

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

En cumplimiento de las directrices establecidas para iniciar los procesos de adquisición de bienes, obras y/o servicios en la Administración Central del Distrito de Santiago de Cali (con excepción de los contratos directos por la causal de prestación de servicios), a continuación, se detalla la información del requerimiento:

a.	Justificación de la necesidad que se pretende satisfacer con la contratación La Administración Distrital de Santiago de Cali está orientada al servicio de los intereses generales de sus habitantes y actúa con fundamento en los principios de igualdad, imparcialidad, buena fe, eficacia, eficiencia, economía, celeridad, responsabilidad, transparencia, publicidad, contradicción, polivalencia e interdisciplinariedad. Todo ello, sin perjuicio de la aplicación de los demás principios generales y especiales que rigen la actuación de la Administración Pública y de sus servidores. Como ente esencial dentro de la organización político-administrativa del Distrito, Santiago de Cali tiene la responsabilidad de atender de manera adecuada las obligaciones y exigencias establecidas por la Constitución Política de 1991 y la Ley, garantizando su cumplimiento pleno y efectivo. En cumplimiento de lo dispuesto en el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional”, se procede a elaborar el estudio y los documentos previos requeridos para adelantar el proceso de contratación correspondiente, incluyendo el requerimiento para la adquisición de bienes, obras y/o servicios. Como sustento de la descripción de la necesidad para esta contratación, el Departamento Administrativo de Tecnologías de la Información y las Comunicaciones (DATIC) se acoge al Acuerdo 0578 de 2024, mediante el cual se adopta el Plan de Desarrollo del Distrito Especial, Deportivo, Cultural, Turístico, Empresarial y de Servicios de Santiago de Cali 2024-2027, titulado “Cali, Capital Pacífica de Colombia”. Nombre del plan: Cali Capital Pacífica de Colombia Vigencia del plan: 2024-2027 Propósito: 63 Cali con Buen Gobierno Reto: 6302 Gestión Pública para los Ciudadanos Programa: 6302001 Fortalecimiento Institucional Metas: 63020010021 Infraestructura Tecnológica de la Administración Municipal con índice de disponibilidad consolidado Nombre del proyecto: Fortalecimiento de la Plataforma Tecnológica de la Alcaldía de Santiago de Cali. BP: 26005260 Por otro lado, en cumplimiento al Plan estratégico de tecnologías de la Información - PETI este proceso aporta al objetivo estratégico de TI 3 que establece lo siguiente: “Transformar la infraestructura tecnológica de la entidad hacia un modelo ágil y escalable
----	--

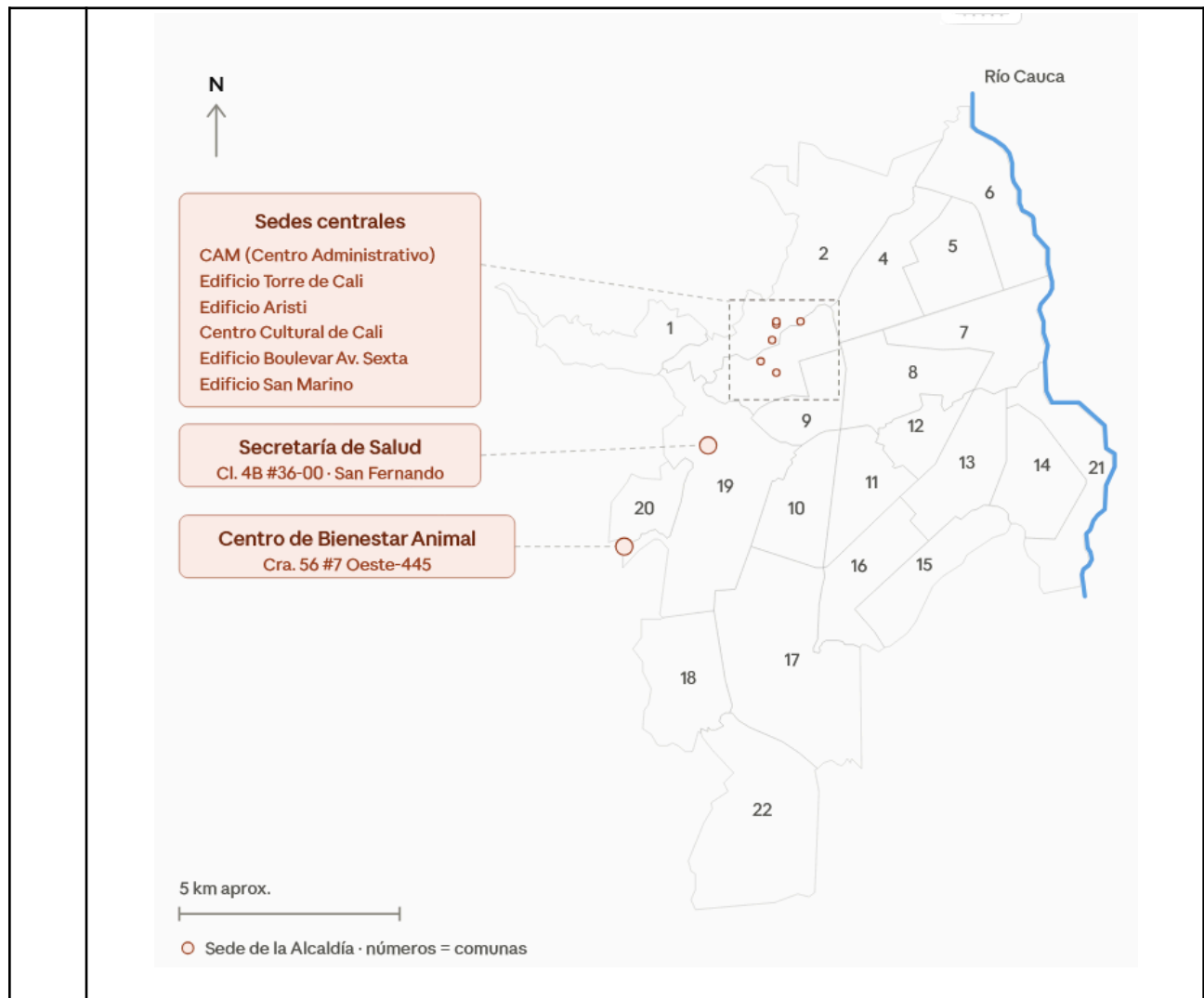
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

que permita responder de manera eficiente a las demandas instruccionales asegurando la continuidad operativa y optimizando los costos operativos mediante el uso de tecnologías innovadoras y prácticas.” Adicionalmente y en pro del cumplimiento de la estrategia de Gobierno Digital se busca generar un enfoque de valor agregado a la necesidad de contratación y así no solo producir un cumplimiento tácito de las obligaciones enunciadas anteriormente. En este sentido, es menester que la necesidad solucione adicionalmente una problemática, para determinar el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público, por lo cual se buscará dar cumplimiento al nuevo objetivo establecido en la política de Gobierno Digital, que es la siguiente: “Impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio” Bajo este contexto, el enfoque se dará en búsqueda del cumplimiento del dominio de Servicios Tecnológicos del Marco de Referencia de AE para la Gestión de TI, donde se dan cumplimiento a los siguientes lineamientos: ● MGGTI.LI.ST.04 “Continuidad y disponibilidad de los Servicios de TI” ● MGGTI.LI.ST.05 “Alta disponibilidad de los Servicios de TI” ● MGGTI.LI.ST.06 “Capacidad de los Servicios tecnológicos” ● MGGTI.LI.ST.10 “Monitoreo de la infraestructura de TI” ● MGGTI.LI.ST.11 “Respaldo y recuperación de los Servicios tecnológicos” ● MGGTI.LI.ST.13 “Seguridad informática” ● MGGTI.LI.ST.16 “Implementación del protocolo de internet versión 6 (IPv6)” De conformidad con lo señalado en el Decreto Extraordinario No.411.0.20.0516 de 2016 "Por el cual se determina la estructura de la Administración Central y las funciones de sus dependencias", el Departamento Administrativo de Tecnologías de la Información y las Comunicaciones, tiene la siguiente estructura: 1. Despacho del director. 2. Subdirección de Tecnología Digital 3. Subdirección de Innovación Digital 4. Unidad de Apoyo a la Gestión. En el ejercicio de las funciones asignadas al Departamento Administrativo de Tecnologías
--

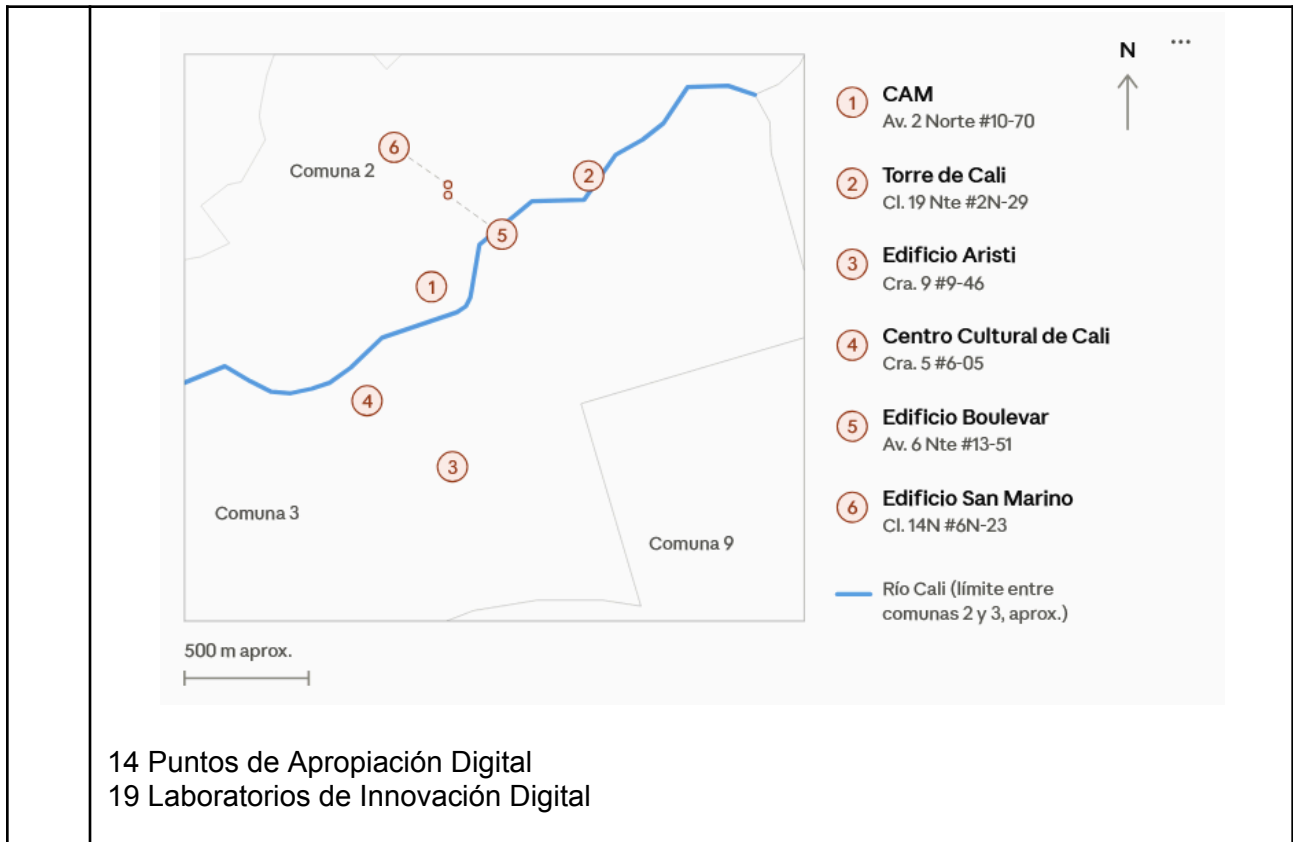
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	de la Información y las Comunicaciones (DATIC), como entidad responsable de liderar la gestión estratégica y operativa de las tecnologías de la información y las comunicaciones, se adelanta la definición, implementación, ejecución, seguimiento y divulgación de políticas, planes, programas y proyectos alineados con los planes estratégicos del distrito y el modelo integrado de gestión institucional. En cumplimiento de este mandato y de las competencias conferidas a la Subdirección de Tecnología Digital, se busca fortalecer la eficiencia institucional, impulsar la transformación social y atender la necesidad planteada. Ante los desafíos que representa el crecimiento demográfico, los efectos del cambio climático y las exigencias de una sociedad globalizada y cada vez más conectada, es indispensable que las ciudades adopten estrategias innovadoras que impulsen proyectos orientados a brindar soluciones integrales. Estas soluciones deben encaminar la vida urbana hacia la sostenibilidad y la mejora continua de la calidad de vida de los ciudadanos. Para afrontar estos desafíos, es fundamental la modernización tecnológica permanente, generando un valor agregado dentro de la administración pública. En concordancia con la Política de Gobierno Digital, establecida mediante el Decreto 767 de 2022, y en articulación con las estrategias de Ciudades y Territorios Inteligentes, es fundamental materializar proyectos que aprovechen las Tecnologías de la Información y las Comunicaciones (TIC) como instrumentos clave para la transformación social, económica y ambiental de los territorios. Estas iniciativas tienen como propósito fortalecer los procesos de desarrollo urbano, incorporando tecnologías emergentes que generen un impacto tangible y positivo en la vida de los ciudadanos. Bajo el enfoque anterior y teniendo en cuenta la dinámica de operación con la que la administración cubre las necesidades tecnológicas de la población y la de sus funcionarios en diferentes puntos de la ciudad entre los que se destacan: Centro de Administración de Cali - CAM Edificio Torre de Cali Edificio Aristi Centro Cultural de Cali Edificio Boulevard Av. Sexta Edificio San Marino (Calle 14N # 6N-23) Centro de Bienestar Animal Secretaría de Salud operando en - Calle 4B # 36-00 Barrio San Fernando
--	---

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)		MAJA01.04.01.P001.F003
	REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS		VERSIÓN 003



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003





ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

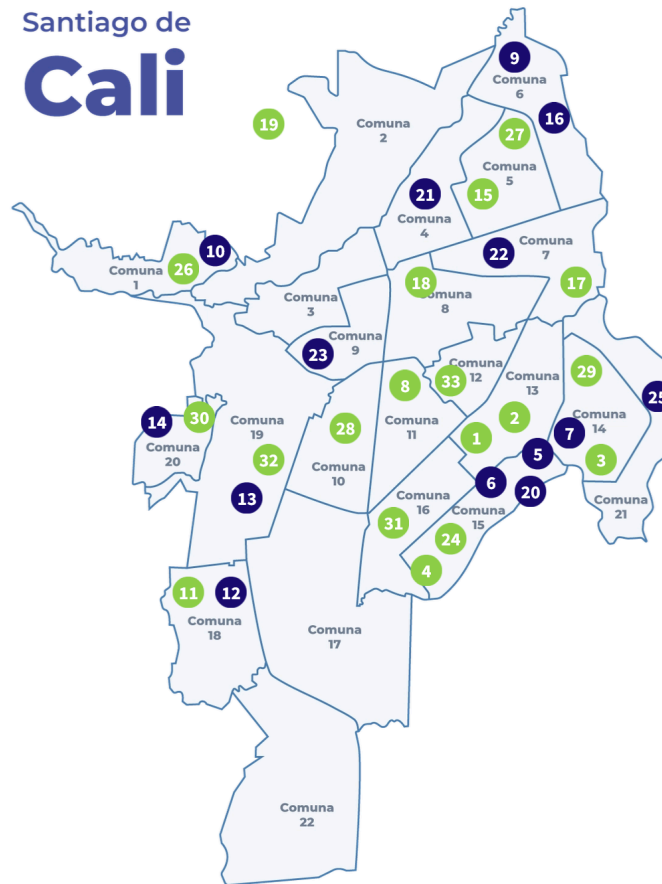
REQUERIMIENTO PARA
ADQUISICIÓN DE BIENES,
OBRAS Y/O SERVICIOS

MAJA01.04.01.P001.F003

VERSIÓN

003

Santiago de
Cali



PAD Puntos de
Apropiación
Digital

LID Laboratorios
de Innovación
Digital

Imagen tomada de:

<https://www.cali.gov.co/tic/publicaciones/105364/puntos-de-apropiacion-digital-y-laboratorios-de-innovacion-digital/>

Es preciso indicar que la red que soporta la capa de datos se encuentra soportada por nuestra Red Municipal Integrada (REMI) que transporta los servicios de datos de todos los puntos físicos anteriormente mencionados.

De igual manera en la operación que se da en cada uno de los puntos anteriormente mencionados se encuentran en operación:

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

- Endpoints o estaciones de trabajo de usuario final que se encuentran distribuidos de la siguiente forma:

Cantidad PCS x OU	
Etiquetas de fila	Cuenta de Name
DA (DESPACHO ALCALDE)	2
DACI (Departamento Administrativo de CONTROL INTERNO)	38
DACID (Departamento Administrativo de CONTROL DISCIPLINARIO INTERNO)	46
DACIDJ (Departamento Administrativo de Control Disciplinario Interno de Juzgamiento)	14
DACP (Departamento Administrativo de CONTRATACION PUBLICA)	250
DADII	242
DAGJP (Departamento Administrativo DE GESTION JURIDICA PUBLICA)	89
DAGMA	258
DAH (Departamento Administrativo de HACIENDA)	822
DAP (Departamento Administrativo de PLANEACION)	149
DATIC	121
SBS (Secretaria de BIENESTAR SOCIAL)	65
SC (Secretaria de CULTURA)	164
SDE (Secretaria de DESARROLLO ECONOMICO)	43
SDR (Secretaria del DEPORTE y RECREACION)	109
SDTPC (Secretaria de DESARROLLO TERRITORIAL y PARTICIPACION CIUDADANA)	103
SE (Secretaria de EDUCACION)	1
SG (Secretaria de GOBIERNO)	78
SGRED (Secretaria de GESTION de RIESGO de EMERGENCIA y DESASTRES)	73
SM (Secretaria de MOVILIDAD)	229
SPCC (Secretaria de PAZ y CULTURA CIUDADANA)	35
SSJ (Secretaria de SEGURIDAD y JUSTICIA)	87
SSP	394
ST (Secretaria de TURISMO)	37
SVSH (Secretaria de VIVIENDA SOCIAL y HABITAT)	190
TI (ADMINISTRACION INFORMATICA)	3
UAEPA (Unidad Administrativa Especial de Proteccion Animal)	33
Total general	3675

Datos tomados de: Mapa de Riesgos - Control N° 1

https://drive.google.com/drive/folders/1SoQzhWiVJsOKQnqNNDNL-9Dfwjg9WPJ1?usp=drive_link

- Servidores lógicos que son alcanzados desde las diferentes dependencias para operar en los sistemas de información.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)		MAJA01.04.01.P001.F003
	REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS		VERSIÓN 003

	<table> <tr> <th>Cantidad</th><th>Centro de Datos de Operación</th></tr> <tr> <td>111</td><td>Nube Pública - AWS</td></tr> <tr> <td>66</td><td>Nube Pública - OCI</td></tr> <tr> <td>180</td><td>Nube Privada - Cotel</td></tr> <tr> <td>56</td><td>On Premise</td></tr> </table> Cuentas de Correo electrónico <table> <tr> <th>OU primaria</th><th>Total</th></tr> <tr><td>Concejodecali.gov.co</td><td>94</td></tr> <tr><td>contraloriacali.gov.co</td><td>230</td></tr> <tr><td>DA (DESPACHO ALCALDE)</td><td>40</td></tr> <tr><td>DACI (Departamento Administrativo de CONTROL INTERNO)</td><td>96</td></tr> <tr><td>DACID (Departamento Administrativo de CONTROL DISCIPLINARIO INTERNO)</td><td>49</td></tr> <tr><td>DACIDJ (Departamento Administrativo de Control Disciplinario Interno de Juzgamiento)</td><td>20</td></tr> <tr><td>DACP (Departamento Administrativo de CONTRATACION PUBLICA)</td><td>119</td></tr> <tr><td>DADII</td><td>270</td></tr> <tr><td>DAGJP (Departamento Administrativo DE GESTION JURIDICA PUBLICA)</td><td>63</td></tr> <tr><td>DAGMA</td><td>219</td></tr> <tr><td>DAH (Departamento Administrativo de HACIENDA)</td><td>627</td></tr> <tr><td>DAP (Departamento Administrativo de PLANEACION)</td><td>195</td></tr> <tr><td>DATIC</td><td>72</td></tr> <tr><td>DATIC/SID (Subdireccion de Innovacion Digital)</td><td>39</td></tr> <tr><td>DATIC/SID (Subdireccion de Innovacion Digital)/Apropiacion TIC Ciudadano Externo</td><td>40</td></tr> <tr><td>DATIC/STD (Subdireccion de Tecnologia Digital)</td><td>84</td></tr> <tr><td>DATIC/STD (Subdireccion de Tecnologia Digital)/ZonasWifi</td><td>1</td></tr> <tr><td>DATIC/UAG</td><td>51</td></tr> <tr><td>personeriacali.gov.co</td><td>120</td></tr> <tr><td>Plan Jarillon</td><td>64</td></tr> <tr><td>SBS (Secretaria de BIENESTAR SOCIAL)</td><td>189</td></tr> <tr><td>SC (Secretaria de CULTURA)</td><td>297</td></tr> <tr><td>SDE (Secretaria de DESARROLLO ECONOMICO)</td><td>100</td></tr> <tr><td>SDR (Secretaria del DEPORTE y RECREACION)</td><td>244</td></tr> <tr><td>SDTPC (Secretaria de DESARROLLO TERRITORIAL y PARTICIPACION CIUDADANA)</td><td>187</td></tr> <tr><td>SE (Secretaria de EDUCACION)</td><td>136</td></tr> <tr><td>SG (Secretaria de GOBIERNO)</td><td>159</td></tr> <tr><td>SGRED (Secretaria de GESTION de RIESGO de EMERGENCIA y DESASTRES)</td><td>80</td></tr> <tr><td>SI (Secretaria de INFRAESTRUCTURA)</td><td>120</td></tr> <tr><td>SM (Secretaria de MOVILIDAD)</td><td>715</td></tr> <tr><td>SPCC (Secretaria de PAZ y CULTURA CIUDADANA)</td><td>93</td></tr> <tr><td>SSJ (Secretaria de SEGURIDAD y JUSTICIA)</td><td>336</td></tr> <tr><td>SSP</td><td>600</td></tr> <tr><td>ST (Secretaria de TURISMO)</td><td>72</td></tr> <tr><td>SVSH (Secretaria de VIVIENDA SOCIAL y HABITAT)</td><td>94</td></tr> <tr><td>TI (ADMINISTRACION INFORMATICA)</td><td>32</td></tr> <tr><td>TO (TRABAJADORES OFICIALES)</td><td>1</td></tr> <tr><td>UAEGBS (Unidad Administrativa Especial de Gestion de Bienes y Servicios)</td><td>154</td></tr> <tr><td>UAEPA (Unidad Administrativa Especial de Proteccion Animal)</td><td>46</td></tr> <tr><td>UAESPM (Unidad Admi Especial de Servicios Publicos Municipales)</td><td>131</td></tr> <tr><td>Total general</td><td>6279</td></tr> </table>	Cantidad	Centro de Datos de Operación	111	Nube Pública - AWS	66	Nube Pública - OCI	180	Nube Privada - Cotel	56	On Premise	OU primaria	Total	Concejodecali.gov.co	94	contraloriacali.gov.co	230	DA (DESPACHO ALCALDE)	40	DACI (Departamento Administrativo de CONTROL INTERNO)	96	DACID (Departamento Administrativo de CONTROL DISCIPLINARIO INTERNO)	49	DACIDJ (Departamento Administrativo de Control Disciplinario Interno de Juzgamiento)	20	DACP (Departamento Administrativo de CONTRATACION PUBLICA)	119	DADII	270	DAGJP (Departamento Administrativo DE GESTION JURIDICA PUBLICA)	63	DAGMA	219	DAH (Departamento Administrativo de HACIENDA)	627	DAP (Departamento Administrativo de PLANEACION)	195	DATIC	72	DATIC/SID (Subdireccion de Innovacion Digital)	39	DATIC/SID (Subdireccion de Innovacion Digital)/Apropiacion TIC Ciudadano Externo	40	DATIC/STD (Subdireccion de Tecnologia Digital)	84	DATIC/STD (Subdireccion de Tecnologia Digital)/ZonasWifi	1	DATIC/UAG	51	personeriacali.gov.co	120	Plan Jarillon	64	SBS (Secretaria de BIENESTAR SOCIAL)	189	SC (Secretaria de CULTURA)	297	SDE (Secretaria de DESARROLLO ECONOMICO)	100	SDR (Secretaria del DEPORTE y RECREACION)	244	SDTPC (Secretaria de DESARROLLO TERRITORIAL y PARTICIPACION CIUDADANA)	187	SE (Secretaria de EDUCACION)	136	SG (Secretaria de GOBIERNO)	159	SGRED (Secretaria de GESTION de RIESGO de EMERGENCIA y DESASTRES)	80	SI (Secretaria de INFRAESTRUCTURA)	120	SM (Secretaria de MOVILIDAD)	715	SPCC (Secretaria de PAZ y CULTURA CIUDADANA)	93	SSJ (Secretaria de SEGURIDAD y JUSTICIA)	336	SSP	600	ST (Secretaria de TURISMO)	72	SVSH (Secretaria de VIVIENDA SOCIAL y HABITAT)	94	TI (ADMINISTRACION INFORMATICA)	32	TO (TRABAJADORES OFICIALES)	1	UAEGBS (Unidad Administrativa Especial de Gestion de Bienes y Servicios)	154	UAEPA (Unidad Administrativa Especial de Proteccion Animal)	46	UAESPM (Unidad Admi Especial de Servicios Publicos Municipales)	131	Total general	6279
Cantidad	Centro de Datos de Operación																																																																																														
111	Nube Pública - AWS																																																																																														
66	Nube Pública - OCI																																																																																														
180	Nube Privada - Cotel																																																																																														
56	On Premise																																																																																														
OU primaria	Total																																																																																														
Concejodecali.gov.co	94																																																																																														
contraloriacali.gov.co	230																																																																																														
DA (DESPACHO ALCALDE)	40																																																																																														
DACI (Departamento Administrativo de CONTROL INTERNO)	96																																																																																														
DACID (Departamento Administrativo de CONTROL DISCIPLINARIO INTERNO)	49																																																																																														
DACIDJ (Departamento Administrativo de Control Disciplinario Interno de Juzgamiento)	20																																																																																														
DACP (Departamento Administrativo de CONTRATACION PUBLICA)	119																																																																																														
DADII	270																																																																																														
DAGJP (Departamento Administrativo DE GESTION JURIDICA PUBLICA)	63																																																																																														
DAGMA	219																																																																																														
DAH (Departamento Administrativo de HACIENDA)	627																																																																																														
DAP (Departamento Administrativo de PLANEACION)	195																																																																																														
DATIC	72																																																																																														
DATIC/SID (Subdireccion de Innovacion Digital)	39																																																																																														
DATIC/SID (Subdireccion de Innovacion Digital)/Apropiacion TIC Ciudadano Externo	40																																																																																														
DATIC/STD (Subdireccion de Tecnologia Digital)	84																																																																																														
DATIC/STD (Subdireccion de Tecnologia Digital)/ZonasWifi	1																																																																																														
DATIC/UAG	51																																																																																														
personeriacali.gov.co	120																																																																																														
Plan Jarillon	64																																																																																														
SBS (Secretaria de BIENESTAR SOCIAL)	189																																																																																														
SC (Secretaria de CULTURA)	297																																																																																														
SDE (Secretaria de DESARROLLO ECONOMICO)	100																																																																																														
SDR (Secretaria del DEPORTE y RECREACION)	244																																																																																														
SDTPC (Secretaria de DESARROLLO TERRITORIAL y PARTICIPACION CIUDADANA)	187																																																																																														
SE (Secretaria de EDUCACION)	136																																																																																														
SG (Secretaria de GOBIERNO)	159																																																																																														
SGRED (Secretaria de GESTION de RIESGO de EMERGENCIA y DESASTRES)	80																																																																																														
SI (Secretaria de INFRAESTRUCTURA)	120																																																																																														
SM (Secretaria de MOVILIDAD)	715																																																																																														
SPCC (Secretaria de PAZ y CULTURA CIUDADANA)	93																																																																																														
SSJ (Secretaria de SEGURIDAD y JUSTICIA)	336																																																																																														
SSP	600																																																																																														
ST (Secretaria de TURISMO)	72																																																																																														
SVSH (Secretaria de VIVIENDA SOCIAL y HABITAT)	94																																																																																														
TI (ADMINISTRACION INFORMATICA)	32																																																																																														
TO (TRABAJADORES OFICIALES)	1																																																																																														
UAEGBS (Unidad Administrativa Especial de Gestion de Bienes y Servicios)	154																																																																																														
UAEPA (Unidad Administrativa Especial de Proteccion Animal)	46																																																																																														
UAESPM (Unidad Admi Especial de Servicios Publicos Municipales)	131																																																																																														
Total general	6279																																																																																														

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	Por el volumen y la criticidad de la información tratada desde los diferentes lugares referenciados y recursos que posibilitan el proceso, la entidad requiere una capa de protección continua que brinde seguridad integrada para endpoints, cargas de trabajo y correo electrónico y con ello cubrir la lo que se enmarca en la Política de Gobierno Digital y su habilitador de Seguridad y Privacidad de la Información, cuyo instrumento de implementación es el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, alineado con la norma NTC-ISO/IEC 27001:2022. De acuerdo a lo anteriormente expuesto, se necesita la renovación por un año de la plataforma de protección de puntos finales, para que no se vea comprometida la protección de la información y el correcto funcionamiento de los equipos de la organización, de las 4460 licencias de antivirus actuales de la entidad para protección de endpoint más servidores, además de la renovación de protección antivirus para las 6600 cuentas de correo con que cuenta la entidad en Google Workspace más XDR con gestión centralizada 100% nube Con lo anterior se renueva y fortalece la solución antivirus con la que cuenta actualmente la Administración Distrital, abarcando puntos finales (equipos de usuario final) y servidores, con lo cual se podrán combatir los diferentes vectores de seguridad como lo son ataques y amenazas originadas por la navegación de los usuarios, tanto internos como externos, así como la publicación de aplicaciones. También las que provienen de los equipos de usuarios los cuales experimentan una conectividad tanto local como remota por las necesidades de teletrabajo y movilidad. Es importante resaltar que, dentro de los beneficios de contratar la renovación de la plataforma de endpoint de nueva generación para la Alcaldía Distrital de Santiago de Cali se caracterizan los siguientes: • Protección integral de equipos de cómputo y servidores contra virus, ransomware, spyware y amenazas de día cero. • Consola centralizada en la nube que permite detección y respuesta en tiempo real (EDR), con aislamiento automático de máquinas comprometidas. • Cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales, garantizando políticas de bloqueo y control de accesos. • Mantiene la infraestructura tecnológica protegida y disponible, evitando interrupciones en los servicios digitales de la Alcaldía.
--	--

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	- Actualizaciones automáticas y gestión remota que reducen tiempos de inactividad y aseguran que todos los equipos estén al día. - Dashboard en tiempo real para monitorear incidentes, estado de actualizaciones y estadísticas de seguridad. - Integración con sistemas de correlación de eventos (SIEM), lo que facilita la toma de decisiones basadas en información confiable - Reportes gráficos y detallados para auditorías, cumplimiento normativo y control interno. - Consola 100% en la nube, accesible desde cualquier ubicación, lo que facilita la administración distribuida. - Un único agente para endpoints y servidores, simplificando la instalación y reduciendo costos de gestión. - Adaptabilidad para ambientes virtualizados y compatibilidad con múltiples sistemas operativos (Windows, Linux, macOS). - Garantiza que los servicios digitales ofrecidos a la ciudadanía estén protegidos contra ataques informáticos. - Refuerza la percepción de seguridad y confiabilidad en la gestión pública digital. En atención a lo anterior, esta contratación asegura protección avanzada, continuidad de los servicios, eficiencia en la gestión y cumplimiento normativo, todo bajo una plataforma moderna y escalable que respalda la transformación digital del Distrito.
b.	Objeto a contratar (con el correspondiente alcance si aplica) Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC)
c.	Descripción detallada del bien y/o servicio a adquirir con las especificaciones técnicas de acuerdo a la necesidad. Aportar ficha técnica si aplica. El contratista deberá proveer 4460 licencias de antivirus y 6600 licencias de protección de correo con XDR con gestión centralizada 100% nube y una vigencia por 12 meses distribuidas de la siguiente manera:

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

Nombre	Unidades
XDR for Email (EmDR) [#of users, mailbox if AD sync is unavailable]	6.600
Endpoint Security Essentials [# of endpoints including servers]	4.000
Endpoint Security Pro [# of endpoints including servers]	460
Email and Collaboration Security Core [#of users]	6.600

- Licenciamiento para 4000 Usuarios (Equipos de Cómputo)
- Licenciamiento para 460 Servidores.
- Licenciamiento de protección de correo para 6600 cuentas de correo electrónico con XDR
- Se debe disponer de una gestión centralizada, por lo tanto, es necesario que la consola sea cien por ciento 100% en la nube.
- Se deberán configurar las políticas de bloqueo orientadas al cumplimiento de la ley 1581 del año 2012 (protección de datos personales)
- La herramienta antivirus y configuraciones generales deben cumplir con:
 - Consola de administración 100% en la nube
 - La consola de administración centralizada debe tener la capacidad de ser consultada mediante navegador web desde cualquier ubicación.
 - Permitir crear grupos y generar políticas a los mismos.
 - La solución debe ser desplegada mediante un agente.
 - Servicios de limpieza de daños en tiempo real para eliminar remanentes de virus, troyanos, spyware y entradas en el registro del sistema.
 - Antimalware para Endpoint (Windows y macOS) y Servers (Windows y Linux)
 - Debe permitir visualizar, de forma rápida y sencilla, el estado y estadísticas de las infecciones generadas y permitir también visualizar las estaciones de trabajo y/o servidores donde ocurrió la detección o infección.
 - La solución debe contar con un dashboard que proporcione visibilidad en tiempo real de la incidencia de virus, estado de la actualización de las máquinas y cualquier aviso o errores que puedan ocurrir
 - La herramienta debe soportar la funcionalidad de DLP por medio del mismo agente destinado para la protección de endpoint.
 - Debe tener funcionalidad de protección contra ransomware.
 - La solución debe poderse integrar con sistemas para correlacionar Eventos (SIEM).
 - Se debe incluir un módulo de detección y respuesta para Endpoint (EDR) para todas las maquinas contempladas
 - Los servicios de gestión de detección y respuesta para Endpoint (EDR)

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	deben ser gestionados sobre la misma consola de antivirus en la nube - Se deben incluir como mínimo los siguientes servicios. - El oferente deberá verificar y validar que la renovación del licenciamiento haya sido ejecutada correctamente, de conformidad con las condiciones técnicas y el alcance establecidos en el presente proceso. 3.1 Contexto Técnico ANTIVIRUS CONDICIONES TÉCNICAS MÍNIMAS - La solución propuesta debe tener una tasa de mínimo 91% en el componente de analítica en los resultados de la evaluación MITRE Wizard Spider & Sandworm Evaluation Results 2025. - La consola de administración de la herramienta antivirus y configuraciones generales deben cumplir con: - Consola de administración en nube - Agentes específico para servidores (Windows/linux) Protección Antimalware - Agentes para endpoints (Windows) Protección Antimalware - Permitir crear grupos y generar políticas a los mismos. - Contar con un módulo de generación de reportes. - La consola debe permitir la creación de diversos usuarios para su administración y con diferentes niveles de acceso (Roles). - La consola de administración centralizada debe tener la capacidad de ser consultada mediante navegador web desde cualquier Ubicación. - La consola de administración debe tener la capacidad de notificar los intentos de infección de virus de acuerdo con parámetros definidos por el administrador de la solución. - La consola deberá permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre la solución de seguridad. - Servicios de limpieza de daños en tiempo real para eliminar remanentes de virus, troyanos, spyware y entradas en el registro del sistema. - Notificación inmediata y centralizada sobre ataques masivos de virus y/o código malicioso. - Características mínimas incluidas: - Antimalware para Endpoint (Windows y macOS) y Servers (Windows y Linux) - Control de URL maliciosas por reputación
--	---

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	• Control de dispositivos extraíbles (Ejemplo USB) • HIPS • Análisis de descargas por reputación • Prevención de fugas de datos (DLP) básico • La herramienta debe tener la función de programación basada en fecha hora para control de aplicaciones control de dispositivos • Detección de tráfico malicioso (MTD) • Prevención Anti-exploit • Cryptoguard - Anti-ransomware, no solo por firmas, sino por comportamiento. • Localizar brechas de seguridad y eliminarlas • Deberá tener sistemas de reputación en nube para que reúna información acerca de las amenazas a nivel mundial. • Permitir crear grupos o importarlos de directorio activo y generar políticas a los mismos. • Contar con un módulo de generación de reportes. • La consola de administración debe tener la capacidad de notificar los intentos de infección de virus de acuerdo con parámetros definidos por el administrador de la solución. • La solución debe incluir actualizaciones automáticas de las listas de definiciones de virus a partir de una ubicación en nube. • La solución debe contar con un mecanismo de control de modificación del endpoint y contra la remoción no autorizada del agente por parte del cliente a través de una contraseña. • La solución debe permitir el cambio de la configuración de los antivirus en los clientes de forma remota y a través de reglas aplicables a una máquina, un grupo de máquinas, etc. • La solución debe permitir visualizar, de forma rápida y sencilla, el estado de las estaciones de trabajo y servidores en una sola pantalla de Summary o resumen. • La solución debe permitir visualizar, de forma rápida y sencilla, el estado y estadísticas de las infecciones generadas y permitir también visualizar las estaciones de trabajo y servidores donde ocurrió la detección o infección. • La solución debe permitir visualizar, de forma rápida y sencilla, un resumen del estatus de las actualizaciones de firmas en las estaciones de trabajo y servidores, cantidad de equipos actualizados y desactualizados. • La solución debe permitir agregar, modificar o eliminar grupos para administración de los clientes con políticas diferentes. • La solución debe contar con un dashboard que proporcione visibilidad en tiempo real de la incidencia de virus, estado de la actualización de las máquinas y cualquier aviso o errores que puedan ocurrir. • Los agentes antivirus para endpoints debe proteger a los siguientes sistemas
--	--

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	operativos, puestos de trabajo fijo y móvil (portátiles) en las plataformas Intel y AMD, los sistemas operativos: Windows 8, Windows 8.1 windows 10. • Los agentes antivirus para servidores deben soportar la instalación sobre los siguientes sistemas operativos: Windows Server 2012, Red Hat Linux 6, CentOS Linux 6, Oracle Linux 6, SUSE Enterprise Linux 11, Debian 8, Ubuntu 16.04 y superiores hasta la fecha. • La solución debe permitir la utilización de tecnologías avanzadas, para la protección contra amenazas desconocidas que generen riesgos de seguridad en los procesos o archivos sospechosos originados desde medios de almacenamiento externos, internos, servicios web o canales de correo. • La solución debe proteger los navegadores de Internet Explorer, Firefox, Chrome, Opera y Safari, bloqueando el acceso a sitios infectados conocidos y comprobando los datos descargados antes de ejecutarse. • La solución debe permitir generar acciones sobre archivos y procesos que permitan enviar a cuarentena, lograr registro y/o terminar procesos o acciones. • La solución debe permitir manualmente registrar excepciones de archivos que ya fueron analizados y descartados de acciones maliciosas ya sea por ser procesos permitidos o aplicaciones de uso interno. • La solución debe permitir la instalación silenciosa a través de políticas de Directorio activo, script de login, etc. • La solución debe permitir la administración de las políticas desde la consola centralizada en la nube. • La solución debe contar con Control y bloqueo de URL basado en reputación. • La solución debe tener un Control de periféricos. (USB, Unidades de CD, Bluetooth, etc.) • La solución debe permitir la prevención de fugas de datos básico. • La solución debe permitir el monitoreo en tiempo real de los procesos en memoria para capturar los virus que son ejecutados en memoria sin necesidad de escribir el archivo. • La solución debe contar con módulo de HIPS. • Detección y protección de técnicas de explotación de DLL Injection • Protección de amenazas de día cero a través de tecnología de machine Learning o Deep Learning. • La solución debe contar con sistemas basados en el comportamiento de la amenaza. • Protección contra malware escondido en aplicaciones legítimas (code cave) • El módulo de comportamiento debe ser capaz de detectar amenazas de día cero. • La solución debe permitir detección y reacción contra Ransomware que inicie el cifrado de información, así no se tenga firma de detección de malware para detenerlo. Este módulo debe terminar el proceso de cifrado malicioso de forma automática.
--	---

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	• Debe tener funcionalidad de escudo contra ransomware. • La solución debe permitir el bloqueo de procesos comúnmente asociados con ransomware. • La solución debe permitir evitar o monitorear que un programa con comportamiento sospechoso pueda incrustar complementos en los navegadores. • La solución debe evitar o monitorear que un programa con comportamiento sospechoso pueda instalar librería del programa malicioso. • La solución debe tener un módulo que proteja contra el cifrado no autorizado del sector boot del disco duro del computador. • La solución debe evitar o monitorear que un programa con comportamiento sospechoso modifique archivos del sistema. • La solución debe integrarse con sistema de SIEM para correlacionar Eventos. • La solución debe tener un módulo de amenazas donde se verificará los detalles de malware que pueda estar ocurriendo en los Endpoint con funcionalidad de marcar como resuelto o no resuelto el evento del incidente. • La solución deberá ser versátil en proceso de actualización del agente y antivirus, debe filtrar las máquinas por su respectivo nombre y no permitirá duplicidad por este campo, en los equipos dentro de la organización. • La solución debe ser compatible Windows 8 con últimas actualizaciones, Windows 8.1 últimas actualizaciones, Windows 10 últimas actualizaciones. • La herramienta deberá enviar un informe de seguridad vía correo electrónico y de forma periódica al administrador de la plataforma, independientemente del servicio de correo que esté en uso. • La instalación deberá garantizar la implementación del agente por GPO, desatendido o sistema de despliegue que soporte paquetes con extensiones MSI. • El software deberá contar con un modo de coexistencia, para evaluar el funcionamiento de la herramienta, sin detener los procesos de la entidad. • La solución deberá permitir ejecutar reglas de seguridad que permita proteger los archivos confidenciales. • La solución debe tener la funcionalidad de controlar el uso de las aplicaciones utilizando listas que permita o deniegue la ejecución. • La solución deberá permitir la creación de conjuntos de sitios Web para que solo sean accesibles a determinados grupos de usuarios. • La solución deberá bloquear servidores específicos o crear reglas basadas en niveles de criticidad de reputación de URL. • La solución deberá impedir que los usuarios conecten dispositivos extraíbles, no autorizados en los hosts. • La solución debe permitir el monitoreo de cambios en archivos específicos en servidores • La solución debe permitir el monitoreo de cambios en llaves de registro
--	--

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	• El agente para servidores no debe solicitar reinicio del servidor en la instalación y desinstalación del agente • La solución deberá permitir proteger los buzones de correo en nube de la entidad con integración directa con el tenant de la solución por medio de API. • La solución debe permitir bloquear el paso de URL maliciosas y archivos con malware que se detecten en cuerpos y adjuntos de correo electrónico. • La solución debe realizar análisis de malware en cuerpos y adjuntos de correo electrónico usando técnicas de machine learning. • La solución debe realizar bloqueo de URL maliciosas en cuerpos y adjuntos de correo electrónico usando listas de reputación. • La solución debe detectar mensajes con intentos de robo de credenciales o phishing. • La solución debe detectar mensajes con intentos de fraude o técnicas BEC. • La solución debe contar con análisis tipo sandbox para URL, archivos y MAC.														
ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA ANTIVIRUS															
<table><tr><th>CARACTERÍSTICAS</th><th>DESCRIPCIÓN</th></tr><tr><td>1. Motor de Exploración del Antivirus.</td><td>El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos. Deberá tener integrada una tecnología de Servicio de Mapeo, que permita acceder por debajo del sistema operativo para un análisis y una reparación completa.</td></tr><tr><td>2. Administración Consola en nube</td><td>La entidad espera que las consolas sean 100% en la nube, las cuales permite la administración centralizada de los equipos mediante un acceso web.</td></tr><tr><td>3. Acciones posteriores a la detección.</td><td>Capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado, moverlo a cuarentena, no tomar acción, eliminar el archivo,etc.</td></tr><tr><td>4. Exclusiones en la exploración</td><td>Capacidad para excluir de la exploración archivos, carpetas, procesos, etc. específicos.</td></tr><tr><td>5. Endpoint Detección y respuesta</td><td>Capacidad de detección y respuesta desde el mismo agente.</td></tr><tr><td>6. Detección de</td><td>El antivirus debe ser capaz de detectar y eliminar</td></tr></table>	CARACTERÍSTICAS	DESCRIPCIÓN	1. Motor de Exploración del Antivirus.	El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos. Deberá tener integrada una tecnología de Servicio de Mapeo, que permita acceder por debajo del sistema operativo para un análisis y una reparación completa.	2. Administración Consola en nube	La entidad espera que las consolas sean 100% en la nube, las cuales permite la administración centralizada de los equipos mediante un acceso web.	3. Acciones posteriores a la detección.	Capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado, moverlo a cuarentena, no tomar acción, eliminar el archivo,etc.	4. Exclusiones en la exploración	Capacidad para excluir de la exploración archivos, carpetas, procesos, etc. específicos.	5. Endpoint Detección y respuesta	Capacidad de detección y respuesta desde el mismo agente.	6. Detección de	El antivirus debe ser capaz de detectar y eliminar	
CARACTERÍSTICAS	DESCRIPCIÓN														
1. Motor de Exploración del Antivirus.	El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos. Deberá tener integrada una tecnología de Servicio de Mapeo, que permita acceder por debajo del sistema operativo para un análisis y una reparación completa.														
2. Administración Consola en nube	La entidad espera que las consolas sean 100% en la nube, las cuales permite la administración centralizada de los equipos mediante un acceso web.														
3. Acciones posteriores a la detección.	Capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado, moverlo a cuarentena, no tomar acción, eliminar el archivo,etc.														
4. Exclusiones en la exploración	Capacidad para excluir de la exploración archivos, carpetas, procesos, etc. específicos.														
5. Endpoint Detección y respuesta	Capacidad de detección y respuesta desde el mismo agente.														
6. Detección de	El antivirus debe ser capaz de detectar y eliminar														

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	Programas no Deseados	diferentes tipos de programas tales como: adware-spyware- jokeprograms -Keyloggers, trackware, hacktools, remote Access tools, dialers.
	7. Instalación remota	La solución debe tener la capacidad de desplegar su agente de manera remota, a través de la Consola, Directorio Activo (GPO) o Herramienta de despliegue de terceros, de manera transparente para el usuario final y estableciendo la comunicación entre los equipos y la consola en la nube.
	8. Programación de tareas	Capacidad para programar tareas de exploración, actualización, etc.
	9. Registro de eventos LOG's	Por cada uno de los eventos deberá mostrar: riesgos, amenazas, tiempo cuando fue generado el evento, host (IP, MAC, Sistema Operativo, Usuario), Tipo de amenaza, acción afectada, número de detecciones, Ubicación Archivo y nombre del archivo.
	10. Protección & escaneo Acceso Spyware	Deberá escanear y bloquear en tiempo real cualquier acceso e instalación de cualquier spyware, adware, malware, keylogger, herramientas de administración remota, Dialer, trackware, hacktools, etc., no solamente por escaneo en demanda.
	11. Escaneo de Spyware en Registro	Deberá evitar que programas maliciosos modifiquen el registro.
	12. Sistemas Operativos	La solución debe tener la capacidad de soportar sistemas operativos de 32 o 64 bits de Windows, MacOS y Linux en las siguientes versiones: - Windows 8, 10 y posteriores. - Windows Server 2012, 2016 y posteriores - MacOS 10.13 y posteriores. - Linux/Unix: • Amazon Linux, Amazon Linux 2 • CentOS 6/7/8 • Debian 9, 10 • Oracle Linux 6/7/8 • Red Hat Enterprise Linux 6/7/8 • SUSE • Ubuntu • Solaris
	13. Reportes	Deberá proveer reportes gráficos desde la consola de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

		administración centralizada del producto sin necesidad de productos adicionales. Deberá permitir generar reportes de riesgos, Cumplimiento de políticas, escaneos, estado de los equipos, estado de la licencia, historial de ataques en los últimos 30 días según sea necesario, entre otros.
	14. Único Agente	La herramienta de protección no deberá requerir aplicaciones adicionales para comunicarse a la consola de administración. Es decir, con sólo una vez que se ejecute el instalador la herramienta cubrirá los aspectos de seguridad y comunicación con la consola.
	15. Icono Único	La herramienta solamente presentará un ícono en el área de notificación de la barra de tareas.
	16. Integración transparente de tecnologías de seguridad	Debe integrar de forma transparente las tecnologías principales de antivirus, antispymware, prevención de intrusos y control de dispositivos en un solo agente.
	17. Análisis proactivo de amenazas	Debe contar con protección basada en comportamiento que protege contra las amenazas de día cero y amenazas nunca antes vistas.
	18. Control de las aplicaciones	Debe permitir a los administradores controlar el acceso a procesos, archivos y carpetas específicas creadas por usuarios y/o otras aplicaciones. Debe brindar análisis de aplicaciones, control de procesos, registro, control de módulos y librerías DLL. Debe permitir a los administradores proteger, restringir ciertas actividades consideradas sospechosas o de alto riesgo. Asimismo, si el administrador por política interna de la institución desea controlar la ejecución de aplicaciones mediante el código hash de las mismas o mediante el registro de la aplicación en la consola debe tener la capacidad de controlarlo con la solución.
	19. Control de dispositivos	Deberá permitir al administrador controlar qué periféricos pueden conectarse a un equipo y cómo se usan. Bloquea las estaciones o servidores para impedir que se conecten las unidades, grabadoras de CD, impresoras y otros dispositivos USB. Debe igualmente contar con la capacidad no sólo de bloquear en su totalidad un dispositivo, sino de restringir parcialmente actividades en los periféricos, tales como memorias USB; haciendo que sean de sólo lectura, o que

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

		no permita la ejecución de aplicaciones desde dichos periféricos. Adicionalmente el administrador podrá definir si restringe el acceso a todos los dispositivos USB o permitir que dispositivos se pueden conectar.
	20. Flexibilidad en administración	Los administradores deben poder personalizar la interfaz y decidir qué tecnologías ejecutar en los equipos cliente y qué opciones de configuración no estarán disponibles para los usuarios finales.
	21. Adaptabilidad	La herramienta debe permitir que los clientes no dependan de un solo servidor de actualización local, y que en caso de que sean equipos móviles, puedan buscar según prioridad su servidor local más cercano o en su defecto puedan obtener las actualizaciones directamente desde Internet por la consola de gestión en la nube.
	22. Integración con LDAP	Debe permitir la integración con Active Directory.
	23. Firmas personalizadas de IDS/IPS	Debe contar con un IPS/IDS en cuyas características se incluya que el administrador pueda crear reglas personalizadas.
	24. Protección específica para los procesos y archivos propios de la herramienta	Debe contar con una protección específica para los procesos y archivos propios de la herramienta (Protección Contra Manipulaciones).
	25. Políticas por computador.	Debe permitir que las políticas sean aplicadas por equipos.
	26. Soporte para virtualización	La solución debe ser compatible para ser instalados en máquinas virtuales
	ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EDR-ENDPOINT DETECTION AND RESPONSE - La consola debe incluir un módulo de detección y respuesta para Endpoint (EDR) para todas las máquinas contempladas por la Alcaldía Distrital de Santiago de Cali. - Los servicios de gestión de detección y respuesta para Endpoint (EDR) deben ser gestionados sobre una consola en la nube, no se debe requerir licencias adicionales, de igual manera, los servicios se deben ejecutar sobre el mismo agente Endpoint de antivirus, por lo cual, no debe requerir un agente adicional en los equipos finales. - La solución de EDR debe permitir la creación de análisis causa raíz	

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	- La herramienta de gestión de incidentes debe mostrar un resumen de las alertas de amenazas organizado en forma de casos para su fácil gestión. - La solución de EDR debe ser 100% Cloud (Nube). - Se debe tener la capacidad de “aislar” máquinas con posibles amenazas mientras se ejecuta el debido análisis de la amenaza presentada. Cuando una máquina esté aislada la comunicación hacia internet, carpetas compartidas y conexiones de SSH deben ser cortadas de forma automática, la única comunicación debe estar establecida con la consola de administración del Endpoint. - La herramienta debe permitir una búsqueda y detección de amenazas en los endpoint basadas en hash, nombre de archivo, direcciones IP, dominios (completos o parciales) o líneas de comandos. SOPORTE TÉCNICO - El proveedor debe encargarse de la instalación y despliegue de todas las licencias de protección de correo, Endpoint (Antivirus) y EDR adquiridos por la entidad. - Debe incluir el soporte técnico 5X8 para escalar los incidentes o tickets de la solución. Con un tiempo de respuesta del estado de la solicitud no superior a 4 horas, dicho soporte puede ser web, email, telefónico o presencial. Ahora bien, frente al Personal mínimo requerido (En caso de que se requiera para la ejecución que el contratista cuente con un personal específico, se debe de detallar la cantidad, la formación, la experiencia y dedicación).																	
	<table border="1"> <thead> <tr> <th>Cargo</th><th>Cantidad</th><th>Perfil</th><th>Certificaciones mínimas</th><th>Experiencia</th></tr> </thead> <tbody> <tr> <td>Gerente de Proyecto</td><td>1</td><td> Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en gerencia de proyectos o áreas afines a su carrera profesional </td><td> Certificación PMP - Project Management Professional vigente. Auditor Líder ISO/IEC 27001:2022 </td><td> Contar con mínimo ocho (8) años de experiencia general contados a partir de la expedición de la tarjeta profesional </td></tr> <tr> <td>Especialista en seguridad informática</td><td>1</td><td> Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en Seguridad Informática </td><td> El profesional deberá acreditar certificación expedida directamente por el fabricante de la solución de seguridad ofertada, que certifique sus conocimientos y competencias para la instalación, configuración, despliegue y administración de la solución de protección de EndPoint bajo modalidad de servicio en la nube. </td><td> Contar con mínimo cuatro (4) años de experiencia general contados a partir de la expedición de la tarjeta profesional </td></tr> </tbody> </table>	Cargo	Cantidad	Perfil	Certificaciones mínimas	Experiencia	Gerente de Proyecto	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en gerencia de proyectos o áreas afines a su carrera profesional	Certificación PMP - Project Management Professional vigente. Auditor Líder ISO/IEC 27001:2022	Contar con mínimo ocho (8) años de experiencia general contados a partir de la expedición de la tarjeta profesional	Especialista en seguridad informática	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en Seguridad Informática	El profesional deberá acreditar certificación expedida directamente por el fabricante de la solución de seguridad ofertada, que certifique sus conocimientos y competencias para la instalación, configuración, despliegue y administración de la solución de protección de EndPoint bajo modalidad de servicio en la nube.	Contar con mínimo cuatro (4) años de experiencia general contados a partir de la expedición de la tarjeta profesional		
Cargo	Cantidad	Perfil	Certificaciones mínimas	Experiencia														
Gerente de Proyecto	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en gerencia de proyectos o áreas afines a su carrera profesional	Certificación PMP - Project Management Professional vigente. Auditor Líder ISO/IEC 27001:2022	Contar con mínimo ocho (8) años de experiencia general contados a partir de la expedición de la tarjeta profesional														
Especialista en seguridad informática	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente Contar con título de postgrado en Seguridad Informática	El profesional deberá acreditar certificación expedida directamente por el fabricante de la solución de seguridad ofertada, que certifique sus conocimientos y competencias para la instalación, configuración, despliegue y administración de la solución de protección de EndPoint bajo modalidad de servicio en la nube.	Contar con mínimo cuatro (4) años de experiencia general contados a partir de la expedición de la tarjeta profesional														

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)		MAJA01.04.01.P001.F003
	REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS		VERSIÓN 003

	Ingeniero de seguridad y protección de la Información:	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente	El profesional deberá acreditar certificación o curso expedido directamente por el fabricante de la solución ofertada, que demuestre conocimientos sobre la plataforma integral de ciberseguridad, su arquitectura, funcionalidades, componentes, capacidades de protección y mecanismos de integración para la gestión de la seguridad de la información.	Contar con mínimo un (1) años de experiencia general contados a partir de la expedición de la tarjeta profesional
	Coordinador de servicios de soporte	1	Ingeniero sistemas, industrial, electrónico o de telecomunicaciones con tarjeta profesional vigente	El profesional deberá acreditar certificación o curso, expedido directamente por el fabricante de la solución ofertada, que demuestre formación y competencias técnicas para la implementación, configuración, administración y gestión de soluciones de seguridad para cargas de trabajo en ambientes de nube, incluyendo la aplicación de políticas de protección y controles de seguridad sobre servidores y recursos computacionales.	Contar con mínimo cuatro (4) años de experiencia general contados a partir de la expedición de la tarjeta profesional
d.	Número del Id de la adquisición en el PAA.				
	Información pendiente por la UAG				
e.	Fecha en la que requiere satisfacer la necesidad, plazo y lugar de ejecución (tener en cuenta los tiempos de planeación, contratación y perfeccionamiento).				
	- Fecha aproximada de inicio de ejecución: Octubre 2026 - Plazo: Hasta diciembre de 2026 - Lugar de ejecución: Alcaldía de Santiago de Cali.				
f.	Obligaciones específicas del contratista.				
	1. Acreditar su vigencia como canal autorizado del fabricante y registrar las 4.460 licencias a nombre de la Entidad. 2. Entregar y activar las 4.460 licencias de Endpoint, Servidores y las 6.600 de Correo Electrónico dentro de los diez (10) días hábiles siguientes a la firma del acta de inicio, garantizando una vigencia de doce (12) meses sin interrupción de la protección actual. 3. Realizar la renovación sobre el <i>tenant</i> vigente de la Entidad, conservando las configuraciones, políticas e histórico de registros, y entregando la constancia oficial emitida por el fabricante. 4. Suministrar, renovar, activar, configurar y soportar la Solución Unificada de Seguridad para Endpoint, Servidores y Correo Electrónico en la Nube sobre el <i>tenant</i> vigente de la entidad cumpliendo de manera estricta con la totalidad de los requisitos funcionales, arquitectónicos, de protección y gestión establecidos en el Anexo Técnico (Condiciones Técnicas Mínimas), el cual hace parte integral y				

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

	vinculante del presente contrato. 5. Garantizar la confidencialidad de la información, informar formalmente la ubicación del procesamiento de datos y sus subencargados, y notificar cualquier incidente de seguridad en un tiempo inferior a 1.5 horas desde su detección. 6. Mantener el personal profesional ofertado durante la ejecución contractual; cualquier reemplazo deberá contar con un perfil equivalente o superior y requerirá la aprobación previa del supervisor del contrato. 7. Presentar un informe final de ejecución acompañado de todas las actas, reportes y evidencias que soporten el cumplimiento de las obligaciones.
g.	En caso de requerimientos financiados con recursos de inversión remitir Ficha EBI y cadena de valor. BP-26005260. Fortalecimiento de la Plataforma Tecnológica de la Alcaldía de Santiago de Cali.
h.	Cuando el objeto del proceso de contratación requiera de su validación por parte de otro organismo, de acuerdo a sus funciones, se debe anexar el respectivo aval en la forma que lo establezca este organismo. Viabilidad tramitada mediante orfeo No. 202641340100011494 del 09 de octubre de 2026
i.	¿Esta adquisición corresponde a bienes de uso común? Si _____ No ☒X_____ Si son bienes o servicios de uso común adjuntar ficha técnica, si aplica.
j	¿Es susceptible de incluir criterios de compra responsable? Si _____ No ☒X_____ ¿Si la respuesta anterior fue “sí” por favor indique a qué enfoque corresponde? Ambiental _____ Social _____ Innovación _____

Este documento es el insumo base para la estructuración del proceso de selección. No obstante, la información aquí contenida puede variar en virtud del estudio del sector que se desarrolle durante el proceso de planeación de la adquisición.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) REQUERIMIENTO PARA ADQUISICIÓN DE BIENES, OBRAS Y/O SERVICIOS	MAJA01.04.01.P001.F003	
		VERSIÓN	003

Atentamente,

ERMILSON DIAZ MARTÍNEZ
Subdirector de Tecnología Digital
Departamento Administrativo de Tecnologías de la Información y las Comunicaciones

Vo.Bo. ORDENADOR DEL GASTO
ALEXANDER MONDRAGON VALENCIA
Director

EQUIPO ESTRUCTURADOR

ROL FINANCIERO

ROL TÉCNICO

Paula Andrea Aristizabal García
Contratista

Hanner Arturo Fajardo
Contratista

ROL JURÍDICO

Jesenia Rojas Muñoz
Contratista

Proyectó: Paulo Cesar Guerrero – Profesional Universitario
Ermilson Díaz Martínez – Subdirector
Revisó: Jesenia Rojas Muñoz – Contratista