DIP. JESÚS SESMA SUÁREZ,
PRESIDENTE DE LA MESA DIRECTIVA DEL
CONGRESO DE LA CIUDAD DE MÉXICO,
III LEGISLATURA
P R E S E N T E.

I. ENCABEZADO

El suscrito Diputado Mario Enrique Sánchez Flores, integrante del Grupo Parlamentario del Partido Acción Nacional, de la III Legislatura del Congreso de la Ciudad de México, con fundamento en lo dispuesto por el artículo 122, Apartado A, Fracción II de la Constitución Política de los Estados Unidos Mexicanos; 10 Apartado C, 29, Apartado A, numeral 1 y Apartado D incisos a) y b); y 30 fracción I inciso b) de la Constitución Política de la Ciudad de México; 1, 12 fracción II y 13 fracción LXXIV de la Ley Orgánica del Congreso de la Ciudad de México, así como el 1, 2 fracción XXI, 5 fracción I, 95 fracción II y 96 del Reglamento del Congreso de la Ciudad de México, someto a la consideración de este H. Congreso **Iniciativa con Proyecto de Decreto por el que se adicionan diversas disposiciones a la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal, en materia de pruebas obligatorias, mantenimiento y publicación mensual de fallas y tiempos de reparación de la infraestructura de seguridad**, al tenor de lo siguiente:

ANTECEDENTES

La Ciudad de México ha construido en la última década un **andamiaje tecnológico** para seguridad y justicia cívica (C2/C5, 911, cámaras, lectoras de placas, semáforos y controladores, botones de auxilio, radio de despacho, sistemas de denuncia y módulos de atención a víctimas). Este ecosistema, valioso pero **heterogéneo en origen y antigüedad**, opera con contratos y estándares dispares. Cuando falla, **la ciudad invisible se detiene**: emergencias que tardan más en atenderse, investigaciones sin evidencia útil y sanciones cuestionadas.

a) Patrón de fallas en C5 y 911

- **Intermitencias y caídas parciales** de despacho, radiocomunicación o geolocalización por sectores, especialmente en picos (marchas, eventos masivos, lluvias intensas, sismos).
- **Ventanas sin grabación** o pérdida temporal de streaming por fallas de almacenamiento/replicación, lo que impide reconstruir hechos.
- **Congestión de llamadas** y tiempos de espera elevados en 911, con tasas de abandono que comprometen la atención oportuna.
- **Desfase horario (NTP)** entre equipos y servidores que invalida sellos de tiempo y afecta la **cadena de custodia**.

- **Dependencia de terceros** (enlaces, energía, sitios de hospedaje) sin métricas públicas de disponibilidad ni mecanismos claros de **continuidad operativa**.
- **Fallas de redundancia** (respaldos, enlaces, energía) que transforman incidentes menores en interrupciones mayores.

b) Cámaras no operativas al denunciar: el "no hay video"

Cuando una persona acude a denunciar o reportar un hecho, es frecuente que se encuentre con respuestas como: **la cámara estaba en mantenimiento**, **no grabó**, **no apuntaba al sitio** o la **resolución no permite identificar**. Las causas típicas son:

- **Mantenimiento preventivo insuficiente** (lentes sucios, carcasas dañadas, conectores sulfatados, antenas desalineadas).
- **Vandalismo u obstrucciones** sin reposición oportuna.
- **Ángulos y parametrización inadecuados** (WDR, FPS, bitrate, rotación, zonas de interés).
- **Retención de video insuficiente** o sin respaldo alterno.

- **Pérdida de metadatos** (ubicación, hora, hash) que debilita el valor probatorio.

  Resultado: **menor capacidad de investigación**, **desincentivo a denunciar** y **desconfianza ciudadana**.

c) Infracciones electrónicas y equipos de medición: "multas fantasma" y calibración

Las sanciones por exceso de velocidad u otras infracciones apoyadas en dispositivos de medición son **controvertidas** cuando:

- El equipo **carece de calibración vigente** o **reprobó pruebas**;
- No existe **constancia** de la última prueba, parámetros y tolerancias;
- Hay **divergencia de reloj**, metadatos incompletos o mala identificación de placas;
- La evidencia **no incorpora** el **hash**/sello de tiempo o no es posible verificar su integridad. Ello da pie a **"multas fantasma"**, litigios y percepción de que el enfoque es **recaudatorio**, no preventivo. La solución es simple: **pruebas obligatorias**, **calibración certificada** y **efectos procesales claros** (si no hay integridad, la evidencia **no es válida**).

d) Gobernanza contractual y de activos: fragmentación y opacidad

- **Inventarios inconexos** por dependencia o proveedor; activos sin **identificador único** ni **trazabilidad** de intervenciones.
- Contratos por **silos tecnológicos** que **no** incorporan **SLA**, métricas (disponibilidad, MTTR, MTBF) ni **bonos/penalidades**.
- **Bitácoras físicas** o cerradas que impiden auditar y comparar desempeño entre proveedores y Alcaldías.
- Ausencia de **APIs** y tableros públicos con series históricas.

e) Vacíos normativos

Hoy **no existe** un estándar legal uniforme que obligue a:

1. Realizar **pruebas periódicas** (funcionales, de recuperación, de integridad y **calibración**);
2. Mantener un **Inventario Único de Activos** con trazabilidad;
3. Establecer **metas de servicio** por severidad (SLA con tiempos máximos de reparación);
4. **Publicar mensualmente** fallas y tiempos de reparación en **datos abiertos**, con agregación territorial (**cuadrante/colonia/AGEB**) para proteger la operación.

f) Impactos acumulados

- **Seguridad ciudadana**: mayor tiempo de respuesta y menor disuasión.

- **Derechos de las víctimas**: investigación debilitada por falta de evidencia útil.
- **Debido proceso**: sanciones vulnerables cuando la evidencia proviene de equipos **sin calibración** o **sin pruebas**.
- **Recursos públicos**: gasto ineficiente por **reparaciones reactivas** y litigios.
- **Confianza**: narrativa oficial de "tecnología de punta" sin **datos verificables** de disponibilidad.
- **Gestión del riesgo**: incidentes repetitivos por ausencia de **mejora continua** y **lecciones aprendidas**.

g) Buenas prácticas aplicables

La experiencia internacional es consistente: sistemas críticos se administran con **gestión de servicios y activos** (p. ej. marcos tipo ITSM/ITIL, ISO de gestión de servicios y seguridad de la información), **metrología** para equipos de medición (calibración con trazabilidad y tolerancias) y **transparencia proactiva** (datos abiertos con series históricas). Común denominador:

- **Pruebas calendarizadas**, **listas de verificación** y **evidencia** de cierre;
- **SLA medibles** (disponibilidad, MTTR, MTBF) con **penalidades y bonificaciones**;

- **Monitoreo 24/7** (NOC/SOC) con alertamiento y tickets trazables;
- **Inventarios vivos** y **APIs**;
- Publicación en **datos abiertos** con resguardos de seguridad y privacidad.

h) Justificación de la reforma

La reforma propone **tres palancas**:

1. **Pruebas obligatorias** y **calibración certificada**, con evidencia técnica verificable;
2. **Gestión con métricas** (inventario único, severidad, disponibilidad, MTTR, MTBF) y **tiempos máximos de reparación**;
3. **Transparencia mensual** en datos abiertos (tablero público, series históricas e informes al Congreso).

   Con ello se atiende el **problema estructural**: C5/911 con fallas recurrentes, **cámaras inoperantes** al denunciar y **multas electrónicas** sin respaldo técnico suficiente. La regla central es simple y garantista: **sin calibración vigente o con pruebas reprobadas, la evidencia no es utilizable**; y todo lo demás debe **medirse y publicarse**.

EXPOSICIÓN DE MOTIVOS

En la Ciudad de México operan miles de equipos y sistemas que sostienen la seguridad pública y la justicia cívica: cámaras del C5, lectoras de placas, cinemómetros, alcoholímetros, semáforos y controladores, radios de despacho, software de denuncias, módulos de atención a víctimas, patrullas y sus dispositivos periféricos, entre otros. Cuando esta infraestructura falla o no está calibrada, se compromete la seguridad de las personas, se vulnera el debido proceso y se mina la confianza pública.

Hoy no existe un estándar legal uniforme que obligue a **realizar pruebas periódicas de funcionamiento e integridad** ni a **publicar mensualmente la información de fallas y tiempos de reparación** con criterios de datos abiertos. La opacidad ha permitido que el Gobierno local presuma capacidad tecnológica sin acreditar su **disponibilidad real**, la **calibración** de instrumentos de medición (p. ej. cinemómetros) o los **tiempos de recuperación** ante incidentes.

Para la ciudadanía, esto se traduce en riesgos concretos:

- Ausencia de video en hechos de alto impacto;
- Invalidación de infracciones por equipos sin verificación;
- Zonas con luminarias o semáforos fuera de servicio por semanas;
- Deficiencias en módulos y sistemas que atienden a víctimas.

La presente iniciativa responde con tres ejes:

1. **Pruebas obligatorias** de funcionamiento, integridad, seguridad y calibración, con evidencia técnica verificable;
2. **Gestión de mantenimiento basada en métricas** (inventario, MTBF, MTTR, disponibilidad, severidad de fallas), con metas y servicio por niveles (SLA) para entes públicos y proveedores;
3. **Transparencia obligatoria mensual**: publicación en datos abiertos de fallas y tiempos de reparación, con salvaguardas de seguridad operativa y datos personales.

Beneficios esperados:

- Mejora de tiempos de atención y reducción de reincidencia de fallas;
- Evidencia confiable para procedimientos cívicos y penales;
- Control de calidad a proveedores y contratistas;
- Rendición de cuentas al Congreso y a la sociedad.

La propuesta se alinea con los principios de parlamento abierto, máxima publicidad, buena administración y protección de derechos de víctimas y de personas sujetas a procedimientos de justicia cívica.

La Suprema Corte de Justicia de la Nación ha establecido en la tesis 2024232 que la implementación y uso de sistemas de videovigilancia deben sujetarse a los principios de legalidad, necesidad, proporcionalidad y finalidad, garantizando la integridad técnica y la trazabilidad de los medios electrónicos empleados para la obtención de pruebas, de modo que su validez jurídica dependa de un adecuado mantenimiento y calibración de los equipos. Asimismo, en el Amparo en Revisión 307/2016, la Primera Sala precisó que la omisión estatal en la conservación o funcionamiento de infraestructura pública esencial puede constituir una violación al derecho a la seguridad y al acceso a la justicia, al poner en riesgo la vida o integridad de las personas.

Ambos criterios reafirman la obligación de las autoridades locales de asegurar que los sistemas tecnológicos empleados en tareas de seguridad, movilidad y justicia cívica operen bajo estándares verificables de disponibilidad, integridad y transparencia, como los que se establecen en el presente instrumento legislativo.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, conocido como Reglamento General de Protección de Datos (GDPR), establece que la protección de las personas físicas en relación con el tratamiento de datos personales constituye un derecho fundamental, conforme al artículo 8 de la Carta de los Derechos Fundamentales de la

Unión Europea y al artículo 16 del Tratado de Funcionamiento de la Unión Europea. Su objetivo es garantizar que el uso de tecnologías para la recopilación, gestión y transferencia de datos se realice con pleno respeto a las libertades y derechos fundamentales, asegurando la integridad, disponibilidad y seguridad de los sistemas que los procesan. Este marco normativo subraya que la tecnología debe servir a la humanidad, por lo que su empleo en tareas de seguridad, justicia o administración pública debe regirse por los principios de legalidad, proporcionalidad, transparencia y responsabilidad técnica, buscando siempre un equilibrio entre el interés público y la protección de los derechos individuales.

La prevención del delito se ha consolidado como el pilar de la seguridad ciudadana, respaldada por organismos internacionales que promueven soluciones sostenibles.

De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito, los países que invierten en tecnología de seguridad, políticas de proximidad y participación social logran reducciones sostenidas en sus índices de criminalidad.

Expertos de Seguritech señalan que en México, donde los delitos de alto impacto continúan representando un desafío, se requieren enfoques a prevención del delito se ha consolidado como el pilar de la seguridad

ciudadana, respaldada por organismos internacionales que promueven soluciones sostenibles. De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito, los países que invierten en tecnología de seguridad, políticas de proximidad y participación social logran reducciones sostenidas en sus índices de criminalidad.

Expertos de Seguritech señalan que en México, donde los delitos de alto impacto continúan representando un desafío, se requieren enfoques innovadores que integren vigilancia, análisis de datos y colaboración comunitaria. Informes del Banco Interamericano de Desarrollo, destacan que la inversión en sistemas de videovigilancia, programas de prevención temprana y anlítica predictiva reduce hasta en 30 por ciento los delitos violentos en zonas urbanas.

Ariel Picker, CEO de Seguritech, señala que el uso de big data e Inteligencia Artificial permite anticipar patrones delictivos y mejorar la capacidad de respuesta de las fuerzas de seguridad, fortaleciendo la confianza ciudadana y la cooperación entre gobiernos locales y federales.

CONSIDERANDOS

PRIMERO. Idoneidad. Para garantizar seguridad pública efectiva y debido proceso, es indispensable que los equipos y sistemas que generan evidencia o soportan la operación estén probados, calibrados y disponibles. La obligación de realizar pruebas con periodicidad definida y de mantener un inventario trazable es una medida idónea para asegurar continuidad del servicio y confiabilidad probatoria.

SEGUNDO. Necesidad. Actualmente no hay un marco homogéneo que obligue a medir y a publicar fallas y tiempos de reparación; por ello, la transparencia proactiva y la fijación de SLA mínimos resultan necesarias para cerrar brechas de información y para alinear incentivos con proveedores y áreas operativas.

TERCERO. Proporcionalidad. La iniciativa limita riesgos operativos al ordenar que la publicación se haga con agregación geográfica (cuadrante, colonia o AGEB) y prevé exclusiones por fuerza mayor y mantenimientos programados; de esta manera, se protege la seguridad operativa y los datos personales sin sacrificar la rendición de cuentas.

CUARTO. Eficacia y mejora continua. Al establecer metas de disponibilidad y tiempos máximos de reparación por severidad, y al exigir evidencia de cierre de las intervenciones, se crea un sistema de mejora continua que

reduce reincidencias, estandariza la calidad del servicio y robustece la validez de las sanciones derivadas de equipos de medición.

QUINTO. Integridad probatoria y derechos. Se protege el debido proceso al impedir el uso de evidencias provenientes de equipos sin calibración vigente o con pruebas reprobadas, y al exigir que toda infracción electrónica incorpore constancias de calibración e integridad del equipo.

SEXTO. Transparencia y control legislativo. La publicación mensual en datos abiertos y los informes trimestrales permiten supervisión social y parlamentaria, así como comparabilidad entre dependencias y Alcaldías mediante métricas estandarizadas (MTBF, MTTR, disponibilidad).

ORDENAMIENTOS A MODIFICAR

1. Con base en las consideraciones anteriores, se propone la adición de un capítulo IX a la **Ley que Regula el Usos de Tecnología para la Seguridad Pública del Distrito Federal** con el siguiente texto:

Ley que Regula el Usos de Tecnología para la Seguridad Pública del Distrito Federal	
TEXTO NORMATIVO VIGENTE	**TEXTO NORMATIVO PROPUESTO**
Sin correlativo	Capítulo IX Del Mantenimiento, Pruebas y Transparencia de la Infraestructura Tecnológica de Seguridad Artículo 46. Definiciones**.** Para efectos de este Capítulo se entiende por: I. Infraestructura Crítica de Seguridad y Justicia (ICSyJ): Conjunto de equipos, sistemas, software y mobiliario urbano que soportan funciones de seguridad pública, protección civil y justicia cívica (incluye, de manera enunciativa: cámaras y servidores del C2/C5, lectoras de placas, cinemómetros, alcoholímetros, radios, patrullas y periféricos, semáforos, luminarias de seguridad, botones de auxilio, kioscos de denuncia, módulos de atención a víctimas, sistemas de cadena de custodia digital y plataformas de gestión). II. Falla: Evento que impide o degrada el servicio conforme a especificaciones. III. Tiempo Medio Entre Fallas (MTBF): Intervalo promedio entre fallas. IV. Tiempo Medio de Reparación (MTTR): Tiempo promedio desde la detección a la restauración del servicio. V. Disponibilidad: Porcentaje de tiempo que el activo presta servicio conforme a especificación. VI. Pruebas de Integridad: Conjunto de verificaciones funcionales, de seguridad, de calibración o de recuperación, según aplique al activo.

	VII. Inventario Único de Activos (IUA): Registro oficial, estandarizado y público de la ICSyJ. VIII. SLA (Acuerdos de Nivel de Servicio): Conjunto de métricas, metas y condiciones de medición, con exclusiones, escalamiento y consecuencias (penalizaciones/bonos), que obligan a las dependencias y proveedores a garantizar la disponibilidad, tiempos de reparación y calidad de la infraestructura de seguridad y justicia cívica. Artículo 47. Inventario y trazabilidad. Las dependencias y Alcaldías responsables deberán: I. Integrar y mantener actualizado el Inventario Único de Activos (IUA) con identificador único, tipo, fabricante, serie, ubicación (con niveles de agregación por seguridad), responsable, proveedor y estado operativo; II. Etiquetar cada activo con su identificador y código QR para consulta de su ficha técnica pública; III. Registrar cada incidencia, intervención de mantenimiento, refacción y actualización, con sello de tiempo. Artículo 48. Pruebas obligatorias. Las dependencias y Alcaldías responsables deberán realizar pruebas obligatorias en la ICSyJ a su cargo con las siguientes temporalidades: I. Mensuales: verificación funcional y de disponibilidad de todos los activos de la ICSyJ; II. Trimestrales: pruebas de recuperación y respaldo en sistemas informáticos y de video; III. Semestrales: calibración certificada de equipos de medición (cinemómetros, alcoholímetros, balanzas, sonómetros, etc.);

	IV. Anuales: pruebas de integridad de cadena de custodia digital y auditoría técnica de una muestra representativa por tercero independiente; Toda prueba generará dictamen técnico con evidencia (logs, fotografías, video, bitácoras, parámetros), resguardado y publicable en versión anonimizada. Artículo 49. Metas de servicio y tiempos de reparación (SLA). Las dependencias y Alcaldías responsables deberán mantener los siguientes parámetros mínimos y máximos respecto a su ICSyJ: I. Disponibilidad mínima anual por tipo de activo: ● Cámaras y lectoras de placas: igual o mayor a 95%; ● Semáforos de cruces principales: igual o mayor a 98%; ● Botones de auxilio y módulos de denuncia: igual o mayor a 95%; ● Plataformas críticas (C5, despacho y radiocomunicación): igual o mayor a 99.5% (exceptuando los mantenimientos programados). II. Tiempos máximos de reparación desde reporte: ● Falla crítica nivel 1 (riesgo a la vida / alto flujo vial): en menos de 24 horas; ● Falla mayor nivel 2: en menos de 72 horas; ● Falla menor nivel 3: en menos de 7 días hábiles. III. Los contratos incluirán penalidades automáticas por incumplimiento de SLAs. Artículo 50. Clasificación de severidad de fallas. I. Criterios generales. La severidad se determina con base en: a. Riesgo inmediato a la vida o integridad, b. Afectación a la continuidad del servicio, c. Impacto probatorio o de justicia cívica, d. Alcance territorial/volumétrico de la afectación; y

	e. Pérdida de redundancia. II. Definiciones operativas. Alto flujo vial: Intersección o tramo clasificado como vía primaria por la autoridad competente, o con Volumen Medio Diario ≥ 18,000 vehículos/día, o flujo peatonal ≥ 2,000 personas/hora en hora pico. Ante ausencia de medición reciente, se aplicará el catálogo oficial de vías primarias y estaciones de transporte masivo. Cuadrante: Unidad operativa definida por la SSC/C5 para despacho. Indisponibilidad: Imposibilidad de prestar el servicio conforme a especificación por más de 3 minutos continuos, salvo que se señale otro umbral. III. Niveles de severidad. 1. Falla crítica – Nivel 1 (riesgo a la vida / alto flujo vial): a. Semáforos: apagado total o destello no programado en cruce de alto flujo vial o con cruce peatonal de alto riesgo; controlador fuera de servicio sin respaldo en corredores principales. b. 911/C5/Despacho: caída total del servicio de despacho, radiocomunicación o geolocalización en un sector por más de 5 minutos o a nivel ciudad por más de 1 minuto; pérdida de grabación/streaming mayor o igual al 50% de cámaras de un cuadrante por más 15 min. c. Botones de auxilio y puntos seguros: inoperantes en estaciones de transporte masivo, escuelas, hospitales o espacios con protocolos de violencia de género. d. Equipos de medición (cinemómetros, alcoholímetros): sin calibración vigente o con prueba reprobada mientras están en operación; cadena de custodia digital con hash/sello de tiempo inválido.

	e. Eventos masivos/emergencias: falla de infraestructura crítica en el perímetro de 500 metros de eventos masivos autorizados o durante atención de emergencia activa. f. Cobertura: caída simultánea de más del 30% de cámaras, lectoras o sensores de un cuadrante por más de 30 min. 2. Falla mayor – Nivel 2: a. Semáforos: fase o cara apagada, desincronización grave o detección faltante en cruce no clasificado de alto flujo. b. Sistemas: indisponibilidad de módulos no críticos del C5/denuncia por más de 30 min con alternativa temporal; pérdida de redundancia (respaldos, enlaces o energía) en plataformas críticas aún con servicio activo. c. Video y sensores: caída de entre el 10 y el 30% de cámaras/sensores de un cuadrante por más de 30 min; cámara individual fuera en zona prioritaria (polígono con alta incidencia). d. Atención a víctimas: módulos operativos con hardware caído (impresoras para medidas de protección, captura biométrica) existiendo sede alterna a menos de 3 km. 3. Falla menor – Nivel 3: a. Deterioros que no impiden la operación: pixelación, lente sucio, carcasa rota sin exposición a riesgo, etiqueta/QR ilegible, latencia elevada sin pérdida de servicio, software con workaround documentado. b. Incumplimientos menores de formato de datos o metadatos que no afecten la integridad probatoria. IV. Reglas de escalamiento. La severidad se eleva un nivel cuando: i. Hay evento activo (emergencia, operativo, evento masivo), ii. Se trate de reiteración de la misma falla 3 o más veces en 30 días, iii. Exista vulnerabilidad de personas en situación de riesgo (niñas, niños, mujeres en protocolos de violencia, personas mayores), o iv. Se pierda redundancia primaria.

V. Detonadores del cómputo de SLA. El tiempo corre desde el primer sello de tiempo entre:

i. Alerta del sistema de monitoreo (NOC/SOC),
ii. Reporte ciudadano validado (911/Locatel), o
iii. Registro en bitácora de la dependencia/Alcaldía. Las pausas de reloj solo proceden por fuerza mayor (clima extremo, bloqueo social, riesgo para el personal) y deberán justificarse, documentarse y publicarse.

VI. Cierre y verificación. Toda reparación se validará con evidencia (fotografía/video/logs/calibración) y prueba funcional; el activo no podrá volver a operación sancionatoria sin constancia vigente.

VII. Tabla guía por tipo de activo:

Activo	Nivel 1 (ejemplos)	Nivel 2 (ejemplos)	Nivel 3 (ejemplos)
Semáforo	Apagado total en vía primaria; flash no programado	Fase "roja" apagada en vía secundaria; desincronización severa	Lente opaco; visera dañada
Cámara C5	≥30% del cuadrante caído >30 min; pérdida de grabación	Cámara clave en polígono prioritario fuera	Pixelación; rotación desajustada
Radiocomunicación	Caída sectorial >5 min; ciudad >1 min	Canal degradado; cobertura parcial	Audio con ruido
Botón de auxilio	Inoperante en Metro/Metrobús/ escuela/hospital	Inoperante en parque o módulo	Retraso en notificación
Cinemómetro/ Alcoholímetro	Sin calibración vigente / prueba reprobada	Advertencia de calibración próxima a vencer	Etiqueta/QR ilegible

Módulo de Atención a víctimas	Sistema de folio caído sin alterno	Impresora de medidas de protección inservible con alterno	Mobiliario deteriorado

VIII. Exclusiones y seguridad operativa. Mantenimientos programados y comunicados con 48 h de anticipación, pruebas de contingencia y cortes por obras autorizadas se registrarán pero no generarán penalidad. La difusión pública se hará con agregación geográfica para no exponer puntos sensibles.

Artículo 51. Publicación mensual en datos abiertos.

I. Los sujetos obligados publicarán mensualmente, a más tardar el día 10 de cada mes, la base de datos de fallas y reparaciones del mes inmediato anterior con, al menos: identificador del activo, tipo, dependencia/Alcaldía, fecha y hora de falla, severidad, causa, fecha y hora de reparación, MTTR, fecha de última prueba, proveedor responsable y estatus;

II. La información se agregará geográficamente por cuadrante, colonia o AGEB cuando la difusión puntual ponga en riesgo operaciones;

III. La ADIP habilitará un tablero público con métricas de disponibilidad por dependencia y Alcaldía (MTBF, MTTR, % disponibilidad, backlog);

IV. El C5, SSC y Alcaldías remitirán informe trimestral al Congreso con análisis de tendencias y plan de mejora.

Artículo 52. Efectos procesales y de integridad probatoria.
I. Las evidencias provenientes de equipos de medición sin calibración vigente o con pruebas reprobadas no podrán usarse para sancionar en procedimientos administrativos y/o judiciales;

	II. Las infracciones viales electrónicas deberán incluir constancia de calibración y de prueba de integridad del equipo que generó la evidencia; III. La omisión será causa de nulidad de la sanción y de responsabilidad administrativa del servidor público que la emita. Artículo 53. Supervisión y responsabilidades. I. La Contraloría y la Auditoría Superior de la CDMX auditarán el cumplimiento; II. El INFOCDMX verificará la publicación y calidad de datos abiertos; III. El incumplimiento reiterado será falta administrativa grave y causal de rescisión de contratos. Artículo 54. Atención a víctimas y accesibilidad. I. Los módulos y sistemas de atención a víctimas deberán cumplir estándares de accesibilidad y redundancia; II. Toda persona usuaria podrá consultar, en lectura fácil, el estado de la infraestructura de su colonia y el plan de reparación.

LECTURA FÁCIL (Anexo ciudadano)

¿Qué cambia? El Gobierno deberá probar cada mes que sus equipos (cámaras, semáforos, aparatos que miden velocidad y alcohol, etc.) sí funcionan. Cuando algo se descomponga, tendrá tiempos máximos para arreglarlo. Cada mes deberá publicar cuántas fallas hubo y cuánto tardó

en repararlas. Si un aparato que te sanciona no estaba calibrado, la sanción no vale.

¿Cómo podrás verlo? Habrá un sitio con un tablero y una base de datos abiertos. Podrás revisar por tu colonia.

¿Por qué te conviene? Porque habrá más transparencia, seguridad y justicia.

DECRETO

ÚNICO. Se adiciona un Capítulo IX "Del Mantenimiento, Pruebas y Transparencia de la Infraestructura Tecnológica de Seguridad y Justicia" a la Ley que Regula el Usos de Tecnología para la Seguridad Pública del Distrito Federal, para quedar como sigue:

Capítulo IX

"Del Mantenimiento, Pruebas y Transparencia de la Infraestructura Tecnológica de Seguridad y Justicia"

Artículo 46. Definiciones. Para efectos de este Capítulo se entiende por:

I. Infraestructura Crítica de Seguridad y Justicia (ICSyJ): Conjunto de equipos, sistemas, software y mobiliario urbano que soportan funciones de seguridad pública, protección civil y justicia cívica (incluye, de manera enunciativa: cámaras y servidores del C2/C5, lectoras de placas, cinemómetros, alcoholímetros, radios, patrullas y periféricos, semáforos, luminarias de seguridad, botones de auxilio, kioscos de denuncia, módulos de atención a víctimas, sistemas de cadena de custodia digital y plataformas de gestión).

II. Falla: Evento que impide o degrada el servicio conforme a especificaciones.

III. Tiempo Medio Entre Fallas (MTBF): Intervalo promedio entre fallas.

IV. Tiempo Medio de Reparación (MTTR): Tiempo promedio desde la detección a la restauración del servicio.

V. Disponibilidad: Porcentaje de tiempo que el activo presta servicio conforme a especificación.

VI. Pruebas de Integridad: Conjunto de verificaciones funcionales, de seguridad, de calibración o de recuperación, según aplique al activo.

VII. Inventario Único de Activos (IUA): Registro oficial, estandarizado y público de la ICSyJ.

VIII. SLA (Acuerdos de Nivel de Servicio): Conjunto de métricas, metas y condiciones de medición, con exclusiones, escalamiento y

consecuencias (penalizaciones/bonos), que obligan a las dependencias y proveedores a garantizar la disponibilidad, tiempos de reparación y calidad de la infraestructura de seguridad y justicia cívica.

Artículo 47. Inventario y trazabilidad. Las dependencias y Alcaldías responsables deberán:

I. Integrar y mantener actualizado el Inventario Único de Activos (IUA) con identificador único, tipo, fabricante, serie, ubicación (con niveles de agregación por seguridad), responsable, proveedor y estado operativo;
II. Etiquetar cada activo con su identificador y código QR para consulta de su ficha técnica pública;
III. Registrar cada incidencia, intervención de mantenimiento, refacción y actualización, con sello de tiempo.

Artículo 48. Pruebas obligatorias. Las dependencias y Alcaldías responsables deberán realizar pruebas obligatorias en la ICSyJ a su cargo con las siguientes temporalidades:

I. Mensuales: verificación funcional y de disponibilidad de todos los activos de la ICSyJ;

II. Trimestrales: pruebas de recuperación y respaldo en sistemas informáticos y de video;

III. Semestrales: calibración certificada de equipos de medición (cinemómetros, alcoholímetros, balanzas, sonómetros, etc.);

IV. Anuales: pruebas de integridad de cadena de custodia digital y auditoría técnica de una muestra representativa por tercero independiente;

Toda prueba generará dictamen técnico con evidencia (logs, fotografías, video, bitácoras, parámetros), resguardado y publicable en versión anonimizada.

Artículo 49. Metas de servicio y tiempos de reparación (SLA). Las dependencias y Alcaldías responsables deberán mantener los siguientes parámetros mínimos y máximos respecto a su ICSyJ:

I. Disponibilidad mínima anual por tipo de activo:

a) Cámaras y lectoras de placas: igual o mayor a 95%;

b) Semáforos de cruces principales: igual o mayor a 98%;

c) Botones de auxilio y módulos de denuncia: igual o mayor a 95%;

d) Plataformas críticas (C5, despacho y radiocomunicación): igual o mayor a 99.5% (exceptuando los mantenimientos programados).

II. Tiempos máximos de reparación desde reporte:

a) Falla crítica nivel 1 (riesgo a la vida / alto flujo vial): en menos de 24 horas;
b) Falla mayor nivel 2: en menos de 72 horas;
c) Falla menor nivel 3: en menos de 7 días hábiles.

III. Los contratos incluirán penalidades automáticas por incumplimiento de SLAs.

Artículo 50. Clasificación de severidad de fallas.

I. Criterios generales. La severidad se determina con base en:

a. Riesgo inmediato a la vida o integridad,
b. Afectación a la continuidad del servicio,
c. Impacto probatorio o de justicia cívica,
d. Alcance territorial/volumétrico de la afectación; y
e. Pérdida de redundancia.

II. Definiciones operativas.

a. Alto flujo vial: Intersección o tramo clasificado como vía primaria por la autoridad competente, o con Volumen Medio Diario ≥ 18,000 vehículos/día, o flujo peatonal ≥ 2,000 personas/hora en hora pico. Ante ausencia de medición reciente, se aplicará el catálogo oficial de vías primarias y estaciones de transporte masivo.
b. Cuadrante: Unidad operativa definida por la SSC/C5 para despacho.
c. Indisponibilidad: Imposibilidad de prestar el servicio conforme a especificación por más de 3 minutos continuos, salvo que se señale otro umbral.

III. Niveles de severidad.

1. Falla crítica – Nivel 1 (riesgo a la vida / alto flujo vial):

a. Semáforos: apagado total o destello no programado en cruce de alto flujo vial o con cruce peatonal de alto riesgo; controlador fuera de servicio sin respaldo en corredores principales.
b. 911/C5/Despacho: caída total del servicio de despacho, radiocomunicación o geolocalización en un sector por más de 5 minutos o a nivel ciudad por más de 1 minuto;

pérdida de grabación/streaming mayor o igual al 50% de cámaras de un cuadrante por más 15 min.

c. Botones de auxilio y puntos seguros: inoperantes en estaciones de transporte masivo, escuelas, hospitales o espacios con protocolos de violencia de género.
d. Equipos de medición (cinemómetros, alcoholímetros): sin calibración vigente o con prueba reprobada mientras están en operación; cadena de custodia digital con hash/sello de tiempo inválido.
e. Eventos masivos/emergencias: falla de infraestructura crítica en el perímetro de 500 metros de eventos masivos autorizados o durante atención de emergencia activa.
f. Cobertura: caída simultánea de más del 30% de cámaras, lectoras o sensores de un cuadrante por más de 30 min.

2. Falla mayor – Nivel 2:

a. Semáforos: fase o cara apagada, desincronización grave o detección faltante en cruce no clasificado de alto flujo.
b. Sistemas: indisponibilidad de módulos no críticos del C5/denuncia por más de 30 min con alternativa

temporal; pérdida de redundancia (respaldos, enlaces o energía) en plataformas críticas aún con servicio activo.

c. Video y sensores: caída de entre el 10 y el 30% de cámaras/sensores de un cuadrante por más de 30 min; cámara individual fuera en zona prioritaria (polígono con alta incidencia).
d. Atención a víctimas: módulos operativos con hardware caído (impresoras para medidas de protección, captura biométrica) existiendo sede alterna a menos de 3 km.

3. Falla menor – Nivel 3:

a. Deterioros que no impiden la operación: pixelación, lente sucio, carcasa rota sin exposición a riesgo, etiqueta/QR ilegible, latencia elevada sin pérdida de servicio, software con workaround documentado.
b. Incumplimientos menores de formato de datos o metadatos que no afecten la integridad probatoria.

IV. Reglas de escalamiento. La severidad se eleva un nivel cuando:

i. Hay evento activo (emergencia, operativo, evento masivo),
ii. Se trate de reiteración de la misma falla 3 o más veces en 30 días,

iii. Exista vulnerabilidad de personas en situación de riesgo (niñas, niños, mujeres en protocolos de violencia, personas mayores), o

iv. Se pierda redundancia primaria.

V. Detonadores del cómputo de SLA. El tiempo corre desde el primer sello de tiempo entre:

i. Alerta del sistema de monitoreo (NOC/SOC),

ii. Reporte ciudadano validado (911/Locatel), o

iii. Registro en bitácora de la dependencia/Alcaldía. Las pausas de reloj solo proceden por fuerza mayor (clima extremo, bloqueo social, riesgo para el personal) y deberán justificarse, documentarse y publicarse.

VI. Cierre y verificación. Toda reparación se validará con evidencia (fotografía/video/logs/calibración) y prueba funcional; el activo no podrá volver a operación sancionatoria sin constancia vigente.

VII. Tabla guía por tipo de activo:

Activo	Nivel 1 (ejemplos)	Nivel 2 (ejemplos)	Nivel 3 (ejemplos)
Semáforo	Apagado total en vía primaria; flash no programado	Fase “roja” apagada en vía secundaria; desincronización severa	Lente opaco; visera dañada

Cámara C5	≥30% del cuadrante caído >30 min; pérdida de grabación	Cámara clave en polígono prioritario fuera	Pixelación; rotación desajustada
Radiocomunicación	Caída sectorial >5 min; ciudad >1 min	Canal degradado; cobertura parcial	Audio con ruido
Botón de auxilio	Inoperante en Metro/Metrobús/escuela/hospital	Inoperante en parque o módulo	Retraso en notificación
Cinemómetro/ Alcoholímetro	Sin calibración vigente / prueba reprobada	Advertencia de calibración próxima a vencer	Etiqueta/QR ilegible
Módulo de Atención a víctimas	Sistema de folio caído sin alterno	Impresora de medidas de protección inservible con alterno	Mobiliario deteriorado

VIII. Exclusiones y seguridad operativa. Mantenimientos programados y comunicados con 48 h de anticipación, pruebas de contingencia y cortes por obras autorizadas se registrarán pero no generarán penalidad. La difusión pública se hará con agregación geográfica para no exponer puntos sensibles.

Artículo 51. Publicación mensual en datos abiertos.

I. Los sujetos obligados publicarán mensualmente, a más tardar el día 10 de cada mes, la base de datos de fallas y reparaciones del mes inmediato anterior con, al menos: identificador del activo, tipo, dependencia/Alcaldía, fecha y hora de falla, severidad, causa, fecha y hora de reparación, MTTR,

fecha de última prueba, proveedor responsable y estatus;

II. La información se agregará geográficamente por cuadrante, colonia o AGEB cuando la difusión puntual ponga en riesgo operaciones;

III. La ADIP habilitará un tablero público con métricas de disponibilidad por dependencia y Alcaldía (MTBF, MTTR, % disponibilidad, backlog);

IV. El C5, SSC y Alcaldías remitirán informe trimestral al Congreso con análisis de tendencias y plan de mejora.

Artículo 52. Efectos procesales y de integridad probatoria.

I. Las evidencias provenientes de equipos de medición sin calibración vigente o con pruebas reprobadas no podrán usarse para sancionar en procedimientos administrativos y/o judiciales;

II. Las infracciones viales electrónicas deberán incluir constancia de calibración y de prueba de integridad del equipo que generó la evidencia;

III. La omisión será causa de nulidad de la sanción y de responsabilidad administrativa del servidor público que la emita.

Artículo 53. Supervisión y responsabilidades.

I. La Contraloría y la Auditoría Superior de la CDMX auditarán el cumplimiento;

II. El INFOCDMX verificará la publicación y calidad de datos abiertos;

III. El incumplimiento reiterado será falta administrativa grave y causal de rescisión de contratos.

Artículo 54. Atención a víctimas y accesibilidad.

I. Los módulos y sistemas de atención a víctimas deberán cumplir estándares de accesibilidad y redundancia;

II. Toda persona usuaria podrá consultar, en lectura fácil, el estado de la infraestructura de su colonia y el plan de reparación.

TRANSITORIOS

Primero. El presente Decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial.

Segundo. En un plazo no mayor a 90 días naturales, los sujetos obligados integrarán el Inventario Único de Activos y publicarán su primer corte.

Tercero. En 180 días naturales, la ADIP emitirá lineamientos técnicos de pruebas, formatos de datos y niveles de agregación geográfica, con participación ciudadana.

Cuarto. En 365 días, todos los equipos de medición deberán contar con calibración vigente y evidencias de pruebas, conforme a los lineamientos.

Quinto. La implementación se realizará con recursos existentes mediante reprogramación de mantenimiento y obligaciones contractuales de proveedores. Los costos de calibración y auditorías técnicas se cubrirán con partidas vigentes y con las penalizaciones por incumplimiento de los Acuerdo de Nivel de Servicio.

Sexto. El Gobierno de la Ciudad de México, a través de la ADIP y la Secretaría de Seguridad Ciudadana, establecerá un programa anual de mantenimiento preventivo y correctivo de infraestructura tecnológica, con indicadores de desempeño público y comparativo.

Séptimo. La Comisión de Seguridad Ciudadana del Congreso de la Ciudad de México deberá emitir, en un plazo no mayor a 120 días naturales, lineamientos para la supervisión legislativa de los informes trimestrales que presenten las dependencias responsables.

ATENTAMENTE,

Mario Enrique Sánchez Flores

DIP. MARIO ENRIQUE SÁNCHEZ FLORES