

ORDEN ADMINISTRATIVA DSP-2024-OA-001

**ORDEN ADMINISTRATIVA PARA CREAR LA
SECRETARÍA AUXILIAR DE MANEJO DE INFORMACIÓN DE
SEGURIDAD Y ANÁLISIS DEL DEPARTAMENTO DE
SEGURIDAD PÚBLICA**

Tabla de Contenido

I.	Propósito y Declaración de Política Pública	3
II.	Base Legal	4
III.	Definiciones.....	4
IV.	Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis (SAMISA).....	8
V.	Bases de Datos.....	9
VI.	Composición de la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis	9
A.	División del Centro de Fusión	10
B.	División de Manejo de Información de Seguridad	10
C.	División de Coordinación Operacional y Logística	11
VII.	Normas de Seguridad y Control de Acceso	12
VIII.	Registro de solicitudes de búsqueda de información	12
IX.	Designación del Personal y Equipo	13
X.	Uso indebido o ilícito de los equipos o sistemas	14
XI.	Jurisdicción.....	14
XII.	Disposiciones Generales	14
XIII.	Derogación	15
XIV.	Cláusula de Separabilidad.....	16
XV.	Vigencia.....	16

ORDEN ADMINISTRATIVA DSP-2024-OA-001

ORDEN ADMINISTRATIVA PARA CREAR LA SECRETARÍA AUXILIAR DE MANEJO DE INFORMACIÓN DE SEGURIDAD Y ANÁLISIS DEL DEPARTAMENTO DE SEGURIDAD PÚBLICA

I. Propósito y Declaración de Política Pública

Los avances tecnológicos más recientes han generado una transformación significativa tanto en la dinámica cotidiana como en el entorno laboral de nuestra sociedad contemporánea. Es innegable que la tecnología se ha vuelto un componente intrínseco e indispensable en nuestras vidas. Paralelamente, estos desarrollos han incidido en los comportamientos delictivos y en los hábitos rutinarios, dado que las organizaciones criminales evolucionan de manera continua, aprovechando herramientas tecnológicas y recursos económicos para potenciar su capacidad organizativa y, lamentablemente, intensificar el grado de violencia, lo que incide directamente en la seguridad y bienestar de nuestra ciudadanía.

La expectativa de la ciudadanía respecto al desempeño de los organismos encargados de hacer cumplir la ley es que dispongan de tecnología avanzada y la utilicen para prevenir delitos, responder a emergencias y llevar a cabo investigaciones que aseguren la convicción de los culpables. Sin duda, la tecnología abre puertas al permitir el análisis ágil y preciso de diferentes tipos de información. Además, nuestro marco constitucional brinda protección en cuanto a la obtención, divulgación, uso y resguardo de datos obtenidos a través de nuevas tecnologías, con el fin de proteger la privacidad y seguridad de la información

La Ley 20-2017, según enmendada, conocida como “Ley del Departamento de Seguridad Pública de Puerto Rico”, creó un Departamento (en lo sucesivo, Departamento o DSP), cuya función principal es operar como primera línea de defensa enfocada en prevenir el crimen, atender emergencias y proteger la ciudadanía. Además, tiene la responsabilidad de reorganizar, reformar, modernizar y fortalecer nuestros instrumentos de seguridad pública a nivel estatal para incrementar su capacidad, eficiencia y efectividad; integrar de manera efectiva todos los servicios que ofrece el Departamento y sus Negociados; y coordinar todos los recursos gubernamentales, incluyendo las agencias federales y el sector privado, para proveer de forma rápida y efectiva los servicios requeridos antes, durante y después de una emergencia de manera que se logre asegurar la vida y propiedad de los ciudadanos.

Esta Orden Administrativa tiene el propósito de crear la Secretaría Auxiliar de Manejo de Seguridad y Análisis del Departamento de Seguridad Pública (en lo sucesivo SAMISA), establecer las normas y procedimientos que regirán su funcionamiento.

II. Base Legal

Esta Orden Administrativa se adopta en virtud de las facultades conferidas en el Artículo 1.05 (m) de la Ley Núm. 20-2017, conocida como según enmendada, conocida como, "Ley del Departamento de Seguridad Pública de Puerto Rico".

III. Definiciones

- A. 28 CFR Parte 23** - Reglamento federal que proporciona orientación a los organismos encargados de hacer cumplir la ley sobre las normas de aplicación para el funcionamiento de los sistemas de inteligencia criminal multi jurisdiccionales financiados en virtud de la Ley Omnibus de Control de la Delincuencia y Calles Seguras de 1968 en su versión modificada (Ley de Control de la Delincuencia). El objetivo del reglamento es garantizar la protección de los derechos constitucionales y proteger la expectativa razonable de privacidad de las personas.

Proporciona directrices para regir los sistemas de inteligencia criminal en relación con:

1. Presentación/introducción (recogida) de información.
2. Información de inteligencia criminal.
3. Investigación.
4. Difusión.
5. Revisión y depuración o validación.
6. Auditoría e inspección.
7. Seguridad.

- B. Agente del Orden Público** - Todo miembro oficial bajo la jurisdicción del Gobierno de Puerto Rico, cuyos deberes impuestos por Ley se incluyan prevenir, detectar, investigar y efectuar arrestos de personas sospechosas de haber cometido delito. Incluye además a los agentes de las agencias federales.

- C. Clasificación secreta** - Según la Orden Ejecutiva 12356 "National Security Information", Sección 1.2, la autoridad para clasificar

información originalmente como secreta sólo podrá ser ejercida por:

1. Jefes de agencia y funcionarios designados por el Presidente de EE. UU en el Registro Federal.
 2. Funcionarios con autoridad de clasificación original "Top Secret".
 3. Funcionarios en los que se le delegue dicha autoridad de conformidad con la Sección 1.2(d); y cuya divulgación de este material podría causar graves daños a la seguridad nacional.
- D. **Contratista** - Persona que mediante pacto, convenio o negocio jurídico remunerado o no remunerado se obliga a dar alguna cosa o servicio, con relación a un objeto cierto, materia del contrato.
- E. **Control de acceso** - Mecanismo para limitar el acceso a cierta información en función de la identidad de un usuario y su pertenencia a varios grupos predefinidos. El control de acceso puede ser obligatorio, discrecional o basado en roles.
- F. **Cuarto Seguro** - es un cuarto o área construida y operada conforme a esta directiva, con el propósito de salvaguardar información de seguridad nacional que, debido a su alcance, naturaleza, o necesidad operativa, no puede ser protegida adecuadamente por las salvaguardas normales o almacenada durante horas no laborables en contenedores aprobados.
- G. **Departamento** – Departamento de Seguridad Pública de Puerto Rico.
- H. **Derechos constitucionales** – Derechos que emanan de la Constitución de los Estado Unidos y de Puerto Rico.
- I. **Empleado** - Persona que rinde servicios en el DSP mediante nombramiento con estatus probatorio o regular en el servicio de carrera, en el servicio de confianza, transitorio o acuerdo interagencial.
- J. **Entorno de intercambio de información** (ISE, por sus siglas en inglés) - De acuerdo con la Sección 1016 de la Ley de Reforma de Inteligencia y Prevención del Terrorismo de 2004 (IRTPA, por sus siglas en inglés), y sus enmiendas, el ISE es un marco conceptual compuesto por las políticas, procedimientos y tecnologías que vinculan los recursos (personas, sistemas, bases de datos e

información) de las agencias estatales, locales, tribus y territorios (SLTT, por sus siglas en inglés); las agencias federales; y el sector privado para facilitar el intercambio de información relacionada con el terrorismo, el acceso a la misma y la colaboración.

- K. Funcionario** - Aquellas personas que ocupan puestos o cargos en el Departamento, que están investidos por la soberanía del Estado, por lo que intervienen en la formulación de política pública.
- L. Homeland Security Information Network o Red de Información de Seguridad Nacional (HSIN)** - Es una red de información utilizada por el Departamento de Seguridad Nacional de los Estados Unidos (DHS) y sus socios para compartir información relevante sobre seguridad, inteligencia y respuesta a emergencias. Esta red proporciona una plataforma segura para la comunicación y colaboración entre agencias gubernamentales, organismos de seguridad pública, personal de primera respuesta y otros socios clave en la protección de la patria. Su objetivo es mejorar la coordinación y la capacidad de respuesta en situaciones de seguridad nacional y emergencias. En español, se podría traducir como "Red de Información de Seguridad Nacional".
- M. Identificación Provisional** - Identificación provista por la Oficina de Seguridad Interna con el fin de identificar a todo visitante de la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis.
- N. Información** - Se refiere a datos procesados y organizados que tienen significado y utilidad para quienes los utilizan. Puede tomar diversas formas, como texto, imágenes, sonidos o números, y se utiliza para comunicar conocimiento, transmitir ideas o tomar decisiones.
- O. Información Personal de Identificación (PII en inglés)** - Es cualquier información que se pueda utilizar para identificar un individuo. Como regla general se considera PII, la siguiente información del individuo:
1. Nombre completo.
 2. Número de identificación nacional, cédula de identificación o seguro social.
 3. Número de pasaporte.
 4. Número de teléfono.
 5. Dirección postal completa.
 6. Dirección residencial completa.
 7. Dirección de correo electrónico.
 8. Número de licencia de conducir.

9. Fecha de nacimiento.
 10. Fotografía.
 11. Información de empleo.
 12. Información biométrica (ADN, huellas, voz).
 13. Información relacionada a la salud personal.
- P. Informe de Actividades Sospechosas (SAR en inglés)** - Documento utilizado por instituciones financieras y otras entidades para informar sobre actividades sospechosas que podrían indicar lavado de dinero, financiamiento del terrorismo u otras actividades delictivas. Estos informes se envían a las autoridades regulatorias para su investigación.
- Q. Inteligencia Criminal** - Se refiere al proceso de recopilación, análisis y aplicación de información para identificar y prevenir actividades delictivas o para apoyar la aplicación de la ley. Esto implica el uso de diversas fuentes de información, técnicas de análisis y tecnología para comprender y responder a las amenazas criminales. La inteligencia criminal ayuda a las agencias policiales y de seguridad a tomar decisiones informadas y estratégicas para abordar eficazmente la delincuencia y proteger a la comunidad.
- R. Law Enforcement Enterprise Portal (LEEP, por sus siglas en inglés)** - Plataforma segura para agencias policíacas, grupos de inteligencia y entidades de justicia criminal. LEEP proporciona herramientas de investigación y recursos analíticos basados en la web y los ofrecimientos de esta son únicos con respecto a con otras plataformas disponibles para las fuerzas de ley y orden. Los usuarios colaboran en un entorno seguro, utilizan herramientas para fortalecer sus casos y comparten documentos de sus agencias.
- S. Oficina de Seguridad Interna** – Oficina adscrita a la Oficina del Secretario, encargada de la seguridad de las facilidades del Departamento, de los visitantes y empleados.
- T. Privacidad** - Se refiere a los intereses de los individuos en la prevención de la recopilación, uso y divulgación inapropiada de PII. Los intereses de privacidad incluyen la privacidad de la conducta personal, la privacidad de las comunicaciones personales y la privacidad de los datos personales.
- U. Recepcionista** - Persona designada por el Secretario Auxiliar para recibir a los visitantes, contratistas y empleados en la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis. Será la persona encargada de mantener el control del Registro de Visitantes.

- V. **Registro de Empleados** – Documento donde se anotará la información de los empleados que laboran en los turnos de trabajo manejando los distintos sistemas de vigilancia, incluyendo fecha y horario trabajado.
- W. **Registro de Visitantes** - Documento que será completado por el Recepcionista donde se anotará la entrada y salida de toda persona que visite la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis y que será firmado por el visitante y/o contratista.
- X. **Secretario** – Secretario del Departamento de Seguridad Pública de Puerto Rico.
- Y. **Secretario Auxiliar** – Secretario Auxiliar de la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis.
- Z. **Terrorismo** – Uso ilegal o la amenaza de violencia para fines políticos, religiosos, ideológicos o sociales, con la intención de provocar miedo, intimidar o coaccionar a una población civil o a cualquier segmento de esta; o influir en la política de un gobierno mediante la intimidación o la coacción.
- AA. **Visitante** - Toda persona que acuda a la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis con un propósito oficial y legítimo. Incluye además, a los contratistas.

IV. **Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis (SAMISA)**

De conformidad con el Artículo 1.15 de la Ley Núm. 20-2017, se crea la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis (en adelante, SAMISA), la cual estará bajo la dirección de un Secretario Auxiliar, nombrado por el Secretario. La SAMISA tendrá las siguientes funciones:

- a. Asegurar el acceso y la continua e inmediata transferencia de información entre los diferentes Negociados a los fines de que cada uno de ellos pueda cumplir con las funciones, obligaciones y deberes.
- b. Establecer aquellos sistemas de comunicaciones que faciliten la operación eficiente del DSP y sus negociados y que, además, permitan y faciliten la comunicación interagencial durante situaciones de emergencia o desastre.

- c. Servir de enlace con las agencias federales para coordinar y compartir la información entre las distintas bases de datos estatales y federales.

V. Bases de Datos

La SAMISA procurará el más amplio acceso a todas las bases de datos de las agencias locales que sean pertinentes a las funciones del DSP, a las bases de datos de las agencias federales de seguridad, a las bases de datos de organismos internacionales de seguridad, y a cualquiera otra que sea consistente con los propósitos de esta Ley. La SAMISA procurará salvaguardar la confidencialidad de la información contenida en estas bases de datos y solo permitirá el acceso y el compartir de información, entre aquel personal autorizado.

A su vez, tendrá acceso y/o manejará, sin que se entienda como una limitación, los siguientes sistemas de información y bases de datos:

- Sistema DAVID+
- Registro Criminal Integrado (RCI)
- Registro de Armas de Fuego
- Sistema 9-1-1
- Centro de Fusión (Fusion Center)
- Sistema Autoexpreso
- Sistemas de Inteligencia, Informática y Bases de Datos de DCR
- Sistemas de Credenciales
- Sistema de Información Geográfica (GIS).
- Y cualquier base de datos o sistemas de información autorizado por el Secretario

No obstante, los sistemas de información y bases de datos del Negociado de Investigaciones Especiales se mantendrán separados e independiente del resto de los negociados que comprenden el Departamento, a los fines de garantizar la confidencialidad y pureza de las investigaciones.

VI. Composición de la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis

La SAMISA estará compuesta de las siguientes divisiones:

- División del Centro de Fusión
- División de Manejo de Información de Seguridad
- División de Coordinación Operacional y Logística.

A. División del Centro de Fusión

Se crea la División del Centro de Fusión (PRFC, por sus siglas en inglés), la cual estará bajo la dirección de un Director, designado por el Secretario. El PRFC estará integrado por las siguientes agencias y/o negociados:

1. Negociado de la Policía de Puerto Rico.
2. Negociado de Investigaciones Especiales.
3. Negociado para el Manejo de Emergencias y Administración de Desastres.
4. Departamento de Salud.
5. Departamento de Hacienda.
6. Departamento de Corrección y Rehabilitación.
7. Guardia Nacional de Puerto Rico.
8. Cualquier otra agencia estatal que el Secretario del DSP determine integrar.
9. Enlace con las agencias federales.

El PRFC tendrá la responsabilidad de recopilar, analizar, corroborar y diseminar información sobre asuntos relacionados a terrorismo doméstico e internacional, organizaciones transnacionales, ataques cibernéticos, infraestructura crítica, tráfico y contrabando de personas, fraude y nuevas modalidades para cometer actos criminales. Dicha información se compartirá con las diferentes unidades de investigación y de inteligencia municipal, estatal y federal a través de correo electrónico y en las plataformas de HSIN y LEEP.

Mantendrá en estricta confidencialidad la información que se trabaja en el PRFC y manejará información clasificada como No Clasificada Para Uso Oficial "U//FOUO"; No Clasificada pero Sensitiva "U//LES"; de acuerdo con los estándares de diseminación de cada uno. En caso de que la información esté clasificada secreta mantendrá los más estrictos estándares de seguridad y no manejará dicha información fuera del Cuarto Seguro certificado por el Departamento de Seguridad Nacional (DHS).

Atenderá toda solicitud de información por parte de un agente del orden público y realizará la búsqueda en la base de datos de conformidad con dicha solicitud. Será requisito que toda solicitud contenga número de querrela, caso o asunto.

B. División de Manejo de Información de Seguridad

Se crea la División de Manejo de Información de Seguridad, bajo la supervisión de un Director designado por el Secretario. Esta división será responsable de recopilar, evaluar, analizar y diseminar toda la información criminal de las actividades relacionadas al narcotráfico, crimen organizado, armas ilegales y cualquier otra actividad delictiva.

Tendrá la responsabilidad de compartir la información con las diferentes unidades de investigación criminales del Negociado de la Policía de Puerto Rico, Negociado de Investigaciones Especiales, agencias estatales, federales y/o municipales de ley y orden. Asimismo, analizar y corroborar el historial criminal de la persona sospechosa por medio de los sistemas computarizados disponibles, utilizando el formulario correspondiente.

Mantendrá informado al supervisor de la división de todos los aspectos de su área de trabajo incluyendo la actividad delictiva, y coordinará con las unidades de trabajo del NPPR y NIE, todo aspecto de información criminal que les compete. Conservará estrecha comunicación, coordinación y colaboración con diferentes agencias locales y federales a fin de poder intercambiar información relacionada a la inteligencia criminal. Verificará diariamente los informes relacionados a los asesinatos para analizar si algunas de las víctimas están relacionadas al crimen organizado o alguna investigación en curso. Analizará y diseminará toda la información recibida a través del "*National Integrated Ballistic Information Network*" (NIBIN), donde se vinculen múltiples casos de asesinatos.

Del mismo modo, tendrá la responsabilidad de recopilar, analizar, corroborar, y diseminar información sobre asuntos relacionados a los crímenes financieros y todas las actividades delictivas. Dicha información se compartirá con las diferentes unidades del NPPR y NIE, así como otras agencias estatales y/o federales con acuerdo colaborativo existente. Realizará análisis financieros confidenciales sobre la economía de las organizaciones criminales, con el fin de detectar la procedencia del capital y el flujo de este en la búsqueda de lavado de dinero.

Operará los siguientes sistemas:

- Sistema Unificado de Reconocimiento Facial (SURF)
- Monitoreo de las cámaras corporales.
- Sistema de lectura de tablillas de vehículos de motor (LPR, por sus siglas en inglés).
- Centro de Seguridad del monitoreo de cámaras de circuito cerrado (CCTV, por sus siglas en inglés), entre otros.
- Cualquier otra base de datos o sistemas de información autorizado por el Secretario

C. División de Coordinación Operacional y Logística

Se crea la División de Coordinación Operacional y Logística, bajo la supervisión de un Director designado por el Secretario. Esta división será responsable de brindar todo el apoyo operacional a las demás divisiones de la SAMISA y a los negociados en los asuntos de

Tendrá la responsabilidad de desarrollar estrategias para abordar problemas criminales específicos y evaluar la efectividad de las medidas tomadas. Además, coordinará las actividades operativas y logísticas necesarias para recopilar, analizar y utilizar la información relacionada con actividades delictivas. Esto puede incluir la planificación y ejecución de operaciones, la gestión de recursos humanos y materiales, la coordinación con otras agencias y la supervisión de la logística para garantizar que los análisis de información se realicen de manera efectiva y eficiente.

VII. Normas de Seguridad y Control de Acceso

A. Normas de Seguridad:

1. No se permite la portación de armas de fuego, excepto los agentes del orden público y aquellos funcionarios autorizados por ley a portar un arma de fuego, debidamente identificados.
2. No se permite la entrada de animales, excepto aquellos que estén debidamente entrenados para servir de guía o de servicio, así como aquellos que estén entrenados para asuntos de seguridad, acompañados de un Agente del Orden Público.
3. Todo visitante deberá estar acompañado, en todo momento, por un empleado adscrito a la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis durante el tiempo de la visita.

B. Control de Acceso:

1. Toda persona que visite la Secretaría Auxiliar de Manejo de Información de Seguridad y Análisis registrará su entrada y salida en el formulario de Registro de Visitantes Digital. Dicho registro ubicará en la recepción de la SAMISA.
2. Además, utilizará la identificación provisional que se le entregará en la Oficina de Seguridad Interna durante el tiempo que esté visitando las facilidades.

VIII. Registro de solicitudes de búsqueda de información

A. Toda búsqueda de información en los sistemas y/o bases de datos deberá cumplir estrictamente el siguiente procedimiento:

1. El solicitante deberá cumplimentar y firmar el formulario titulado "Solicitud de Búsqueda en los Sistemas de Información Criminal".
2. El supervisor del analista asignado autorizará, mediante su firma, la búsqueda en los sistemas de información y asignará un número de control, con el siguiente código:

- a. Las búsquedas realizadas por la División del Centro de Fusión llevarán las siglas del DSP, las siglas PRFC, año y número correlativo. A modo ilustrativo: DSP-PRFC-AÑO-00000.
 - b. Las búsquedas realizadas por la División de Manejo de Información de Seguridad llevarán las siglas del DSP, las siglas DMIS, año y número correlativo. A modo ilustrativo: DSP-DMIS-AÑO-00000.
3. El analista realizará la búsqueda, cumplimentará el encasillado identificado "Para Uso Oficial" y firmará el documento. A su vez, será responsabilidad del supervisor firmar el formulario una vez se complete la búsqueda y antes de entregar la información al solicitante.
- A. Cada división deberá tener un libro de registro donde se identifiquen, con número de control, todas las búsquedas a realizarse, previa autorización el supervisor.
 - B. Cada supervisor tendrá la responsabilidad de realizar una auditoría, semanal, en los sistemas y bases de datos sobre toda búsqueda realizada por los empleados bajo su supervisión.
 - C. Será responsabilidad de cada supervisor remitir un informe mensual al Secretario Auxiliar sobre todas las búsquedas realizadas, cumplimentando el formulario titulado "Informe Mensual de Búsquedas en los Sistemas de Información Criminal y/o Bases de Datos".

IX. Designación del Personal y Equipo

- A. Previa autorización del Secretario asignará equipo, materiales y vehículos necesarios para las tareas diarias del personal.
- B. El empleado deberá tener conocimiento en manejo de computadoras, sistema operativo de Windows, así como en programas como Word, Excel, PowerPoint y Outlook.
- C. El empleado asignado no podrá tener señalamientos, ya sean activos o sostenidos, en los últimos cinco (5) años por las siguientes causales:
 1. Uso de la Fuerza
 2. Arrestos o Detenciones ilegales o irrazonables
 3. Registros, allanamientos e incautaciones ilegales o irrazonables
 4. Acometimiento y/o agresiones injustificadas o excesivas

5. Uso de violencia injustificada, coacción física o psicológica contra una persona arrestada
6. Conducta inmoral
7. Agresión física
8. Maltrato Verbal
9. Uso indebido de sustancias controladas
10. Violencia Doméstica
11. Violación de Derechos civiles
12. Hostigamiento sexual
13. Discrimen

X. Uso indebido o ilícito de los equipos o sistemas

El personal del DSP, personal en destaque de otra agencia estatal o federal y/o contratista independiente, incluyendo los empleados de ésta, que haga uso indebido o ilícito de los equipos o sistemas de la SAMISA incurrirá en falta, violación a la Ley de Ética Gubernamental o delito según tipificado por el Código Penal y se procederá conforme dicte la ley o reglamento. Se dispone que, en cuanto al proceso disciplinario, los miembros del sistema de rango del NPPR estarán sujetos al Reglamento 9001 "Reglamento para Enmendar el Artículo 14 del Reglamento de Personal de la Policía de Puerto Rico" o su equivalente vigente.

XI. Jurisdicción

La jurisdicción de la SAMISA será el espacio terrestre, marítimo y aéreo que, de Puerto Rico, según lo dispone el Artículo I, sección 3 de la Constitución de Puerto Rico.

XII. Disposiciones Generales

A. Interpretación

1. Las palabras y frases utilizadas en esta Orden Administrativa se interpretan según el contexto y el significado sancionado por el uso común y corriente.
2. Los términos usados en esta Orden Administrativa en el tiempo futuro incluyen también el presente, los usados en el género masculino incluyen el femenino y el neutro, salvo los casos en los cuales tan interpretación resulte absurda; el número singular incluye el plural y viceversa.

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

B. Cumplimiento

1. Los supervisores y personal del a SAMISA se asegurarán del cumplimiento de esta Orden Administrativa, así como de que aquel personal que infrinja en cualquiera de las disposiciones contenidas en esta política será remitido a la Oficina de Responsabilidad Personal del Departamento de Seguridad Pública.
2. No se permitirá la grabación de imágenes y/o audio en teléfonos celulares, cámaras y/o cualquier otro equipo electrónico diseñado para esos fines, en las instalaciones de la SAMISA y en contra del personal que no sea el equipo autorizado y asignado por el DSP.
3. Toda información recopilada, almacenada y eliminada por el PRFC, SIAC y RTCC, será conforme con el estatuto 28 CFR Part 23.
4. El personal asignado al SAMISA y todas sus unidades, tomará adiestramientos presenciales o a través del web relacionados a, pero sin limitarse al análisis de inteligencia, organizaciones transnacionales, gangas, ataques cibernéticos, Sistema de Información Geográfica y de cualquier plataforma o base de datos que se utilice.
5. Cada año todos los analistas del PRFC, SIAC y Real Time deben certificarse en 28 CFR Part 23. Los analistas que tengan una clasificación de seguridad "SECRET" deben tomar el "Annual Security Refresher Briefing".

XIII. Derogación

Esta Orden Administrativa deroga cualquier orden administrativa anterior que sea contraria a las disposiciones de ésta.

XIV. Cláusula de Separabilidad

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

XV. Vigencia

Esta Orden Administrativa entrará en vigor el 25 de abril de 2024.



Alexis Torres Ríos
Secretario