ORDEN GENERAL

Capítulo: 400	Sección: 405	Fecha de Efectividad: 28 de Junio de 2018	Núm. Páginas 6
Título: Repositorio Central para la Captura de Datos Relacionada al Crimen (CIW)			
Reglamentación Derogada: N/A			

I. Propósito

Esta Orden General tiene el propósito de establecer las normas y procedimientos para el uso del Repositorio Central para la Captura de Datos Relacionada al Crimen (CIW) en el Negociado de la Policía de Puerto Rico (NPPR).

II. Definiciones

1. **Repositorio de datos (Data Warehouse)**: área central para el almacenamiento y procesamiento de datos, internos y externos, orientada a un determinado ámbito integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza.

2. **Base de datos**: almacén que permite guardar grandes cantidades de datos depurados, estructurados y centralizados, los cuales son recolectados y descargados por los sistemas de información de una entidad en particular.

3. **Almacén de Datos de Incidentes Criminales (Criminal Information Warehouse, CIW por sus siglas en inglés)**: área central para recoger los datos e información sobre la incidencia criminal con el fin de combatir el crimen mediante el uso de herramientas tecnológicas para la toma de decisiones a través del análisis de incidentes, estadísticas y mejor entendimiento de patrones criminales.

4. **Personal Autorizado**: Empleado o persona autorizada por el director del Negociado o División para acceder un área restringida específica de trabajo.

5. **Resguardo de datos e información (Backup)**: Copia de seguridad, en algún medio análogo o digital, donde se almacenan los datos e información contenidos en un computador y/o servidor de modo que se pueda utilizar para restaurar la información original después de una eventual pérdida o falla de los sistemas de información, así como de los equipos computadorizados.

6. **Servidor (Host)**: Computadora central de un sistema de red, que está destinado a proveer y administrar servicios, los recursos, las aplicaciones, los archivos y la seguridad de la misma.

7. **Programas (Software)**: Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber programas de sistema que

controlan el funcionamiento de las computadoras y de las redes de informática y también programas de aplicación que facilitan y/o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

III. Normas y Procedimientos

A. Asignación de cuentas

1. **Limitaciones de acceso**: los usuarios registrados para el uso y manejo del CIW tienen un primer nivel de autorización, el cual se relaciona con el directorio activo (Active Directory) de la Agencia, que contiene el nivel centralizado de seguridad de todos sus usuarios en términos de sus credenciales de acceso. Por ejemplo, administradores, usuarios (end-users) y técnicos de IT. Ningún usuario tiene acceso directo a los servidores o las bases de datos del CIW. Todos los accesos a los datos son permitidos a través de los portales electrónicos. La seguridad se controla por la política de acceso de la Agencia y las autorizaciones en el sistema de seguridad del CIW otorgadas por el director del Negociado de Tecnologías y Comunicaciones (NTC) o el director de la División de Tecnologías.

2. **Limitaciones de uso**: los usuarios con acceso al CIW, solicitarán autorización separada para ingresar al CIW. Dicha autorización informará los accesos y las áreas a las cuales tendrán acceso. Estas son el área de Análisis e Inteligencia, o Estadísticas.

3. **Contraseñas**: las contraseñas son renovadas por el usuario, acorde a las políticas de la Agencia, en intervalos de 60 días, las cuales se controlan a través del Active Directory.

HPR

B. Fuentes de datos

Las fuentes de datos y/o aplicaciones que se utilizan para consultas, análisis estadísticos e investigaciones criminales son propiedad del NPPR. Las fuentes externas son solicitadas por el NPPR y autorizadas por las diferentes agencias u organizaciones mediante acuerdos entre las partes. entre las fuentes de datos más utilizadas se encuentran las siguientes:

1. Departamento de Justicia, Registro Criminal Integrado (RCI)
2. Departamento de Transportación y Obras Públicas (David +)
3. Departamento de Corrección y Rehabilitación
4. Administración de Compensaciones por Accidentes de Automóviles
5. Departamento de Recursos Naturales
6. Comisión Estatal de Elecciones
7. Departamento de Salud
8. Sistema de Análisis y Estadísticas Computarizado (SAEC)
9. Lector de tablillas (License Plate Hunter)
10. Sistema de despacho de incidentes y recursos (CAD)

11. Registro Electrónico de Licencias y Armas (REAL)
12. Sistema Automático de Identificación Dactilar (Automated Fingerprint Identification System (A.F.I.S.) / Mugshots)
13. Línea de Confidencias 787-343-2020
14. Arrestos Especiales y Extradiciones
15. Base de Datos de Casos de Crimen Cibernético (Cyber Crime Database)
16. Programa de Registro de Investigaciones del Crimen Organizado (PRICO)
17. Sistema Histórico de Antecedentes Penales (ANPE)
18. Sistema Alterno para Expedientes de Antecedentes Penales

C. **Disponibilidad del Sistema de Información**: la plataforma de servidores, sistemas operativos, bases de datos, interfaces del CIW y los reportes están diseñados y construidos para operar en misión crítica (24/7/365), a todas horas durante todo el año, desde cualquier dependencia del NPPR.

D. **Resguardos ("Backups") periódicos**: el sistema de respaldo general del NPPR, está interconectado con diferentes servidores y dos localidades distintas, para hacer una copia diaria de los sistemas operativos y bases de datos. Luego, las copias se almacenan en el equipo de alta capacidad para un resguardo permanente de los datos e información, así como la operación de la Agencia. El esquema y arquitectura para el resguardo de datos e información de los sistemas de información y tecnología están descritos en el Manual para la Administración de los Sistemas Computadorizados.

E. **Categorías de bases de datos cubiertas por el repositorio**: el repositorio central, tienen una sola categoría de base de datos. En el almacén de datos del CIW, reside el modelo de datos y las bases de datos donde se registran todas las transacciones diarias de los recursos identificados en la sección para las fuentes de datos (Sección III-B, del presente documento). El Director del Negociado de Tecnologías y Comunicaciones autorizará el uso y disponibilidad de las categorías cubiertas en el repositorio. Además, determinará dichas categorías basado en las necesidades de la Agencia.

F. **Categorías de registros de datos del repositorio**: las categorías de registros del modelo de datos consisten en querellas, tipos de delitos, zonas geográficas, personas, tipos de autos, colores, marcas, modelos, autos, direcciones, tipos de eventos, tipos de marcas, tipos de tatuajes y marcas visibles, modelos de armas, calibre de armas, tipos de armas, entre otros. El Director del NTC determinará y autorizará el uso, así como la disponibilidad de las categorías cubiertas en el repositorio, basado en las necesidades de la Agencia.

G. **Mantenimiento del repositorio**

El personal autorizado y designado por el Director del Negociado de Tecnologías y Comunicaciones tendrán las siguientes tareas y deberes para el mantenimiento del CIW:

1. **Almacenamiento**: evaluarán los espacios del repositorio y las bases de datos diariamente. Además, compararán y determinarán los patrones de crecimiento, con el fin de remover los archivos de registro (logs files) y expandir los espacios asignados a las bases de datos, acorde con el patrón de incremento semanal del repositorio.

2. **Mantenimiento de registros**: monitorear los procesos que las interfaces desarrollan diariamente sobre los registros provenientes de las fuentes de datos que se consultan, tanto internas como externas. Además, evaluar que dichas interfaces extraigan los datos y depuren los registros conforme a las reglas o estructuras de los datos que contienen las fuentes consultadas, con el propósito de ingresarlos en el repositorio.

3. **Medidas de seguridad en las interfaces**: establecer los mecanismos de seguridad necesarios, que estén disponibles, con el fin de proteger la plataforma del CIW. Además, mantener los datos encriptados desde el repositorio central hasta la entrega de informes a los usuarios.

4. **Conservación de datos**: asegurar que los datos registrados en el CIW, se almacenen permanentemente, y de esta forma reutilizar las fuentes de datos ingresadas al repositorio para futuras investigaciones criminales.

5. **Eliminación de datos**: asegurar que los registros de las fuentes de datos que sean eliminados del repositorio, se marquen como eliminados lógicamente según sea autorizado por la Agencia que así lo requiera. Verificar que ningún registro se elimine físicamente del CIW.

H. Adquisición de licencias y apoyo técnico

El proceso para la adquisición de licencias con el propósito de operar, mantener y el apoyo técnico del CIW, con todos sus componentes, está incluido en el Manual para la Administración de los Sistemas Computadorizados.

IV. Disposiciones Generales

A. Interpretación

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

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

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

B. Cumplimiento

1. El Director del NTC en coordinación con la Superintendencia Auxiliar en Educación y Adiestramiento (SAEA) mantendrá un programa de talleres para mantener informado a los empleados del NPPR sobre las normas y controles de los sistemas computarizados.

2. Todo programa desarrollado internamente es propiedad del NPPR y no podrá ser divulgado, copiada o utilizado sin autorización.

3. La División de Tecnologías 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.

4. 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 electrónico de los empleados del NPPR que terminen sus funciones administrativas u operacionales en la Agencia.

5. Esta política estará sujeta a revisión por motivo de cualquier directriz o normativa procesal emitida por la Oficina de Gerencia y Presupuesto del Estado Libre Asociado de Puerto Rico.

6. En el futuro cualquier nuevo procedimiento, políticas de seguridad y controles (acceso y administración), plan de contingencia y normativas de uso de los sistemas tecnológicos y comunicaciones del NPPR estará contenido en el Manual de Políticas y Procedimientos en Seguridad Informática el cual será desarrollado y aprobado por el Director del NTC, y sus componentes.

7. Se prohíbe a cualquier persona realizar una instalación sin la documentación o sin el certificado de licencia que evidencia la autorización.

8. Se prohíbe copiar o duplicar programas no autorizados en las computadoras de la agencia.

9. Todo empleado 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 SAEA a tenor con las normas aplicables.

10. El personal adscrito al Negociado y/o a sus Divisiones tendrán la obligación de cumplir con los adiestramientos y/o readiestramientos requeridos por las tareas asignadas en su área de trabajo. Por ejemplo: adiestramientos y/o readiestramientos provistos por los proveedores de los sistemas de información y/o equipos electrónicos computadorizados instalados e implementados, en la Agencia. En el caso de los uniformados tendrán la obligación de cumplir con los adiestramientos y/o readiestramientos requeridos por el NPPR. Asimismo, los supervisores se asegurarán del cumplimiento de los mismos.

11. El Director del Negociado, los Directores de las Divisiones y Coordinadores de Tecnología de las Áreas serán responsables de realizar durante el mes de junio, o cuando sea requerido, el inventario de equipo y licencias del software adquiridos e implementados en sus unidades de trabajo. Durante los últimos diez (10) días del mes de junio, se rendirá el informe correspondiente a la División de Propiedad conteniendo todos los cambios efectuados correspondiente al año fiscal. Cumpliendo con las estipulaciones descritas en la Orden General Capítulo 200 Sección 208, titulada "NORMAS PARA EL CONTROL Y CONTABILIDAD DE LA PROPIEDAD PÚBLICA EN USO POR LA POLICÍA DE PUERTO RICO".

12. 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 Miembro del NPPR que incumpla con cualquier disposición de esta Orden General estará sujeto a sanciones disciplinarias, posibles cargos criminales y/o acciones civiles, según corresponda.

C. Derogación

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

D. Vigencia

Esta Orden General entrará en vigor el 28 de Junio de 2018.

Henry Escalera Rivera
Comisionado