

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**CONTRALORIA GENERAL DE SANTIAGO DE CALI**

**SANTIAGO DE CALI**  
**Enero de 2020**

*¡Mejor gestión pública, mayor calidad de vida!*



SC3895-1

## DERECHOS DE AUTOR

La Ley N°1915 del 12 julio de 2018 “Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.” Determina que en todo proceso relativo al derecho de autor, y ante cualquier jurisdicción nacional se presumirá, salvo prueba en contrario, que la persona bajo cuyo nombre, seudónimo o su equivalente se haya divulgado la obra, será el titular de los derechos de autor. También se presumirá, salvo prueba en contrario, que la obra se encuentra protegida.

Es por ello que el copyright (traducido como derecho de copia que comprende la parte patrimonial de los derechos de autor) del texto, de las tablas y figuras incluidas en este documento es de propiedad de la Contraloría General de Santiago de Cali. Es por ello que si se desea copiar el contenido (texto, tablas o figuras) de más del 40% del documento, debe solicitarse el permiso entrando en contacto con la dirección de sistemas o Secretaría General.

## CONTENIDO

	<b>Pág.</b>
<b>INTRODUCCIÓN .....</b>	<b>5</b>
<b>1. GLOSARIO .....</b>	<b>5</b>
<b>2. MARCO NORMATIVO .....</b>	<b>7</b>
<b>3. LINEAMIENTOS CONCEPTUALES Y METODOLÓGICOS .....</b>	<b>7</b>
<b>4. POLITICAS DE OPERACIÓN .....</b>	<b>7</b>
<b>5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO .....</b>	<b>8</b>
6.1 Análisis contexto estratégico	9
6.2 Desarrollo práctico - Contexto Estratégico	10
<b>7. OBJETIVOS.....</b>	<b>10</b>
7.1 Objetivo general	10
<b>8. ALCANCE.....</b>	<b>11</b>
<b>9. DIAGNOSTICO SITUACIONAL .....</b>	<b>11</b>
<b>10. ESTRATEGIAS.....</b>	<b>11</b>
10.1 Liderazgo	11
10.2 Apropiación de la gestión del conocimiento	11
10.3 Comunicación y divulgación	12
10.4 Evaluación y seguimiento	12
<b>11. ETAPAS PARA LA EJECUCIÓN DE LAS ESTRATEGIAS .....</b>	<b>12</b>
11.1 Desarrollo	12
11.2 Aplicación	12
11.3 Ejecución	12
11.4 Control	12
<b>12. ALIENACIÓN DE ESTRATEGIAS CON EL PLAN ESTRATÉGICO 2020-2021 .....</b>	<b>13</b>
<b>13. PARTES INTERESADAS Y/O CARACTERIZACIÓN DE GRUPOS DE VALOR.....</b>	<b>14</b>
<b>14. INDICADORES Y RESULTADOS DE IMPACTO .....</b>	<b>15</b>
<b>15. RIESGOS.....</b>	<b>15</b>

**16. RECURSOS ..... 15**  
**17. ESTRATEGIAS PARA COMUNICAR Y DIVULGAR EL PLAN ..... 15**  
**18. RESPONSABLE DEL DOCUMENTO ..... 15**



## INTRODUCCIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades a través de una política de administración de riesgos minimizar pérdidas y maximizar oportunidades.

Los servidores públicos de la Contraloría General de Santiago de Cali, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión o incumplimiento de metas.

Es por ello que se hace necesario adoptar todas las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente Plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en esta entidad

De esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad

### 1. GLOSARIO

**Aceptación de riesgo:** Decisión informada de aceptar las consecuencias y probabilidades de un riesgo en particular.

**Administración de riesgos:** Cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

**Amenazas:** Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

**Análisis de riesgo:** Uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.



*¡Mejor gestión pública, mayor calidad de vida!*

**Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

**Control:** Medida que modifica al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones)

**Control de riesgos:** Parte de la administración de riesgos que involucra la implementación de políticas, estándares, procedimientos para eliminar o minimizar los riesgos adversos.

**Corrupción:** Mal uso del poder para beneficio propio.

**Evaluación de riesgos:** Proceso global de análisis de riesgo y evaluación de riesgo. El proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo, objetivos u otro criterio.

**Gestión de riesgos:** Aplicación sistemática de políticas, procedimientos, estructuras y prácticas de administración a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos. Cultura, procesos y estructuras dirigidas a obtener oportunidades potenciales mientras se administran los efectos adversos.

**Grupos de interés o grupos de valor:** Aquellas personas, grupos de individuos u organizaciones que pueden afectar, ser afectados por, o percibir ellos mismos ser afectados (positiva o negativamente) por una decisión o actividad.

**Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**Integridad:** Propiedad de exactitud y completitud.

**Lucha contra la corrupción:** Conjunto de medidas o acciones específicas que buscan prevenir, investigar y sancionar los delitos asociados con la corrupción.

**Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.

## 2. MARCO NORMATIVO

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

## 3. LINEAMIENTOS CONCEPTUALES Y METODOLÓGICOS

Atendiendo los lineamientos del plan de seguridad y privacidad de la información, se ha diseñado por la Contraloría General de Santiago de Cali, el mapa de riesgos de seguridad y privacidad de la información, bajo la estructura de espina de pescado.

## 4. POLITICAS DE OPERACIÓN

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso.

- No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.
- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

## 5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La contraloría general de Santiago de Cali adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

***¡Mejor gestión pública, mayor calidad de vida!***



SC3895-1



Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo

## 6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: determinar los factores externos e internos del riesgo.
- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: evaluación integral de los riesgos.

### 6.1 Análisis contexto estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos

(amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

## 6.2 Desarrollo práctico - Contexto Estratégico

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad
- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe diligenciar el formato Matriz DOFA para identificación de riesgos:

## 7. OBJETIVOS

### 7.1 Objetivo general

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento

### 7.2 Objetivo específicos

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

## 8. ALCANCE

Este PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

## 9. DIAGNOSTICO SITUACIONAL

Esta entidad cuenta con una política de administración de la cual cumple los estándares de la función pública, conforme a los autodiagnósticos se pudo evidenciar un resultado de 91,3 puntos en la política de Transparencia y Acceso a la Información y 97 puntos en la de Gestión Documental, lo que permite colegir que existe una debida coherencia frente a los valores para el resultado, en especial los riesgos y su no materialización dada su mitigación.

## 10. ESTRATEGIAS

Para el presente plan se adopta las siguientes:

### 10.1 Liderazgo

Busca que el liderazgo en la entidad no se ejerce por una sola persona, se requiere que todo el grupo de gestión de la organización actúe con grado de eficacia e influencia, para el desarrollo del presente plan.

### 10.2 Apropriación de la gestión del conocimiento

El conocimiento es uno de los mayores activos dentro de la entidad, a través de su gestión se puede lograr una mayor riqueza o valor añadido en la seguridad y privacidad de la información; La gestión del conocimiento es arma con la cual puede uno atacar los problemas organizacionales, ya que el conocimiento individual de cada persona dentro de la empresa se puede convertir en conocimiento colectivo, dando mayor peso a la información y pudiendo así integrar mejores ideas para atacar el problema en cuestión.

El conocimiento que posee una organización puede convertirse en una fuente de ventaja que permita originar acciones innovadoras para generar productos, servicios, procesos y sistemas de gestión que optimicen los recursos y capacidades de la entidad.

***¡Mejor gestión pública, mayor calidad de vida!***



SC3895-1

### **10.3 Comunicación y divulgación**

Busca visibilizar y empoderar todos los procesos y resultados de las actividades institucionales frente a los riesgos inherentes a la seguridad y privacidad de la información

### **10.4 Evaluación y seguimiento**

En la ejecución del plan será necesario consolidar informes exactos y basados en pruebas, que proporcionen datos a los responsables de la gestión y de la adopción de decisiones de modo que dirijan la intervención y mejoren sus resultados; lo anterior para minimizar el riesgo.

## **11. ETAPAS PARA LA EJECUCIÓN DE LAS ESTRATEGIAS**

La ejecución de las estrategias requiere seguir un proceso metodológico que permita que sean aplicadas adecuadamente:

### **11.1 Desarrollo**

Se refiere a la planeación; en ella se diseña la estrategia y se desarrollan las tácticas. Es importante que en esta etapa se consideren todos los factores del macro y microambiente que puedan afectar su aplicación, es decir, se debe visualizar la situación presente.

### **11.2 Aplicación**

Es la etapa en la que se integran las tácticas en un solo concepto estratégico; dejan de visualizarse como acciones independientes y se integran en una idea única, que debe corresponder al diseño de la estrategia.

### **11.3 Ejecución**

Se pone en marcha la estrategia, siguiendo el calendario y las tácticas previstas; en su etapa inicial, es posible hacerle algunas modificaciones, de acuerdo con las condiciones que se observen.

### **11.4 Control**

Es la etapa en la cual se verifica el correcto funcionamiento de la estrategia, a través de supervisiones y procesos de control; nos ofrecerá retroalimentación para determinar si es necesario establecer acciones alternas.

## 12. ALIENACIÓN DE ESTRATEGIAS CON EL PLAN ESTRATÉGICO 2020-2021

La Contraloría General de Santiago de Cali como entidad pública, debe alinearse, con el plan estratégico institucional y los planes de acción; y con esto generar una estrategia para facilitar el logro de los objetivos de la Entidad, apoyando la transformación de la organización y generando valor.

Conforme al objetivo No 1 la gestión global de CGSC atiende principios y estrategias de una gestión pública moderna, este plan se alinea con los objetivos específicos 1.1.4 Y 1.2.4.

### 13. PARTES INTERESADAS Y/O CARACTERIZACIÓN DE GRUPOS DE VALOR

IDENTIFICACIÓN DE LAS PARTES INTERESADAS	REQUISITO NECESIDADES Y/O EXPECTATIVAS DE LAS PARTES INTERESADAS	PROCESO Y/O ÁREAS ENCARGADAS DE ATENDER LA NECESIDAD Y/O PARTE INTERESADA	ORIGEN DE LAS PARTES INTERESADAS	CAPACIDAD		INFLUENCIA		MEDIO IDENTIFICACIÓN DEL REQUISITO	PRIORIDAD	ACCIONES Y COMPROMISOS
				NIVEL (Alta - Media - Baja)	JUSTIFICACION	NIVEL (Alta - Media - Baja)	JUSTIFICACION			
Auditoría General de la República	Administración y Soporte técnico oportuno y confiable brindado acerca de los sistemas SIA Contralorías y SIA Observa a usuarios de la CGSC.	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediante convenio.	Alta.	Se pueden Generar sanciones por incumplimientos legales de ley.	Correos Electrónicos. Aplicativo SICIS.	Alta	Administrar los usuarios y atender las solicitudes de los usuarios.
Contraloría General de la República	Administración y Soporte técnico oportuno y confiable brindado acerca del PNA a usuarios de la CGSC.	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediante convenio.	Alta.	Se pueden Generar sanciones por incumplimientos legales de ley.	Correos Electrónicos. Aplicativo SICIS.	Alta	Administrar los usuarios y atender las solicitudes de los usuarios.
Contralorías Territoriales con las cuales se tienen convenios	Aplicativos funcionales entregados mediante convenio que contribuyen al cumplimiento de la labor misional administrativa de las contralorías Territoriales. Claridad y precisión en los conceptos transmitidos, capacitaciones y soportes.	Oficina de Informática	Externo	Alta	Personal idoneo en el desarrollo de aplicaciones internas entregadas o recibidas mediante convenio.	Alta	Unificación de procesos en las Contralorías y posicionamiento a nivel nacional de la CGSC.	Documentos soporte de legalización de convenios. -Convenio firmado, instalación configuración, parametrización de los sistemas de acuerdo a cada necesidad. -Certificación de acompañamiento en sitio.	Alta	Cumplir con el convenio haciendo parametrización, entrega, capacitaciones y acompañamiento permanente en el uso de los aplicativos.
Todas las Áreas de la CGSC	Información disponible, confiable y segura. -Servicio y mantenimiento oportuno, eficiente y eficaz. Aplicativos funcionales que contribuyen al cumplimiento de la labor misional y administrativa de la Contraloría. Claridad y precisión en los	Oficina de Informática	Interna	media	No se cuenta con suficiente personal para cubrir con todas las necesidades de los procesos.	Alta	Por ser una oficina transversal a todos los procesos de la entidad.	Publicación de planes en intranet -Listado de bienes informáticos Hardware, software. -Plan de mantenimiento preventivo. -Aplicación SICIS -Encuesta de satisfacción del cliente Interno	Alta	Atención de solicitudes de soporte. Realizar el Mantenimiento Preventivo para el adecuado funcionamiento de los equipos. Actualizar el aplicativo SICIS para tener el control de los bienes informáticos. Realizar backups para salvaguardar la información.
Contralor, Oficina De Planeación Normalización Y Calidad, Oficina de Control Interno	Información oportuna, confiable y coherente.	Oficina de Informática	Interna	Alta	Informes veraces, coherentes, oportunos y conforme a las disposiciones legales y reglamentarias.	Alta	Incumplimiento a procedimientos internos.	Documento remisión de informes. - Carpeta Informes de la red corporativa.	Alta	remitir los informes de acuerdo al SGC.
Auditoría General de la República	Información oportuna, confiable y coherente.	Oficina de Informática	Externo	Alta	Informes veraces, coherentes, oportunos y conforme a las disposiciones legales y reglamentarias.	Alta	Se pueden Generar sanciones por incumplimientos legales de ley.	Informe de rendición de la Entidad. Carpeta Informes de la Red corporativa.	Alta	Enviar la información requerida por el ente de control.
Sujetos y Puntos de control	Soporte técnico oportuno, y confiable. Personal entrenado en los sistemas recibidos mediante convenio con la AGR -Claridad y precisión en los conceptos transmitidos	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediante convenio.	Alta	Se pueden Generar sanciones por incumplimientos legales de ley.	correos Electronicos. Aplicativo Sici Registro de convocatoria y asistencia a capacitación	Alta	Atender las solicitudes de soporte, realizados por los usuarios
Proveedores	Claridad y oportunidad en la definición de las necesidades tecnológicas requeridas	Oficina de Informática	Externo	Alta	Continuo sondeo del mercado TI, por parte del Jefe de la oficina de Informática	Media	La contratación se hace por subasta publica lo que implica tener varias opciones a la hora de elegir el proveedor que cumpla con todo lo solicitado	Contratos de Prestacion de servicios	Alta	Gestionar la renovacion oportuna de los contratos

#### **14. INDICADORES Y RESULTADOS DE IMPACTO**

Se han definido indicadores de gestión que representan una medida del logro de los objetivos, pero no de manera específica, es por ello que, para final de la vigencia, se adoptaran nuevos riesgos

#### **15. RIESGOS**

Para el tratamiento se adoptan los del Plan de seguridad y privacidad de la información, aplican así mismo los riesgos de gestión y de corrupción cuya materialización afectarían la continuidad de las operaciones institucionales.

#### **16. RECURSOS**

Este plan se lleva a cabo con recursos propios: humanos, físicos, tecnológicos y financieros; con énfasis en aplicación de controles y acciones para gestionar el riesgo.

#### **17. ESTRATEGIAS PARA COMUNICAR Y DIVULGAR EL PLAN**

La eficacia en el tratamiento de los riesgos de seguridad de la información se sustenta, entre otros, en el conocimiento y el trabajo colectivo de los servidores públicos de la entidad. Para ello, tanto el Plan como la información relacionada con el mismo se socializará internamente a través de medios institucionales, tales como Docunet, intranet, carteleras, comités, etc.

#### **18. RESPONSABLE DEL DOCUMENTO**

Secretaria General, Comunicaciones y Oficina de Informática

T:\Ofi\_Planea\Ofi\_Planea\Planes\Plan Estratégico\PLANES DECRETO 612-18\2020\PLANES RECIBIDOS 2020