (PPR-621.1, orden de arresto, orden de protección), doble cotejo y validación.
- b. El conocer cuándo se puede hacer una búsqueda de un caso.
- c. Las normas para las restricciones de diseminación de información.

## 5. Confirmación de Acierto (hit confirmation)

Cuando la unidad de trabajo reciba una petición de confirmación de acierto deberá realizar el siguiente proceso:

- a. Verificar si la solicitud de confirmación de acierto es urgente o rutinaria.
- b. La confirmación urgente se contestará en un término no mayor de diez (10) minutos y la de rutina dentro de una (1) hora.
- c. Contactar la agencia o unidad que hizo la entrada para confirmar la información.
- d. Asegurarse que la orden de arresto, informe de persona desaparecida, orden de protección o informe de hurto sigue vigente.
- e. Obtener decisión con respecto a la extradición (cuando aplique), información relacionada al regreso de la persona desaparecida, los términos y condiciones de la orden de protección o la entrega de la propiedad a su legítimo dueño.
- f. La confirmación de acierto se realizará a través de NLETS, aunque inicialmente se haya manejado por teléfono, facsímil o cualquier otro medio.

## 6. Registro de Búsqueda de Récord Criminal

- a. Cada unidad de trabajo que realice una búsqueda en el sistema NCIC deberá mantener un récord del formulario PPR-135.4.
- b. Deberán ser registradas en el PPR-135.4 las siguientes transacciones:
  - i. Búsqueda de récord criminal y orden de arresto (QWI)
  - ii. Récord Criminal (QH)
  - iii. Historial Criminal (QR)
- c. El POC revisará mensualmente este registro para asegurarse que se mantiene actualizado.

## K. Archivos Restringidos

Sólo tendrán acceso a los siguientes archivos los operadores y los MNPPR que así lo soliciten con el propósito de funciones oficiales.

1. *Gang Files*
2. *Known or Appropriately Suspected Terrorist Files*
3. *Supervised Release Files*

4. *National Sex Offender Registry Files*
5. *Historical Protection Order Files of the NCIC*
6. *Identity Theft Files*
7. *Protective Interest Files*
8. *Person With Information (PWI) data in the Missing Person Files*
9. *Violent Person File*
10. *NICS Denied Transactions File*

## L. Coordinadores

### 1. Coordinador Agencial de Terminales (TAC)

El Coordinador Agencial de Terminales (TAC) será designado por el Comisionado, y será un empleado del sistema de rango o del sistema clasificado. El TAC tendrá los siguientes deberes y responsabilidades:

- ALF
- a. Será el enlace entre SIJC y el FBI.
  - b. Administrar la operación de los terminales NCIC en el NPPR.
  - c. Asegurar que se apliquen las políticas estatales y federales.
  - d. Asignar nombre de usuario y contraseña para los usuarios del Sistema NCIC.
  - e. Cumplir y asegurarse que los empleados del NPPR cumplan con el acuerdo de no divulgación de datos e información entre el Departamento de Justicia Federal, Departamento de Justicia de Puerto Rico y el NPPR. Este acuerdo es extensivo a las agencias externas que soliciten información del sistema.
  - f. Participará activamente en el desarrollo y ofrecimiento de adiestramientos de los SIJC.
  - g. Realizará y/o participará activamente en las auditorías que se requieren en esta Orden general y/o Agencias Federales y/o Estatales pertinentes.
  - h. Se mantendrá actualizado en las políticas estatales y federales sobre los SIJC.
  - i. Recomendará cambios en políticas y/o adiestramientos de ser necesario.
  - j. Estará disponible para asesorar a los MNPPR en relación con el SIJC.
  - k. Someterá al FBI, informes de personal con acceso a los sistemas, auditorías, entre otros que le sean requeridos.
  - l. Asegurarse de que se lleven los registros de búsqueda de información criminal de forma correcta.
  - m. Asegurarse de que se realice la cancelación de clave cuando proceda y peticionar la clave de acceso.
  - n. Velar que se cumpla con los procedimientos, mantenimiento de récords y la política de confirmación de acierto.

### 2. Coordinador del Área (POC)

El POC será designado de conformidad con la Orden General 100-126, titulada: "Centro de Operaciones de Radio Control y Centro de Mando". Tendrá los siguientes deberes y responsabilidades:



- 142F
- a. Asistir a las reuniones relacionadas al Sistema de Información de Justicia Criminal.
  - b. Velar por la seguridad del sistema, entiéndase:
    - i. Asegurarse que personal ajeno a la agencia no intente realizar cambio al NCIC, ya sea en términos de hardware o software.
    - ii. Asegurarse que personas no autorizadas estén entrando en el NCIC, en el área de trabajo o donde está el equipo del NCIC.
    - iii. Operadores no compartan contraseña.
    - iv. Seguir las guías del NCIC respecto a la disseminación de documentos o trituración de los mismos.
    - v. Asegurarse que el personal entienda las reglas de disseminación de la información del sistema NCIC.
    - vi. Notificar al supervisor y al TAC cualquier sospecha de violaciones de seguridad.
    - vii. Ser contactado si alguien solicita información y hay dudas en cuanto a la autoridad legal para acceder a esa información.
  - c. Actualizar la información mediante la discusión de boletines de actualización en línea (Newsletter).
  - d. Coordinar los adiestramientos y/o readiestramientos de los operadores.
  - e. Realizar validaciones.
  - f. Asistir en las auditorías.
  - g. Asegurarse que se lleve un registro de búsqueda de antecedentes penales.
  - h. Solicitar la cancelación de clave cuando proceda y peticionar la clave de acceso.
  - i. Velar que se cumpla con los procedimientos, mantenimiento de récords y la política de confirmación de acierto.

#### **M. Deberes de los empleados del NPPR**

El MNPPR tendrá los siguientes deberes y responsabilidades:

1. Solicitar la verificación de la tablilla y/o número de serie impreso por el fabricante (VIN por sus siglas en inglés) en el sistema NCIC en toda intervención vehicular, investigación de choque de auto o cualquier investigación criminal asignada donde esté involucrado un vehículo según se define en el NCIC y/o la Ley 22, titulada: "Ley de Vehículos y Tránsito de Puerto Rico".
2. Verificar los antecedentes penales de toda persona bajo investigación criminal.
3. Todo empleado que utilice los datos o información del NCIC, RCI u otro Sistema de Justicia Criminal para asuntos personales estará sujeto a acciones disciplinarias según dispone el Reglamento 9001, titulado: "Reglamento para


Enmendar el Artículo 14 del Reglamento de Personal de la Policía de Puerto Rico”, acciones penales o civiles según dispone 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. Toda transacción en el sistema NCIC se registrará según las regulaciones del **NCIC Operating Manual y el Criminal Justice Information Services (CJIS) Security Policy**, última versión.
  2. En todo plan de trabajo, los Directores de Unidad de Trabajo se asegurarán de la continuidad de los servicios del TAC/POC.
  3. Todos los MNPPR tendrán que completar y aprobar el adiestramiento de seguridad básica (Security Awareness), para poder tener acceso al CAD Móvil/NCIC. Dicho adiestramiento se podrá ofrecer de manera virtual.
  4. El Director del Negociado de Tecnología y Comunicaciones en coordinación con la SAEA mantendrá un programa de talleres para mantener informado a los empleados del NPPR sobre las normas y controles de los sistemas computarizados.
  5. Todo programa desarrollado internamente es propiedad del NPPR y no podrá ser divulgado, copiada o utilizado sin autorización.
  6. La División de Tecnología tendrá la responsabilidad de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que la propiedad se utilice para propósitos y gestiones relacionados al trabajo.
  7. Los Coordinadores de Tecnología de las Áreas Policiacas tendrán la responsabilidad de someter trimestralmente a la División de Tecnología, un listado con la cancelación de las cuentas de dominio y/o las cuentas de correo

8. Esta política estará sujeta a revisión por motivo de cualquier directriz o normativa procesal emitida por el Departamento de Justicia de Puerto Rico o el Centro Nacional de Información Criminal.
9. 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.
10. 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 sanciones disciplinarias, posibles cargos criminales y/o acciones civiles, según corresponda.

### C. Cláusula de Separabilidad

Si cualquier disposición de esta Orden General fuese declarada inconstitucional o nula por un Tribunal competente, la sentencia o resolución dictada a tal efecto no afectará las demás disposiciones de esta Orden, las cuales continuarán vigentes.

### D. Derogación

Esta orden general deroga cualquier otra orden, reglamento, normas, comunicación verbal o escrita o partes de las mismas que entren en conflictos con esta.

### E. Aprobación

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

### F. Vigencia

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

  
\_\_\_\_\_  
Cnel. Antonio López Figueroa  
Comisionado