CONTENIDO

1. OBJETIVO

Determinar las actividades y acciones a seguir en caso de una falla o evento disruptivo en el sistema de videovigilancia ciudadana, a través de una descripción detallada de tareas que se deban ejecutar teniendo en cuenta las diferentes fallas o eventos que se puedan presentar, con el fin de garantizar una respuesta rápida y eficiente para minimizar el impacto en la seguridad y convivencia ciudadana y asegurar la continuidad y monitoreo del sistema.

2. ALCANCE

Este plan está organizado para que al momento en el que se presente un evento disruptivo o falla en el sistema de videovigilancia se procedan con las actividades de identificación, gestión y restablecimiento normal del servicio.

El plan aborda los siguientes escenarios disruptivos con mayor probabilidad de ocurrencia:

- Falla en Cámara de Videovigilancia.
- Falla en el Centro de Datos
- Falla en Infraestructura de Red (Conectividad)
- Falla en Centro de Monitoreo
- Imposibilidad de acceso a las instalaciones del C4

Este plan es aplicable a todo el personal involucrado en la operación y mantenimiento del sistema de videovigilancia ciudadana.

3. AMBITO DE APLICACIÓN

El presente documento es aplicable en el proceso de Gestión Tecnológica de Seguridad y Emergencias del Centro de Comando, Control, Comunicaciones y Cómputo – C4 de Bogotá, D.C.

4. NORMATIVIDAD ASOCIADA

Ver Normas asociados del documento en https://portalmipg.scj.gov.co

5. DOCUMENTOS ASOCIADOS

Acta de Reunión F-FI-1380

6. GLOSARIO

C4: Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá.

CAD Policía: Centro Automático de Despacho - (Policía Metropolitana de Bogotá).

CAD: Computer Aided Dispatch (CAD-por sus siglas en inglés): Sistema de despacho asistido por computador. Se refiere al subsistema de la plataforma tecnológica del Sistema Integrado de Seguridad y Emergencias, destinado a la gestión de la información de seguridad o emergencias de la ciudad.

Disruptivos: Se refiere a eventos, tecnologías o innovaciones que causan una interrupción significativa en una organización

ETB: Empresa de Telecomunicaciones de Bogotá S.A. E.S.P

Gbps: Gigabits por segundo.

MEBOG: Policía Metropolitana de Bogotá.

Operador Tecnológico: es el encargado de brindar el soporte tecnológico necesario para que se pueda cumplir con los objetivos de la misionalidad de las agencias.

PIVOT3: Soluciones de infraestructura hiperconvergentes simples, inteligentes y automatizadas para admitir cualquier carga de trabajo, cualquier iniciativa de centro de datos en cualquier entorno de TI.

RPO (Recovery Point Objective - por sus siglas en inglés): Determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

RTO (**Recovery Time Objective** - por sus siglas en inglés): Define el tiempo límite para la restauración de sistemas y servicios para minimizar el impacto en el negocio.

SDSCJ: Secretaría Distrital de Seguridad, Convivencia y Justicia

SecurOS - ISS: Security Operating System – Intelligent Security Systems, es una plataforma de software avanzada utilizada para la gestión y el análisis de sistemas de videovigilancia y seguridad.

UAECOBB: Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá

VMS (Video Management Software - por sus siglas en inglés): Software mediante el cual se administra el sistema de videovigilancia.

7. DESCRIPCIÓN DEL SISTEMA DE VIDEOVIGILANCIA

El sistema de videovigilancia ciudadana del Distrito Capital es el conjunto de infraestructura física y tecnológica, los protocolos y el personal necesario para capturar, transportar, almacenar, monitorear y analizar la información proveniente de las cámaras instaladas por el Distrito en toda la ciudad y aquellas de otras entidades públicas o privadas que por su potencial aporte a la seguridad ciudadana hacen parte del mismo. Conforme los lineamientos aprobados por el Comité Operativo de Apoyo y Seguimiento del C4, están al servicio de la Policía Metropolitana de Bogotá – MEBOG y las demás entidades que en el marco del cumplimiento de los objetivos del C4, se considere que deben acceder, con el fin de aportar a la atención y prevención de incidentes de seguridad y emergencias en Bogotá. D. C.

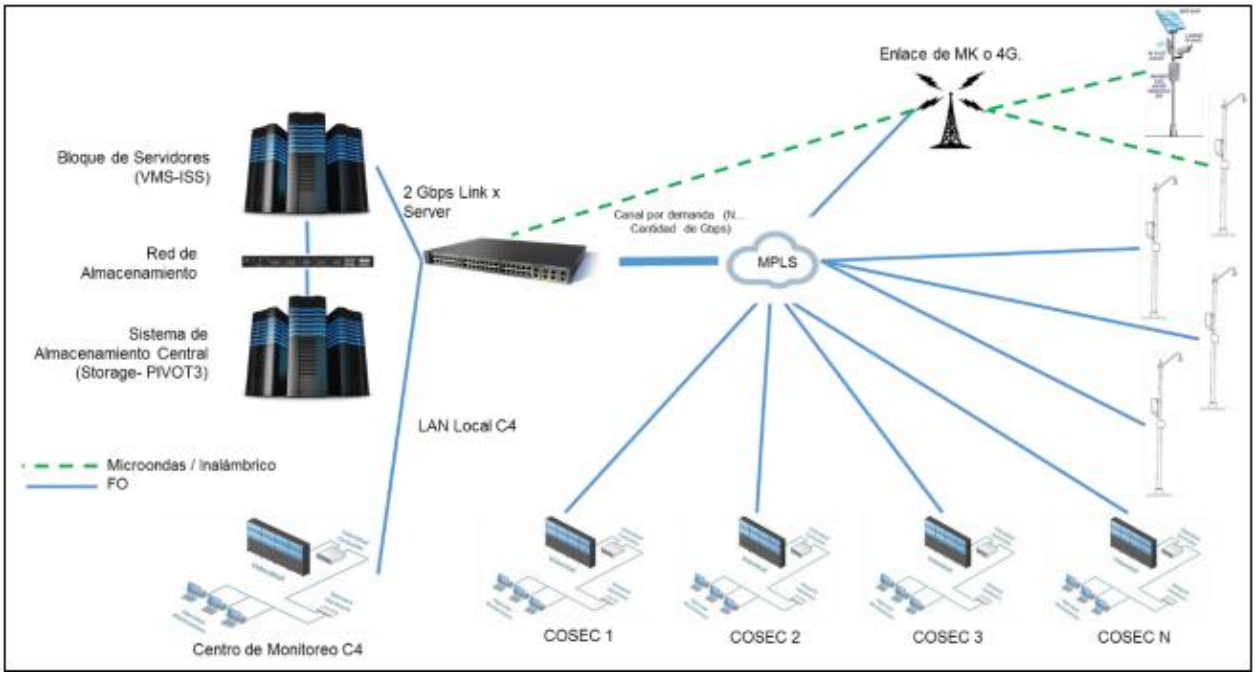
Así mismo, el Sistema de Videovigilancia Ciudadana de Bogotá está concebido como una solución integral, de misión crítica (alta disponibilidad), que tiene una arquitectura centralizada para la plataforma de administración y almacenamiento (referida a la plataforma de administración del video – VMS (SecurOS-ISS) y plataforma de grabación del video – PIVOT3), y una arquitectura distribuida a nivel de monitoreo y visualización. La topología de conexión de red está configurada en estrella tipo punto a punto, por enlace dedicado desde el C4, hacia cada centro de monitoreo y enlace descendente desde cada Centro de Monitoreo al C4.

La infraestructura del sistema de videovigilancia actualmente cuenta con una estructura centralizada de 53 servidores físicos con alta disponibilidad, dentro de estos se encuentran 47 servidores virtuales y que en conjunto conforman la plataforma de hiperconvergencia, mediante la cual los sistemas de grabación, administración de VMS y servidores de archivo se encuentran alojadas en data center del edificio UAECOBB sede principal de la Unidad Administrativa Especial Cuerpo Oficial Bomberos Bogotá

7.1 Composición actual del Sistema de Videovigilancia Ciudadana

La composición del Sistema de Videovigilancia se encuentra descrito en el numeral 7.2.1 del Manual Operación Sistema de Videovigilancia MA-GTS-01.

7.2 Topología de red



7.3 Roles y Responsabilidades

Los roles y responsabilidades se encuentran descritos en el numeral 7.3.2 del Manual Operación Sistema de Videovigilancia MA-GTS-01.

8. MATRIZ DE COMUNICACIONES

Una vez que el operador tecnológico y/o operadores del sistema, identifican una falla o evento disruptivo en el sistema de videovigilancia deben informar a todos los miembros relacionados a través de llamada, mensaje de texto o correo electrónico. Así mismo, si la falla o incidente afecta otros componentes tecnológicos del C4 y/o Policía Nacional, que tienen a cargo la operacionalización del sistema.

8.1 Equipo estratégico

NOMBRE	ROL	CORREO
Cesar Andrés Restrepo Flórez	Secretario de seguridad	cesar.restrepo@scj.gov.co
Ada Luz Sandoval Herazo	Jefe oficina C4	ada.sandoval@scj.gov.co
Iván Hersayn Pinilla Herrera	Director de tecnologías y sistemas de información	ivan.pinilla@scj.gov.co
Rafael Humberto López Saavedra	Responsable de infraestructura DTSI	rafael.lopez@scj.gov.co
Fabio Andrés Albornoz Quintero	Líder tecnológico C4	fabio.albornoz@scj.gov.co
Javier Felipe Espeleta Martínez	Líder administrativo C4	javier.espeleta@scj.gov.co

8.2 Equipo apoyo técnico por escenarios

ESCENARIOS	ROL	RESPONSABLES	CORREO
1. Falla en cámara de videovigilancia	Apoyo técnico SVV	Gerly David Verano Ariolfo Márquez	gerly.verano@scj.gov.co ariolfo.marquez@scj.gov.co
2. Falla en el centro de datos	Apoyo técnico SVV	Gerly David Verano Ariolfo Márquez	gerly.verano@scj.gov.co ariolfo.marquez@scj.gov.co
3. Falla en infraestructura de red (Conectividad)	Apoyo técnico SVV	Jennifer Guatavita Jorge Marcelo Lozano	jennifer.guatavita@scj.gov.co jorge.lozanoa@scj.gov.co
4. Falla en centro de monitoreo	Apoyo técnico SVV	Pedro Martín Sierra Jaime Enrique Pinto	pedro.sierra@scj.gov.co jaime.pinto@scj.gov.co
5. Imposibilidad de acceso a las instalaciones del C4	Apoyo técnico SVV	Pedro Martín Sierra Jaime Enrique Pinto	pedro.sierra@scj.gov.co jaime.pinto@scj.gov.co

9. ESCENARIOS DISRUPTIVOS SISTEMA DE VIDEOVIGILANCIA

El sistema de videovigilancia no está exento de riesgos y pueden enfrentarse a una variedad de escenarios disruptivos que comprometen su funcionamiento y efectividad, desde fallos técnicos hasta infección de software malicioso, pasando por desastres naturales y actos de vandalismo, es esencial comprender y prepararse para estos eventos adversos.

A continuación, se presentan 4 escenarios generales de posibles fallas que puede presentar en el sistema de videovigilancia junto con la descripción de cada falla, el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO), así:

ESCENARIOS	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
1. Falla en cámara de videovigilancia.	La cámara no transmite video o presenta fallos intermitentes debido a problemas en los componentes electrónicos, conectividad o daño físico.	1. Identificación y diagnóstico del problema mediante monitoreo y pruebas físicas. 2. Reemplazar los componentes defectuosos o problemas de conectividad según sea necesario. 3. Realizar las reparaciones o actualizaciones. 4. Pruebas de funcionamiento.	4 horas	0 horas
2. Falla en el centro de datos.	Problemas en los servidores o almacenamiento que afectan la grabación y procesamiento de video. Puede ser debido a fallos de hardware, software o energía.	1. Identificación del origen del problema, (Hardware, software o de energía) 2. Proceder con la reparación o el reemplazo de los equipos afectados. 3. Restauración de los elementos.	4 horas	1 hora
3. Falla en infraestructura de red (Conectividad).	Problemas de conectividad que impiden la transmisión de video desde las cámaras al centro de monitoreo. Pueden ser causados por fallos en los routers, switches, o cables de red.	1. Realizar un diagnóstico para identificar los componentes de red afectados, como routers, switches o cables. 2. Reparar o reemplazar los componentes defectuosos. 3. Configurar rutas alternativas para garantizar la transmisión continua de video.	2 horas	0 horas
4. Falla en centro de monitoreo.	Problemas en el centro de monitoreo que impiden la visualización y gestión de las cámaras de videovigilancia. Pueden ser causados por fallos en los equipos de monitoreo, software, o infraestructura física.	1. Identificación de fallos en los equipos de monitoreo, el software de gestión o la infraestructura física, conectividad o eléctrica. 2. Reparar o reemplazar los equipos dañados 3. Restaurar el software necesario para la visualización y gestión de las cámaras.	3 horas	0 horas
5. Imposibilidad de acceso a las instalaciones del C4.	Se refiere a situaciones en las que el personal no pueda ingresar al centro de monitoreo debido a factores externos como desastres naturales, disturbios civiles, incidentes de seguridad, o cualquier otra circunstancia que impida el acceso físico.	1. Identificación de situación presentada 2. Notificación de desplazamiento a centro alterno. 3. Monitoreo en centro alterno. 4. Restablecimiento en el centro principal	1 hora	0 horas

9.1 Descripción de escenarios disruptivos sistema de videovigilancia

Identificados los grandes escenarios generales disruptivos, a continuación, se procede a realizar una descripción de las problemáticas o fallos que se pueden presentar en cada uno de ellos, acompañados de las actividades y tiempos de recuperación aproximados.

9.1.1 Escenario Nro. 1: Falla en cámara de videovigilancia

PROBLEMÁTICA	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
Daño componentes electrónicos.	Detectar y confirmar un daño en los componentes electrónicos de las cámaras de videovigilancia.	1. Identificación del problema 2. Inspección física 3. Diagnóstico técnico 4. Reemplazo de componentes electrónicos 5. Pruebas de Funcionamiento	2 horas	0 horas
Fallo de alimentación en cámara(s).	Las cámaras dejan de transmitir imágenes debido a una falta de energía eléctrica.	1. Verificación inicial 2. Inspección de conexiones 3. Revisión fuente de alimentación 4. Restablecimiento de energía 5. Mantenimiento preventivo y/o correctivo 6. Pruebas de funcionalidad	2 horas	0 horas
Pérdida de conectividad de red.	Las cámaras no transmiten imágenes al centro de monitoreo debido a problemas de conectividad de red.	1. Diagnóstico inicial 2. Prueba de conectividad 3. Reiniciar dispositivos de red 4. Inspección de cables 5. Configuración de red 6. Mantenimiento de la red.	2 horas	15 min
Problemas de calidad de imagen.	Las imágenes de las cámaras están borrosas, pixeladas o tienen mala calidad.	1. Limpieza de la lente 2. Ajustes de enfoque 3. Verificación de la iluminación 4. Revisión de la resolución 5. Revisión de la compresión de video 6. Mantenimiento preventivo y/o correctivo	2 horas	1 hora
Vandalismo/hurto/ accidente.	Las cámaras sufren daños a causa de vandalismo ciudadano.	1. Verificación y evaluación inicial 2. Notificación y registro 3. Aislamiento y seguridad del área 4. Reparación o reemplazo 5. Refuerzo de seguridad 6. Revisión y mejora de políticas	4 horas	1 hora

9.1.2 Escenario Nro. 2: Falla en el centro de datos

PROBLEMÁTICA	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
Fallo de alimentación eléctrica.	Pérdida de suministro eléctrico que afecta la operatividad del data center.	1. Verificación Inicial 2. Activación de sistemas de respaldo 3. Monitoreo y reporte 4. Restauración del suministro 5. Pruebas y mantenimiento	1 hora	0 horas

Fallo en el sistema de refrigeración.	El sistema de climatización falla, lo que puede llevar al sobrecalentamiento de los servidores.	1. Identificación del problema 2. Activación de planes de contingencia 3. Reparación del sistema 4. Reubicación temporal 5. Monitoreo y mantenimiento	2 horas	0 horas
Fallo de Hardware.	Fallo en uno o más componentes de hardware (servidores, discos duros, etc.).	1. Diagnóstico inicial 2. Activación de sistemas redundantes 3. Reemplazo de hardware 4. Restauración de datos 5. Pruebas y monitoreo	4 horas	1 hora
Fallo de Software.	Un error en el software o una actualización fallida interrumpe los servicios.	1. Identificación del problema 2. Reversión de actualización 3. Reinicio de servicios 4. Aplicación de parches 5. Pruebas y monitoreo	2 horas	30 min
Materialización de un riesgo informático.	Materialización de un software malicioso, impidiendo el acceso a datos críticos y causando la interrupción de las operaciones.	1. Detección del ataque 2. Aislamiento del sistema 3. Evaluación del daño 4. Restauración desde copias de seguridad 5. Investigación y refuerzo de seguridad	8 horas	1 hora

9.1.3 Escenario Nro. 3: Falla en infraestructura de red (Conectividad)

PROBLEMÁTICA	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
Fallo red de conectividad troncal.	Un fallo en la interrupción significativa en la infraestructura principal que conecta diversos segmentos de la red.	1. Detección y diagnóstico 2. Contención 3. Reparación 4. Verificación y restauración 5. Revisión Post-Incidente	2 hora	0 hora
Fallo en el enrutador (Router).	Un fallo en el enrutador principal puede interrumpir el acceso a la red.	1. Diagnóstico inicial 2. Reinicio del enrutador 3. Reemplazo del enrutador 4. Configuración y pruebas 5. Monitoreo continuo	1 hora	0 hora
Fallo en el switch de red.	Un fallo en uno de los switches de red dispuestos en operación en el data center.	1. Identificación del problema 2. Reinicio del switch 3. Reemplazo del switch 4. Restauración de la configuración 5. Pruebas y monitoreo	2 horas	15 min
Problemas de configuración de red.	Una configuración errónea puede causar problemas de conectividad en toda la red.	1. Revisión de configuración 2. Reversión de cambios 3. Aplicación de configuración 4. Implementación de controles 5. Capacitación del personal	1 hora	0 hora

9.1.4 Escenario Nro. 4: Falla en centro de monitoreo

PROBLEMÁTICA	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
Fallo en la infraestructura de conectividad.	Fallo en los cables de red, switches, routers u otros componentes de la red que interrumpen la conectividad.	1. Diagnóstico inicial 2. Reinicio de dispositivos de red 3. Reemplazo de componentes 4. Defectuosos 5. Pruebas de conectividad 6. Monitoreo y mantenimiento	1 hora	1 hora
Fallo en el sistema de alimentación eléctrica.	Pérdida de suministro eléctrico que afecta la operatividad del centro de monitoreo.	1. Verificación inicial (Interno y/o externo 2. Activación de sistemas de respaldo 3. Monitoreo y reporte 4. Restauración del suministro 5. Pruebas y mantenimiento	2 horas	0 hora
Fallo en sistema de visualización (Video Wall).	Perdida de la imagen en los monitores o pantallas interconectadas que muestran datos y video en un formato de gran escala.	1. Detección y diagnóstico 2. Contención 3. Reparación 4. Verificación y restauración 5. Revisión Post-Incidente	2 horas	0 hora
Daño en estaciones de trabajo.	Fallo en una estación de trabajo utilizadas por los operadores para supervisar sistemas, analizar datos y responder a incidentes en tiempo real.	1. Detección y diagnóstico 2. Contención 3. Reparación 4. Verificación y restauración 5. Revisión Post-Incidente	2 horas	0 hora

9.1.5 Escenario Nro. 5: Imposibilidad de acceso a las instalaciones del C4

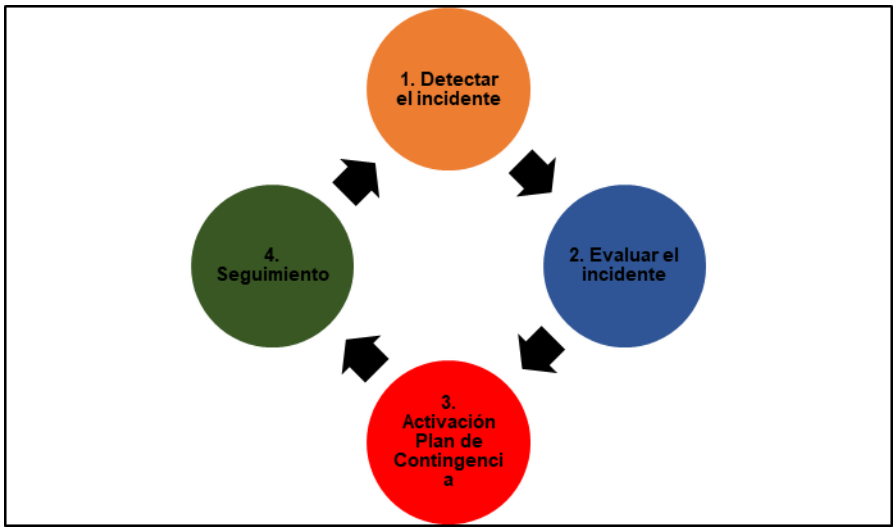
PROBLEMÁTICA	DESCRIPCIÓN	ACTIVIDADES	RTO	RPO
Desastres Naturales.	Eventos que pueden causar daño físico significativo a las instalaciones y dificultar el acceso.	1. Activar protocolos de evacuación y traslado a una ubicación segura 2. Coordinar con autoridades locales para el acceso seguro y evaluar los daños 3. Activar sitio alterno 4. Retorno a la normalidad	6 horas	1 hora
Fallo en el Sistema de Alimentación Eléctrica prolongado.	Falta de suministro eléctrico prolongado que imposibilita el funcionamiento de los equipos de monitoreo.	1. Activar actividades de respaldo y verificar el funcionamiento de los sistemas críticos 2. Contactar al proveedor de energía para la restauración del suministro 3. Retorno a la normalidad	2 horas	0 horas
Accesos Bloqueados.	Situaciones que impiden físicamente al personal llegar a las instalaciones.	1. Activar centros de operaciones alternativos 2. Monitorear la situación y coordinar con las autoridades para el restablecimiento del acceso 3. Retorno a la normalidad	2 horas	0 horas

Amenazas de Seguridad.	Riesgos que requieren la evacuación o el cierre temporal de las instalaciones para proteger al personal y los activos.	1. Seguir protocolos de seguridad 2. Evacuar si es necesario y coordinar con fuerzas del orden 3. Activar plan de contingencia 4. Asegurar las instalaciones y realizar inspecciones de seguridad antes del retorno del personal 5. Retorno a normalidad	2 horas	0 horas

9.2 Activación plan de contingencia de sistema de videovigilancia

Como parte de las estrategias inmediatas ante un posible escenario, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos.

A continuación, se enumeran las fases de manera general que se deben considerar para la activación del plan de contingencia:



Así mismo se listan algunas actividades de manera general descritas en el siguiente cuadro anexo a las fases definidas anteriormente:

No	ACTIVIDAD	DESCRIPCION	RESPONSABLES	REGISTRO	TIEMPO
1	Falla detectada en el sistema de videovigilancia.	Se detecta una falla en el sistema de videovigilancia, afectando la transmisión y/o almacenamiento de imágenes.	Operadores del sistema Operador Tecnológico (Monitoreo) Jefe CAD	Correo Electrónico Llamadas Telefónicas	Inmediato
2	Informar mesa de Servicio (Creación de Ticket).	Informar a la Mesa de Servicio sobre el incidente	Operadores del sistema	Correo Electrónico Ticket en Mesa de	Inmediato

		presentado.	Jefe CAD	Servicios	
3	Verificar la falla.	Se realiza la verificación de la falla en el sistema, confirmando su origen y alcance para tomar las acciones correctivas necesarias.	Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de servicio Informe de Verificación	15 minutos
4	Realizar diagnóstico inicial de la falla.	Se efectúa un diagnóstico inicial de la falla para identificar posibles causas.	Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de servicio Informe diagnóstico	15 minutos
5	Notificar Equipo de Gestión (Jefatura C4, Líder tecnología C4, DTSI, SDSCJ).	Se notifica al Equipo de Gestión sobre el incidente, proporcionando un resumen del diagnóstico inicial y las acciones a tomar para la resolución de la falla.	Apoyo Técnico SVV C4 Operador Tecnológico	Correo Electrónico Llamadas Telefónicas	Inmediato
6	Notificar servicios afectados.	Se notifica a los responsables de los servicios afectados, detallando el impacto de la falla y estimando los tiempos de resolución según el diagnóstico inicial.	Apoyo Técnico SVV C4 Operador Tecnológico Jefe CAD	Correo Electrónico	Inmediato
7	Activar plan.	Se activa el plan de contingencia, siguiendo los procedimientos establecidos para mitigar el impacto de la falla y restaurar los servicios afectados.	Apoyo Técnico SVV C4 Operador Tecnológico Jefe CAD	Correo Electrónico	Inmediato
8	Medidas correctivas (Software/Hardware/conectividad).	Se implementan las medidas correctivas identificadas durante el diagnóstico, reparando los componentes afectados y verificando la estabilidad del sistema para asegurar su correcto funcionamiento.	Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de Servicios Informe de Medidas Correctivas	30 minutos
9	Ejecutar procedimientos de contingencia.	Se ejecutan los procedimientos de contingencia, implementando las medidas predefinidas para manejar situaciones de emergencia y asegurar la continuidad del servicio mientras se resuelve la falla.	Apoyo Técnico SVV C4 Operador Tecnológico Jefe CAD	Ticket en Mesa de Servicios Informe medidas de contingencia	15 minutos
10	Pruebas.	Se realizan pruebas para verificar la efectividad de las actividades aplicadas y asegurar que el sistema de	Operadores del Sistema Apoyo Técnico SVV C4	Informe medidas de contingencia	15 minutos

		videovigilancia funcione correctamente antes de su reactivación total.	Operador Tecnológico		
11	Regresar a la normalidad.	Se restaura el sistema a su funcionamiento normal, confirmando que todos los componentes están operativos y que los servicios afectados han sido completamente recuperados.	Operadores del Sistema Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de Servicios	15 minutos
12	Registrar incidente (Documentar).	Se documenta el incidente detalladamente, incluyendo la descripción del problema, las medidas correctivas implementadas, el impacto en los servicios y cualquier otra información relevante para un análisis posterior y la mejora continua de los procesos.	Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de servicios	Inmediato
13	Cerrar incidente.	Se cierra el incidente tras confirmar que todos los problemas han sido resueltos y que el sistema está funcionando normalmente.	Apoyo Técnico SVV C4 Operador Tecnológico	Ticket en Mesa de Servicios	Inmediato
14	Monitorear funcionalidad.	Se lleva a cabo un monitoreo continuo de la funcionalidad del sistema para asegurar que se mantenga en estado óptimo y para detectar cualquier posible problema adicional a tiempo."	Operadores del Sistema Apoyo Técnico SVV C4 Operador Tecnológico	Informe de Monitoreo	Inmediato

9.3 Notificación de la contingencia - escenarios

Cuando se presenta un escenario de contingencia, se debe tener en cuenta que se debe gestionar el mismo con el fin de iniciar con el proceso de contingencia, teniendo en cuenta lo anterior, la responsabilidad para gestionar los escenarios descritos es la siguiente:

9.3.1 Falla en cámara de videovigilancia

PROBLEMÁTICA	RESPONSABLE	CORREO ELECTRÓNICO
Daño componentes electrónicos.	Gerly David Verano Ariolfo Márquez	gerly.verano@scj.gov.co ariolfo.marquez@scj.gov.co
Fallo de alimentación eléctrica en cámara(s).	Camilo Andrés Rubiano Gerly David Verano	camilo.rubiano@scj.gov.co gerly.verano@scj.gov.co

Pérdida de conectividad de red.	Jennifer Guatavita Jorge Marcelo Lozano	jennifer.guatavita@scj.gov.co jorge.lozanoa@scj.gov.co
Problemas de calidad de imagen.	Pedro Martin Sierra Ariolfo Márquez	pedro.sierra@scj.gov.co gerly.verano@scj.gov.co
Vandalismo/hurto/ Accidente.	Pedro Martin Sierra Luis Hernán Moya	pedro.sierra@scj.gov.co luis.moya@scj.gov.co

9.3.2 Falla en el centro de datos

PROBLEMÁTICA	RESPONSABLE	CORREO ELECTRÓNICO
Fallo de alimentación eléctrica.	Diego Alberto Díaz Mantilla Jeimar Hernando Pineda	diego.diaz@scj.gov.co jeimar.pineda@scj.gov.co
Fallo en el sistema de refrigeración.	Diego Alberto Díaz Mantilla Jeimar Hernando Pineda	diego.diaz@scj.gov.co jeimar.pineda@scj.gov.co
Fallo de hardware.	Gerly David Verano Ariolfo Márquez	gerly.verano@scj.gov.co ariolfo.marquez@scj.gov.co
Fallo de software.	Gerly David Verano Ariolfo Márquez	gerly.verano@scj.gov.co ariolfo.marquez@scj.gov.co
Materialización de un riesgo informático.	Alexander Palacios Palacios Harold Casas	alexander.palacios@scj.gov.co harold.casas@scj.gov.co

9.3.3 Falla en infraestructura de red (Conectividad)

PROBLEMÁTICA	RESPONSABLE	CORREO ELECTRÓNICO
Fallo red de conectividad troncal.	Jennifer Guatavita Jorge Marcelo Lozano	jennifer.guatavita@scj.gov.co jorge.lozanoa@scj.gov.co
Fallo en el enrutador (Router).		
Fallo en el switch de red.		
Problemas de configuración de red.		

9.3.4 Falla en centro de monitoreo

PROBLEMÁTICA	RESPONSABLE	CORREO ELECTRÓNICO
Fallo en la infraestructura de conectividad.	Jennifer Guatavita Jorge Marcelo Lozano	jennifer.guatavita@scj.gov.co jorge.lozanoa@scj.gov.co
Fallo en el sistema de alimentación eléctrica.	Giovanni Ricardo Ángel	giovanni.angel@scj.gov.co
Fallo en sistema de visualización (Video Wall).	Pedro Martin Sierra Ariolfo Márquez Quiroga	pedro.sierra@scj.gov.co ariolfo.marquez@scj.gov.co
Daño en estaciones de trabajo.	Pedro Martin Sierra Ariolfo Márquez Quiroga	pedro.sierra@scj.gov.co ariolfo.marquez@scj.gov.co

9.3.5 Imposibilidad de acceso a las instalaciones del C4

PROBLEMÁTICA	RESPONSABLE	CORREO ELECTRÓNICO
Desastres naturales.	Jefe CAD Ángela Lisbeth Romero Andrea García Ayala	mebog.cad-coman@policia.gov.co
Fallo en el sistema de alimentación eléctrica prolongado.		
Accesos bloqueados.		
Amenazas de seguridad.		

10. ESTRATEGIAS PREVENTIVAS

Las estrategias preventivas están diseñadas para anticipar, mitigar y en la medida de lo posible, evitar los efectos adversos de eventos imprevistos, al adoptar un enfoque proactivo y sistemático, se pueden reducir significativamente el impacto de las crisis, asegurando la resiliencia y la recuperación rápida ante cualquier eventualidad.

A continuación, se enuncian las estrategias preventivas que el Centro de Comando, Control, Comunicaciones y Cómputo, tiene adoptadas que permiten anticipar, identificar y mitigar posibles incidentes antes de que impacten el funcionamiento del sistema de videovigilancia.

10.1 Mantenimiento preventivo infraestructura de videovigilancia

La SDSCJ – C4, cuenta en la actualidad con contrato de Mantenimiento Preventivo, Mantenimiento Correctivo y Soporte al Sistema de Videovigilancia de Bogotá, con disponibilidad de bolsa de repuestos. Este contrato es renovado de manera periódica.

De la misma forma se cuenta con contrato de garantía extendida del sistema de almacenamiento y VMS para el sistema de grabación de Videovigilancia.

Esta infraestructura es monitoreada por parte del contratista de mantenimiento y personal de apoyo de supervisión del C4, los cuales están organizados para cumplir las siguientes actividades preventivas:

Acción	Frecuencia	Responsable
Monitoreo del sistema	Diaria	Mesa de Servicio Operador Tecnológico
Inspección física al funcionamiento del data center	Dos veces a la semana	Mesa de Servicio Operador Tecnológico
Cambio de componentes identificados en falla	Por demanda	Contratista Garantía Extendidas

10.2 Infraestructura de red – conectividad

La infraestructura de conectividad actual cuenta con contrato de conectividad para el sistema de videovigilancia de Bogotá, la red WAN, internet móvil y voz, empleados por los organismos de seguridad e inteligencia del estado con jurisdicción en el distrito capital y la secretaría distrital de seguridad, convivencia y justicia".

El contrato provee una infraestructura robusta, redundante y con alta disponibilidad, así como con enrutamiento alterno, provistos por un proveedor de telecomunicaciones en el distrito capital, que considera la red MPLS, WAN y LAN.

En lo relacionado con la conectividad y sistema de conmutación, se cuenta con infraestructura redundante mediante dos enlaces uno principal y otro de contingencia o backup, con anchos de bandas robustos, 30 y 20 Gbps, respectivamente.

Igualmente cuenta con un Router: principal y respaldo, que permite la continuidad del servicio, en caso de presentarse una falla o evento disruptivo.

Para el enrutamiento del tráfico se cuenta con tecnología VRF (Virtual Routing and Forwarding) que permite en cada router físico tener de manera virtual, múltiples routers virtuales, los cuales cuentan con tabla de enrutamiento independiente y separada una de otra, es decir, múltiples rutas para garantizar la continuidad y contingencia del servicio. Esta tecnología VRF, está configurada en los dos equipos, una para el tráfico de los centros de monitoreo y otra para el resto de tráfico de la red WAN del servicio de videovigilancia. Ambos tráficos se encuentran configurados, como contingencia en los dos equipos.

En forma general el C4 se conecta al Switch de la Secretaría, SCJ Core, red LAN, este conecta al Router principal de ETB mediante la agregación virtual de enlaces (LACP). En la WAN se realiza conexión LACP y de esta forma garantiza disponibilidad en caso de que una de las líneas falle. Por medio de la WAN el Router de ETB tiene comunicación con la MPLS, donde se encuentran configuradas las VRF del tráfico INTERWAN de cámaras y del tráfico de los centros de monitoreo.

10.3 Centros de monitoreo

La infraestructura del sistema de videovigilancia actualmente cuenta con ocho centros de monitoreo (Chapinero, Usaquén, Kennedy, Puente Aranda, Teusaquillo, Barrios Unidos, Engativá y Ciudad Bolívar, Rafael Uribe Uribe y Santafé) que deberán aportar cada uno, una o dos estaciones de operador con la cual se conformará la sala de monitoreo alterna, que se ubicaría por contingencia en caso de ser necesario.

Centro de Monitoreo	Ubicación
C4	Carrera 68 Nro. 20-06
Engativá	Kr 78A No. 70 54
Barrios unidos	Calle 72 # 62-81

Teusaquillo	Cra 13 # 39-86
Chapinero	Av. Circunvalar con calle 57 - 02
Ciudad bolívar	Diag 70 Sur Con Transv 54
Kennedy	Transv 78 K Con Calle 41 D Sur
Puente Aranda	Cra 39 Con Calle 10
Usaquén	Calle 165 con Carrera 8 A
Rafael Uribe Uribe	Cl. 27 Sur #24-39
Santafé	Cra. 5 #29-11

Los centros de monitoreo cuentan con planta eléctrica y con UPS, que soportan la autonomía eléctrica que se requiere para el funcionamiento del sistema, de la misma forma, cuentan con topología y sistemas de respaldo principal y backup de conectividad los cuales se conectan a los diferentes puntos de la MPLS de ETB.

En lo relacionado con la conectividad y sistema de conmutación, se cuenta con infraestructura redundante mediante dos enlaces uno principal y otro de contingencia o backup, con anchos de bandas de acuerdo con las necesidades de cada centro, Ejemplo 1 Gbps y 512 Mbps, respectivamente, así como dos equipos Router: principal y respaldo, que permite la continuidad del servicio, en caso de presentarse una falla o evento disruptivo.

10.4 Contingencia operativa centros de monitoreo

Centro de Monitoreo	Monitoreo Actual	Cámaras	Monitoreo Contingencia	Responsable	RTO
Principal C4	Principal C4	4850	Engativá	Jefe CAD Operador tecnológico	1 hora
Usaquén	Usaquén	186	Teusaquillo	Jefe CAD Operador tecnológico	1 hora
Chapinero	Chapinero	224	Teusaquillo	Jefe CAD Operador tecnológico	1 hora
Engativá	Engativá	390	Barrios Unidos	Jefe CAD Operador tecnológico	1 hora
	Fontibón	177			
Puente Aranda	Puente Aranda	203	Kennedy	Jefe CAD Operador tecnológico	1 hora
	Mártires	195			
	Antonio Nariño	132			
	Candelaria	78			
Kennedy	Kennedy	431	Rafael Uribe	Jefe CAD Operador tecnológico	1 hora
	Bosa	424			
Ciudad Bolívar	Ciudad Bolívar	431	Kennedy	Jefe CAD Operador tecnológico	1 hora
	San Cristóbal	309			
	Usme	234			
	Tunjuelito	140			
Barrios Unidos	Barrios Unidos	134	Teusaquillo	Jefe CAD Operador tecnológico	1 hora
	Suba	441			

Teusaquillo	Teusaquillo	192	Barrios Unidos	Jefe CAD Operador tecnológico	1 hora
Santafé	Santafé	249	Puente Aranda	Jefe CAD Operador tecnológico	1 hora
Rafael Uribe	Rafael Uribe	280	Puente Aranda	Jefe CAD Operador tecnológico	1 hora

Nota: Una vez se establezca la contingencia, el operador tecnológico realiza configuración remota del o los equipos para que puedan hacer el monitoreo sólo de las cámaras de la localidad a la cual está asignado el usuario del aplicativo de visualización.

10.5 Sistema eléctrico C4

El C4 ante la caída o fallas en la energía eléctrica, cuenta con infraestructura robusta que le permite continuar con la prestación de los servicios a los ciudadanos a través de planta eléctrica, UPS, aires acondicionados, transformadores, así como cobertura mediante contratos de soporte y mantenimiento tal como se detalla a continuación:

- ✓ Contrato Mantenimiento correctivo y preventivo de aires acondicionados.
- ✓ Contrato Mantenimiento correctivo y preventivo de Plantas eléctricas.
- ✓ Contrato Mantenimiento correctivo y preventivo de UPS.

10.6 Instalaciones físicas

El C4, en su edificio de la sede principal tiene ubicados los sistemas de respaldo eléctrico en el sótano, instalaciones y en los cuartos técnicos ubicados en los diferentes pisos, los cuales tiene asignación y distribución específicas que permiten garantizar la continuidad de las operaciones y servicios a la ciudadanía.

10.7 UPS

El edificio del C4, sede principal, cuenta con un total de seis UPS, con asignación y distribución de la siguiente manera:

- Dos UPS de marca Emerson de 90 Kva, redundante aislado que soporta el datacenter de Bomberos, edificio contiguo al C4.

11. PRUEBAS

Las pruebas de contingencia son un proceso sistemático y planificado que tiene como objetivo verificar y asegurar que una organización esté preparada para enfrentar y gestionar escenarios de contingencia o interrupciones imprevistas en sus procesos operativos. Estas

pruebas buscan evaluar la efectividad de los planes de contingencia diseñados para minimizar el impacto de eventos adversos, garantizando la continuidad del negocio y la rápida recuperación de funciones críticas.

Estás deben ejecutarse durante un tiempo en el que las afectaciones de la operación normal sean mínimas y debe comprender elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral de la Entidad.

Estas como mínimo se realizan con una periodicidad anual, con la coordinación y supervisión de los líderes responsables de los escenarios y las problemáticas planteadas.

Las pruebas tienen la siguiente finalidad:

1. Verificar la totalidad y precisión de las acciones de contingencia.
2. Evaluar el desempeño del personal involucrado.
3. Evaluar la coordinación entre los responsables de los escenarios, operadores tecnológicos y usuarios funcionales y agencias.
4. Medir el desempeño de la plataforma tecnológica del SVV.
5. Identificar los posibles brechas o falencias que puedan tener el plan de contingencia.

11.1 Preparación de las pruebas

La preparación de las pruebas se debe contemplar las siguientes actividades:

Actividades	Responsable	Registro
Establecer y aprobar programación de la Prueba.	Jefe oficina C4 Líder tecnológico C4	Acta de reunión (F-FI-1380)
Informar e involucrar a los participantes en las pruebas.	Apoyo técnico SVV C4	Correo electrónico
Gestionar reuniones con los equipos involucrados en las pruebas (Objetivo, Alcance, tipo de Prueba, Resultados esperados y riesgos)	Apoyo técnico SVV C4	Acta de reunión (F-FI-1380) Correo electrónico
Definir el cronograma y el tiempo en las que se ejecutarán las pruebas.	Apoyo técnico SVV C4	Acta de reunión (F-FI-1380)
Garantizar la asistencia de las personas involucradas en la ejecución de la prueba	Apoyo técnico SVV C4	Acta de reunión (F-FI-1380)
Disponibilidad de las áreas de soporte, operador tecnológico y demás entes involucrados en la ejecución de la prueba.	Apoyo técnico SVV C4	Acta de reunión (F-FI-1380)
Ejecución de la prueba	Apoyo técnico SVV C4	Informe de resultados
Informe de Resultados	Apoyo técnico SVV C4	Informe de resultados

Nota: Para cada uno de los escenarios se desarrollará un protocolo de prueba que permita garantizar la contingencia y verificación la eficacia de las actividades.

Nota 2: Se aclara que los nombres de los responsables tanto por escenarios como por problemática varían de acuerdo con el momento, en este sentido se tiene más en cuenta el rol o la dependencia.

Elaboró: Alexander Palacios Palacios – Contratista C4

Revisó: Fabio Andrés Albornoz Quintero – Contratista C4
Edith Nathalie Romero Barrera – Profesional Universitario
Sandra Milena Martínez Martínez - Contratista C4

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co