PROPUESTA DE RENOVACIÓN FUNCIONAL Y TECNOLÓGICA DEL C5 CIUDAD DE MÉXICO

Consejo Científico Asesor
Noviembre 15, 2018

Tabla de contenido

PRESENTACIÓN

Por convocatoria de la Jefa de Gobierno electa de la Ciudad de México, Claudia Sheinbaum, el Consejo Científico Asesor fue constituido formalmente el 18 de agosto de 2018.

El Consejo está coordinado por el Dr. José Ignacio Chapela Castañares, e integrado por Dr. Fabián García Nocetti (UNAM), Dr. Christian Lemaître León (UAM), Dr. César Carlos Díaz Torrejón (UAP), Dra. Daniela Alejandra Moctezuma Ochoa (CentroGeo), Dr. Salvador Botello Rionda (CIMAT), Mtro. Sadot Arciniega Montiel (CIDESI), Mtro. Jorge Luis Orozco Pérez (CentroGeo) y Mtra. María del Socorro Romero de la Paz (CentroGeo) como Secretaria Técnica.

Se planteó como objetivo de este grupo, el asesorar a la Jefa de Gobierno en materia de innovación y tecnología; estableciéndose la prioridad de llevar a cabo una valoración de la eficacia y eficiencia del C5-Ciudad de México y su correlación con las Secretaria de Seguridad Pública y Protección Civil.

Con este propósito, el Consejo Científico Asesor celebró siete reuniones con dependencias del gobierno de la Ciudad de México: (en su conjunto tuvieron una duración de 17 horas).

NÚM.	DEPENDENCIA	FECHA
1	C5	28 Ago/05 Sep/12 Nov
2	Secretaría de Protección Civil	04 Sep
3	Secretaría de Seguridad Pública	07 Sep
4	C5, instalaciones del C2 Poniente	12 Sep
5	SSP Puesto de Mando	17 Sep

En todas las reuniones se contó con la asistencia de personal del grupo de transición. Anexo 1: “Minutas de reuniones con dependencias de la Ciudad de México”.

Se elaboró un amplio cuestionario y solicitud de información como guía de las entrevistas con los directivos del C5. Anexo 2: Respuesta al “Cuestionario del Consejo Científico Asesor”

También se llevaron a cabo también reuniones con tres equipos de transición de la Jefa de Gobierno electa:

- Grupo de trabajo del Dr. José Merino, encargado de la Agencia de Operación e Innovación Digital.
- Equipo de la Dra. Myriam Urzúa, próxima Secretaria de Protección Civil.
- Grupo de trabajo del Mtro. Juan Manuel García Ortegón, próximo Coordinador General del C5. (en dos ocasiones).

Asimismo, se llevó a cabo un taller denominado Soluciones Inteligentes para Comunidades Seguras, los días 17 y 18 de octubre con la participación activa de los miembros del Consejo Científico Asesor y con integrantes del Equipo de Transición del gobierno de la Ciudad de México. Anexo 3: “Programa del Taller de Soluciones Inteligentes para Comunidades Seguras”.

Cabe destacar que el Consejo Científico Asesor se reunió en ocho ocasiones por videoconferencia y/o presencialmente (18 horas), con el propósito de elaborar un Diagnóstico y Formular Propuestas para el Desarrollo Funcional y Tecnológico del C5-Ciudad de México. Anexo 4: "Minutas de las reuniones del Consejo Científico Asesor".

El presente reporte ejecutivo refleja la visión de conjunto de los participantes; así como, las necesarias especificidades de cada tema y especialidad.

El reporte se estructura con la valoración de la eficiencia y eficacia del funcionamiento del C5 y de su relación con las secretarías de Seguridad Pública y Protección Civil; con esta base, se elabora la propuesta de la renovación institucional del C5 como *Unidad Estratégica de Gestión de Gobierno y Servicios a la Ciudadanía*.

Se identifican, fundamentan y desarrollan nueve temas críticos de decisión para el desarrollo tecnológico de la Unidad Estratégica y se avanza en una primera estimación de sus costos.

Finalmente, se integra una agenda de temas estratégicos a desarrollarse en el mediano plazo, que darán pauta a la transformación integral de la institución.

RENOVACIÓN FUNCIONAL Y TECNOLÓGICA

RENOVACIÓN FUNCIONAL

Como elemento central del llamado "Proyecto Bicentenario Ciudad Segura", en Junio de 2009 se creó el Centro de Atención a Emergencias y Protección Ciudadana de la Ciudad de México, con la tarea de desarrollar e implementar un sistema de videovigilancia orientado a mejorar el desempeño operativo y de coordinación interinstitucional entre la Secretaria de Seguridad Pública, la Procuraduría General de Justicia y la Secretaria de Protección Civil.

A nueve años de constituido, destaca el aislamiento institucional del Centro de Atención a Emergencias y Protección Ciudadana (ahora denominado C5) respecto de la operación policial y de las tareas de protección civil. La descoordinación institucional se manifiesta en la incapacidad de los Centros C5 y C2 de cumplir la función principal de despacho y seguimiento automático de los recursos policiales o de protección civil en la atención de emergencias.

Adicionalmente, es importante señalar el alto grado de obsolescencia tecnológica de las cámaras de videovigilancia (6,588 adquiridas en 2009) y de los equipos de monitoreo, procesamiento y almacenamiento; principalmente los de misión crítica. Lo anterior se agrava con la operación de diversos sistemas con tecnología propietaria, cuyo mantenimiento, actualización o renovación resulta muy onerosa

La renovación funcional y tecnológica del C5 y los C2; deberá orientarse al pleno aprovechamiento de la importante inversión e infraestructura tecnológica existente; a la efectiva coordinación con las instituciones de seguridad pública y protección ciudadana; y, a su potencial desarrollo como "Unidad Estratégica de Gestión de Gobierno y Servicios a la Ciudadanía", como se presenta en el siguiente esquema:

Como resultado del diagnóstico realizado, se presentan nueve temas críticos de decisión, cuya efectiva atención, permitirá soluciones a corto plazo, así como, crear las condiciones para un desarrollo sostenible de la infraestructura tecnológica del C5-Ciudad de México

INTEGRACIÓN DE SOLUCIONES A CORTO PLAZO

1. Reducción de la Dependencia Tecnológica de los Sistemas de Videovigilancia en Operación.

   Los sistemas de videovigilancia son elementos tecnológicos esenciales en el cumplimiento de la misión actual del C5-Ciudad de México y lo serán para atender las funciones que se incorporarán en la renovación institucional.

   El C5-Ciudad de México administra y gestiona en la actualidad 14,588 videocámaras.

AÑO	NÚMERO DE CÁMARAS	GESTIONAN
2009	6,588	SATHI VMS
2014	6,500	SATHI VMS
2017	1,500	GENETEC

   Ambos sistemas son soluciones propietarias y con grandes restricciones para interoperar con equipos de marcas diferentes lo que implica una doble administración e ineficiencia en la gestión.

   Es esencial y prioritario reducir la dependencia tecnológica de estos dos sistemas, bajo las siguientes consideraciones:

   - Plataforma abierta
   - Sistema basado en estándares de la industria para la compresión y transmisión del video
   - Escalable y flexible
   - Operable en ambientes virtuales
   - Compatible con SO Linux
   - Compatible con múltiples Bases de Datos, abiertas (Open Source) y propietarias
   - Integración de notificaciones y actualizaciones en tiempo real

   Adicionalmente, se requiere contar con la facilidad de interoperar con otros conjuntos de videocámaras, pertenecientes a otras dependencias o incluso a particulares (cámaras de tránsito, Metro, Metrobús, sistema de fotomultas, centros comerciales, entre otras).

   En consecuencia, se propone llevar a cabo un estudio comparativo de los sistemas de gestión de videovigilancia, disponible con tecnología abierta, a fin de seleccionar la alternativa que garantice las características descritas y que permita, en el corto plazo (2019), asegurar la interoperabilidad de los sistemas de videovigilancia en operación.

2. Actualización e interoperabilidad de los sistemas de geolocalización y Sistemas de Información.

   Es esencial la geolocalización de los recursos con que cuentan los servicios de seguridad y de emergencia, es decir, conocer su ubicación y su estatus: activo, inactivo, disponible, no disponible, en ruta, en actuación, ente otros.

   El sistema actual de gestión de geolocalización en uso es el que cuenta la SSP, administrado desde el Puesto de Mando, el cual; es obsoleto y muy ineficiente, la información disponible no es confiable, ni se dispone en tiempo real; no se cuenta con esquemas de alertamiento sistemáticos, por desconexión temporal o total de los recursos, debido a fallas convencionales o por manipulaciones intencionadas no autorizadas.

   Es necesario que se cuente con una base de datos confiable y disponible en tiempo real de la geolocalización de los elementos de actuación y recursos para cada una de las áreas involucradas en la atención de incidencias: Secretaria de Seguridad Pública, Secretaria de Protección Civil, ERUM, Cruz Roja y bomberos, entre otras.

   La geolocalización de todos los elementos de actuación y recursos se deberá colectar, concentrar y distribuir a través de la infraestructura tecnológica del C5-Ciudad de México. Para ello, se considera necesario definir un nuevo estándar de infraestructura de geolocalización (GPS), con mayor tolerancia a fallas o a manipulaciones mal intencionadas, un esquema más eficiente de recolección de los datos georreferenciados con tiempos de consulta-respuesta lo más cercano a tiempo real.

   En complemento a la efectiva geolocalización se requiere contar con un Sistema de Información Geográfica (GIS) actualizado, confiable e interoperable basado en todos aquellos "GIS-individuales" que se han ido construyendo y robusteciendo por las diferentes dependencias, a lo largo de los años.

   Este sistema debería residir en la infraestructura tecnológica del C5-Ciudad de México y compartido en tiempo real, de manera segura, confiable y expedita, con las dependencias que así lo requieran a través de la red de datos local.

   Para este único GIS-Ciudad de México se debe tomar en cuenta:

   - Interoperable de plataforma abierta (Open Source) y de estándar internacional, que permita la incorporación de nuevas capas especializadas, según las propias necesidades de la dependencia que la construya y actualice.
   - Instalado sobre una plataforma de procesamiento y almacenamiento de alto rendimiento y con replicas funcionales en cada uno de los C2. Asimismo, deberá poder ser accesible vía web, por cada una de las dependencias que así lo requieran, incluido acceso público a determinadas capas.

Los sistemas de Geolocalización y de información Geográfica habrán de ser administrados por un grupo específico de personal técnico especializado, con asiento en cada una de las dependencias que contribuyan a su conformación, con perfiles jerarquizados de acceso y políticas de modificación muy bien definidas.

INFRAESTRUCTURA BÁSICA

3. Anillo Primario de Fibra Óptica (Backbone), Anillos Secundarios y LAN/WAN.

   El anillo de fibra óptica que actualmente une físicamente al C5-Ciudad de México con los cinco C2, es el elemento de infraestructura base para el intercambio de datos, imágenes e información; hoy en día, esta tecnología está rebasada, por lo que se propone su inmediata revisión, actualización y gradual expansión; para convertirse en un Backbone robusto.

   Un anillo de fibra, robusto, estable y eficiente, que acceda la incorporación de nuevos elementos de monitoreo, sensorización y mejora en la calidad de las imágenes/video; ampliación de la cobertura de interconexión entre dependencias estratégicas y de gestión; y permita el acercamiento de la ciudadanía con áreas de conexión a Internet y con sus autoridades, su desarrollo requerirá de las siguientes consideraciones:

   - Revisión y reemplazo de la red actual de fibra óptica que une al C5 con los C2 mediante la medición de valores disminución de la potencia de la señal óptica, para determinar si aún se tiene vida útil.
   - Remplazo por obsolescencia de los equipos activos que en conjunto con la nueva fibra óptica, asegurare un Backbone que en toda su trayectoria principal ofrezca anchos de banda sostenidos de al menos 100 Gbps, garantizando con ello, una vida útil estimada de 10 años.
   - Una vez actualizado el anillo de fibra óptica, es recomendable aprovechar el costo del derecho de vía de la red del Metro para construir el Backbone de la Ciudad de México, que permitirá unir a cada una de las dependencias con operaciones basadas en información proveniente del C5-Ciudad de México de manera eficiente y expedita (voz, datos, imágenes y video), con derivaciones de segundo, tercer y cuarto nivel (anchos de banda promedios entre 40, 10 y 1Gbps respectivamente) a través de las actuales estaciones del metro.
   - Se deberá contemplar la existencia física, dentro del C5, de un Network Operation Center (NOC) y un Security Operation Center (SOC), que garanticen el funcionamiento óptimo de la red y su seguridad informática (esta seguridad informática debería estar complementada con un área especializada en Ciberseguridad).
   - Con el proceso de actualización y expansión del anillo de fibra, se deberán ir consolidando los contratos individuales de las distintas dependencias en telefonía, datos e Internet[1], lo

[1] *Con gestión del servicio a través de un ancho de banda y telefonía VoIP consolidado en el C5 y gestionado a través del SOC/NOC capitalino*

cual permitirá ahorros por contratos individuales de cada dependencia con los proveedores, además de la mejora en la capacidad de ancho de banda disponible[2].

- El mantenimiento preventivo y correctivo deberá estar contemplado, tanto para el presupuesto de inversión, como para la operación futura.

4. Gradual Renovación de las Videocámaras con Alto Nivel de Obsolescencia.

   Es imprescindible considerar un programa gradual de renovación de las videocámaras en operación, ya que aún prevalecen 6,588 que fueron adquiridas en 2009, por lo que ya presentan un alto nivel de obsolesencia, lo que significa que dejaran de funcionar en el corto plazo o requieran de un elevado costo de mantenimiento.

   La estrategia de renovación de las videocámaras, está estrechamente vinculada con la propuesta de despliegue y crecimiento de la red de fibra óptica, a través de las líneas del Metro, ya que, con el crecimiento del Backbone en operación, se podrá iniciar en paralelo, el reemplazo de enlaces de interconexión de 2Mbps (SHDSL) de las actuales 6,588 videocámaras (equipos 2009), con enlace de fibra óptica con anchos de banda mínimos de 100 Mbps.

   Lo anterior, contribuirá en la mejora en la calidad de imagen, video y audio que transmiten las videocámaras, sino también la capacidad para transmitir datos de múltiples sensores que se pudieran instalar en los mismos postes (sensores de inundaciones, CO2, sismicidad, temperatura, humedad, expansión de la cobertura WiFi de la Ciudad de México, entre otros).

5. Renovación del Hardware y Software de Misión Crítica.

   Es de muy alta importancia que en el C5-Ciudad México se incorporen infraestructuras de cómputo del alto rendimiento y de Supercómputo, con las que hoy no cuentan, que sirvan para hacer labores de gestión inteligente de los datos en tránsito y almacenados, que permitan análisis tipo Big Data, de Business Intelligence, para la creación de Bases de Datos confiables de reconocimiento facial, de placas vehiculares, de análisis en tiempo real de redes sociales, entre otras.

   Esta infraestructura también deberá emplearse para realizar labores reales de ciberseguridad, que permitan mediante el análisis de datos en tiempo real, la detección anticipada de vulnerabilidades, intentos de acceso no autorizados, análisis forenses, puesta en marcha de acciones de control y mitigación de contingencias digitales, así como labores de ciberinteligencia para contrarrestar determinados ciberdelitos patrimoniales y de afectación directa a la población.

[2] *El costo estimado anual de gastos de la Ciudad de México por concepto de estos servicios es de aproximadamente 500 millones de pesos, distribuidos en alrededor de 500 enlaces de distintas capacidades, a su vez, distribuidos entre todas las dependencias del gobierno, destacando que tan solo la SSP-Ciudad de México tiene contratados, 200 de este total.*

Las recomendaciones en este rubro deberán considerar al menos los siguientes elementos:

- Reemplazo del hardware de procesamiento y almacenamiento de misión crítica, con grado de obsolescencia mayor al ciclo de vida determinado por el fabricante (5 años promedio, 7 como máximo), en función de la disponibilidad de partes de hardware de reemplazo y versiones seguras de sistemas operativos y aplicativos.
- Considerar las soluciones basadas en entornos virtuales (en hardware local) que permiten el uso y crecimiento en función de la demanda, disminuyendo los costos (operación, mantenimiento, licenciamiento) por hardware ocioso.
- Migrar el esquema de licenciamiento de software de esquemas cliente-servidor, a esquemas tipo web, que elimine la dependencia de hardware con características específicas y límiten la renovación tecnológica al término de su ciclo de vida.

Se recomienda en el corto plazo el reforzamiento de la seguridad física, de personal y de acceso a la información; así como, la actualización de los planes de mantenimiento preventivo y correctivo .Se considera necesario elaborar planes de contingencia y recuperación ante desastres, asimismo actualizar y mejorar continuamente los procedimientos y escalamiento para atención de incidentes el desarrollo de

6. Centro de Datos Alterno (Site Secundario)

A pesar de que la infraestructura de los Centros de Datos del actual C5-Ciudad de México (incluidos los cinco C2) se consideran de alta disponibilidad, alta seguridad y redundantes, no se cuenta con un Centro de Datos Alterno, donde se pueda recuperar el 100% de la operación en caso de contingencias parciales o desastre total.

Actualmente solo parte de los servicios de misión crítica que opera el C5-CDMX se podrían recuperar en los C2, se replican solamente algunos de los sistemas para gestionar el sistema de videovigilancia de la ciudad, sin embargo, en un caso de contingencia plena, hay un alto riesgo de pérdida permanente de información y la consecuente inoperancia para llevar a cabo las labores sustantivas del centro.

Es en ese sentido que se recomienda ampliamente, la construcción de un Centro de Datos Alterno que cumpla con la norma internacional ANSI/TIA-942 del Uptime Institute a nivel TIER IV, que lo especifica como una infraestructura (Centro de Datos) completamente tolerante a fallos y con un nivel de disponibilidad del 99.995% de minutos en el año.

Cabe mencionar que una infraestructura como esta, no sólo podría contribuir a garantizar la continuidad ante eventualidades del C5 y los cinco C2, si no; que además, se podría emplear como el Centro de Datos de misión crítica, para otras áreas sustanciales de la Ciudad de México.

Sería recomendable asegurar un adecuado nivel de disponibilidad, redundancia y seguridad de 2019 a través de la renta del servicio con proveedores certificados.

SISTEMAS INTELIGENTES

7. Consolidar las Bases de Datos con Información Complementaria.

   Se requiere garantizar la disponibilidad de datos confiables en las distintas fuentes de información que los proveen (sensores físicos y lógicos) de las distintas bases de datos que posee el propio C5, por lo que se hace necesaria la consolidación, mediante interfaces de hardware especializado con bases de datos de otras dependencias relacionadas, e incluso bases de datos públicas (estructuradas y no estructuradas).

   La consolidación de bases de datos con información complementaria requiere al menos las siguientes consideraciones para su implementación:

   - Voluntad política y la gestión necesaria para permitir el intercambio de datos entre las distintas bases de datos (eliminación de los cotos de poder, por control de la información).
   - Desarrollo de los elementos esenciales de interoperabilidad, a través de software y hardware.
   - Desarrollo de Bases de Datos centralizadas con administración y gestión múltiple y procesamiento en paralelo (Bases de Datos Distribuidas).
   - Implementación de Bases de Datos de Código Abierto (Open Source) para datos sensibles, sólo en aquellos casos donde se pueda garantizar la seguridad de la información almacenada en ellas, a través de contar con personal altamente especializado en el manejo de este tipo de Bases de Datos y con el continuo mantenimiento en la aplicación de parches de seguridad publicados por la propia Comunidad Open Source.

8. Procesos Automatizados para el Análisis Inteligente del Sistema de Vídeo Vigilancia.

   Dentro de las necesidades planteadas y detectadas en el C5 respecto al sistema de vídeo vigilancia, están los sistemas automatizados para el análisis inteligente del contenido de los vídeos.

   Este tipo de sistemas puede ser adquirido tanto por medio de empresas especializadas, como por transferencia de conocimiento y desarrollo tecnológico de las universidades y centros de investigación del país.

   Dentro de los principales aspectos con los que se desean contar en el sistema de vídeo vigilancia están los siguientes:

   - Seguimiento de coches por color
   - Reconocimiento de rostros
   - Detección de cierto tipo de acciones
   - Análisis de eventos masivos (manifestaciones, eventos deportivos, conciertos, entre otros)
   - Entendimiento a más alto nivel de la escena
   - Reconocimiento de personas

9. Sistemas Automatizados para el Monitoreo y Análisis del Contenido de Redes Sociales.

   El monitoreo de redes sociales como un elemento para acceder a información valiosa de manera indirecta, contribuye de manera significativa en la efectividad de los tiempos de respuesta en incidencias detectadas y en su la predicción.

   Para ello es importante contar con herramientas de inteligencia basadas en el análisis de técnicas de procesamiento del lenguaje natural y aprendizaje computacional, ambas áreas pertenecientes a la Inteligencia Artificial

   Estas herramientas de análisis automático de texto que pueden rápidamente incorporarse a la dinámica de funcionamiento de este análisis de redes sociales.

   Por mencionar algunos de los algoritmos desarrollados por el CentroGeo en conjunto con INFOTEC están las siguientes:

   - Clasificación de tópicos, búsqueda de palabras clave, contabilizar frecuencia de palabras, frases.
   - Clasificación de la emoción (tristeza, enojo, felicidad, miedo) contenida en los textos
   - Ver si el contenido es agresivo, tiene algún nivel de misoginia, la polaridad (negativo, neutral, positivo)
   - Inferir características de los usuarios o autores de los textos, como: edad, sexo, variedad de idioma e incluso perfilado de los mismos según las emociones que expresan en sus textos.
   - Detección de eventos basados en la frecuencia de tweets, palabras clave, entre otros.
   - Análisis de tendencias, eventos atípicos.

TEMAS ESTRATÉGICOS A MEDIANO PLAZO

GRUPO DE PLANEACIÓN DE LA GESTIÓN TECNOLÓGICA

Se propone la creación de un Grupo de Planeación de Gestión Tecnológica orientado a la detección de oportunidades de innovación, proyectos de desarrollo y propuesta de integración de soluciones específicas para los distintos ámbitos tecnológicos, cuyos objetivos sean:

i. Establecer la vinculación con Centros Públicos de Investigación y/o universidades para proyectos especializados.

ii. Definir los lineamientos de mediano y largo plazo orientados a formular el plan y presupuesto institucional, para la actualización y desarrollo de la nueva plataforma tecnológica.

iii. Determinar parámetros de cuantificación de los impactos que se quieren medir, con el fin de tener referencias en las adecuaciones, cambios tecnológicos, proyectos especializados, que incidan en la mejora de servicios del C5, entre dependencias y con la ciudadanía.

A continuación se enuncian tres temas que se consideran prioritarios para su planeación y desarrollo en el mediano plazo.

1. Diseño de un Centro Digital para el Desarrollo de Soluciones Tecnológicas

   Se propone la creación en el mediano plazo de un Centro Digital que desarrolle, implemente y administre una plataforma tecnológica escalable para el despliegue de iniciativas en los temas de salud, seguridad y protección civil, entre otros.

   Las principales funciones del Centro Digital serían:

   - Contar con una infraestructura tecnológica para brindar soluciones al desarrollo tecnológico y formación de recursos humanos, en la generación de aplicaciones inteligentes.
   - Fomentar la cultura de cambio a la era digital en las diferentes secretarías de gobierno de la Ciudad de México.
   - Analizar las plataformas tecnológicas para el desarrollo de la red de sensores y sistemas electrónicos de ciudad inteligente en la Ciudad de México.
   - Enlace con universidades y centros públicos para la formación de recursos humanos especializados requeridos en el desarrollo del C5
   - Evaluación de tecnologías para la operación del centro de mando de control en temas de informática, conectividad y sensorización

   Dentro de la prospectiva de crecimiento de este Centro Digital es que sea sostenible, y que debido a su escalabilidad de infraestructura y recursos humanos, propicie atender nuevas demandas sociales tales como: medio ambiente, movilidad, fugas de agua, contenderos de basura, energía, tiempo de arribo de transporte urbano, entre otros.

2. Integración de un Área de Ciberseguridad (*Security Operation Center* -SOC-)

Se considera indispensable la creación del área de Ciberseguridad en el mediano plazo, para poder ofrecer un grado mínimo de disponibilidad y alarmas tempranas. Por tanto, es necesario contar con una infraestructura de Supervisión y Monitorización. Ambas funciones se llevan a cabo mediante el NOC (*Network Operation Center*) y el SOC (*Security Operation Center*).

Estas funciones deberán ser congruentes con el tipo de red y se deberán asignar los recursos adecuados para cada una de éstas, pero lo importante es ser conscientes de la importancia que tiene esta actividad y plantearse cómo se llevará a cabo, por mínima que sea la infraestructura.

El NOC concentrará toda la información de supervisión, monitorización y alarmas de la red o de la infraestructura que tiene bajo su responsabilidad. Las funciones básicas de este conjunto de recursos humanos y materiales, que están 24x7 los 365 días del año, son:

- Monitorización y detección de eventos
- Clasificación y categorización (determinación del impacto)
- Gestión de alarmas
- Gestión de incidentes
- Gestión de peticiones (control de cambios)
- Gestión de accesos
- Gestión de inventario

Deberá registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias y fallos observables en un sistema de información o red de comunicación que puedan estar relacionados con la confidencialidad, integridad y/o disponibilidad de la información. Registrará la actividad de los administradores y operadores de los sistemas de información.

Deberá existir un procedimiento para establecer qué infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán los informes periódicos con los resultados de la monitorización. Se recomienda el uso de un sistema centralizado para la monitorización y supervisión de red que sea independiente del resto de los equipos y aplicaciones, que permita la definición de reglas de correlación para la identificación de ataques y modelos de comportamiento.

El SOC, de manera similar al NOC, requiere de una ubicación física donde se concentrarán los recursos humanos y materiales, con la responsabilidad de la monitorización, detección, análisis, prevención y seguimiento de los eventos de seguridad en las redes e infraestructuras del sistema.

El SOC deberá proporcionar al menos los siguientes servicios:

- Monitorización y gestión de la infraestructura de seguridad
- Gestión de incidentes de seguridad
- Gestión de vulnerabilidades
- Auditorias de seguridad

- Apoyo al cumplimiento regulatorio
- Investigación de seguridad en Internet
- Análisis y detección de malware
- Prevención de la seguridad
- Cadenas de contactos y escalada en incidentes de seguridad
- Propuesta y seguimiento de acciones de mejora en seguridad

Como parte de la mejora continua y el alcance de la madurez de la institución, se considera conveniente desarrollar herramientas de gestión y análisis de vulnerabilidades; así como, el adoptar un marco normativo de estándares internacionales de calidad de los servicios, tales como ISO-20000, ITIL y CMMI for Services, que le permita:

- Mejorar los procesos de la entrega de sus servicios
- Mantener el control de las actividades realizadas por el personal
- Crear un ambiente en el cual no se dependa de las personas para cualquier actividad o toma de decisiones.

3. Desarrollo de una Plataforma Colaborativa para el Manejo de Emergencias

Una de las fuentes de información en tiempo real que más utilidad ha mostrado en diversas situaciones de emergencia a nivel mundial, son las redes sociales, particularmente Twitter por su facilidad de acceso y manipulación. En México esto no ha sido la excepción, gracias a la información proporcionada por usuarios de esta red se pudieron llevar a cabo diversas tareas de ayuda y rescate.

La experiencia de la creación de una organización ciudadana que emergió en la Ciudad de México, poco después del terremoto del 19 de septiembre de 2017, debe ser estudiada detenidamente para poder diseñar una política general de resiliencia de la Ciudad que incluya de manera sinérgica la voluntad de ayudar en circunstancias de gran emergencia de la población de la Ciudad con la infraestructura y logística y capacidades del gobierno de la Ciudad.

En el caso del 19 de septiembre de 2017, la sociedad civil se organizó de manera independiente, utilizando redes sociales, aplicaciones geomáticas propietarias como Google Maps, y desarrollando conforme se fueron necesitando bases de datos que permitieron ordenar la información proveniente de múltiples fuentes heterogéneas.

El gobierno de la Ciudad no puede hacer frente solo a emergencias de gran magnitud como los sismos de 2017, y mucho menos uno como el de 1985. Pero lo que si puede hacer, es tener la infraestructura informática que permita la incorporación inmediata de los distintos tipos de voluntarios ciudadanos dispuestos a participar en las enormes tareas de salvamento, y apoyo a las víctimas, junto con las brigadas especializadas de Protección Civil.

Una plataforma abierta basada en un sistema de información geográfica consultable por todos en línea, en donde se vayan geolocalizando las zonas de colapso, las zonas de acopio de

materiales y de acopio de comida y cobijo de las víctimas, todo esto bajo medidas flexibles de verificación y actualización de la información basadas en la participación ciudadana.

La centralización de esta información en la infraestructura del C5, podría ser de enorme utilidad tanto para mantener la coherencia y coordinación de las actividades de todas las partes, dependencias del gobierno y grupos de ciudadanos. En las fases posteriores a la emergencia, esta información podría servir para las fases de verificación de daños y de planeación y ejecución de la reconstrucción. La participación ciudadana tendría un papel que jugar igualmente en estas etapas. La información pública contenida en esta plataforma ayudaría a todos a conocer las prioridades y la distribución de los esfuerzos y los avances obtenidos.

El desarrollo de una infraestructura computacional como la descrita podría integrarse en pocos meses a partir de sistemas ya existentes tanto en el C5 como en otras dependencias gubernamentales e instituciones de educación superior de la Ciudad y con la participación de las asociaciones civiles y personas con experiencia en estos temas.