REGLAMENTO INTERIOR DEL SECRETARIADO EJECUTIVO DEL SISTEMA ESTATAL DE SEGURIDAD PÚBLICA

PERIÓDICO OFICIAL NO. 34 DÉCIMA TERCERA SECCIÓN, AGOSTO 20 DEL 2025

DIRECCIÓN DE OPERACIONES DE TECNOLOGÍAS DE INFORMACIÓN

Artículo 39.- La persona titular de la Dirección de Operaciones de Tecnologías de Información tendrá las facultades y obligaciones siguientes:

I. Participar en la operación e instrumentación de las tecnologías de información del Secretariado Ejecutivo y las que solicite el Secretariado Ejecutivo Nacional para satisfacer las necesidades de procesamiento e intercambio de información seguros, para la coordinación y colaboración de los tres órdenes de gobierno en la investigación de delitos.
II. Colaborar en el procesamiento de la información que genere en el Secretariado Ejecutivo para producir productos de inteligencia operables;
III. Proponer e implementar las estrategias de seguridad de información del Secretariado Ejecutivo para la prevención y atención de incidentes de seguridad y la continuidad de las operaciones de las tecnologías de información;
IV. Presentar a la persona titular del Secretariado Ejecutivo elementos para el diseño y desarrollo de la estrategia y política estatal de ciberseguridad ciudadana que contendrá las acciones
necesarias para reducir riesgos a las operaciones de tecnología de información, proteger la información, los bienes, los derechos de las personas y su seguridad;
V. Generar y ejecutar protocolos y mecanismos para la prevención, disuasión, contención y desactivación de riesgos y amenazas a las tecnologías de información, así como para la preservación de la evidencia digital;
VI. Crear y operar un Centro Estatal de Respuesta a Incidentes de tecnología de información, tanto públicos como privados;
VII. Apoyar en las actividades para la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades de tecnología de información que apoyen la toma de decisiones;
VIII. Plantear a la persona titular del Secretariado Ejecutivo la adquisición, administración, normalización, desarrollo y evaluación de tecnologías de información especializadas para la investigación y difusión confiable de la información análoga o digital de los tres niveles de gobierno en materia de seguridad ciudadana, así como para la protección de la información e infraestructura asociadas;
IX. Implementar mecanismos de coordinación pública y privada con procedimientos y recursos específicos que permitan el cumplimiento de los objetivos de prevención, investigación, ciber inteligencia, disuasión, procuración e impartición de justicia;
X. Definir medidas de seguridad y mapas de riesgos de las infraestructuras críticas de información, basadas en un análisis transversal de riesgos que considere a todos los sectores;

XI. Coadyuvar en el desarrollo de mecanismos de prevención, atención y respuesta frente a ataques cibernéticos contra las infraestructuras críticas de información, en coordinación con las instancias competentes tanto nacionales como internacionales;
XII. Fungir como un órgano de consulta y coordinador de actividades de los entes públicos, municipios y la iniciativa privada para realizar las funciones de ciberseguridad en la Entidad; XIII. Contribuir en el diseño y realización de programas que promuevan el fortalecimiento de la cultura de la ciberseguridad estatal y de prevención en el uso indebido de tecnologías de información y comunicación;
XIV. Coordinar programas para fortalecer la seguridad de información y ciberseguridad, a través de la formación, capacitación y certificación del personal servidor público y la ciudadanía, con instituciones educativas, centros de investigación, entidades públicas y privadas tanto nacionales como internacionales;
XV. Formular criterios técnicos, desarrollo de aplicaciones y tecnologías de la información de vanguardia para la detección, monitoreo, pronóstico y medición de riesgos en las tecnologías de la información y comunicaciones;
XVI. Proponer a la persona titular del Secretariado Ejecutivo acciones y estrategias para mejorar la ciberseguridad en empresas, especialmente micro, pequeñas y medianas empresas (MIPYMES);
XVII. Emitir opinión sobre la armonización legal en materia de ciberseguridad, para contar con instrumentos estatales para el cumplimiento de los objetivos estratégicos;
XVIII. Auxiliar a las unidades administrativas, en la auditoría y el cumplimiento normativo de las políticas de seguridad de información en los términos, plazos y condiciones pactados en los contratos de adquisición, arrendamiento de bienes de informática, telecomunicaciones o equipos especializados o prestación de servicios relacionados con ellos;
XIX. Participar en convenios específicos de colaboración con la iniciativa privada, centros de investigación, instituciones universitarias públicas y privadas en México, para desarrollar proyectos específicos de transferencia tecnológica, investigación básica y aplicada de interés para el Secretariado Ejecutivo;
XX. Proponer la implementación de tecnologías de punta y ciberseguridad en el Secretariado Ejecutivo, y
XXI. Las demás que le encomiende la persona titular del Secretariado Ejecutivo y disposiciones aplicables.

Artículo 40.- La persona titular del Departamento de Operación de la Seguridad de la Información tendrá las facultades y obligaciones siguientes:

I. Vigilar el correcto funcionamiento de los componentes virtuales y físicos de Tecnologías de Información empleados para el intercambio de información entre las Dependencias y Entidades de los órdenes de gobierno;
II. Determinar las estrategias de operación de seguridad de Información para implementar medidas operativas para la prevención y atención de incidentes cibernéticos, continuidad de las operaciones de tecnología de información;
III. Proponer elementos para el diseño y desarrollo de la Política Estatal de Ciberseguridad Ciudadana, la Estrategia Estatal de Ciberseguridad Ciudadana, y el Marco de Gobierno, Riesgo y Cumplimiento;
IV. Gestionar el uso del Registro Nacional y Estatal de Incidentes Cibernéticos;

V. Implementar el Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital;
VI. Realizar el Protocolo de Gestión de Incidentes Cibernéticos para la contención y mitigación de amenazas cibernéticas a las Infraestructuras Críticas de Información;
VII. Establecer mecanismos de coordinación y colaboración de los equipos de respuesta a incidentes públicos y privados a través del establecimiento de un Equipo Estatal de Respuesta a Incidentes Cibernéticos;
VIII. Definir medidas de seguridad de información y mapa de riesgos de las Infraestructuras Críticas de Información, basadas en un análisis transversal de riesgos que considere a todos los sectores críticos;
IX. Formular medidas de prevención, disuasión, contención y desactivación de riesgos y amenazas que pretendan vulnerar a través del ciberespacio las garantías individuales o los derechos humanos, instituciones estatales, la gobernabilidad democrática o el Estado de Derecho;
X. Desarrollar y evaluar programas que promuevan el fortalecimiento de la cultura de la ciberseguridad estatal y la prevención en el uso indebido de tecnologías de información y comunicación;
XI. Prestar auxilio técnico a cualquiera de las instancias estatales de gobierno representadas en el Consejo o son parte de la Administración Pública Estatal o iniciativa privada conforme a los acuerdos que se adopten en su seno; y
XII. Las demás que le encomiende la persona titular de la unidad administrativa y disposiciones aplicables.