



Suprema Corte  
de Justicia de la Nación



# Manual de Operaciones

Centro de Control de  
Seguridad Integral de la Corte

C2SIC



## TABLA DE CONTENIDO

### **Introducción**

**Propósito del documento**

**Ámbito**

**Audiencia objetivo**

**Necesidad de un Centro de Mando**

**Marco jurídico**

### **Contexto**

**Reseña histórica**

**Misión**

**Visión**

**Valores**

**Objetivos y metas**

### **Organigrama**

### **Descripción de puestos**

### **Ejes principales y Reglas de Operación**

### **Políticas, reglas y restricciones**

### **Indicadores de gestión**

### **Glosario**

### **Referencias**

### **Referencias al anexo técnico**



## Introducción

### Propósito del documento

Este documento tiene como propósito proveer el manual de operaciones del Centro de Control de Seguridad Integral de la Corte (C2SIC) perteneciente a la SCJN, con la intención de dar a conocer cómo funciona, documentar la interrelación que existe entre sus diferentes áreas, normalizar los procedimientos de actuación y evitar las indefiniciones e improvisaciones que puedan producir problemas o deficiencias en la realización de sus funciones.

Pretende contribuir a reducir el margen de error y mejorar la eficiencia del servicio mediante la definición clara de roles, responsabilidades, actividades y cómo se deben de realizar en una secuencia ordenada de pasos, evitando que cada operador haga el trabajo a su consideración y que el logro de resultados dependa de su apreciación; al tener documentada la forma correcta de proceder, las personas podrán conocer exactamente qué se espera de ellas y cómo realizar su trabajo.

Respaldar el conocimiento y experiencia del personal actual y con ello evitar iniciar de cero al momento de cambios del personal responsable, al mantenerlo documentado es factible asegurar la continuidad y la actuación con base a procedimientos y protocolos establecidos.

### Ámbito

Los conceptos que se mencionan en el presente documento definen los parámetros de los aspectos que conforman el Centro de Control de Seguridad Integral de la Corte (C2SIC), para lograr una organización operativa coordinada, tener perfiles de puesto claros y sin ambigüedad, establecer una operación homogénea y protocolizada que a su vez pueda ser útil para hacer el servicio medible y evaluable, definir los elementos normativos y brindar servicio acorde a los objetivos de la Dirección General de Seguridad y en lo aplicable a los de la Suprema Corte de Justicia de la Nación.

### Audiencia objetivo

Este documento está dirigido a todas las personas que tengan alguna relación con el Centro de Control de Seguridad Integral de la Corte (C2SIC), como lo son directores, jefes de departamento y operadores, así como a empleados activos o de nuevo ingreso de la Dirección General de

Seguridad de la SCJN que de acuerdo con sus funciones o atribuciones y tengan algún interés en conocer acerca del mismo.

El lenguaje empleado en el presente documento no busca generar ninguna clase de discriminación, ni marcar diferencia alguna, tampoco crear algún tipo de polémica o controversia, por lo que de acuerdo con la Real Academia Española las referencias o alusiones hechas al género masculino representan siempre, tanto a hombres como a mujeres.<sup>1</sup>

## Necesidad de un centro de mando

Se ha comprobado el efecto positivo que tiene la tecnología, no solamente en la disuasión del delito, sino también en las propias tareas preventivas y acciones específicas de las personas a cargo de la seguridad; cuando la tecnología opera en coordinación con las áreas y organismos de mantenimiento del orden, la percepción de una mayor certidumbre en el desempeño de su labor es evidente, así la tecnología no sustituye a las capacidades del capital humano, sino que extiende sus posibilidades y le brinda mayor seguridad para la realización de su trabajo.

Convencidos de la utilidad de uso de la tecnología en materia de seguridad y con el propósito de aprovechar al máximo la funcionalidad y la experiencia del personal del actual centro de monitoreo de la SCJN, se realizó una valoración sobre su forma de operar, encontrando varias áreas de oportunidad, los mecanismos de comunicación no son los ideales, no existen bases de datos en relación a los eventos atendidos, las incidencias no son reportadas en su totalidad, no está especificado algún catálogo de riesgos, el monitoreo se realiza conforme a consignas o solicitud expresa basado sólo en la experiencia, la cual se pierde en caso de que el personal decida retirarse, no se cuenta con reglamentación que obligue a llevar a cabo informes; por ello concluimos sobre la necesidad del fortalecimiento tecnológico, normativo y sobre la formación de las personas que lo integran, escalándolo a un **Centro de Control de Seguridad Integral de la Corte (C2SIC)**, donde los roles, responsabilidades y procedimientos estén claramente definidos, además de la incorporación de herramientas tecnológicas para brindar el servicio de manera oportuna y eficiente, evitando la discrecionalidad en la forma de elaborar los registros, informes, bitácoras y reportes, para que a su vez alimenten las bases de datos con el valor agregado de servir para labores de inteligencia.

A pesar de las ventajas del uso de la tecnología en tareas de seguridad, existe un debate permanente con algunas organizaciones de la sociedad civil sobre el balance que debe existir entre la seguridad y los derechos como la privacidad, la transparencia o la proporcionalidad, en

---

<sup>1</sup> Real Academia Española: <https://www.rae.es/espanol-al-dia/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas>

cuanto a esto la Comisión Europea para la Democracia a través de la Ley (2007) explica que, en el espacio público, las personas tienen una expectativa menor de privacidad, aunque eso no implica que esperen ser impedidos de sus libertades y derechos en su esfera íntima.

Este documento aboga por la observancia de los derechos a la privacidad y la no discriminación, de modo que sugiere que las tecnologías se utilicen con apego a la ley y exhorta al personal a evitar tomar decisiones bajo prejuicios de raza, género, origen, idioma, posición económica, entre otros.

## **Marco Jurídico**

Constitución Política de los Estados Unidos Mexicanos.

Declaración Universal de los Derechos Humanos.

Convención Americana sobre los Derechos Humanos.

Estatuto de la Corte Interamericana de Derechos Humanos.

Ley General del Sistema Nacional de Seguridad Pública.

Ley de Seguridad Nacional.

Ley de Vías de Comunicación.

Ley General de Bienes Nacionales.

Ley General de Protección Civil.

Ley General de Responsabilidades Patrimoniales.

Ley General de Víctimas.

Ley Nacional sobre el Uso de la Fuerza.

Ley General de Responsabilidades Administrativas.

Ley general de Transparencia y Acceso a la Información Pública.

Ley General de Protección de datos personales en posesión de sujetos obligados.

Ley Federal de responsabilidades de los Servidores Públicos.

Ley General para la Igualdad entre Mujeres y Hombres.

Ley General de Acceso a las Mujeres a una Vida Libre de Violencia.

Ley del Instituto Nacional de las Mujeres.

Reglamento de la Ley General de Protección Civil.

Ley Orgánica del Poder Judicial de la Federación.

Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.

Manual de Organización General en Materia Administrativa de la Suprema Corte de Justicia de la Nación.

Manual de Organización Específico de la Dirección General de Seguridad.





## Contexto

### Reseña histórica

En el mes de julio de 2022 la Dirección General de Seguridad de la Suprema Corte de Justicia de la Nación persiguiendo su objetivo primordial de “*preservar en todo momento la integridad de las personas servidoras públicas, visitantes, bienes muebles e inmuebles...*”, encargó a la empresa externa GRUPO SIAYEC, especializada en el área de seguridad y gestión de riesgos, realizar un diagnóstico con la finalidad de definir, analizar, evaluar y calcular las vulnerabilidades que pudieran impactar en la Institución y sus principales activos, habiéndose encontrado la necesidad de consolidar un sistema integral de seguridad que incluyera elevar las capacidades del centro de monitoreo actual, que contara con la infraestructura y equipamiento tecnológico necesarios para minimizar posibilidades de riesgo, además de la implementación de una plataforma tecnológica específica, como resultado fue creado el **Centro de Control de Seguridad Integral de la Corte**, espacio donde se concentrará la gestión de la seguridad y los riesgos a través del uso de la tecnología y la implementación del Sistema Integral de Seguridad y Gestión de Riesgos

### Misión

Coadyuvar con la Dirección General de Seguridad de la Suprema Corte de Justicia de la Nación en su objetivo primordial de preservar en todo momento la integridad de las personas servidoras públicas, visitantes, bienes muebles e inmuebles y el acervo cultural de la Suprema Corte de Justicia de la Nación haciendo uso de los recursos humanos y tecnológicos de la forma más eficiente para minimizar posibilidades y prevenir riesgo ante cualquier situación.

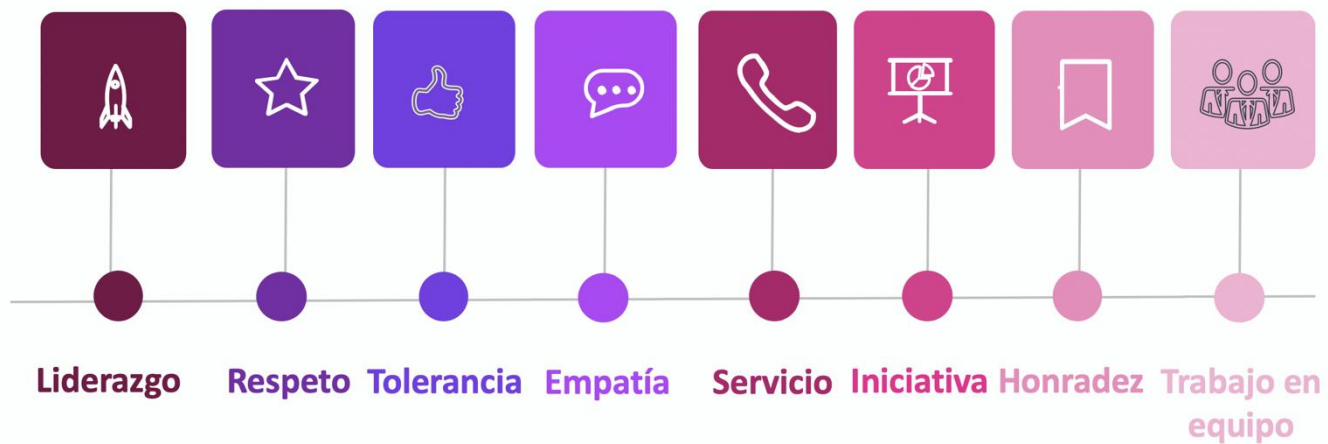
### Visión

Incrementar la calidad en los servicios de seguridad mediante la formación de las personas que integran el equipo de la Dirección General de Seguridad, el uso adecuado de las mejores tecnologías en la materia, que permita desarrollar un modelo de actuación preventiva sustentado en la aplicación de procedimientos y protocolos de actuación que aseguren el cumplimiento de objetivos, metas establecidas y el cumplimiento de la normatividad vigente dando prioridad al respeto de los derechos humanos de las personas que ahí confluyen

### Valores

Los valores que nos definen son:





## Objetivos particulares

Consolidar un ***Centro de Control de Seguridad Integral de la Corte (C2SIC)***, como parte del *Sistema Integral de Seguridad* y Gestión de Riesgos en la Suprema Corte de Justicia de la Nación que cuente con personal, infraestructura tecnológica y equipamiento necesarios para minimizar las posibilidades de riesgo a sus principales activos: las personas, los bienes, el inmueble y el patrimonio cultural, la información y su imagen.

Identificar, prevenir y mitigar los factores de riesgo que se puedan presentar dentro de las instalaciones de la Suprema Corte de Justicia de la Nación, en tiempo real y con información histórica

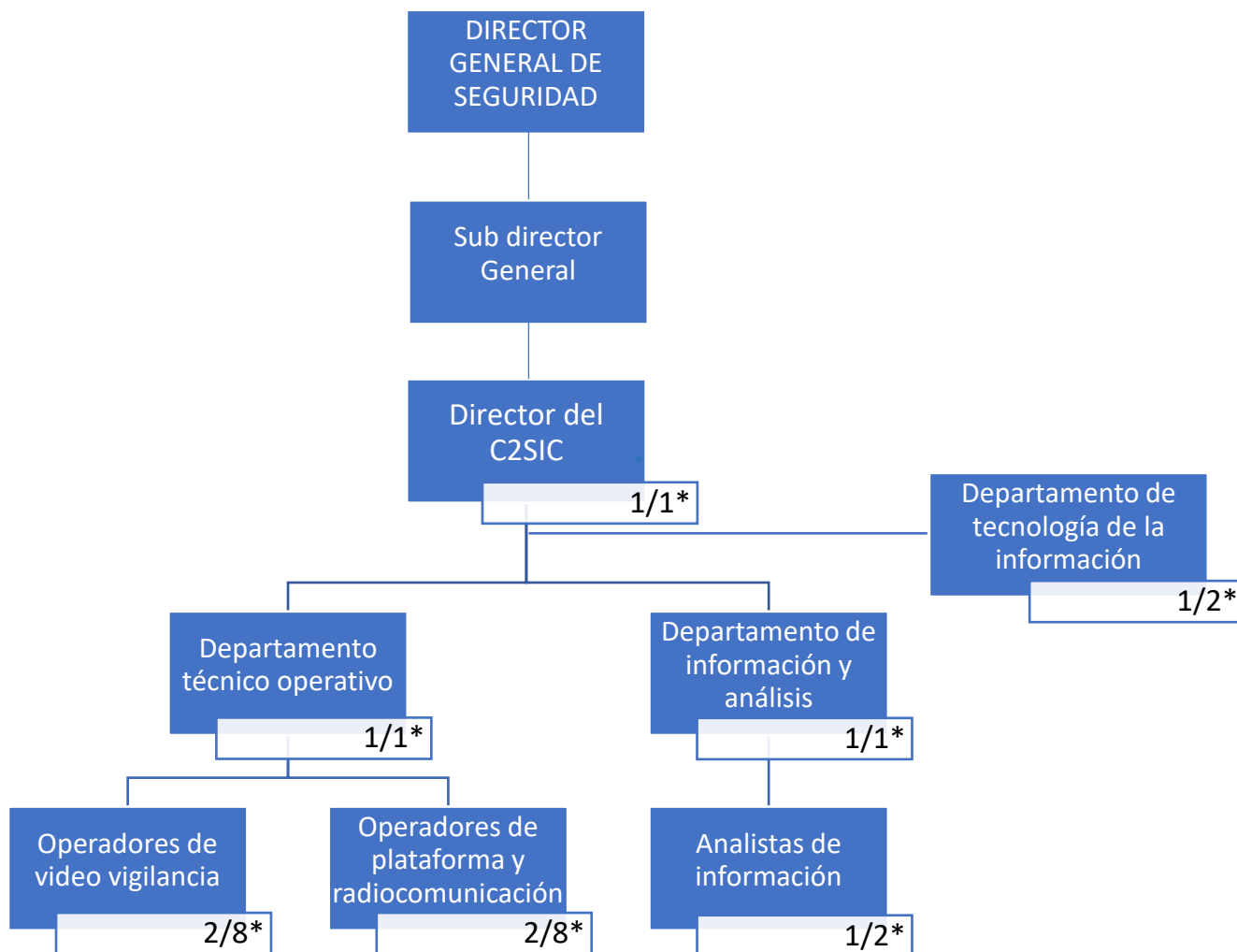
Controlar los procesos de administración de eventos críticos que se puedan presentar en la SCJN.

Mantener permanentemente procesos de mejora continua en el modelo de Seguridad y Gestión de Riesgos.

Fortalecer las tareas del personal de seguridad con el uso de tecnología e información sistematizada que les permita atender y gestionar las emergencias y anticiparse a los riesgos con método, actuando con base a estándares de operación para asegurar un ambiente de paz y tranquilidad.



## Organigrama



\* Personal por turno / total de plazas incluyendo todos los turnos

Los números de plazas mencionados en el organigrama son para la propuesta con personal actual

## Catálogo de puestos y propuesta de plazas

NOMBRE DEL PUESTO	PROPUESTA CON PERSONAL ACTUAL		PROPUESTA A MEDIANO PLAZO		HORARIOS
	POR TURNO	TOTAL	POR TURNO	TOTAL	
DIRECTOR DEL CENTRO DE CONTROL DE SEGURIDAD INTEGRAL DE LA CORTE	1	1	1	1	HORARIO ADMINISTRATIVO
JEFE DE DEPARTAMENTO TÉCNICO OPERATIVO	1	1	1	1	HORARIO ADMINISTRATIVO
JEFE DE DEPARTAMENTO DE INFORMACIÓN Y ANÁLISIS	1	1	1	1	HORARIO ADMINISTRATIVO
OPERADOR DE VIDEOVIGILANCIA VIRTUAL	*2	8	***4	16	3 TURNOS DE 8 HORAS
OPERADOR DE PLATAFORMA TECNOLÓGICA Y RADIO COMUNICACIÓN	**2	8	****2	8	3 TURNOS DE 8 HORAS
ANALISTA DE INFORMACIÓN	1	2	2	4	2 TURNOS DE 8 HORAS
JEFE DE DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN (SOC/NOC IMPLANT)	1	2	1	2	2 TURNOS DE 8 HORAS
<b>TOTAL, DE PERSONAL</b>	<b>9</b>	<b>23</b>	<b>12</b>	<b>33</b>	

*	2 ELEMENTOS POR TURNO DE 8 HORAS EN 3 TURNOS CON 2 ELEMENTOS DE DESCANSO
**	1 ELEMENTO POR TURNO DE 8 HORAS 1 ELEMENTO DE DESCANSO
***	4 ELEMENTOS POR TURNO DE 8 HORAS EN 3 TURNOS CON 4 ELEMENTOS DE DESCANSO
****	2 ELEMENTOS POR TURNO DE 8 HORAS EN 3 TURNOS CON 2 ELEMENTOS DE DESCANSO

## Descripción de áreas principales

### Departamento Técnico Operativo

Es el área encargada de vigilar y cuidar la seguridad, mediante el uso y explotación de las herramientas tecnológicas a su alcance, como lo son: la plataforma Everbridge, BI (Business Intelligence), la plataforma de video vigilancia, sistema de control de accesos, dispositivos de alertamiento y cualquier otro medio disponible, para conocer los hechos que puedan considerarse de riesgo en la seguridad y aplicar las estrategias y protocolos correspondientes de acuerdo con lo detectado.

### Departamento de Información y Análisis

Su función principal es el procesamiento y administración de la información para generar productos de inteligencia que permitan la toma de decisiones estratégicas de forma eficiente y oportuna para la mitigación y prevención de los riesgos.

Por medio de objetivos definidos en función de la visualización de posibles riesgos y la necesidad de mitigar los existentes, desarrollarán capacidades para recolectar información de diversas fuentes abiertas y cerradas, realizando trabajo de campo y de gabinete. Apoyados en el personal de vigilancia, en la plataforma Everbridge y el módulo del BI (Business Intelligence) deberán clasificar, procesar y analizar la información con lo cual se generarán ordenes de trabajo para el personal responsable de vigilancia virtual o presencial realizando acciones preventivas que permitan evitar o mitigar los riesgos visualizados.

Su función incluye la evaluación e identificación de los niveles de seguridad, detectar los factores que incidan en las amenazas, diseñar, integrar y proponer medidas en el corto, mediano y largo plazo para la prevención de estas, la disminución de las debilidades, el incremento de las fortalezas y el aprovechamiento de las oportunidades en beneficio de la seguridad de la institución.

## Departamento de tecnologías de la información

### SOC/NOC

Security Operations Center o Centro de Operaciones de Seguridad /  
Network Operations Center o Centro de Operaciones de Red.

Dedicado a proteger los activos tecnológicos y de información, mantenerlos lejos de amenazas o riesgos innecesarios, y asegurarse de su perfecto funcionamiento las 24 horas del día los 7 días de la semana.

Su objetivo principal es la seguridad de la información y los datos, la identificación de las amenazas de seguridad para el entorno de las tecnologías y el monitoreo del entorno de la red a fin de que cumpla con los requisitos de rendimiento y disponibilidad.



## Descripción de puestos

Describimos los puestos que integran el *Centro de Control de Seguridad Integral de la Corte* de la Suprema Corte de Justicia de la Nación, donde detallamos las funciones y atributos que de quien los ocupe, se especifican las tareas y las responsabilidades inherentes a cada puesto de trabajo, los requisitos necesarios, las actividades a desarrollar y el ámbito de ejecución.

Con lo anterior se pretende facilitar el proceso de reclutamiento, selección, inducción, operación y formación del capital humano que ya integra la institución y los futuros aspirantes.

Con la descripción de las actividades a realizar y los requisitos necesarios para cubrir el puesto, permite que personal que ya integra la institución pueda aspirar a ocupar la vacante y con ello mejorar el clima organizacional promoviendo el desarrollo profesional del capital humano, además de facilitar los procesos de inducción, capacitación y trámites administrativos de contrataciones

La definición precisa de las funciones brinda un marco de referencia para que el nuevo ocupante conozca los requerimientos de la plaza, establece la magnitud y el grado de responsabilidad que se espera de cada persona.



## Director del Centro de Control de Seguridad Integral de la Corte (C2SIC)

### Superior Jerárquico

El Director del *Centro de Control de Seguridad Integral de la Corte* le reporta directamente al Subdirector General de Seguridad y es de quien recibe instrucciones, ordenes, consignas y directrices, sin perjuicio de que a solicitud expresa deba reportar al Director General de Seguridad.

### Funciones

Definir y coordinar las acciones y estrategias de la Dirección del *Centro de Control de Seguridad Integral de la Corte*, con la finalidad de captar la mayor cantidad de eventos e incidentes, apoyándose en los recursos humanos y tecnológicos, para inhibir, minimizar o actuar ante cualquier riesgo que altere la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen.

Vigilar que los procedimientos sean transmitidos a los operadores y analistas de manera adecuada con la finalidad de brindar un servicio más eficiente y adecuado.

Establecer consignas de operación y vigilancia de acuerdo a los productos de inteligencia generados por el área de Información y análisis y las que determine el mando Superior.

Concretar la forma de adquisición, operación, uso y manejo de la información del C2SIC. Establecer las políticas generales y específicas de la Dirección.

Expedir mensualmente o cuando sea requerido por el superior jerárquico, informes derivados del análisis de la información e incidencia registrada en la plataforma tecnológica y elaborada por el área de información y análisis que permitan coadyuvar en la toma de decisiones operativas, con la finalidad de inhibir o mitigar los posibles riesgos que puedan afectar los activos pertenecientes al edificio Sede de la SCJN.

Atender los reportes de anomalías del equipamiento tecnológico utilizado en el Centro de Control de Seguridad Integral de la Corte (C2SIC) solicitando la inmediata atención del personal técnico interno o externo con la finalidad de garantizar la correcta operación del Centro de Control de Seguridad Integral de la Corte (C2SIC).

### Responsabilidades del puesto:

- Dar cumplimiento a las directrices y consignas operativas que designe la Subdirección General.

- Definir y coordinar las acciones y estrategias del Centro de Control de Seguridad Integral de la Corte (C2SIC).
- Concretar la forma de administrar la información del C2SIC.
- Expedir informes de análisis de la información que faciliten la toma de decisiones del mando superior.
- Establecer consignas de operación y vigilancia en base a los productos de inteligencia generados.
- Vigilar que los procedimientos de actuación sean transmitidos correctamente al personal a su cargo.
- Atender los reportes de anomalías de equipamiento tecnológico, así como sugerir la adquisición de nuevas herramientas tecnológicas.
- Proponer métodos que permitan evaluar y conocer el desempeño laboral del personal
- Determinar y solicitar al mando superior los cursos de capacitación continua para el personal a su cargo.
- Organizar y coordinar los trabajos del C2SIC cuyo objetivo es asegurar una utilización racional, equitativa, eficaz y económica de los activos existentes.
- Mantener y asegurar el óptimo funcionamiento del C2SIC para garantizar un servicio seguro y confiable.
- Velar por el adecuado uso y mantenimiento de los equipos, materiales y demás instrumentos asignados para el cumplimiento de las actividades.
- Resolver problemas de alguna complejidad y tomar decisiones con base en precedentes y procedimientos establecidos.

### Área de adscripción

Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC)

### Jefe inmediato superior

Subdirector General de Seguridad

### Jerarquía



### **Formación**

Licenciatura en informática o Sistemas Computacionales, ingeniería terminada, preferentemente en las áreas de administración o tecnologías de la información carrera afín y/o experiencia curricular comprobable.

### **Requisitos**

Sin antecedentes penales.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

### **Conocimientos específicos (conocimientos tecnológicos)**

Conocimiento en administración de personal.

Conocimiento en manejo de grupos de trabajo.

Aplicación apropiada de la terminología.

Conocimientos en temas de tecnología.

Conocimientos en administración de recursos.

Conocimiento de los reglamentos y leyes que le competen.

### **Experiencia deseable**

Experiencia en el mando directivo u operativo.

Experiencia en el área de emergencias.

Conocimientos en materia de seguridad.

Conocimiento sobre normatividades locales y federal.

### **Habilidades**

Resolución de problemas.

Controlar emociones.

Toma de decisiones en situaciones de estrés.

### **Características de personalidad**

Paciente, dinámico, empático, liderazgo, actitud de servicio, comunicación asertiva, iniciativa, tolerancia a la frustración, honradez, honestidad.

## **Jefe del Departamento Técnico Operativo**

### **Superior Jerárquico**

Su mando superior inmediato es Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de las actividades propias del Departamento Técnico Operativo; es del Director del Centro de Control de Seguridad Integral de la Corte (C2SIC) de quien recibe ordenes, consignas y directrices relacionadas con su departamento, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Subdirector General de Seguridad y el Director General de Seguridad.

### **Funciones**

Poner en práctica las acciones y estrategias, que correspondan al Departamento Técnico Operativo con la finalidad de captar la mayor cantidad de eventos e incidentes, apoyándose en los recursos humanos y tecnológicos a su cargo, para inhibir, minimizar o actuar ante cualquier riesgo que altere la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen, aplicando los procedimientos y protocolos correspondientes.

Colaborar para que los procedimientos sean transmitidos y aplicados por los operadores a su cargo con la finalidad de brindar un servicio más eficiente y adecuado.

Asignar áreas de responsabilidad a los operadores, revisar que los tiempos de monitoreo de video vigilancia se cumplan debidamente.

Atender en tiempo real los incidentes de que se tenga conocimiento por los diferentes canales (video vigilancia, reporte o alertamiento a través de la plataforma tecnológica Everbridge, llamada telefónica, verbal o cualquier otro) mediante la aplicación de los protocolos establecidos.

Informar al mando superior inmediato de los incidentes críticos reportados.

Procurar que el material y el equipo de trabajo asignado a los operadores sea el adecuado para la realización de sus labores.

### **Responsabilidades del puesto:**

- Dar cumplimiento a las directrices y consignas operativas que designe la Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC).
- Aplicar las acciones y estrategias definidas por la Dirección del Centro de Mando Estratégico.
- Colaborar para que los procedimientos de actuación sean transmitidos correctamente al personal a su cargo.
- Asignar áreas de video vigilancia a los operadores de video vigilancia virtual en base a las consignas operativas determinadas por el mando superior.
- Vigilar el uso correcto de la plataforma tecnológica, así como el monitoreo constante de los dispositivos de alertamiento y tratamiento de eventos críticos por los Operadores de plataforma tecnológica.
- Informar al mando superior de cualquier anomalía de los equipos de cómputo y tecnología implementada en el Centro de Control de Seguridad Integral de la Corte (C2SIC)
- Reportar a su superior jerárquico, de forma oportuna y correcta, los eventos observados en los que se requiera toma de decisiones
- Coadyuvar con el director del Centro de Control de Seguridad Integral de la Corte (C2SIC) para determinar los cursos de capacitación continua para el personal a su cargo
- Evaluar al personal
- Velar por el adecuado uso y mantenimiento de los equipos, materiales y demás instrumentos asignados para el cumplimiento de las actividades
- Resolver problemas de alguna complejidad y tomar decisiones con base en precedentes y procedimientos establecidos.
- Capacitar y asesorar a los encargados en el C2SIC.
- Planificar los mantenimientos preventivos y correctivos del C2SIC
- Desarrollar todas aquellas funciones inherentes al área de su competencia.
- Y las demás que determine su jefe inmediato

### **Área de adscripción**

Departamento Técnico Operativo de la Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC)

### **Jefe inmediato superior**

Director del Centro de Control de Seguridad Integral de la Corte (C2SIC)

## Jerarquía



## Formación

Licenciatura o ingeniería terminada en las áreas de Derecho, Administración, Seguridad Pública, Atención a emergencias, Tecnologías de la Información, experiencia comprobable en puesto o funciones similares.

## Requisitos

Sin antecedentes penales.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

## Conocimientos específicos

Conocimiento en administración de personal.

Conocimiento en manejo de grupos de trabajo.

Aplicación apropiada de la terminología.

Conocimiento en temas de tecnología.

Conocimiento en administración de recursos.

Conocimiento de los reglamentos y leyes que le competen.

### **Experiencia deseable**

Experiencia en atención a la ciudadanía.

Experiencia en el mando directivo u operativo.

Experiencia en el área de emergencias.

Conocimiento en materia de seguridad.

Conocimiento sobre normatividades locales y federal.

Conocimiento en el manejo de eventos de prioridad alta.

Conocimiento en el manejo de claves operativas.

### **Habilidades**

Resolución de problemas.

Controlar emociones.

Toma de decisiones en situaciones de estrés.

Habilidad en manejo de eventos de prioridad alta.

### **Características de personalidad**

Paciente, dinámico, empático, liderazgo, actitud de servicio, iniciativa. tolerancia a la frustración, facilidad para comunicarse de forma verbal y escrita. Honradez, honestidad.



## Operador de Videovigilancia Virtual

### Superior Jerárquico

Su mando superior inmediato es el Jefe del Departamento Técnico Operativo, es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de sus funciones; es del Jefe del Departamento Técnico Operativo de quien recibe ordenes, consignas y directrices relacionadas con su área, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), Subdirector General de Seguridad y el Director General de Seguridad.

### Funciones

Observar las imágenes que son transmitidas en tiempo real desde las cámaras de video vigilancia previamente instaladas, para conocer cualquier situación de riesgo con la finalidad de inhibir, minimizar o actuar ante cualquier peligro que altere la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen, y ante cualquier incidente aplicar los procedimientos y protocolos correspondientes.

Dar seguimiento visual de cualquier situación de riesgo detectado, mediante la inspección secuencial de las cámaras cercanas al punto del evento, con la finalidad de proporcionar información en tiempo real para su debida atención.

Informar al mando superior y realizar los registros de los incidentes detectados en la plataforma tecnológica Everbridge de acuerdo con los procedimientos y protocolos establecidos.

Informar de cualquier anomalía del equipo técnico utilizado para la realización de sus funciones.

#### Funciones específicas:

- Cumplir con los procedimientos establecidos.
- Monitorear y vigilar por medio del sistema de video vigilancia de manera eficiente y eficaz contribuyendo a la seguridad y aportando información puntual relativa a los hechos observados.
- Definir áreas de importancia dentro de la cobertura visual de la videocámara.
- Conocer la zona asignada para su monitoreo.
- Identificar ubicaciones que representen riesgos.
- Identificar ubicaciones o situaciones susceptibles.

- Prevenir y detectar situaciones en las que se generen eventos que afecten la integridad de los activos de la SCJN.
- Identificar la presencia de personas que no correspondan al entorno de la zona de cobertura de la videocámara asignada.
- Monitoreo por consigna de zonas y horarios de mayor afluencia.
- Reportar a su superior jerárquico, de forma oportuna y correcta, los eventos observados y a través de los dispositivos de comunicación disponibles.
- Registrar en la plataforma tecnológica, todos los eventos detectados que deban tener especial seguimiento.
- Elaborar bitácoras de incidentes.
- Solicitar la intervención del superior jerárquico en situaciones que así lo requieran.
- Seleccionar el fragmento de video donde se haya registrado un incidente.
- Todas aquellas que se relacionen con el cumplimiento del objetivo del puesto.

### Área de adscripción

Departamento Técnico Operativo de la Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC)

### Jefe inmediato superior

Jefe del Departamento Técnico Operativo / Sub director operativo del C2SIC

### Jerarquía



### **Formación**

Licenciatura en informática, carrera afín y/o experiencia curricular comprobable en puestos similares.

### **Requisitos**

Disponibilidad de horario.

Constancia de no antecedentes penales.

No estar sujeto a proceso penal.

Haber cumplido con el servicio militar nacional en el caso de varones.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

En caso de haber pertenecido al ejército presentar licencia ilimitada o documento de baja.

### **Conocimientos específicos**

Eficiencia en el manejo de dispositivos tecnológicos y de comunicación.

Eficiencia en la captura y redacción de datos.

Excelente ortografía.

Eficiencia en el manejo de software de procesamiento de datos.

Conocimientos generales de operación en sistemas informáticos.

Conocimientos básicos sobre normatividad locales y federal.

Conocimiento en el análisis e interpretación de la información.

Conocimiento en psicología del comportamiento.

### **Experiencia deseable**

1 año en puesto similar.

Conocimientos básicos de primeros auxilios.

Contar con experiencia en el área de emergencias por lo menos un año.

Conocimiento en el manejo de claves operativas.

### **Habilidades**

Resolución de problemas.

Rapidez y eficiencia.

Destreza en estrategias operativas.

Realizar dos actividades a la vez.

Controlar emociones.

Toma de decisiones en situaciones de estrés.

Capacidad de análisis y resolución.

Facilidad para la comunicación verbal y escrita.

Atención en detalles.

Sentido común.

**Características de personalidad**

Paciente, dinámico, empático, discreción, actitud de servicio, iniciativa, cooperativo, apego a las reglas, trabajo en equipo, comunicación asertiva, deseos de superación, honradez, honestidad.

## Operador de Plataforma Tecnológica y Radio Comunicación

### Superior Jerárquico

Su mando superior inmediato es el Jefe del Departamento Técnico Operativo, es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de sus funciones; es del Jefe del Departamento Técnico Operativo de quien recibe ordenes, consignas y directrices relacionadas con su área, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), Subdirector General de Seguridad y el Director General de Seguridad.

### Funciones

Atender los incidentes que le son informados a través de los distintos canales como: plataforma Everbridge, dispositivo de radiocomunicación, llamada telefónica, de forma personal, mensaje de texto, observación directa, o cualquier otro, apegándose a los lineamientos de los protocolos, realizando el registro de los incidentes reportados en la plataforma tecnológica de acuerdo con los procedimientos y protocolos correspondientes, para así poder proporcionar el mejor servicio; y canalizar al área correspondiente para su atención inmediata.

Informar a su superior jerárquico de cualquier evento del que se tome conocimiento y registrarlo en la plataforma tecnológica Everbridge, así como de cualquier anomalía del equipamiento tecnológico utilizado para la realización de sus funciones.

### Funciones específicas:

- Responder las llamadas entrantes al Centro de Monitoreo Estratégico.
- Registrar de forma detallada los reportes de los incidentes.
- Ordenar, clasificar y capturar la información proporcionada, según las condiciones y características del incidente.
- Analizar la información que le es proporcionada para determinar el tipo de incidente y con ello poder canalizar al área correspondiente.
- Tranquilizar y asistir emocionalmente al usuario, en caso de ser posible y necesario.
- Reportar al jefe superior inmediato respecto de los incidentes que se consideren de alto riesgo y cuya atención requiera acciones más complejas.
- Capturar la información adicional que pudiera proporcionar en el caso de avisos repetidos, registrándola en un folio único.
- Atender todos los reportes de incidentes que se presenten.

- Apegarse estrictamente a los protocolos de recepción, las instrucciones, los lineamientos y estrategias de atención.
- Efectuar los registros correcta y adecuadamente.
- Efectuar adecuadamente el envío a las áreas y mandos involucrados en la atención del incidente registrado para su conocimiento y actuación correspondiente.
- Acompañar al usuario hasta que arribe la unidad de apoyo si así lo requiere.
- Atención oportuna de incidentes prioritarios para disminuir tiempos de respuesta.
- Hacer uso correcto del equipo asignado y reportar cualquier anomalía.
- Mantener la vigilancia del incidente reportado a través de los dispositivos tecnológicos a su alcance hasta su conclusión y vuelta a la normalidad.

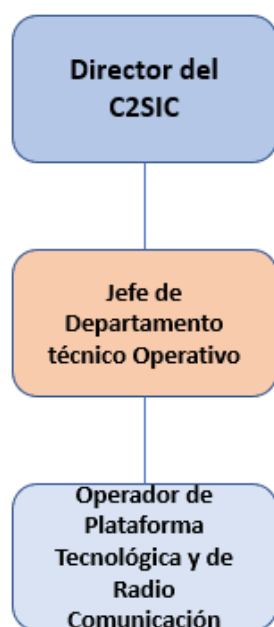
### Área de adscripción

Departamento Técnico Operativo de la Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC)

### Jefe inmediato superior

Jefe del Departamento Técnico Operativo / Sub director del C2SIC

### Jerarquía



### **Formación**

Licenciatura o ingeniería en informática, carrera afín y/o experiencia curricular comprobable en puestos similares.

### **Requisitos**

Disponibilidad de horario.

Constancia de no antecedentes penales.

No estar sujeto a proceso penal.

Haber cumplido con el servicio militar nacional en el caso de varones.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

En caso de haber pertenecido al ejército presentar licencia ilimitada o documento de baja.

### **Conocimientos específicos**

Eficiencia en el manejo del teclado.

Eficiencia en la captura y redacción de datos.

Excelente ortografía.

Manejo de sistemas de radio comunicación

Manejo de claves

Eficiencia en el manejo de software de procesamiento de datos.

Conocimientos generales de operación en sistemas informáticos.

Conocimientos básicos sobre normatividad locales y federal.

Conocimiento psicología del comportamiento.

### **Experiencia deseable**

1 año en puesto similar.

Contar con experiencia en áreas operativas.

### **Habilidades**

Resolución de problemas.

Rapidez y eficiencia.

Destreza en estrategias operativas.

Realizar dos actividades a la vez.

Controlar emociones.

Toma de decisiones en situaciones de estrés.

Capacidad de análisis y resolución.

Facilidad para la comunicación verbal y escrita.

Atención en detalles.



Sentido común.

**Características de personalidad**

Paciente, tolerancia a la frustración, dinámico, empático, discreción, actitud de servicio, iniciativa, cooperativo, comunicación asertiva, apego a las reglas, trabajo en equipo, deseos de superación, honradez, honestidad.

## Jefe del Departamento de Información y Análisis

### Superior Jerárquico

Su mando superior inmediato es Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de las actividades propias del Departamento de Información y Análisis; es del Director del Centro de Control de Seguridad Integral de la Corte (C2SIC) de quien recibe ordenes, consignas y directrices relacionadas con su departamento, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Subdirector General de Seguridad y el Director General de Seguridad.

### Funciones

Efectuar labores de inteligencia consistentes en evaluar, valorar y analizar de forma oportuna y adecuada la información derivada de la plataforma tecnológica Everbridge, Bi (Business Intelligent), atención a las incidencias y de cualquier otra fuente útil y confiable, que lleve a obtener información estratégica para definir acciones, estrategias y políticas que permitan disuadir, contener y neutralizar riesgos y amenazas a la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen, apoyándose en los recursos humanos y tecnológicos a su cargo.

Asumir peticiones urgentes de búsqueda de información, tomando en cuenta prioridades y necesidades específicas. Identificar aquellos contenidos que puedan ser considerados como críticos y que, por tanto, requieran de una rápida atención.

En coordinación con el analista y con el director del Centro de Mando, hacer propuestas de mejora dentro de los procedimientos.

Procurar que el material y el equipo de trabajo asignado sea el adecuado para el cumplimiento de las labores del personal a su cargo.

### Responsabilidades del puesto:

- Realizar labores de inteligencia que permitan generar información útil para la toma de decisiones.
- Dirigir, coordinar y operar los sistemas de recolección, clasificación, registro análisis, explotación y evaluación de la información.
- Determinar las fuentes de información de acuerdo a su veracidad para su procesamiento.
- Realizar informes de avances y resultados para el mando superior que permitan mejorar las acciones operativas y medidas de prevención disuasión, contención y desactivación de

- amenazas y riesgos.
- Elaboración de galerías y bases de datos de individuos sospechosos o grupos de choque que permitan la rápida identificación por los operadores de video vigilancia virtual y personal de seguridad y el tratamiento correspondiente.

### Área de adscripción

Departamento de Información y Análisis de la Dirección del C2SIC

### Jefe Inmediato Superior

Director de Centro de Control de Seguridad Integral de la Corte (C2SIC)

### Jerarquía



### Formación

Licenciatura o ingeniería terminada en las áreas de tecnologías de la información, Licenciatura en matemáticas, Criminalística, Actuaría o carrera afín y/o experiencia curricular comprobable.

### Requisitos

Sin antecedentes penales.

Actitud de apego y respeto a las normas y valores institucionales.

Actitud de compromiso hacia el manejo de información confidencial.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

### **Conocimientos específicos**

Conocimiento en administración de personal.  
Conocimiento en manejo de grupos de trabajo.  
Conocimientos en administración de sistemas.  
Aplicación apropiada de la terminología.  
Conocimiento en temas de tecnología.  
Conocimiento en administración de recursos.  
Conocimiento de los reglamentos y leyes que le competen.

### **Experiencia deseable**

Experiencia en atención a la ciudadanía.  
Experiencia en el mando directivo u operativo.  
Experiencia en el área de emergencias.  
Conocimiento en materia de seguridad.  
Conocimiento sobre normatividades locales y federal.  
Conocimiento en el manejo de eventos de prioridad alta.

### **Habilidades**

Resolución de problemas.  
Controlar emociones.  
Toma de decisiones en situaciones de estrés.  
Habilidad en manejo de eventos de prioridad alta.

### **Características de personalidad**

Paciente, dinámico, empático, liderazgo, actitud de servicio, iniciativa. tolerancia a la frustración, facilidad para comunicarse de forma verbal y escrita, honradez, honestidad.

## Analista de información

### Superior Jerárquico

Su mando superior inmediato es el Jefe del Departamento de Información y Análisis, es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de sus funciones; es del Jefe del Departamento de Información y Análisis de quien recibe ordenes, consignas y directrices relacionadas con su área, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), Subdirector General de Seguridad y el Director General de Seguridad.

### Funciones

Administrar y analizar de forma rigurosa y meticulosa la información existente proporcionando resultados, conclusiones, estadísticas, reportes, resúmenes, etc. que se transforme en conocimiento con un alto valor que ayude a tomar decisiones con la menor incertidumbre posible.

Procesar la información obtenida a través del análisis de las distintas fuentes de información disponibles, con la finalidad de obtener productos de inteligencia que faciliten la toma de decisiones en tiempo real, la mitigación de riesgos y las medidas preventivas que permitan garantizar la seguridad de los Ministros, las personas y los activos del edificio Sede de la SCJN.

Informar de cualquier anomalía del equipo técnico utilizado para la realización de sus funciones.

### Funciones específicas

- Recolección de información.
- Revisión de información.
- Concentración de información de gabinete y campo para realizar la coordinación con el área jurídica y operativa según corresponda.
- Elaboración de tarjetas informativas, redes de vinculación, consignas operativas para la toma de decisiones.
- Seguimiento de los oficios emitidos por las diferentes corporaciones para proporcionar la información correspondiente.
- Emitir galerías al área de video vigilancia, así como estrategias de monitoreo.

- Planear, analizar y almacenar la documentación digital o impresa sobre las solicitudes de información de las diferentes áreas internas o externas de acuerdo a como lo solicite el mando superior.
- Proporcionar la información requerida utilizando los protocolos de resguardo de la información y cadena de custodia según se requiera.
- Elaborar estadística de incidencia, que permita a los titulares la toma de decisiones en cuanto a esquemas de operación para la disminución de tiempos de respuesta y mitigación de riesgos.
- Calcular tiempos promedio en el proceso de atención de eventos críticos y proponer medidas de mejora continua para su la atención.

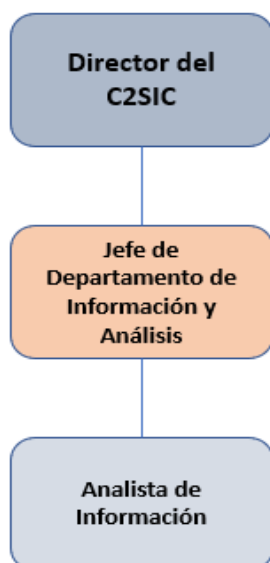
### Área de adscripción

Departamento de Información y Análisis de la Dirección del Centro de Mando

### Jefe Inmediato Superior

Jefe del Departamento de Información y Análisis

### Jerarquía



### Formación

Licenciatura o ingeniería terminada en las áreas de Derecho, Administración, Seguridad Pública, Criminología, Criminalística o Tecnologías de la Información, carrera afín y/o experiencia curricular comprobable.

### **Requisitos**

Disponibilidad de horario

Actitud de apego y respeto a las normas y valores institucionales.

Actitud de compromiso hacia el manejo de información confidencial.

Constancia de no antecedentes penales.

No estar sujeto a proceso penal.

Haber cumplido con el servicio militar nacional en el caso de varones.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

En caso de haber pertenecido al ejército presentar licencia ilimitada o documento de baja.

### **Conocimientos específicos**

Eficiencia en la captura y redacción de datos.

Análisis de datos y estadísticas.

Diseño de base de datos.

Excelente ortografía.

Lectura y redacción.

Eficiencia en el manejo de software de procesamiento de datos.

Conocimientos generales de operación en sistemas informáticos.

Conocimientos básicos sobre normatividad locales y federal.

### **Experiencia deseable**

1 año en puesto similar.

### **Habilidades**

Resolución de problemas.

Realizar dos actividades a la vez.

Orientación a resultados.

Controlar emociones.

Toma de decisiones en situaciones de estrés.

Capacidad de análisis y resolución.

Facilidad para la comunicación verbal y escrita.

Atención en detalles.

Agilidad mental.

### **Características de personalidad**

Paciente, asertivo, tolerancia a la frustración, dinámico, empático, discreción, actitud de servicio, iniciativa, cooperativo, apego a las reglas, trabajo en equipo, deseos de superación, honradez, honestidad.



## Jefe de Departamento de Tecnología de la Información

SOC (Security Operation Center) / NOC (Network Operation Center)

### Superior Jerárquico

Su mando superior inmediato es Director del Centro de Control de Seguridad Integral de la Corte (C2SIC), es a él a quien debe entregar bitácoras, novedades y cualquier otro reporte (físico, verbal o electrónico) derivado de las actividades propias de su área; es del Director del Centro de Control de Seguridad Integral de la Corte (C2SIC) de quien recibe ordenes, consignas y directrices relacionadas con su departamento, sin perjuicio de que a solicitud expresa deba reportar a los mandos jerárquicos superiores, esto es el Subdirector General de Seguridad y el Director General de Seguridad.

### Funciones

Mantener la integridad y funcionamiento de los recursos tecnológicos (video vigilancia, radiocomunicaciones, conmutación telefónica, red de datos y sistemas de información), y garantizar que permanezcan en actividad continua.

Detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques diferentes. Supervisar y analizar la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad.

Garantizar que los posibles incidentes de ciberseguridad se identifiquen, analicen, defiendan, investiguen e informen adecuadamente; asegurarse de que el problema de ciberseguridad se aborde adecuadamente una vez que se ha descubierto.

Monitorear y analizar la infraestructura tecnológica, y al detectar una anomalía, actuar rápidamente para escalar, determinar la naturaleza de la amenaza y resolverla.

### Funciones específicas

- Cumplir con los procedimientos establecidos.
- Garantizar el correcto funcionamiento de la tecnología instalada en el Centro de Control de Seguridad Integral de la Corte (C2SIC).
- Vigilar el correcto funcionamiento de los dispositivos de alertamiento UVIS, cámaras LPR, RFID, XRAY, Arcos Detectores, SCAN ID, y demás dispositivos que se determinen y que se encuentren alojados en la plataforma tecnológica Everbridge.
- Monitorear y vigilar por medio de las consolas NOC los recursos tecnológicos.

- Mantener activa y en funcionamiento la Plataforma Tecnológica Everbridge.
- Administración de las consolas de despacho Radio.
- Consolas de video vigilancia VMS.
- Definir áreas de importancia dentro de la cobertura visual de las consolas de despacho.
- Identificar las amenazas de seguridad para el entorno de las tecnologías de información.
- Cuidar la seguridad de la información y los datos.
- Prevenir y responder a los incidentes de seguridad cibernética.
- Monitorear y desarrollar estrategias de seguridad.
- Gestionar las operaciones de tecnologías de la información y equipamiento en redes como routers, switches, firewalls y puntos de acceso.
- Proveer soporte para resolver los problemas relacionados con la infraestructura de la red.
- Configurar, implementar y dar soporte a todos los componentes de redes.
- Monitorear todos los sistemas de línea e instalaciones digitales.
- Gestionar proveedores de tecnología que implementan soluciones.
- Gestionar, completar, verificar y restaurar respaldos.
- Realizar gestión de accesos.
- Gestionar la disponibilidad y capacidad de la plataforma.
- Reportar al jefe inmediato superior los eventos técnicos observados.
- Identificar y atender emergencias que representen riesgo.
- Prevenir y detectar situaciones en las que se generen eventos técnicos no planeados.
- Elaborar bitácoras de incidentes.
- Solicitar la intervención del supervisor en situaciones que así lo requieran.
- Todas aquellas que se relacionen con el cumplimiento del objetivo del puesto.

### **Área de adscripción**

Departamento de tecnología de la información.

SOC / NOC de la Dirección del C2SIC.

### **Jefe Inmediato Superior**

Director del Centro de Control de Seguridad Integral de la Corte (C2SIC).

### Jerarquía



### Formación

Licenciatura o ingeniería terminada en las áreas de tecnologías de la información.

Ingeniería en Sistemas, Computación, Telecomunicaciones o afines.

Certificaciones NOC, ITIL o afines

### Requisitos

Disponibilidad de horario.

Actitud de apego y respeto a las normas y valores institucionales.

Actitud de compromiso hacia el manejo de información confidencial.

Constancia de no antecedentes penales.

No estar sujeto a proceso penal.

Haber cumplido con el servicio militar nacional en el caso de varones.

No haber sido dado de baja por deserción o comisión de honor y justicia de alguna corporación policial.

En caso de haber pertenecido al ejército presentar licencia ilimitada o documento de baja.

### Conocimientos específicos

Conocimiento en administración de personal.

Conocimiento en manejo de grupos de trabajo.

Conocimientos en administración de sistemas.  
Aplicación apropiada de la terminología.  
Conocimiento en temas de tecnología.  
Conocimiento en temas de ciberseguridad.  
Conocimiento en administración de recursos.  
Conocimiento de los reglamentos y leyes que le competen.

### **Experiencia deseable**

1año en puesto similar.  
Experiencia en el área de emergencias.  
Conocimiento en materia de seguridad.  
Experiencia en materia de ciberseguridad.  
Conocimiento sobre normatividades locales y federal.  
Conocimiento en el manejo de eventos de prioridad alta.

### **Habilidades**

Resolución de problemas.  
Controlar emociones.  
Toma de decisiones en situaciones de estrés.  
Habilidad en manejo de eventos de prioridad alta.

### **Características de personalidad**

Paciente, dinámico, empático, liderazgo, actitud de servicio, iniciativa. tolerancia a la frustración, facilidad para comunicarse de forma verbal y escrita, honradez, honestidad.



## Ejes principales y reglas de operación

### Ejes principales

Los ejes sobre los cuales están definidos los principales procesos y desarrolladas las reglas de operación para el Centro de Control de Seguridad Integral de la Corte (C2SIC)



### Principales procesos

#### A. Técnico Operativo

- Alertamiento por video vigilancia.
- Alertamientos generados por dispositivos tecnológicos (rayos x, arco detector, sistema de inspección de vehículos, cámaras de video vigilancia, tarjetas electrónicas de autenticación, antenas, cámara de solapa, etc.).
- Alertamiento por diferentes canales (plataforma, teléfono, WhatsApp, verbal, redes, etc.).
- Atención a requerimientos de grabaciones de video.

## **B. Información y análisis**

- Acopio de información por tema específico.
- Acopio de información que tenga alguna relación con la SCJN.
- Manejo y explotación de la información para generar productos de Inteligencia.

## **C. Tecnología de la Información (SOC / NOC)**

- Monitoreo de infraestructura tecnológica, sistema de seguridad, red y bases de datos, no se encuentra falla.
- Detección de falla en infraestructura tecnológica mediante plataformas de monitoreo.
- Detección de intrusión malware al sistema de seguridad perimetral.
- Aviso de falla reportada por el usuario.

## Principales reglas de operación

### A. Técnico Operativo

#### Alertamiento por video vigilancia

1. El operador observa un incidente.
2. Informa a su superior inmediato del evento observado.
3. Solicita autorización para activar protocolo en la plataforma Everbridge.
4. Registra en la plataforma Everbridge.
5. Se comunica a las áreas de seguridad correspondientes para su atención utilizando los canales de comunicación ideales según las alternativas.
6. Localiza las cámaras cercanas al lugar del evento.
7. Enfoca y manipula las cámaras para apoyar en la atención.
8. Encuentra el posible trayecto del evento.
9. Brinda información de lo observado a las áreas que estén atendiendo.
10. Informa al mando las acciones tomadas para la solución del evento
11. Registra en la plataforma las acciones realizadas y solicita autorización para el cierre del evento.
12. Cierre del incidente en plataforma.

#### Alertamientos generados por dispositivos tecnológicos

1. Sucede un evento.
2. Alguno de los dispositivos utilizados en las actividades de seguridad como rayos x, arco detector, sistema de inspección de vehículos, cámaras de video vigilancia, tarjetas electrónicas de autenticación, antenas, cámara de solapa, etc. dispara una alerta.
3. Se notifica al centro de mando, de forma manual o automatizada.
4. El operador de plataforma recibe reporte del incidente.
5. Informa a su superior inmediato del evento observado.
6. Solicita autorización para activar protocolo en la plataforma Everbridge.
7. Registra en plataforma Everbridge (De forma manual o automática según la situación) y se genera folio único que identifique el incidente.
8. Identifica prioridad del evento
9. Se comunica a las áreas de seguridad correspondientes para su atención utilizando los canales de comunicación ideales según las alternativas.
10. Comunica al video vigilante.
11. El operador de video vigilancia localiza las cámaras cercanas al lugar del evento.

12. El operador de video vigilancia enfoca y manipula las cámaras para apoyar en el reporte.
13. El operador de video vigilancia encuentra el posible trayecto del evento.
14. Brinda información de lo observado a las áreas que estén atendiendo.
15. Seguimiento del incidente hasta su resolución.
16. Informa al mando las acciones tomadas para la solución del evento.
17. Registra en la plataforma las acciones realizadas y solicita autorización para el cierre del evento.
18. Cierre del incidente en plataforma.

### **Alertamiento por diferentes canales**

1. El operador de plataforma tiene conocimiento de un incidente mediante alguno de los canales de alertamiento: monitoreo de cámaras de video vigilancia, dispositivo, app, llamada telefónica, WhatsApp, verbal, etc.
2. Informa a su superior inmediato del evento observado.
3. Solicita autorización para activar protocolo en la plataforma Everbridge.
4. Registro en plataforma
5. Informar a las áreas de seguridad corresponda para que acudan a dar la atención o apliquen los protocolos debidos.
6. Seguimiento y soporte de la atención que se esté brindando, ubicar en las cámaras el lugar del incidente para apoyo visual.
7. Informa al mando las acciones tomadas para la solución del evento.
8. Registra en la plataforma las acciones realizadas y solicita autorización para el cierre del evento.
9. Cierre del incidente en plataforma.

### **Atención a requerimientos de grabaciones de video**

1. Recepción de la solicitud, debe ser por algún medio formal que dé soporte a la entrega del video (oficio, correo electrónico o alguna otra previa autorización del Director del C2SIC).
2. Registro de la solicitud.
3. Evaluar si se debe entregar el video solicitado, es decir si quien lo está pidiendo tiene facultades para ello.
4. En el caso de que el solicitante no tenga atribuciones para recibir el video, contestar mediante oficio que no es posible atender su solicitud.
5. Si el solicitante está facultado para hacer la petición, buscar la grabación solicitada.
6. Al ser encontrado el video de cuestión, grabarlo en el medio disponible (cd, memoria USB, drive en la nube, etc.).



7. Entregar la grabación mediante oficio, anexando una copia, que sirva de acuse de recibo, en la que se recabe evidencia de la entrega mediante sello y/o firma, y se anote de puño y letra del receptor fecha y hora, conforme a requerimientos de cadena de custodia.
8. Archivar el video solicitado, el acuse de recibo y el oficio de solicitud.

## **B. Información y Análisis**

### **Acopio de información por tema específico**

1. Definir el objetivo del análisis que tenga o pueda tener relación con el objetivo de interés.
2. Realizar búsqueda en bases de datos.
3. Realizar búsqueda en redes sociales.
4. Realizar búsqueda en grupos de WhatsApp.
5. Realizar búsqueda en medios digitales.
6. Realizar Búsqueda en medios impresos.
7. Captura y clasificación de la información en plataforma.
8. Realizar informe y entregar a su superior jerárquico.

### **Acopio de información que tenga alguna relación con la SCJN**

1. Realizar búsqueda en bases de datos disponibles.
2. Realizar búsqueda en redes sociales.
3. Realizar búsqueda en grupos de WhatsApp.
4. Realizar búsqueda en medios digitales.
5. Realizar búsqueda en medios impresos.
6. Captura y clasificación de la información en plataforma.
7. Realizar informe y entregar a su superior jerárquico.

### **Manejo y explotación de la información para generar productos de inteligencia**

1. Definir el objetivo del análisis.
2. Seleccionar y clasificar la información almacenada en las bases de datos que pueda ser útil para el objetivo del análisis.
3. Buscar, valorar, clasificar y en su caso documentar publicaciones, tendencias en medios informales como redes sociales, archivos virtuales, medios de comunicación digital e impresa, que puedan tener relación con el tema de análisis.
4. Clasificar, evaluar, procesar y analizar la información.
5. Generar los productos de inteligencia: reportes, gráficas, estadísticas, tarjetas informativas, carpetas temáticas, documentos de análisis, ordenes de trabajo para personal de vigilancia virtual o presencial y otros que pudieran necesitarse.

6. Llevar registro de los productos de inteligencia generados.
7. Entregar al mando superior, de forma automatizada y/o en documento físico según le sea requerido.

### **C. Tecnología de la Información (SOC / NOC)**

#### **Monitoreo a infraestructura tecnológica, sistema de seguridad, red y bases de datos.**

1. Al iniciar el turno realizar un monitoreo a todos los indicadores de alarma
2. Observar periódicamente los indicadores de alarma durante el turno.
3. Al finalizar el turno si no se encontró ningún indicador de alarma llenar el reporte correspondiente.

#### **Detección de falla en infraestructura tecnológica mediante plataformas de monitoreo.**

1. Registrar en plataforma la falla encontrada.
2. Clasificar y categorizar por tipo.
3. Determinar si se trata de falla tecnológica o de seguridad de información.
4. Brindar información a las áreas que corresponda.
5. Iniciar procedimiento de nivel de servicio:
  - a. Dar soporte técnico local.
  - b. Ponerse en contacto con el proveedor cuando existe póliza de mantenimiento.
  - c. Contratación de solución única.
6. Gestionar LOGS.
7. Dar seguimiento al incidente hasta su resolución.
8. Cierre del incidente en plataforma.
9. Notificar al mando superior la solución e el estatus de la falla

#### **Detección de intrusión malware al sistema de seguridad perimetral.**

1. Se observa alguna notificación que indique la posible intrusión de malware en algún equipo o un punto de la seguridad perimetral.
2. Registrar en plataforma la falla encontrada.
3. Clasificar y categorizar por tipo de evento.
4. Brindar información a las áreas que corresponda el evento.
5. Iniciar procedimiento de nivel de servicio:
  - a. Dar soporte técnico local.
  - b. Ponerse en contacto con el proveedor cuando existe póliza de mantenimiento.
  - c. Contratación de solución única.

6. Gestionar LOGS.
7. Dar seguimiento al incidente hasta su resolución.
8. Cierre del incidente en plataforma.
9. Notificar al mando superior el estatus de la posible intrusión y la información que respalde el reporte

**Aviso de falla reportada por el usuario.**

1. El usuario da aviso de alguna falla.
2. Registrar en plataforma.
3. Clasificar y categorizar por tipo.
4. Determinar si se trata de una falla tecnológica o de seguridad de información.
5. Brindar información a las áreas que corresponda el evento.
6. Iniciar procedimiento de nivel de servicio:
  - a. Dar soporte técnico local.
  - b. Ponerse en contacto con el proveedor cuando existe póliza de mantenimiento.
  - c. Contratación de solución única.
7. Gestionar LOGS.
8. Dar seguimiento al incidente hasta su resolución.
9. Cierre del incidente en plataforma.
10. Reporte de solución aplicada con firma de satisfacción del usuario.



## Políticas, reglas y restricciones

A continuación, se describen las políticas, reglas y restricciones del Centro de Control de Seguridad Integral de la Corte (C2SIC) de la SCJN:

El Director General de Seguridad es la autoridad superior jerárquica y el encargado de establecer las políticas generales y específicas para la toma de decisiones.

El Subdirector General de Seguridad es la autoridad superior jerárquica inmediatamente después del Director General de Seguridad y en su ausencia será quien tome las decisiones; es el encargado de coordinar las labores de los diferentes departamentos de la Dirección General.

El Director del Centro de Control de Seguridad Integral de la Corte (C2SIC) es el encargado de definir y coordinar las acciones y estrategias de la Dirección del Centro de Control de Seguridad Integral de la Corte (C2SIC), con la finalidad de captar la mayor cantidad de eventos e incidentes, apoyándose en los recursos humanos y tecnológicos, para inhibir, minimizar o actuar ante cualquier riesgo que altere la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen. De igual forma es quien debe concretar la forma de adquisición, operación, uso y manejo de la información del centro de mando. Establecer las políticas generales y específicas de la Dirección.

Son funciones del Jefe de departamento Técnico Operativo poner en práctica las acciones y estrategias, que correspondan al Departamento Técnico Operativo con la finalidad de captar la mayor cantidad de eventos e incidentes, apoyándose en los recursos humanos y tecnológicos a su cargo, para inhibir, minimizar o actuar ante cualquier riesgo que altere la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen, aplicando los procedimientos y protocolos correspondientes.

El Jefe del Departamento de Información y Análisis es el encargado de efectuar labores de inteligencia consistentes en evaluar, valorar y analizar de forma oportuna y adecuada la información derivada de la plataforma tecnológica Everbridge, Bi (Business Intelligent), atención a las incidencias y de cualquier otra fuente útil y confiable, que lleve a obtener información estratégica para definir acciones, estrategias y políticas que permitan disuadir, contener y neutralizar riesgos y amenazas a la seguridad de los principales activos de la Suprema Corte de Justicia de la Nación: personas, inmueble, información, patrimonio cultural e imagen, apoyándose en los recursos humanos y tecnológicos a su cargo.

Es responsabilidad de cada jefe de departamento, verificar que la operación y desarrollo de las funciones al interior de su área, se realicen en estricto apego al cumplimiento de los reglamentos.

El personal adscrito, invariablemente, debe cumplir con las reglas de conducta, operación y uso adecuado de la información y equipos especiales de trabajo, observando los códigos de comunicación y vestimenta que determine la Dirección General de Seguridad, a efecto de salvaguardar la disciplina y el orden dentro y fuera del área de trabajo.

Por ningún motivo, el personal debe permanecer en el interior del Centro de Control de Seguridad Integral de la Corte (C2SIC) en horario distinto al de sus labores, a menos de que exista alguna orden directa de su mando superior jerárquico o causa puntual y específica.

Toda persona al interior del Centro de Control de Seguridad Integral de la Corte (C2SIC) debe portar su identificación institucional.

El personal adscrito debe abstenerse del uso de aparatos distractores mientras se encuentre en funciones.

Es responsabilidad del personal adscrito, la entrega en tiempo y forma de su bitácora de inicio y conclusión de actividades, indicando en el formato correspondiente el parte de novedades e incidencias que se presentaron en la jornada laboral.

Es responsabilidad del personal adscrito, la captura en la plataforma Everbridge de los incidentes que atienda, de forma inmediata, completa y correcta, cuidando que la información ingresada sea la más apegada al incidente en cuestión.

Es facultad del director y de cada jefe de departamento convocar al personal operativo a su cargo, las veces necesarias y en cualquier momento, a reuniones de trabajo para evaluar las acciones y resultados del área o bien para instruir sobre las medidas que en materia de seguridad se disponga.

No está permitido ingresar al C2SIC tabletas, teléfonos inteligentes, cámaras fotográficas, memorias USB o cualquier otro dispositivo que sirva para extraer o difundir información, fotografías o cualquier otro que vulnere la integridad y/o la seguridad.



No está permitido introducir o extraer, objetos no autorizados o información, que comprometan la seguridad. Los objetos no autorizados dentro del C2SIC serán definidos por la superioridad jerárquica.

La información a la que se tenga acceso será de estricto carácter confidencial y debe ser usada únicamente con fines de seguridad.

La superioridad jerárquica es la facultada para sancionar cualquier incumplimiento.



## Indicadores de gestión

DEPARTAMENTO TÉCNICO OPERATIVO 	DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN 	DEPARTAMENTO DE INFORMACIÓN Y ANÁLISIS 
<ol style="list-style-type: none"> <li>1 Número de incidentes registrados, por periodo de tiempo, en el Centro de Mando Estratégico, procedentes e improcedentes.</li> <li>2 Número de incidentes, críticos y comunes, atendidos en un periodo de tiempo.</li> <li>3 Número de incidentes registrados, por periodo de tiempo, por operador de video vigilancia.</li> <li>4 Número de incidentes registrados, por periodo de tiempo, por operador de plataforma.</li> <li>4 Número de incidentes detectados, por periodo de tiempo, por dispositivo de alertamiento.</li> <li>4 Número de incidentes detectados, por periodo de tiempo, por cada uno de los diferentes canales de comunicación</li> <li>4 Promedio de tiempos de respuesta de atención a incidentes de seguridad.</li> </ol>	<ol style="list-style-type: none"> <li>1 Número de fallas en infraestructura tecnológica en un periodo de tiempo</li> <li>2 Número de amenazas de intrusión malware al sistema de seguridad perimetral</li> <li>3 Número de fallas en el equipo tecnológico reportadas por el usuario</li> <li>4 Numero de requerimientos técnicos</li> <li>4 Nivel de calidad del equipo tecnológico</li> <li>4 Número de registros de información en la plataforma que tenga relación con la SCIN, por tema específico o en general.</li> </ol>	<ol style="list-style-type: none"> <li>1 Nivel de satisfacción del usuario (se mide mediante encuestas)</li> <li>2 Número de productos de inteligencia generados por analista.</li> <li>3 Número productos de inteligencia entregados, en un periodo de tiempo, derivados de solicitud expresa</li> <li>4 Ordenes directas de trabajo generadas al personal operativo</li> </ol>

Estos indicadores de gestión son propuestas de acuerdo a las actividades del Centro de Control de Seguridad Integral de la Corte (C2SIC), sin embargo es probable que una vez que inicie la operación del Sistema Integral de Seguridad y Gestión de Riesgos y el uso de la plataforma tecnológica que lo administrará, el funcionamiento del departamento de Información y Análisis y todos los componentes que lo integran, los requerimientos de información podrán evolucionar conforme la mitigación de riesgos vaya avanzando, sin olvidar que la seguridad es un ecosistema, que va modificando sus expresiones de acuerdo a varios elementos coyunturales. Por ello es posible que estos indicadores puedan modificarse y es recomendable dar seguimiento y actualización de cada uno de ellos de forma periódica.

**Bitácora de incidencia:** Documento de trabajo que permite de manera lógica y puntual enunciar los principales acontecimientos del día.

**CCTV:** Circuito Cerrado de Televisión.

**C2SIC.** Centro de Control de Seguridad Integral de la Corte.

**Dispositivos de alertamiento.** Equipo técnico utilizado en las actividades de seguridad: rayos x, arco detector, sistema de inspección de vehículos, cámaras de video vigilancia, tarjetas electrónicas de autenticación, antenas, cámara de solapa, etc.

**Evento o Incidente.** Cualquier hecho o circunstancia que indique un posible riesgo o vulnere la seguridad y deba ser atendido según los procedimientos y protocolos.

**Infraestructura tecnológica:** Conjunto de elementos y dispositivos para el almacenamiento de los datos, incluye el hardware, el software y los diferentes servicios para la gestión interna y seguridad de información.

**LOGS.** Registro secuencial de acontecimientos en archivo.

**Novedades:** Seguimiento de observación y vigilancia que permite conocer en tiempo real el estado de seguridad en que se cuenta la sede.

**Procedimiento.** Son pasos claros y objetivos que se deben seguir para completar una tarea.

**Proceso.** Un proceso es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico.

**Protocolo:** Descripción detallada en forma sucinta de las actuaciones que debemos hacer frente a una situación por ejemplo de emergencia, para evacuar un edificio, o para el uso de extintores, solo por nombrar dos de los más conocidos.

**Reporte.** Informe de un evento o documentación del resultado de un procedimiento.



**SCJN.** Suprema Corte de Justicia de la Nación.

**SOC / NOC.** Centro de Operaciones de Seguridad / Centro de Operaciones de Red (Security Operations Center / Network Operations Center, por sus siglas en inglés).



## Referencias

Manual De Organización General En Materia Administrativa Suprema Corte De Justicia De La Nación.

Comisión Nacional de Seguridad –Protección federal. Guía para la elaboración de análisis de riesgos.

[https://www.gob.mx/cms/uploads/attachment/file/200323/Gu\\_a\\_de\\_An\\_lisis\\_de\\_Riesgos\\_OK.pdf](https://www.gob.mx/cms/uploads/attachment/file/200323/Gu_a_de_An_lisis_de_Riesgos_OK.pdf)

Norma Técnica para la Estandarización de los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (nueve, uno, uno). Secretariado Ejecutivo del Sistema Nacional de Seguridad Publica.

[https://www.gob.mx/cms/uploads/attachment/file/290653/Norma\\_CALLES.pdf](https://www.gob.mx/cms/uploads/attachment/file/290653/Norma_CALLES.pdf)

Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video-Vigilancia para la Seguridad Pública. Secretariado Ejecutivo del Sistema Nacional de Seguridad Publica.

[https://secretariadoejecutivo.gob.mx//docs/pdfs/consejo/Norma\\_tecnica\\_sistemas\\_video\\_vigilancia.pdf](https://secretariadoejecutivo.gob.mx//docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf)

Real Academia Española:

<https://www.rae.es/espanol-al-dia/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas>

## REFERENCIAS AL ANEXO TÉCNICO

### Requerimientos mínimos de Tabla de Contenidos del Manual:

#### 1. Introducción

- |    |                                     |  |
|----|-------------------------------------|--|
| a. | Antecedentes                        | Reseña histórica   |
| b. | Necesidad de un C2SIC               | Necesidad de un Centro de Control de Seguridad Integral de la Corte (C2SIC)    |
| c. | Elementos del C2SIC                 | Misión, Visión, Valores, Objetivos y metas, Estructura, Descripción de puestos |
| d. | Estructura organizacional del C2SIC | Estructura   |
| e. | Matriz RACI del C2SIC               | Estructura orgánica y Descripción de puesto                                    |
| f. | Clasificación de incidentes         | Procesos   |

#### 2. Administración de Incidentes

- |    |  |          |
|----|--|----------|
| a. | Flujos de procesos   | Procesos |
| b. | Reconocimiento, identificación y administración                              | Procesos |
| c. | Manejo de una incidencia a través del C2SIC                                  | Procesos |
| d. | Manejo de la hora de crisis- Los primeros 60 minutos después de un incidente | Procesos |
| e. | Regreso a la normalidad  | Procesos |

#### 3. Procedimientos para administrar procesos críticos

- |    |                                |                                       |
|----|--------------------------------|---------------------------------------|
| a. | Incendio                       | Manual de procedimientos y protocolos |
| b. | Emergencia Médica              |                                       |
| c. | Alarma de intrusión            |                                       |
| d. | Desastre natural (sismo)       |                                       |
| e. | Amenaza de bomba               |                                       |
| f. | Violencia en las instalaciones |                                       |

#### 4. Apéndices

- |    |                    |                                       |
|----|--------------------|---------------------------------------|
| a. | Diagramas de flujo | Manual de procedimientos y protocolos |
| b. | Tablas             | Manual de procedimientos y protocolos |



## Anexo fotográfico