

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

1. TIPO DE INFORME	
INFORME PARCIAL <input type="checkbox"/>	INFORME FINAL <input checked="" type="checkbox"/>
Cuota Número 3	
2. ASPECTOS GENERALES DE CONTRATO Y SU EJECUCIÓN	
Orden de compra No. 151305	
Nombre del contratista: Hightech Software S.A.S	
Documento de identificación del Contratista: NIT 900718336-7	
Nombre del supervisor: Paulo Cesar Guerrero Agudelo - Profesional Universitario	
Organismo: Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).	No. Teléfono: 6028879020
Objeto de la Orden de compra No 151305: Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali.	
3. INFORME JURÍDICO	
Fecha de Inicio	Fecha Terminación
14/Sep/2025	15/Mar/2026
Modificación al contrato: N/A	
Suspensión: N/A	
Reanudación: N/A	

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Cesión: N/A

Terminación anticipada: N/A

4. INFORME CONTABLE Y FINANCIERO

Valor inicial del contrato: DIEZ MIL OCHOCIENTOS DIECINUEVE MILLONES NOVECIENTOS CUARENTA Y TRES MIL OCHENTA Y NUEVE PESOS MCTE (\$10.819.943.089).

Adición: N/A

Prórroga: N/A

Resumen contable y financiero:

Valor Total del Contrato	Valor Cuota a Cancelar	Valor Acumulado Cancelado	Saldo por Cancelar
\$ 10.819.943.089	\$2.163.988.618	\$8.655.954.471	\$0

INFORMACIÓN DEL PAGO DE SEGURIDAD SOCIAL

PERSONA JURÍDICA: Hightech Software S.A.S

FECHA DE CERTIFICACIÓN: 13 de febrero de 2026

La certificación será expedida por el Revisor Fiscal YERRY TATIANA PRADA MEJIA identificado con cédula de ciudadanía No. 40330919 de VILLAVICENCIO (META) tarjeta profesional No. TP- 140139-T

PERSONA NATURAL: N/A

Datos Certificación o Planilla de Pago de persona Natural: N/A

No. Planilla: N/A

No. PIN, Autorización, Referencia, Pago: N/A

Operador: N/A

Fecha de Pago: N/A

Periodo de Pago de la Seguridad Social: N/A

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Observaciones al informe contable y financiero: Aportaron la Factura electrónica EHTS-2196 23 de febrero de 2026, por valor de DOS MIL CIENTO SESENTA Y TRES MILLONES NOVECIENTOS OCHENTA Y OCHO MIL SEISCIENTOS DIECIOCHO PESOS MCTE (\$2.163.988.618).

5. INFORME TÉCNICO

RECIBO A SATISFACCIÓN DE BIENES Y/O SERVICIOS:

Se recibe a entera satisfacción del Distrito Especial de Santiago de Cali los bienes y/o servicios entregados, conforme a las condiciones establecidas en la Orden de Compra No. 151305 y sus respectivos estudios previos. A continuación, se describen el consolidado de las actividades ejecutadas y las obligaciones contractuales cumplidas:


El contratista para configurar el cumplimiento del primer ítem de la orden de compra, sxc02---NUV-HOU-03-01 Software General – Otro – High Tech Software S.A.S-N/A-N/A-Dolar-N/A-Mensual-Houndoc:

En virtud de lo establecido en la Orden No. 151303, cuyo objeto es “Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali”, el proveedor realizó la entrega de un certificado de recursos *cloud* a la entidad, destinado al consumo de los servicios de infraestructura *cloud* asociados a esta solución.

Documento Anexo: [Certificación bolsa de recursos Cloud Alcaldía de Cali](#)

Este componente correspondió al uso y operación de la infraestructura virtual desplegada en AWS, la cual fue necesaria para soportar los sistemas de información institucionales del Distrito. Se incluyeron los costos variables asociados al consumo de:

- Recursos de cómputo (instancias, núcleos virtuales y procesamiento)
- Almacenamiento distribuido y en capas (EBS, S3, EFS)
- Servicios de red y transferencia de datos (interconexión, VPN y tráfico interno/externo)

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

- Capacidades nativas de seguridad, respaldo, auditoría y monitoreo

La infraestructura fue configurada bajo un modelo de alta disponibilidad, con mecanismos de recuperación ante fallos y herramientas de monitoreo continuo, lo que permitió garantizar la continuidad operativa y la estabilidad de los servicios institucionales.

Adicionalmente, se implementó un proceso para el monitoreo y optimización permanente del gasto, el cual incluyó:

- Etiquetado estandarizado para trazabilidad por cuenta, servicio y entorno
- Revisión continua de consumos y proyecciones
- Alertas automáticas de desbordamiento presupuestal
- Recomendaciones de optimización
- Reporte mensual de costos, uso y eficiencia

Para el cumplimiento del segundo ítem, sxc02---NUV-HOU-01-05 Software General – Otro – High Tech Software S.A.S-N/A-SAAS-N/A-N/A-Unidad-N/A-Houndoc, el proveedor hace entrega de la plataforma tecnológica Houndoc, que consolida la información para su uso y garantiza que la Alcaldía de Cali cuente con los accesos y derechos necesarios, cumpliendo con las condiciones técnicas y administrativas definidas.

Información de uso de la plataforma:

- Propietario: High Tech Software S.A.S.
- Usado por Santiago de Cali Distrito Especial- Departamento Administrativo de Tecnologías de La Información y las Comunicaciones.
- Modalidad: SaaS exclusiva y no transferible, territorio Colombia.
- Usuarios: Hasta 1000 usuarios nombrados.
- Versión: Houndoc v0.52.6.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Vigencia: Hasta 31 de diciembre de 2026.

El Acceso se encuentra desplegado en la nube, en portal web:

<https://app.ia.cali.gov.co/> en productivo para usuarios de Alcaldía Cali.



Como parte de los entregables del contrato, proveedor realizó la entrega del licenciamiento de la plataforma Houndoc a la Alcaldía de Santiago de Cali, cumpliendo con las condiciones técnicas y administrativas definidas.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Documento Anexo: Certificación licenciamiento houndoc Alcadia de Cali- proyecto Vistualización

Documento Anexo:

https://drive.google.com/drive/folders/1kepZOaBMwmNXUIOZj_lwNOIV00yg63Kc

Para el cumplimiento del tercer ítem de la orden de compra, sxc02---IT-SW-09-02 Software General – Otro – High Tech Software S.A.S-N/A-N/A-Remota-Profesional-Hora-Todas las zonas-N/A- Configuración y parametrización de los Productos. El proveedor entregó certificación del servicio contratado, donde notifica que la entidad cuenta con una bolsa de 3.006 horas de servicios profesionales, destinadas a la creación, personalización e implementación de los casos de uso que conforman la solución de virtualización objeto del contrato. Esta bolsa de horas permite garantizar el acompañamiento técnico necesario para el desarrollo progresivo de los componentes, en articulación con los requerimientos funcionales y operativos definidos por la entidad.



Bogotá D.C, 14 de septiembre de 2025.


Señores
SANTIAGO DE CALI DISTRITO ESPECIAL
DEPARTAMENTO ADMINISTRATIVO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
 Ciudad

Referencia. Certificación servicios profesionales.

Respetados señores, cordial saludo.

DIANA CAROLINA VILLAMIZAR BOHORQUEZ, mayor de edad, identificado con cédula de ciudadanía número 1090.394.391 de Cúcuta, actuando en calidad de representante legal principal de la Compañía **HIGH TECH SOFTWARE S.A.S**, Sociedad Comercial legalmente constituida, identificada con NIT 900.718.336-7, en virtud de lo establecido en la orden No 151303, cuyo objeto es "Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de informaciones transversales del Distrito de Santiago de Cali", nos permitimos certificar que en virtud del servicio contratado la entidad cuenta con una bolsa de horas 3006 horas de servicios profesionales para la creación, personalización e implementación de los casos de uso que harán parte de la solución de virtualización contratada.

Cordialmente,


DIANA CAROLINA VILLAMIZAR BOHORQUEZ
 C.C No 1090.394.391 de Cúcuta
 Representante Legal Principal
 High Tech Software S.A.S

Documento Anexo: Certificación servicios profesionales OC 151305

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

<https://drive.google.com/drive/folders/1uvuWGu-7GhW5O6L0qWvFsUJck7XGWKmH>

Para el cumplimiento del cuarto ítem de la orden de compra, sxc02---IT-SW-02-03 Software General – Otro – High Tech Software S.A.S-N/A-N/A-Presencial-Profesional-Mes-3-N/A-Soporte técnico en sitio.

En el marco de la presente entrega, el proveedor adjuntó el certificado que acredita la provisión de servicios de soporte. Este componente aseguró la disponibilidad de personal técnico especializado para la atención, acompañamiento y operación de la infraestructura virtual contratada por la Alcaldía de Santiago de Cali.

El servicio de soporte cubrió el acompañamiento operativo integral, el cual incluyó: la gestión de incidentes, la atención de requerimientos y ajustes, el soporte directo durante ventanas de mantenimiento y cambios planificados, y las actividades de diagnóstico, estabilización y continuidad de servicios críticos. Adicionalmente, se garantiza la interacción permanente con los equipos de DATIC, facilitando la transferencia de conocimiento y la consecuente apropiación tecnológica durante el proceso de operación.

La ejecución de las actividades se adhirió estrictamente a los Acuerdos de Nivel de Servicio (ANS) definidos con la entidad, respetando los horarios y mecanismos de atención establecidos y manteniendo registros trazables en bitácoras de soporte.

La gestión operativa se centralizó a través de la herramienta oficial Service Center. Esta plataforma habilitó a los usuarios para registrar, modificar y cerrar solicitudes de incidentes, solicitudes de cambio (RFC) y requerimientos de información (RFI). Service Center permite gestionar un amplio espectro de tareas, tales como:

- Creación y eliminación de recursos AWS (EC2, RDS, S3, EBS, Security Groups, IAM Roles, WAF, Load Balancers).
- Gestión de configuraciones en servidores, redes VPC y balanceadores.
- Despliegue y modificación de máquinas virtuales en VMware.
- Validación de conectividad híbrida.
- Revisión de *logs*, análisis de costos, y gestión de copias de seguridad y restauraciones.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

La solución proporcionó reportes técnicos y operativos para el seguimiento integral de cada caso.

Durante el periodo evaluado, se mantuvo la operación continua de Service Center con los usuarios oficiales debidamente habilitados, quienes accedieron al portal <https://soporte.nuvu.cc/index.php?logout=-1> para el registro, consulta y seguimiento de solicitudes. Se completó la entrega y socialización del Manual de Usuario, lo que garantizó el conocimiento operativo para la correcta utilización de la plataforma y la trazabilidad de todos los casos gestionados. Los reportes consolidados confirmaron la gestión de un número considerable de solicitudes (infraestructura, despliegues, configuración de reglas de *firewall*, administración de recursos AWS y validaciones operativas), donde la mayoría fue clasificada con criticidad alta y atendida dentro de los tiempos estipulados por los ANS.

Documento Anexo: [Certificación servicios de soporte OC 151305](#)

Por otro lado, el contratista, para dar cumplimiento a las obligaciones específicas consignadas en los estudios previos, realizó las siguientes actividades:

1 Cumplir los requerimientos establecidos en las especificaciones técnicas, estudios previos, oferta económica y demás documentos que hagan parte del proceso de contratación.

El proveedor en cumplimiento de lo establecido en la obligación contractual que busca asegurar, demostrar y documentar que todas las obligaciones técnicas y contractuales con lo solicitado en los Estudios Previos de la OC 151305, para lograrlo, creó una Matriz de Trazabilidad de Requisitos (MTR) establecidos en los estudios previos, donde se listan uno por uno todos los requisitos técnicos, funcionales y administrativos del proyecto, indicando:

- Obligaciones del contrato.
- Qué entregable o evidencia lo demuestra.
- La periodicidad con la que se entregará

Adicionalmente, elaboró un documento donde se detallan las obligaciones del contrato y la periodicidad de entrega que permitirá revisar el cumplimiento de cada obligación se

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

esté cumpliendo de manera verificable, transparente y acorde con lo estipulado en el contrato.

Documento Anexo: Matriz de Trazabilidad de Requisitos verificable contra estudios previos

2 Entregar un plan de trabajo de la ejecución del contrato, donde se contemple como mínimo las actividades de diseño y arquitectura base de cada solución tecnológica, la configuración de la herramienta de virtualización, la replicación de la data previamente conciliada con el supervisor, las pruebas y la puesta en marcha de los modelos y soluciones tecnológicas. En este plan de trabajo se deberán visualizar con claridad, en su estructura de descomposición de trabajo las líneas y actividades del contrato, así como sus recursos y el avance actual de cada una de ellas.

El proveedor en cumplimiento de las obligaciones contractuales, elaboró y entregó a la entidad el Plan de Trabajo de Ejecución del Contrato, documento que consolida la hoja de ruta técnico–metodológica para la implementación de la solución tecnológica integral objeto del contrato. Dicho plan fue estructurado siguiendo los lineamientos estratégicos de DATIC y las directrices técnicas definidas en los Estudios Previos y en el Requerimiento Técnico.

El Plan de Trabajo contempla una estructura de descomposición de actividades (EDT/WBS) que permite visualizar de manera clara y secuencial cada fase del proyecto, sus actividades asociadas, los responsables, los recursos técnicos y humanos involucrados, y el avance estimado para cada componente.

Documento Anexo: Plan de trabajo

3 Elaborar y entregar informes periódicos de actividades, en el cual se evidencie el desarrollo y avance del objeto contratado, siendo potestad del supervisor designado solicitarlo en cualquier momento de la ejecución del contrato, de acuerdo con las fases de ejecución del contrato.

El proveedor en cumplimiento de lo establecido en la obligación contractual referente a la entrega de informes periódicos de actividades, estructuró un mecanismo formal de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

seguimiento y reporte que permite evidenciar el avance técnico y operativo del proyecto, así como el estado de cumplimiento del objeto contratado.

Durante la ejecución del contrato elaboró y presentó Informes de Ejecución de acuerdo con las fases definidas en el Plan de Trabajo y conforme a los requerimientos del supervisor del contrato, quien podrá solicitar estos informes en cualquier momento para efectos de verificación, trazabilidad y control de avance.

Cada informe incluye:

- Descripción detallada de las actividades ejecutadas en el periodo.
- Estado de avance frente a las obligaciones contractuales.
- Evidencias documentales y técnicas que soportan el cumplimiento.

Documento Anexo: Informes de ejecución mensual

4 Garantizar que las soluciones tecnológicas desplegadas sean compatibles con la operación del modelo de datos almacenado por la Alcaldía del Distrito de Santiago de Cali.

En cumplimiento de esta obligación, garantizamos que las soluciones tecnológicas desplegadas son diseñadas e implementadas de manera compatible con el modelo de datos institucional de la Alcaldía del Distrito de Santiago de Cali. Para ello, realizamos la revisión y entendimiento del modelo de datos existente, sus estructuras, reglas de negocio y lineamientos técnicos, asegurando que las soluciones respetarán la integridad, coherencia y operación de la información. Adicionalmente, validamos la correcta integración y funcionamiento de las soluciones con los sistemas existentes, ejecutando pruebas de compatibilidad y documentando los resultados, de tal forma que se garantizara una operación estable, segura y alineada con los estándares definidos por la entidad.

5 Realizar la gestión de la infraestructura bajo una cuenta designada por la entidad o conforme a las políticas establecidas por esta, utilizando etiquetas (tags) normalizadas para cada recurso (nombre del proyecto, entorno,

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

responsable, criticidad, centro de costo), que faciliten la trazabilidad técnica y financiera de los mismos.

El proveedor en cumplimiento de esta obligación, realizó la gestión integral de la infraestructura tecnológica dentro de la cuenta designada por la entidad, aplicando estrictamente las políticas de etiquetado definidas para garantizar la trazabilidad técnica, operativa y financiera de todos los recursos implementados. Para ello, utilizó la política de tagueo establecida por Blend, en la que se definen las etiquetas obligatorias y opcionales que deben ser incorporadas en cada recurso desplegado en la nube. Estas etiquetas incluyen el nombre del recurso (Name), el entorno de despliegue (Env), la aplicación o producto asociado (App), el identificador del proyecto (ProjectId) y el cliente (Client), todas categorías obligatorias conforme a la política oficial, así como la etiqueta opcional Component cuando se requiere especificar el rol del recurso, ya sea front, back u otro tipo de componente.

Cada etiqueta se aplicó siguiendo las reglas de nomenclatura formal descritas en la política: nombres completamente en minúsculas para los recursos, entornos en mayúsculas con siglas normalizadas, aplicaciones alineadas al maestro de productos y un ProjectId estandarizado que inicia con la letra P seguida de cuatro dígitos. Este modelo de etiquetado permite identificar de manera precisa el propósito, el entorno, la responsabilidad técnica, la criticidad operativa y el centro de costo asociado a cada recurso, lo que asegura un control adecuado en procesos de facturación, auditoría, asociabilidad financiera y gestión operativa de la infraestructura.

La administración de los recursos bajo esta política garantiza que la entidad cuente con una infraestructura ordenada, estandarizada y completamente trazable, facilitando la identificación de consumos, la depuración de costos, la administración de responsabilidades y la alineación del inventario tecnológico con las necesidades de operación del Distrito de Santiago de Cali. Con la aplicación consistente de estas etiquetas, se asegura el cumplimiento de las políticas internas de la entidad, la transparencia en el uso de la infraestructura y la capacidad de dar seguimiento técnico y financiero al ciclo de vida de cada recurso cloud.

Documento Anexo: Política de etiquetado

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

6 Ocuparse de la gestión de administración de la infraestructura de servicios de virtualización, de manera que asegure la disponibilidad de dicha infraestructura en al menos en 99.9% (ANS).

El proveedor en cumplimiento de la obligación, realizó la administración integral de la infraestructura de virtualización garantizando una disponibilidad mínima del 99.9%. El equipo mantiene un monitoreo continuo sobre los componentes críticos cómputo, almacenamiento, red, balanceadores y conectividad— utilizando métricas de rendimiento y disponibilidad que permiten identificar anomalías, atender incidentes de manera oportuna y asegurar la estabilidad del servicio. De forma permanente se aplican acciones de optimización, autosanación, recuperación y ajuste de plataformas, lo que permite preservar la continuidad operativa y la estabilidad del entorno tecnológico. La disponibilidad alcanzada y las actividades de operación se consolidan en informes periódicos que evidencian el nivel de servicio comprometido.



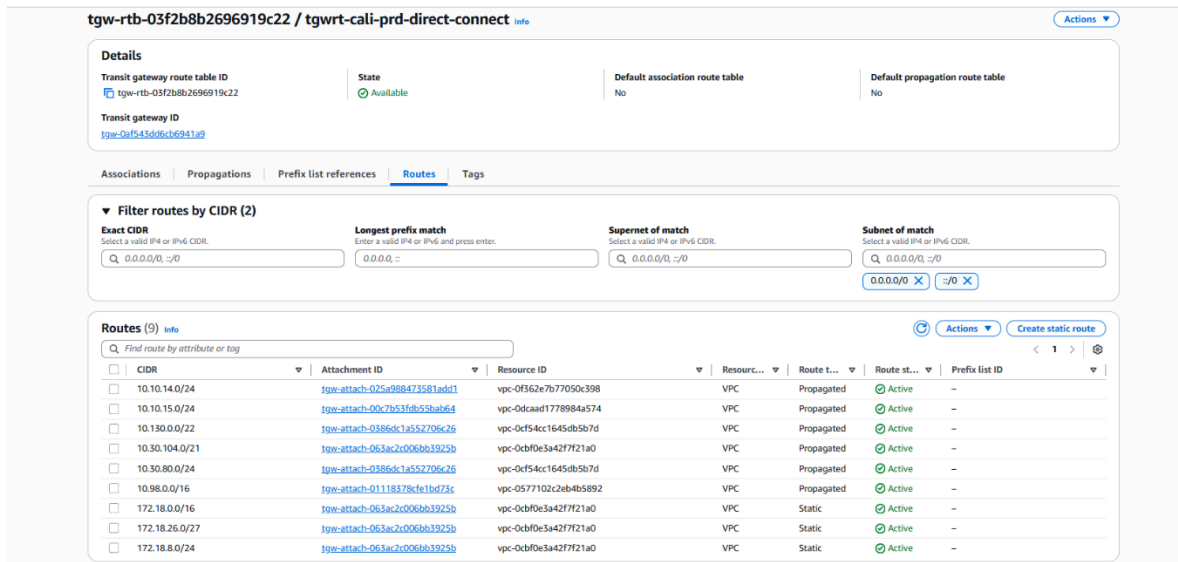
Documento Anexo: [Informe de monitoreo y disponibilidad Alcaldía de Cali](#)

7 Habilitar y configurar un canal de comunicación alternativo mediante VPN, utilizando uno de los canales de Internet proporcionados por la entidad. Esta VPN deberá estar correctamente integrada con el canal Direct Connect (o su equivalente), y ambas conexiones deberán operar bajo un esquema de alta disponibilidad, ya sea en configuración activo-activo o, como mínimo, en activo-pasivo con conmutación automática (failover automático), garantizando la continuidad del servicio ante fallos de conectividad.

En la infraestructura implementada para la Alcaldía de Santiago de Cali el proveedor habilitó y configuró un canal de comunicación alternativo mediante una VPN establecida sobre uno de los canales de Internet suministrados por la entidad, con el fin de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

garantizar continuidad operativa ante cualquier evento de conectividad. Esta VPN se encuentra correctamente integrada con el enlace Direct Connect que opera en la cuenta de networking de la organización, el cual ha sido desplegado, configurado y validado para soportar el intercambio de datos entre la infraestructura local y los servicios de AWS. Conforme al estado del recurso registrado, el Direct Connect se encuentra activo y funcional, mientras que la VPN actúa como un enlace de respaldo plenamente operativo ante posibles fallas o degradaciones del servicio principal.



CIDR	Attachment ID	Resource ID	Resource	Route type	Route status	Prefix list ID
10.10.14.0/24	tgw-attach-025a988473581ad1	vpc-0f362e7b77050c398	VPC	Propagated	Active	-
10.10.15.0/24	tgw-attach-00c7b3f3fb55bab64	vpc-0dcaad1778984a574	VPC	Propagated	Active	-
10.130.0.0/22	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
10.30.104.0/21	tgw-attach-063ac2c06bb3925b	vpc-0cb0e3a427f21a0	VPC	Propagated	Active	-
10.30.80.0/24	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
10.98.0.0/16	tgw-attach-01118378cfe1bd73c	vpc-0577102c2eb4b5892	VPC	Propagated	Active	-
172.18.0.0/16	tgw-attach-063ac2c06bb3925b	vpc-0cb0e3a427f21a0	VPC	Static	Active	-
172.18.26.0/27	tgw-attach-063ac2c06bb3925b	vpc-0cb0e3a427f21a0	VPC	Static	Active	-
172.18.8.0/24	tgw-attach-063ac2c06bb3925b	vpc-0cb0e3a427f21a0	VPC	Static	Active	-

Ambos canales operan bajo un esquema de alta disponibilidad, lo que permite su funcionamiento en configuración activo-activo cuando la arquitectura lo requiere, o como mínimo en un modelo activo-pasivo con conmutación automática (failover) para garantizar que el tránsito del tráfico continúe sin interrupciones ante una caída del enlace principal. El mecanismo de enrutamiento detecta automáticamente pérdidas de conectividad, latencias atípicas o fallos en el Direct Connect, activando de inmediato el túnel VPN como ruta alternativa sin afectar los servicios ni los sistemas que dependen de esta comunicación híbrida.

Esta configuración integrada asegura redundancia, resiliencia y estabilidad en la conectividad entre los sistemas de la Alcaldía y la nube, permitiendo mantener la operación continua de las cargas de trabajo, servicios críticos y procesos institucionales, incluso ante fallos de infraestructura o interrupciones externas. Con ello,

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

se garantiza un modelo de comunicación robusto, seguro y alineado con las buenas prácticas de arquitectura híbrida y los requerimientos establecidos por la entidad.

Documento Anexo: Informe de Estado Direct Connect ACA

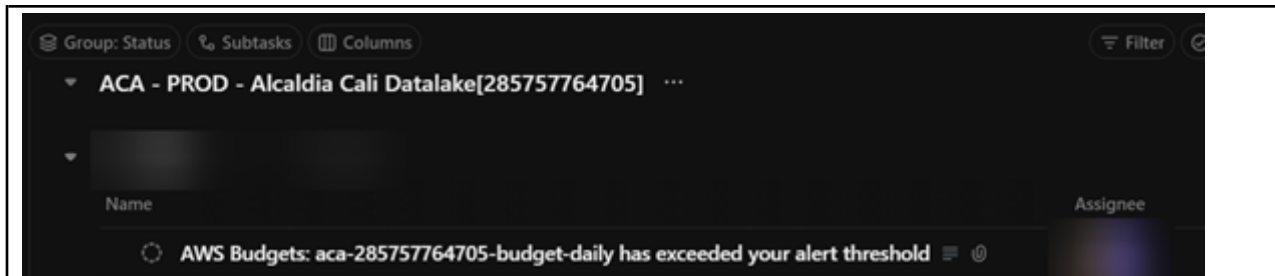
8 Monitorear y reportar mensualmente el consumo de la infraestructura (almacenamiento, cómputo, tráfico, etc.), incluyendo recomendaciones de optimización y alertas sobre posibles desviaciones presupuestales, asegurando la eficiencia del uso de los recursos contratados.

El proveedor realizó el monitoreo continuo del consumo de la infraestructura tecnológica y consolidó la información en los reportes mensuales de consumo de infraestructura, en los cuales se presenta el uso de recursos de cómputo, almacenamiento, tráfico y servicios asociados. En dichos reportes incluyó el análisis del comportamiento del consumo, recomendaciones de optimización orientadas a la eficiencia en el uso de los recursos, así como alertas tempranas sobre posibles desviaciones presupuestales, con el fin de apoyar el control, seguimiento y la toma de decisiones por parte de la Alcaldía del Distrito de Santiago de Cali.

El proveedor configuró procesos de gestión financiera operativa que permiten monitorear y optimizar el consumo de la infraestructura en la nube. Estos procesos incluyen el etiquetado (tagging) sistemático de recursos para mantener trazabilidad del gasto por cuenta, entorno o proyecto, facilitando el análisis detallado del uso y los costos asociados.

Con esta información creo alarmas específicas para cada cuenta en el que se indica y se informa a través de la plataforma de click up cuando un promedio de budget sobrepasa su umbral correspondiente

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



Estas alarmas se verifican de manera diaria y se da una razón y justificación para el aumento de este costo, y se subsane realizando modificaciones en la alarma si es un nuevo despliegue que se haya realizado o se realizan los ajustes necesarios en el recurso que aumentó su costo para disminuirlo

De igual forma se realizará un informe mensual en el que se registren los costos de cada servicio de ese mes y cualquier tipo de cambio o hallazgo que se deba tener en cuenta para informarlo, junto con su respectiva solución para trazabilidad.

Documento Anexo: [Informe de monitoreo y disponibilidad Alcaldía de Cali](#)

9 Implementar política de acceso basada en roles (IAM), que permita controlar, limitar y auditar el acceso a los recursos de la nube, conforme a los principios de menor privilegio y segregación de funciones, entregando a la entidad los registros de acceso generados durante la ejecución del contrato.

El proveedor configuró una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

La gestión de identidades y accesos se realiza mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permite administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

Como parte de la implementación de seguridad en AWS, el proveedor configuró un conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de

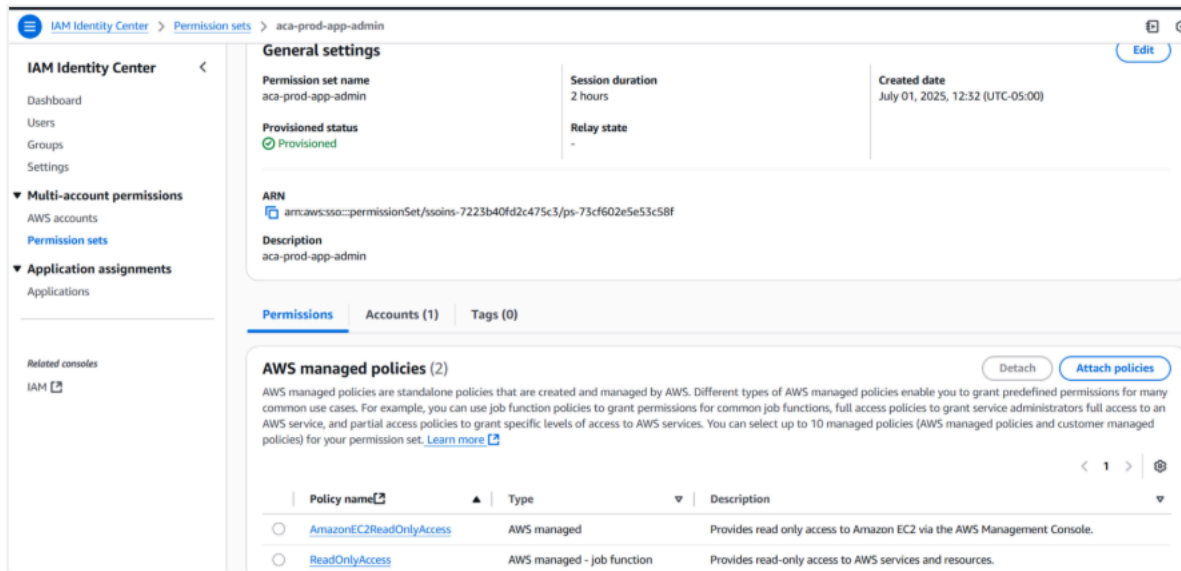
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

A Continuación se detalla el conjunto de grupos de seguridad:

- ACA -AppAdmin

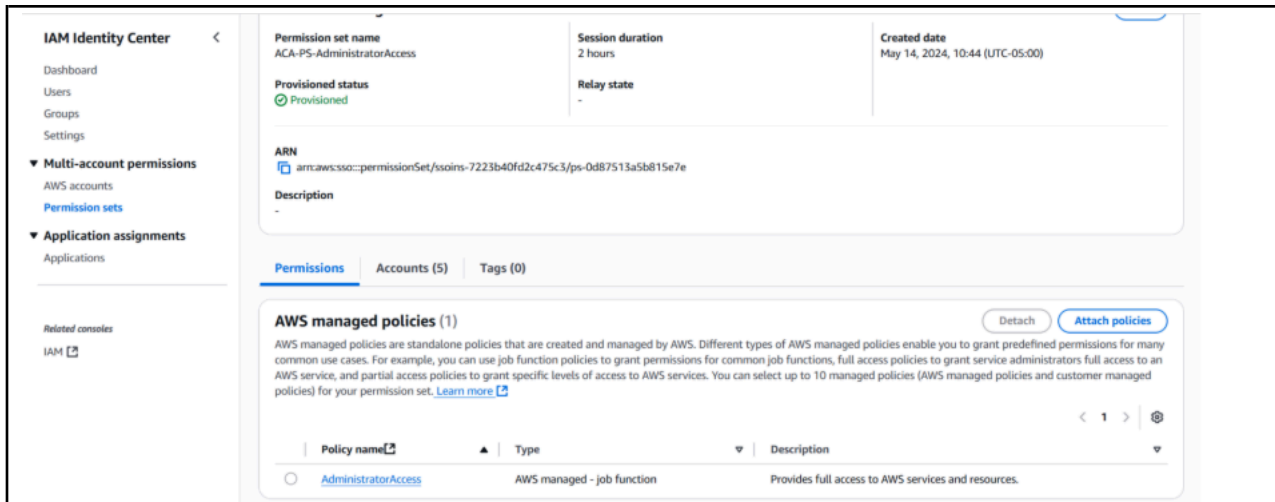
Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD -Workload Alcaldía Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.



- ACA – CloudAdmin

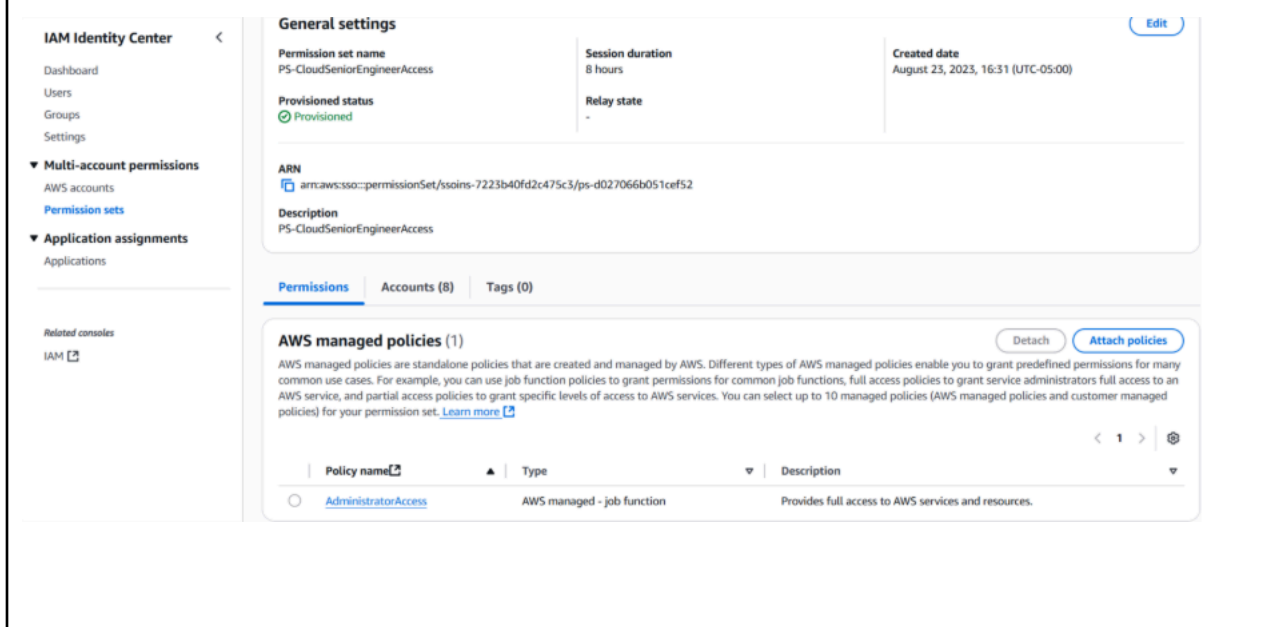
El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



- NUVU – CLOUDCloudSeniorEngineer

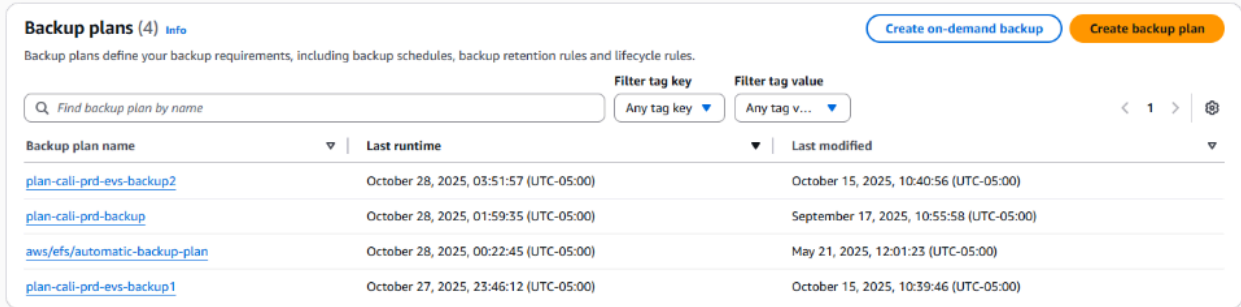
Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Documento Anexo: Documentación Infraestructura AWS

10 Gestionar y mantener actualizadas las copias de seguridad (backups) de los sistemas, datos y configuraciones relacionados con la solución contratada, en los servicios de almacenamiento y respaldo habilitados en la nube de AWS o equivalentes. Las copias de seguridad deberán incluir mecanismos de recuperación (snapshots, volcados de bases de datos, archivos de configuración, etc.), y se deberá realizar al menos una prueba de restauración por trimestre calendario, dejando constancia de los resultados en un informe técnico que deberá ser entregado a la entidad. Para asegurar la portabilidad de la información, los backups deberán estar disponibles en formato descargable. En el caso de servicios gestionados (máquinas nativas o bases de datos nativas), el contratista deberá garantizar la exportación de los datos (por ejemplo, mediante mysqldump, pg_dump u otro método adecuado) y almacenarlos en Amazon S3 u otro repositorio que permita su descarga directa. Al finalizar el contrato, el contratista deberá entregar la totalidad de las copias de seguridad vigentes en el medio de almacenamiento que disponga la Alcaldía Distrital en su momento, asegurando la integridad, trazabilidad y disponibilidad de la información durante el proceso de entrega.



The screenshot shows the AWS Backup console interface. At the top, there are buttons for 'Create on-demand backup' and 'Create backup plan'. Below this is a search bar and filter options for tag keys and values. The main content is a table listing backup plans with columns for name, last runtime, and last modified date.

Backup plan name	Last runtime	Last modified
plan-cali-prd-efs-backup2	October 28, 2025, 03:51:57 (UTC-05:00)	October 15, 2025, 10:40:56 (UTC-05:00)
plan-cali-prd-backup	October 28, 2025, 01:59:35 (UTC-05:00)	September 17, 2025, 10:55:58 (UTC-05:00)
aws/efs/automatic-backup-plan	October 28, 2025, 00:22:45 (UTC-05:00)	May 21, 2025, 12:01:23 (UTC-05:00)
plan-cali-prd-efs-backup1	October 27, 2025, 23:46:12 (UTC-05:00)	October 15, 2025, 10:39:46 (UTC-05:00)



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

Jobs

In jobs, you can monitor the status and other details of backup, restore, and copy activity.

[Backup jobs](#) | [Restore jobs](#) | [Copy jobs](#)

Backup jobs (306+) info

Records of your scheduled or on-demand backups.

Filter backup jobs by job ID, status, resource ID, resource type or message category. 302 matches

Status = Completed

Clear filters

< 1 2 3 4 5 6 7 8 ... >

Backup job ID	Status	Resource name	Message category	Resource ID	Resource type
1DC42716-0627-39C5-546B-02AC4DABD080	Completed	altar	Success	vm/vm-0000478549D2A7FF5	VMware virtual m
7764C3D8-22E9-F143-2366-B4FD4A99E3E8	Completed	SEMTITAAPPEDPT01	Success	vm/vm-0000694BD1A774B04	VMware virtual m
013BC9AF-6A00-2EC5-D29F-FADAD0C00BC7	Completed	nfs-oraclemann	Success	vm/vm-000075EC6FD687278	VMware virtual m
FAAA9F52-25A3-820B-B3EE-4322A79BA752	Completed	Contratacion-Portal-DB-ENIATO	Success	vm/vm-00005D95A511843E7	VMware virtual m
6273B6FE-F192-2748-4F1E-386D73C9808F	Completed	GestionDocumental	Success	vm/vm-000051FE935A15DF1	VMware virtual m
912681E4-B1F3-7E77-F3AB-5536EAB0F8F4	Completed	SiCali-DB-QUIMBAYA	Success	vm/vm-000040869AC0FF332	VMware virtual m
ED743C04-E88D-FF62-AE22-2454BCDFCBA3	Completed	CATASTRO-DataQuality-PRD-App-ESTIGIA	Success	vm/vm-00005E54D34CBBC10	VMware virtual m
9C8A27D6-137E-669B-8BFA-A60279C730AB	Completed	Datic Zimbra mail	Success	vm/vm-00005CAFC4F1BC8B4	VMware virtual m
7B2225DA-556A-E4F5-D52A-CE15AE91E083	Completed	Concejo PRE-PRD Procesos y Apache	Success	vm/vm-00004C396D0A783DA	VMware virtual m
69C3DB12-1303-1F99-E731-8C94694C41F7	Completed	calieducadigital_MYSQL2	Success	vm/vm-000059EB390E535D2	VMware virtual m

El contratista implementó un sistema robusto de copias de seguridad en AWS Backup que protege toda la infraestructura crítica de la solución contratada.

El sistema cuenta con 4 planes de backup activos que respaldan más de 500 recursos, incluyendo 450 máquinas virtuales, 50+ instancias EC2, volúmenes EBS, sistemas de archivos EFS y buckets S3. Todos los backups se almacenan en 4 vaults configurados con cifrado KMS y políticas de retención apropiadas.

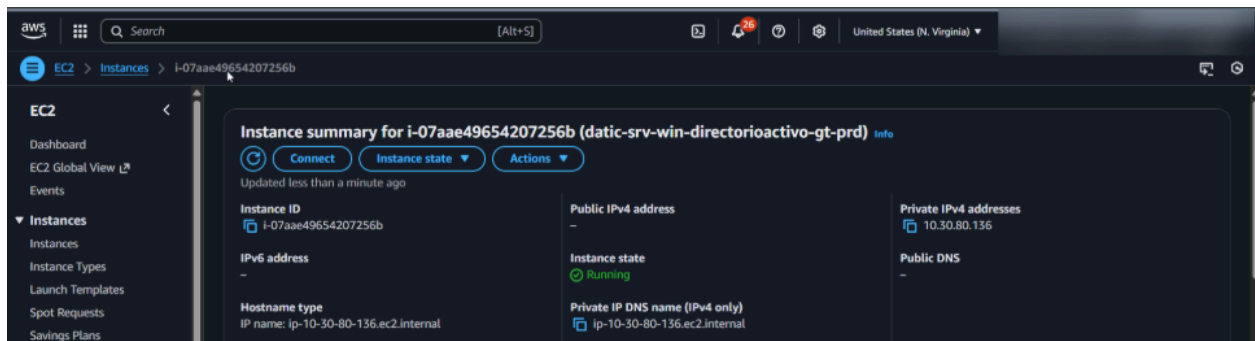
El vault principal "vault-cali-prd-backup" contiene 3,429 puntos de recuperación y está configurado con bloqueo de seguridad. Las ejecuciones son diarias y automáticas.

Los sistemas respaldados incluyen todas las bases de datos críticas (PostgreSQL, Oracle, MySQL), servidores de aplicaciones (GlassFish, Wildfly), sistemas de gestión documental, infraestructura de red, servidores de correo Zimbra, y sistemas ERP y catastro.

En casos de restauración ha realizado para la máquina datic-srv-win-directorioactivo-gt-prd para la cual se solicitó una eliminación a través del

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

portal de la mesa de servicio de Blend y posteriormente una restauración a través del mismo servicio a una copia que se tenía gracias a los planes de backup que se encuentran activos.



Documento Anexo: Documentación Infraestructura AWS

11 Garantizar la disponibilidad de herramientas digitales de administración y gestión de las soluciones tecnológicas desarrolladas, que cuente con acceso a la infraestructura subyacente, permitiendo el monitoreo de todos los servicios de virtualización.

El proveedor garantizó mediante el uso de herramientas nativas de AWS la disponibilidad y gestión de las soluciones tecnológicas desarrolladas, principalmente a través de Amazon CloudWatch, que permite el monitoreo continuo de la infraestructura subyacente y de los servicios de virtualización. Esta herramienta proporciona visibilidad en tiempo real del rendimiento, uso de recursos y estado operativo de los componentes.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

5. DiskReadBytes: Cantidad de datos (en bytes) que la instancia lee desde sus discos. Alto volumen indica una intensa actividad de lectura de información.
6. DiskWriteBytes: Cantidad de datos (en bytes) que la instancia escribe en sus discos. Alto volumen indica una intensa actividad de guardado o modificación de archivos.
7. DiskReadOps: Número de operaciones de lectura individuales que la instancia solicita a sus discos. Muchas operaciones pueden ser demandantes incluso si el volumen de datos es bajo.
8. DiskWriteOps: Número de operaciones de escritura individuales que la instancia realiza en sus discos. Un recuento elevado es común en sistemas con bases de datos activas.
9. NetworkIn: Volumen total de datos (en bytes) que la instancia recibe desde la red.
10. NetworkOut: Volumen total de datos (en bytes) que la instancia envía a la red. Estas dos métricas reflejan el tráfico total de su aplicación.
11. NetworkPacketsIn: Número de paquetes de datos individuales que la instancia recibe. Un número muy alto puede consumir recursos de CPU.
12. NetworkPacketsOut: Número de paquetes de datos individuales que la instancia envía. Es útil para diagnosticar problemas de rendimiento de red o aplicaciones con mucho "chateo" (pequeñas comunicaciones frecuentes).

Documento Anexo: [Informe de monitoreo y disponibilidad Alcaldía de Cali](#)

12 Realizar la gestión del proyecto, asegurando la planificación y el seguimiento adecuado de la ejecución del contrato

El proveedor realizó la gestión del proyecto, asegurando la adecuada planificación y el seguimiento de la ejecución del contrato. Para ello, elaboró un plan de trabajo en el cual se definieron las actividades a ejecutar y poder llevar a cabo un seguimiento continuo y coordinado con la entidad en las solicitudes y requerimientos presentados. Adicionalmente, compartió de manera periódica los reportes mensuales de avance, los cuales permitieron evidenciar el estado de la ejecución del contrato, los avances realizados y el apoyo brindado ante cualquier requerimiento técnico u operativo, garantizando así el cumplimiento de los objetivos contractuales.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Documento Anexo: Plan de trabajo

13 Llevar a cabo la transferencia de conocimiento dirigida a los colaboradores de la Alcaldía de Santiago de Cali sobre el funcionamiento, uso y administración de las soluciones tecnológicas desarrolladas.

El proveedor en cumplimiento de la obligación de realizar la transferencia de conocimiento, llevó a cabo un proceso estructurado de capacitación dirigido a los colaboradores de la Alcaldía de Santiago de Cali, enfocado en el funcionamiento, uso, buenas prácticas y administración de las soluciones tecnológicas implementadas en la infraestructura de virtualización y servicios cloud. Como parte de este proceso, se realizó un Workshop técnico presencial, desarrollado en conjunto entre AWS y Blend360, en el cual se presentaron los conceptos clave necesarios para que el equipo de la Alcaldía pueda operar, administrar y comprender adecuadamente los servicios utilizados.

El contenido impartido incluyó los siguientes módulos fundamentales:

1. Visión General de los Servicios de AWS

Se presentó la estructura global y regional del ecosistema AWS, explicando la distribución de los servicios en componentes globales y regionales, y su relevancia en la operación de la plataforma implementada. Entre los temas tratados:

- Diferenciación entre servicios globales (IAM, Route 53, CloudFront, WAF) y servicios regionales (EC2, S3, RDS, Lambda, entre otros).
- Arquitectura de nube y regiones disponibles.
- Relaciones entre servicios y buenas prácticas de diseño.

2. EC2 – Elastic Compute Cloud

Se profundizó en los conceptos y prácticas esenciales para la gestión de servidores virtuales dentro del entorno AWS:

- Introducción a instancias EC2 y su escalabilidad.
- Creación y configuración de servidores virtuales.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

- Uso de AMI, Security Groups y Key Pairs.
- Configuración y consideraciones de seguridad.
- Lineamientos para escalar la capacidad en función de la demanda.

3. **VPC – Virtual Private Cloud**

Se realizó una explicación detallada sobre la estructura de redes virtualizadas y su importancia para la operación segura de los servicios:

- Funcionamiento de redes privadas y públicas.
- Subredes, tablas de enrutamiento y conectividad a Internet.
- Configuración de Internet Gateways y mecanismos de seguridad.
- Segmentación, aislamiento y control de tráfico dentro de la nube.

4. **IAM – Identity and Access Management**

Se abordaron las prácticas clave de administración de accesos y seguridad:

- Gestión de usuarios, roles y políticas.
- Implementación del principio de “mínimo privilegio”.
- Buenas prácticas de seguridad y control de accesos.
- Administración basada en roles (RBAC) y manejo seguro de credenciales.

5. **S3 – Simple Storage Service**

Se explicó la estructura del servicio de almacenamiento y sus aplicaciones dentro del proyecto:

- Concepto de almacenamiento global/regional.
- Estructura de buckets y objetos.
- Nomenclatura global y su impacto en la operación.
- Uso de políticas, versionamiento e integración con otros servicios.

6. **Práctica Guiada en la Consola AWS**

Efectuó un ejercicio práctico supervisado en el entorno seguro del workshop:

- Acceso a la consola con credenciales temporales.
- Creación y gestión de recursos en EC2, IAM, VPC y S3.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

- Validación de configuraciones y despliegues.
- Ejercicios orientados a fortalecer la autonomía del equipo técnico.

La transferencia de conocimiento permitió:

- Capacitar al personal técnico en los componentes clave de la plataforma.
- Brindar herramientas teóricas y prácticas para la adecuada administración de los servicios tecnológicos.
- Asegurar la continuidad operativa de la solución mediante la apropiación del conocimiento por parte del equipo de la Alcaldía.
- Fortalecer las capacidades internas para la toma de decisiones técnicas informadas y la gestión de incidentes, cambios y mantenimiento.

La sesión contó con el apoyo directo de especialistas de AWS y del equipo profesional de Blend360, garantizando un aprendizaje efectivo y alineado con las mejores prácticas internacionales en computación en la nube.



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



Documento Anexo: [Reporte Capacitación ACA](#)

14 Prestar el servicio especializado para la implementación de las soluciones tecnológicas, durante la vigencia del contrato.

El proveedor brindó acompañamiento técnico y operativo en las iniciativas de modernización de infraestructura en AWS definidas por la Alcaldía de Santiago de Cali. Como parte de esta actividad, ha avanzado en la modernización del sistema Orfeo, la modernización del Portal Municipal de la Alcaldía, así como en el despliegue de ecosistemas digitales, asegurando que las soluciones a modernizar se encuentren alineadas con los lineamientos técnicos, de seguridad y de operación establecidos, y contribuyan a la mejora de la disponibilidad, escalabilidad y sostenibilidad de la infraestructura tecnológica de la entidad.



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

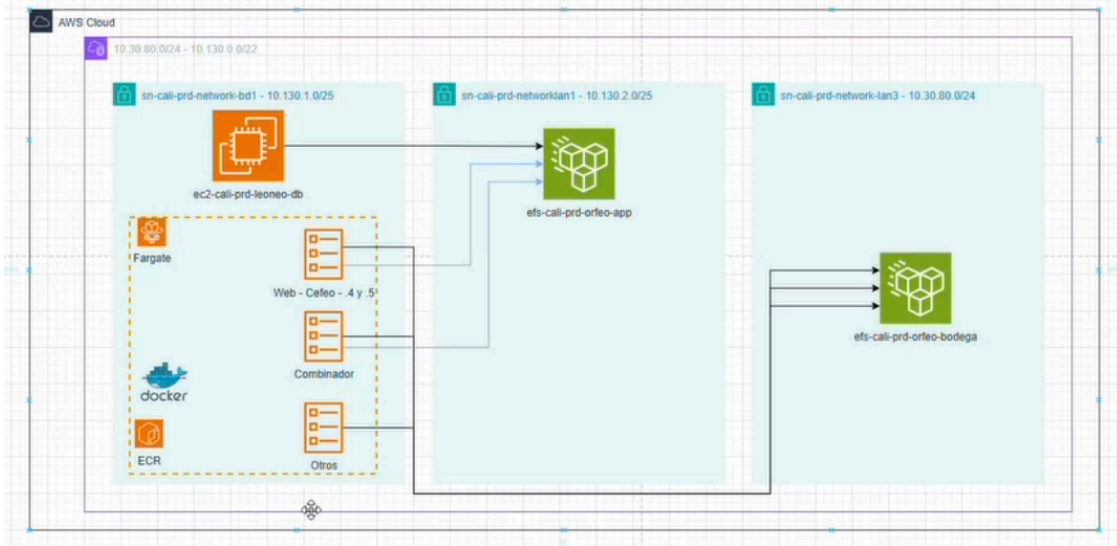
MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002



aplica Statistics intranet.c... SQL a G precic Report Micro Dash... Modulo > + v

No seguro http://52.90.225.124/index_frames.php?fechah=20260223_1771866220&PHPSESSID=200e29e10... Modulo > + v

Comenzar a usar Fir... Ingreso al Portal Tra... Portal de Pagos Gru... PortalPagosDavie... Pagos PSE Falabella Banca Virtual | Banc... Pago factura - Cols... 172.18.26.17/ldap/id...

MUNICIPIO DE SANTIAGO DE CALI

rfeo

AYUDA INFO CREDITOS CONTRASOÑAS ESTADÍSTICAS CERRAR

Solicitados Solicitar Físico

PAGINA ANTERIOR DATOS DEL RADICADO No 20264134020000024

LISTADO DE: Visto.Buono USUARIO: Leonidas Andrade Otalora DEPENDENCIA: Subdireccion de Tecnologia Digital

MOVER A REASIGNAR INFORMAR DEVOLVER Voto FIRMAR ARCHIVAR

INFORMACION GENERAL HISTÓRICO DOCUMENTOS EXPEDIENTES

HISTORICO

USUARIO ACTUAL	Leonidas Andrade Otalora	DEPENDENCIA ACTUAL	Subdireccion de Tecnologia Digital
USUARIO RADICADOR	Leonidas Andrade Otalora	DEPENDENCIA DE RADICACION	Subdireccion de Tecnologia Digital

FLUJO HISTORICO DEL DOCUMENTO

DEPENDENCIA	FECHA	TRANSACCION	US. ORIGEN	COMENTARIO
Subdireccion de Tecnologia Digital	02-01-2026 10:33 AM	Asignaci3n TRD	Leonidas Andrade Otalora	Tipificacion
Subdireccion de Tecnologia Digital	02-01-2026 10:33 AM	Radiciaci3n	Leonidas Andrade Otalora	Se radica el documento

DATOS DE ENVIO

RADICADO	DEPENDENCIA	FECHA	Destinatario	DIRECCION	DEPARTAMENTO	MUNICIPIO	TIPO DE ENVIO	No. PLANILLA	OBSERVACIONES O DESC DE ANEXOS

http://52.90.225.124/curro.php?PHPSESSID=200e29e103e71eFONIDASoANDRADE&krd=LEONIDAS.ANDRADE&adofb=next_pape1&fechah=230226_1771866224&nomcarpeta=Visto.Buono - Firma&carpetas=118tipo_carrn=0&adofb=next_pape1

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

15 Cumplir con las áreas principales del modelo de computación en los servicios digitales, como lo son: despliegue de servicios, orquestación de servicios, administración de los servicios digitales, privacidad y seguridad. Lo anterior en concordancia con lo establecido en la Guía Técnica de Computación en la nube de MinTIC y las versiones que lo modifiquen.

El proveedor en cumplimiento de lo establecido en la Guía Técnica de Computación en la Nube del MinTIC, garantizó que la solución implementada opera bajo las áreas fundamentales del modelo de computación aplicable a los servicios digitales de la entidad. Para ello, ejecutó procesos estructurados de despliegue, orquestación, administración, privacidad y seguridad, asegurando que cada uno de estos componentes se integre de manera coherente dentro de la infraestructura tecnológica de la Alcaldía de Santiago de Cali. El despliegue de los servicios los realizó a través de procedimientos estandarizados que permiten implementar máquinas virtuales, configuraciones de red y servicios complementarios de forma consistente, utilizando plantillas, configuraciones predefinidas y mecanismos que aseguran uniformidad, trazabilidad y estabilidad operativa. Paralelamente, la orquestación de los servicios permite coordinar los distintos recursos de cómputo, red y almacenamiento, integrando la automatización de tareas, el escalamiento de recursos según la demanda, la operación asincrónica y la comunicación segura entre los distintos componentes, garantizando así un funcionamiento unificado y eficiente de los servicios digitales. El proceso de administración se desarrolla de manera continua mediante actividades de supervisión, monitoreo, mantenimiento, gestión de incidencias y optimización, asegurando el rendimiento, la disponibilidad y la estabilidad de la infraestructura. Esto incluye el seguimiento permanente de métricas críticas, la aplicación de ajustes preventivos y correctivos, la operación ininterrumpida de los servicios virtualizados y la gestión completa del ciclo de vida de los recursos. En materia de privacidad, se aplica un tratamiento responsable de la información mediante controles de acceso basados en el principio de mínimo privilegio, segmentación de redes, cifrado en tránsito y en reposo, y mecanismos que aseguran que los datos sensibles se mantengan protegidos durante todo su ciclo de uso. Finalmente, la seguridad la garantizó a través de políticas de control, firewalls, monitoreo de eventos, prácticas de fortalecimiento de sistemas, rutas seguras de comunicación y medidas que protegen la integridad, disponibilidad y confidencialidad de los servicios digitales. Todo lo anterior asegura que la infraestructura y los servicios implementados se encuentren alineados con los lineamientos, principios y estándares definidos por el MinTIC, cumpliendo con las mejores prácticas nacionales para la prestación segura, confiable y eficiente de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

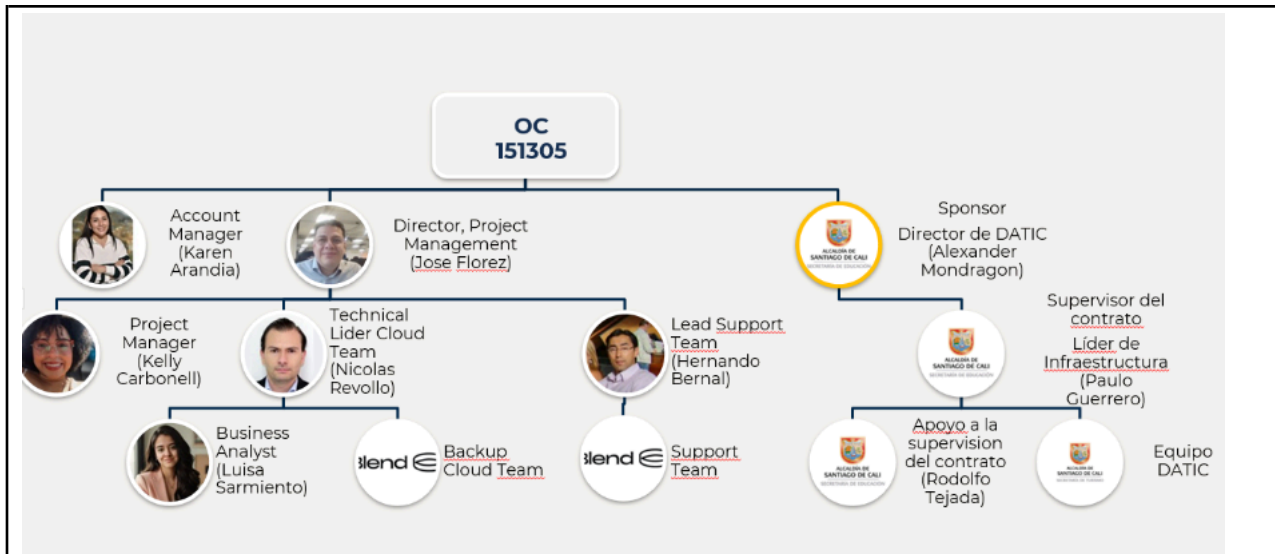
servicios digitales en entornos de computación en la nube.

Documento Anexo: Servicios de AWS Para el Cumplimiento de Modelos de Computación y Estándares Normativos (ACA)

16 Designar un delegado para participar en las mesas de trabajo establecidas por el supervisor del contrato y atender las medidas que allí sean tomadas con el fin de soportar los requerimientos y que los mismo se lleven a cabo de manera articulada.

El proveedor en cumplimiento de esta disposición, designó formalmente a la Gerente de Proyectos Kelly Carbonell Ramos como representante responsable de participar en las mesas de trabajo convocadas por el supervisor del contrato. Esta designación se encuentra establecida dentro del plan de trabajo y garantiza la articulación permanente entre las decisiones adoptadas en dichas sesiones y la ejecución técnica y operativa del proyecto. La delegada asistió de manera activa a los espacios definidos, atendió las directrices impartidas por el supervisor y aseguró que cada medida, requerimiento o ajuste acordado fue incorporado oportunamente dentro del desarrollo de las actividades. Adicionalmente, el proyecto contó con un equipo técnico de apoyo que respalda la gestión de la Gerente de Proyectos, permitiendo una correcta interpretación de los requerimientos, una respuesta oportuna a las necesidades planteadas y una ejecución articulada entre la coordinación, la operación y los frentes técnicos involucrados. Este esquema de trabajo garantiza la trazabilidad de las decisiones, la alineación entre las partes y el cumplimiento eficiente de los objetivos del contrato.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002



17 Elaborar, suscribir y presentar al Distrito de Santiago de Cali - Departamento Administrativo de Tecnologías de la Información y las Comunicaciones las respectivas actas e informes correspondientes a la ejecución de la contratación. Estos documentos deberán ser aprobados por el Supervisor del Contrato.

El proveedor en cumplimiento de lo establecido para la adecuada ejecución contractual, elaboró y presentó al Distrito de Santiago de Cali – Departamento Administrativo de Tecnologías de la Información y las Comunicaciones los informes de ejecución mensual, en los cuales se documentó de manera detallada el avance del proyecto y el cumplimiento de las obligaciones a cargo del contratista. Estos informes se generan con la periodicidad definida en los estudios previos y en el plan de trabajo, es decir, de forma mensual, consolidando las actividades realizadas, los resultados obtenidos, la trazabilidad de los entregables y los soportes correspondientes. Cada informe es remitido al Supervisor del Contrato para su revisión y aprobación, asegurando transparencia, seguimiento oportuno y alineación con los objetivos técnicos y administrativos establecidos por la entidad.

Documento Anexo: Informes de ejecución mensual

18 Dar cumplimiento a la normatividad de protección de datos personales y de confidencialidad de la información, donde garantice una adecuada definición de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

los niveles de seguridad para no generar accesos no autorizados a datos confidenciales de propiedad de la Entidad.

El proveedor configuró una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

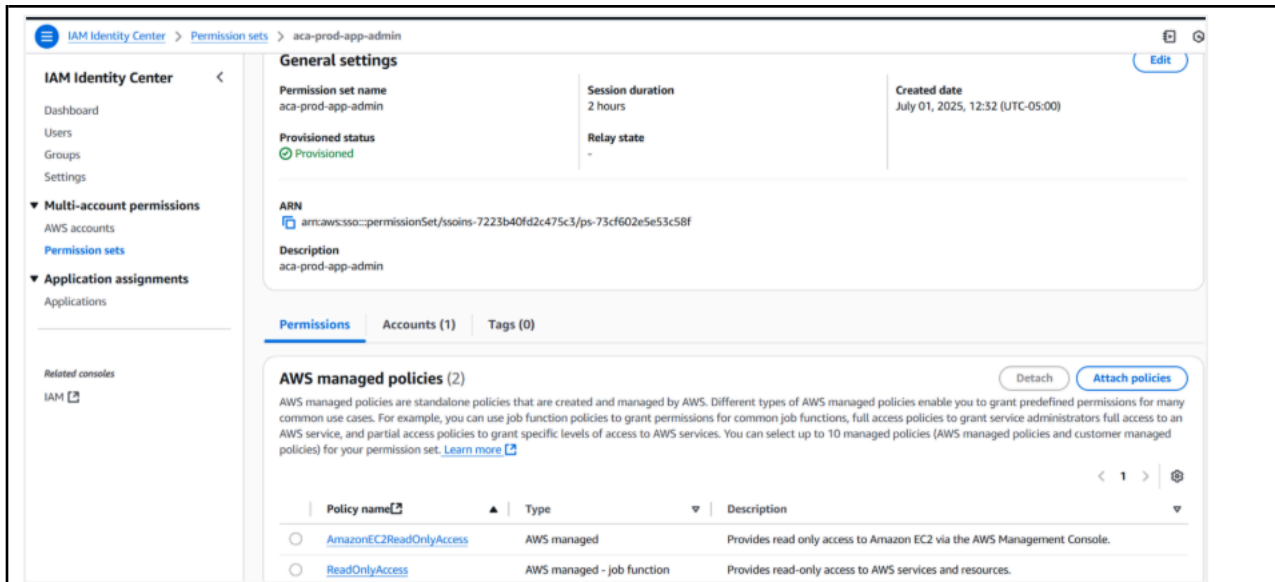
La gestión de identidades y accesos la realizó mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permitió administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

Como parte de la implementación de seguridad en AWS, configuró un conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

- ACA -AppAdmin

Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD - Workload Alcaldía Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.

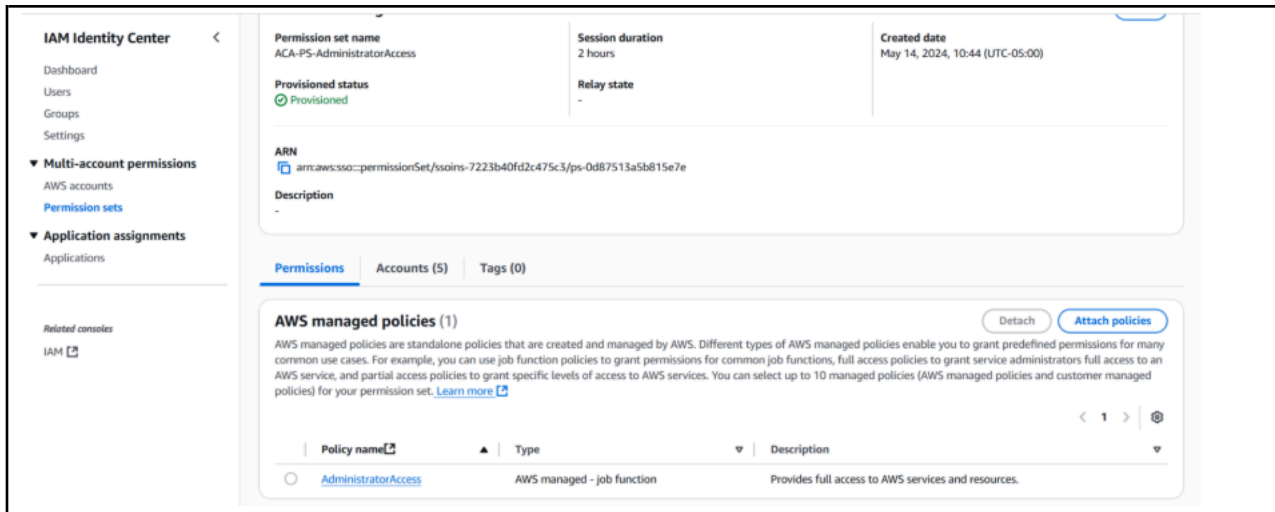
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



- ACA – CloudAdmin

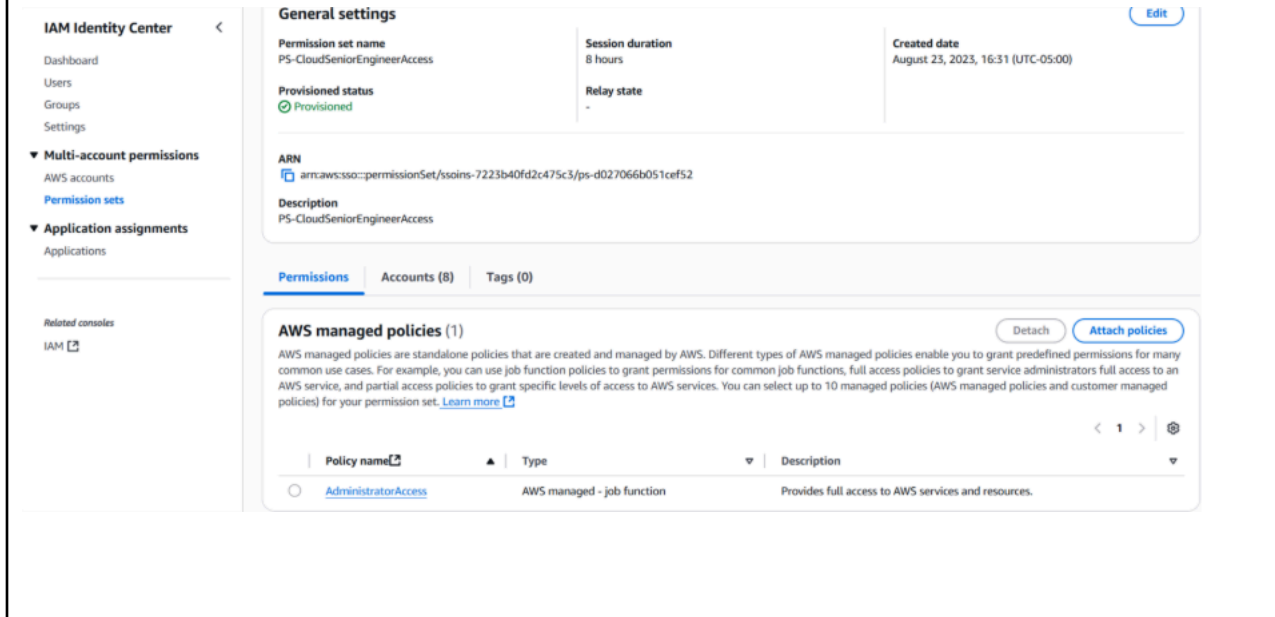
El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



● NUVU – CLOUDCloudSeniorEngineer

Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Documento Anexo: Informe de Políticas de Acceso Para la Organización de ACA

19 Garantizar que siempre la Entidad tendrá la propiedad y el control de su información, así como disponible un mecanismo para el borrado seguro de los datos, si llegare a ocurrir una terminación anticipada, según el modelo computacional.

El proveedor en cumplimiento de esta disposición, garantizó que la Entidad mantiene en todo momento la propiedad, titularidad y control absoluto sobre toda su información, independientemente de que los datos se encuentren procesados, almacenados o respaldados dentro de los servicios de AWS. Toda la arquitectura y operación de la infraestructura se implementa respetando este principio, asegurando que el acceso, tratamiento, administración y gestión de los datos se realiza exclusivamente bajo las directrices y autorizaciones de la Entidad. Con el fin de reforzar este control y asegurar la disponibilidad, integridad y recuperación de la información institucional, se implementa una política robusta de respaldos que forma parte del modelo computacional aplicado en la nube. Esta estrategia se encuentra configurada en AWS mediante el plan plan-cali-prd-backup, el cual administra los respaldos a través del vault vault-cali-prd-backup y se ejecuta mediante el rol IAM role-cali-prd-backup, asegurando que todas las copias de seguridad se generen de manera automatizada, controlada y sin intervención de terceros no autorizados.

plan-cali-prd-backup

[Delete](#) [View JSON](#)




Summary			
Backup plan name plan-cali-prd-backup	Version ID Zjk2MWY2MGUtMmYxNi000 DhhLWJIM2EtZTFhNTJlYTAzY	Last modified July 30, 2025, 10:00:50 (UTC-05:00)	Last runtime September 12, 2025, 01:15:07 (UTC-05:00)
Backup plan ID e17d35df-91fd-4391-9311-33ac5c855379	Tgy		

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

vault-cali-prd-backup Info

Manage vault lock
Delete vault
Edit access policy

Summary

Vault name vault-cali-prd-backup Vault type Backup vault Vault ARN  arn:aws:backup:us-east-1:363934983054:backup-vault:vault-cali-prd-backup	KMS encryption key ID  Creation date June 26, 2025, 14:48:16 (UTC-05:00)	Vault lock  Locked – Governance mode Vault lock is editable. Learn more
		Retention period for vault lock Minimum retention period: 6 days Maximum retention period: –

Backup rules (4) Edit Delete Add backup rule

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Name	Backup vault	Destination Backup vault
DailyBackup-15DayRetention	vault-cali-prd-backup	-
MonthlyBackup-1YearRetention	vault-cali-prd-backup	-
WeeklyBackup-1MonthRetention	vault-cali-prd-backup	-
YearlyBackup-20YearRetention	vault-cali-prd-backup	-

La política incluye ciclos de retención diarios, semanales, mensuales y anuales, con períodos que van desde 15 días hasta 20 años, y contempla la transición automática a almacenamiento frío según corresponda, optimizando costos sin comprometer la disponibilidad ni la trazabilidad de los respaldos. Los recursos sujetos a esta estrategia son identificados mediante la etiqueta “Backup – Enabled”, lo que permite garantizar una administración ordenada y consistente del proceso de protección de datos. Esta estructura de respaldos no solo respalda la continuidad operativa, sino que también constituye un mecanismo seguro de preservación y restauración de información, permitiendo atender incidentes, garantizar cumplimiento normativo y mantener la integridad de los datos institucionales.

De igual forma, y en concordancia con el modelo computacional adoptado, se dispone de un mecanismo de borrado seguro para el caso en que se presente una terminación anticipada del contrato. Este mecanismo asegura que, una vez la Entidad lo solicite, toda la información almacenada en los servicios de AWS pueda ser eliminada de manera definitiva mediante procedimientos certificados que imposibilitan su recuperación posterior, salvaguardando así la confidencialidad y los derechos de propiedad de la Entidad sobre su información. Con esta combinación de control,

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

respaldo y eliminación segura, se garantiza el manejo responsable de los datos durante toda la vigencia contractual y después de su finalización, manteniendo siempre la soberanía y protección de los activos de información de la Alcaldía de Santiago de Cali.

20 Entregar los códigos, manuales, tutoriales y/o instructivos asociados a las soluciones tecnológicas brindadas. También debe entregar los accesos a los aplicativos y a herramientas de monitoreo para acceder por parte del personal de DATIC.

En el marco del cumplimiento de la obligación consistente en entregar los códigos, manuales, tutoriales y/o instructivos asociados a las soluciones tecnológicas brindadas, así como los accesos a los aplicativos y a las herramientas de monitoreo para el personal de DATIC, actualmente se encuentran en ejecución las actividades asociadas a la modernización del sistema Orfeo, del Portal Municipal de la Alcaldía y al despliegue de ecosistemas digitales.

Estas actividades se desarrollan con el objetivo de asegurar que las soluciones tecnológicas a intervenir se alineen progresivamente con los lineamientos técnicos, de seguridad y de operación establecidos por la Entidad, y que contribuyan a la mejora de la disponibilidad, escalabilidad y sostenibilidad de la infraestructura tecnológica institucional. A medida que se consoliden los avances, el proveedor realizará la entrega gradual de los documentos, códigos, manuales y accesos correspondientes, como soporte del cumplimiento de la obligación contractual.

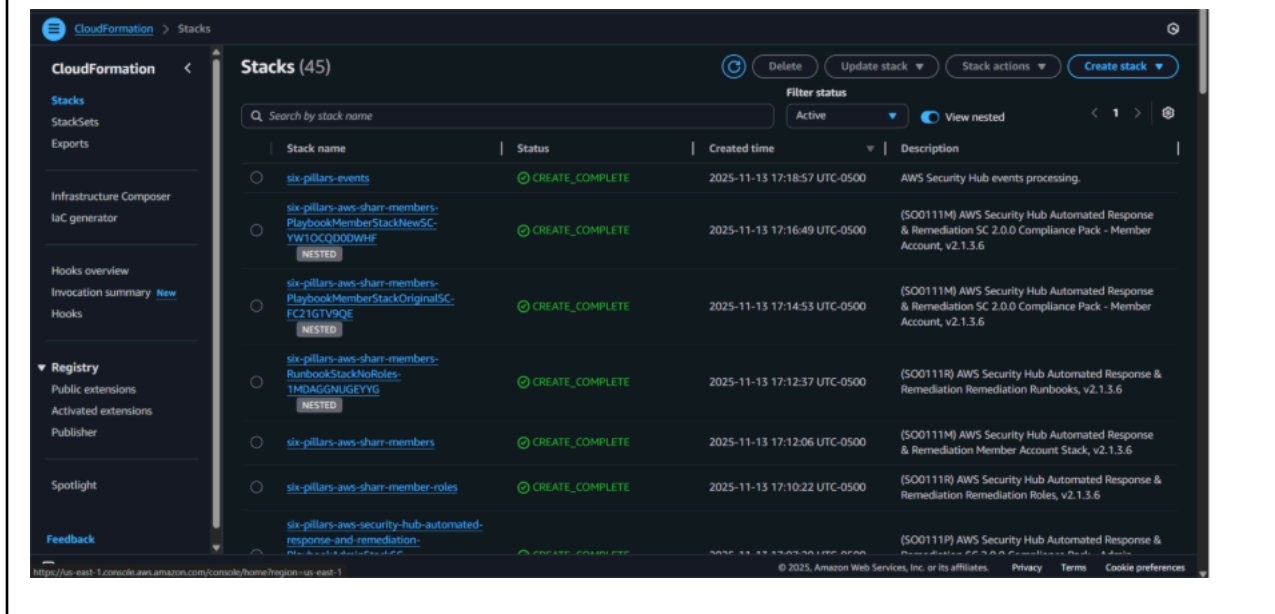
21 Garantizar que los servicios a proveer cumplan con estándares de calidad con las normas vigentes relativas al servicio la infraestructura digital, ISO 9901-ISO 27001 –ISO 27017 –ISO27018 – SOC1 –SOC2 – SOC3 –CSA -FEDRAMP.

En la prestación de los servicios el proveedor garantizó que toda la infraestructura y los componentes tecnológicos implementados cumplen con los estándares internacionales de calidad y seguridad definidos para servicios digitales y entornos de computación en la nube, incluyendo ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, CSA y FEDRAMP. Este cumplimiento se respalda en la adopción de servicios nativos de AWS que han sido diseñados para operar bajo estos marcos normativos y cuyo funcionamiento, certificaciones y controles se encuentran plenamente alineados con las mejores prácticas globales. Tal como se describe en el

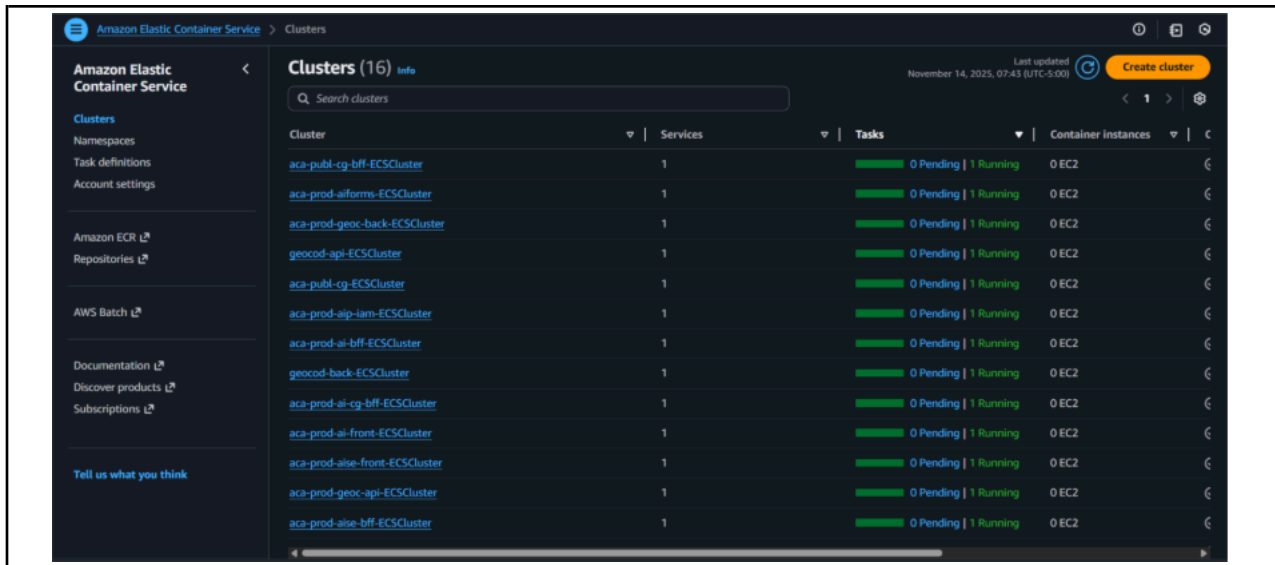
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

documento de referencia, los servicios utilizados para despliegue, orquestación, administración, privacidad y seguridad entre ellos CloudFormation, ECS, EC2, Lambda, Organizations, Control Tower, CloudWatch, CloudTrail, Systems Manager, Config, Trusted Advisor, IAM, IAM Identity Center, KMS, ACM, WAF, GuardDuty y Shield permiten asegurar que la infraestructura funciona bajo políticas estrictas de gobierno, protección, auditoría, cifrado, autenticación y gestión de incidentes, cumpliendo así los lineamientos establecidos por los estándares normativos mencionados.

La arquitectura desplegada incorpora controles técnicos y procedimentales que garantizan la protección de los datos, la segregación de funciones, la trazabilidad, la privacidad, la gestión segura de identidades, el cumplimiento de políticas de seguridad y el aseguramiento de ambientes operativos confiables, todo dentro del marco de certificaciones globales que AWS mantiene permanentemente auditadas. De esta manera, los servicios provistos no solo se ajustan a las normas vigentes aplicables a la infraestructura digital de la Entidad, sino que operan bajo un modelo de cumplimiento sustentado, verificable y acorde a los estándares internacionales más exigentes, asegurando la calidad, integridad y seguridad del servicio durante toda la vigencia del contrato.



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002



Documento Anexo: Servicios de AWS Para el Cumplimiento de Modelos de Computación y Estándares Normativos (ACA)

22 Atender las sugerencias que el Distrito de Santiago de Cali - Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones, considere convenientes y pertinentes para la ejecución del objeto del contrato.

En el marco de la ejecución del contrato el proveedor atendió de manera oportuna, integral y continua todas las sugerencias, recomendaciones y solicitudes emitidas por el Distrito de Santiago de Cali, a través del Departamento Administrativo de Tecnologías de la Información y las Comunicaciones, garantizando que cada requerimiento planteado sea incorporado y gestionado dentro del ciclo operativo de la infraestructura tecnológica. Este proceso se desarrolla mediante la mesa de servicios y el uso de la plataforma Service Center, en la cual se registran las solicitudes que la entidad considera pertinentes para fortalecer, ajustar o validar aspectos relacionados con la operación del entorno cloud y los servicios implementados. Tal como se evidencia en el Informe Mensual de Casos correspondiente al mes, durante dicho periodo se procesaron múltiples solicitudes asociadas a ajustes de infraestructura de red, validaciones de seguridad, configuración de recursos, despliegue de instancias,

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

actualizaciones de reglas de seguridad y verificación de conectividad, todas ellas derivadas de necesidades y sugerencias planteadas por los equipos de DATIC.

Cada una de estas solicitudes fue analizada y gestionada conforme a su criticidad y prioridad, registrando avances, resultados y estados de cierre que demuestran la atención efectiva de las recomendaciones realizadas por la entidad. De acuerdo con el informe, todas las solicitudes presentadas durante el periodo fueron gestionadas adecuadamente y culminaron en su correcta implementación o resolución, evidenciando una respuesta alineada con las directrices de la entidad y una integración permanente entre los equipos técnicos de Blend360 y DATIC. Este proceso de atención continúa asegura que cualquier sugerencia relacionada con ajustes, mejoras, validaciones, fortalecimiento de seguridad o necesidades operativas sea incorporada de inmediato en la ejecución contractual, permitiendo una operación articulada, coherente y plenamente alineada con los objetivos estratégicos y técnicos definidos por la Alcaldía de Santiago de Cali.

En el desarrollo del contrato se atienden de manera oportuna todas las sugerencias, recomendaciones y observaciones que el Distrito de Santiago de Cali, a través del Departamento Administrativo de Tecnologías de la Información y las Comunicaciones, considera pertinentes para la correcta ejecución del objeto contractual. Cada indicación emitida por el supervisor o por los equipos técnicos de la Entidad es analizada, incorporada y gestionada dentro del proceso operativo, asegurando que las actividades, entregables y ajustes necesarios se realicen de forma articulada y alineada con las necesidades institucionales. Este mecanismo de respuesta permanente garantiza que el proyecto se mantenga en coherencia con los lineamientos estratégicos de DATIC, facilite la mejora continua de las soluciones implementadas y permita que las decisiones tomadas en conjunto fortalezcan la calidad, funcionalidad y alcance de los servicios entregados.

Documento Anexo: ACA - Informe de Mensual de Casos

23 Asegurar el manejo del acceso a las soluciones tecnológicas, con el fin de evitar manejos múltiples de administradores y así evitar fraudes y robos de información, migración de datos e información, actualizaciones de aplicaciones personales, aplicaciones adicionales y gestión de sus datos personales

Para asegurar el manejo adecuado del acceso a las soluciones tecnológicas y evitar múltiples administradores, fraudes, robos de información, migraciones no autorizadas

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

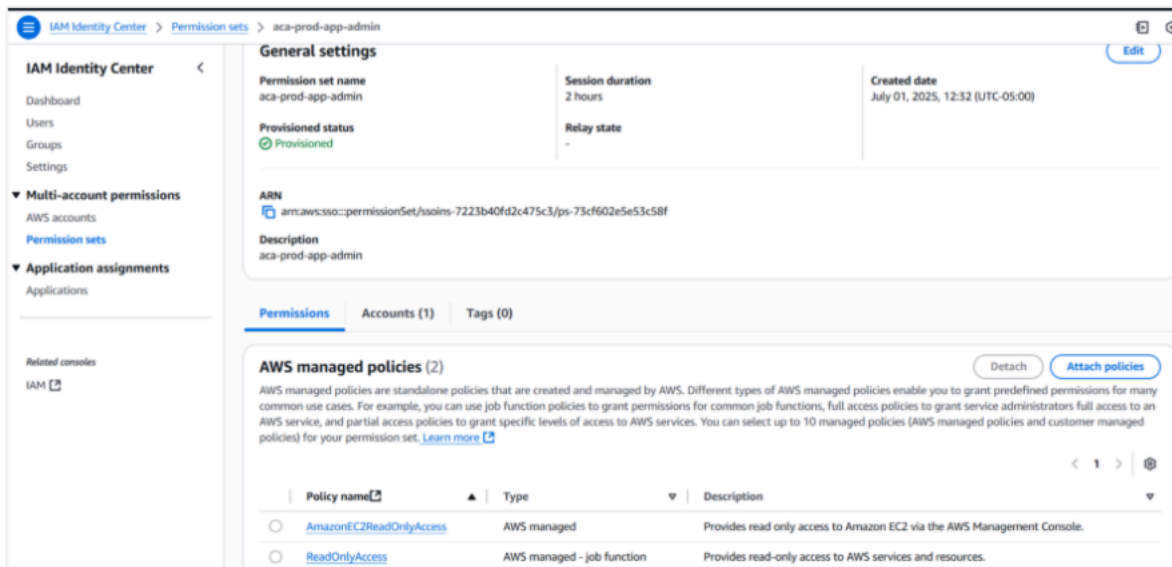
de datos, instalación de aplicaciones personales o manipulación indebida de información institucional, el proveedor implementó un modelo de control de accesos basado en políticas estrictas, roles claramente delimitados y el principio de mínimo privilegio. Conforme a las políticas de acceso definidas para la organización, la administración del entorno se realiza mediante grupos, perfiles y permisos configurados en AWS Identity Center, garantizando que cada usuario cuente únicamente con las capacidades estrictamente necesarias para sus funciones. El documento de políticas de acceso consolida esta estructura, detallando los grupos disponibles y sus responsabilidades: el rol ACA–AppAdmin, destinado a funcionarios de la Alcaldía y Nexura, permite únicamente permisos de lectura sobre aplicaciones y recursos EC2 en la cuenta de producción, evitando cualquier tipo de modificación directa; el grupo ACA–CloudAdmin, asignado a personal de DATIC, otorga capacidades de administración controlada sobre cuentas específicas, manteniendo restricciones explícitas sobre los ambientes sensibles, como la cuenta de producción del proceso de migración; y el grupo NUVU–CLOUDCloudSeniorEngineer, asignado exclusivamente a personal de infraestructura de Blend360, quien posee permisos avanzados necesarios para la gestión de cambios, monitoreo y soporte especializado sobre la plataforma.

Este esquema segmentado de accesos garantiza que no existan administradores múltiples sin control, previene configuraciones no autorizadas, evita la manipulación o extracción indebida de información, impide la instalación de aplicaciones personales o ajenas a la operación institucional y protege la integridad de los datos y servicios. Adicionalmente, toda la actividad de acceso se mantiene trazada y auditada a través de los servicios de seguridad de AWS, asegurando visibilidad total sobre las acciones ejecutadas por cada usuario. Con esta arquitectura de control se establece un modelo seguro, ordenado y alineado con las mejores prácticas de gobernanza digital, garantizando la protección del entorno tecnológico y la gestión responsable de los datos de la Alcaldía de Santiago de Cali.

Se garantiza un manejo controlado y seguro del acceso a las soluciones tecnológicas implementadas, con el propósito de evitar la existencia de múltiples administradores y reducir los riesgos asociados a fraudes, uso indebido de credenciales, robos de información, manipulaciones no autorizadas y alteraciones en los servicios. Para ello, se aplica un esquema centralizado de gestión de identidades y permisos que permite definir perfiles, roles y niveles de acceso estrictamente necesarios para cada usuario, eliminando privilegios excesivos y asegurando que las acciones de administración se limiten exclusivamente al personal autorizado. Este modelo de control también evita la

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

instalación o actualización de aplicaciones personales, la incorporación de software no permitido, manipulaciones de datos no autorizadas y cualquier intento de migración irregular de información. Todo el proceso se encuentra respaldado por políticas de auditoría, monitoreo continuo y registro de actividades, lo que garantiza trazabilidad completa, protección de los datos institucionales y cumplimiento de los estándares de seguridad exigidos por la Entidad.



Documento Anexo: Informe de Políticas de Acceso Para la Organización de ACA

24 Ejecutar un plan de reversibilidad al finalizar el contrato, que contemple la desactivación de servicios, transferencia de recursos, entrega de accesos y documentación, eliminación segura de configuraciones y recursos desplegados, asegurando que la entidad no incurra en costos residuales o innecesarios posteriores a la finalización contractual.

En relación con la Obligación, se deja indicado en el informe de facturación que su cumplimiento se ejecutará al cierre del consumo de la bolsa de recursos de nube

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

actualmente disponible, es decir, una vez finalicen dichos recursos y se adelante el proceso de cierre operativo, momento en el cual se realizará la desactivación ordenada de los servicios, la transferencia de recursos y accesos, y la entrega de documentación, dejando constancia formal mediante el Acta de entrega de infraestructura.

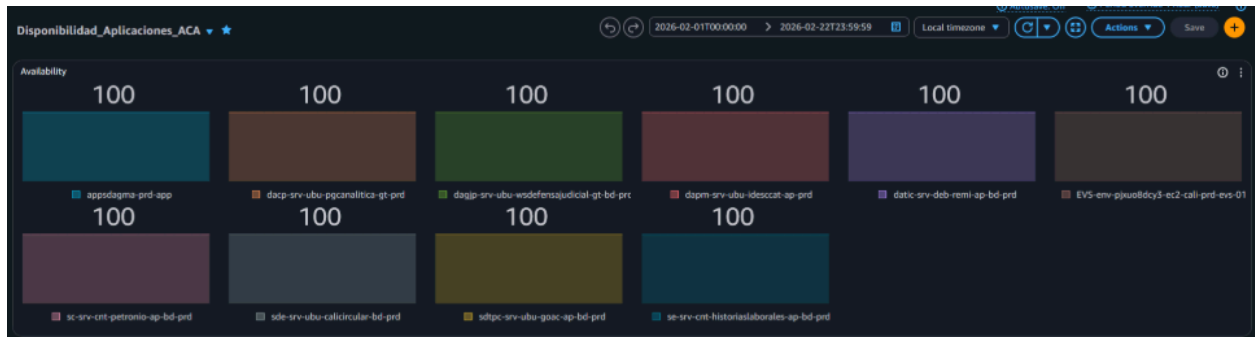
- Para garantizar un cierre controlado y que la Entidad no asuma costos residuales o innecesarios posteriores, efectuaremos las siguientes acciones:
- Inventario final de los recursos desplegados y dependencias (servicios, ambientes, redes, almacenamiento, reglas/políticas y componentes asociados).
- Transferencia de control y accesos a la Entidad: entrega/rotación de credenciales, cuentas, roles y permisos; actualización de responsables y trazabilidad.
- Entrega integral de documentación: arquitectura y configuración “as-is”, procedimientos operativos, respaldos/plantillas aplicables, y guías de continuidad/cierre.
- Plan de desactivación con ventana acordada, validación de impactos y verificación posterior de apagado/corte según corresponda.
- Eliminación segura de configuraciones y recursos: revocación de accesos temporales, rotación de llaves/secretos, cierre de endpoints y borrado seguro cuando aplique.
- Control y verificación de costos post-cierre: revisión de consumos, identificación de recursos huérfanos, alarmas y confirmación del estado de facturación esperado.
- Suscripción del Acta de entrega de infraestructura, con evidencia de accesos entregados, recursos desactivados/eliminados y medidas adoptadas para evitar consumos posteriores.

De esta manera, el informe final dejará claramente trazado que el plan de reversibilidad será cumplido en su integridad al finalizar el consumo de los recursos, asegurando una transición ordenada, documentada y sin impactos financieros posteriores para la Entidad.

25 Garantizar la implementación y el fortalecimiento de la plataforma tecnológica que soporta los sistemas de información transversales con su respectiva disponibilidad, seguridad y eficiencia, así mismo asegurar la compatibilidad con la infraestructura tecnológica existente y proveer capacidad de escalabilidad y redundancia, según la descripción detallada del bien adquirido.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

El proveedor garantizó la implementación, operación y fortalecimiento continuo de la plataforma tecnológica que soporta los sistemas de información transversales de la Alcaldía de Santiago de Cali, asegurando su disponibilidad, seguridad, eficiencia y compatibilidad con la infraestructura tecnológica existente. La solución desplegada se encuentra construida sobre servicios de AWS que, según el análisis presentado en el Informe de Monitoreo y Disponibilidad, han mantenido un comportamiento estable y sin interrupciones durante el periodo evaluado, reflejando niveles de disponibilidad adecuados para los sistemas institucionales. El monitoreo realizado durante los meses activos, demuestran que componentes críticos como EC2, EFS, ELB, VPC, Elastic Disaster Recovery y Site-to-Site VPN operaron sin incidentes, garantizando continuidad en la ejecución de aplicaciones, conectividad segura y acceso persistente a los datos. Asimismo, las métricas de CPU, lectura y escritura en disco, tráfico de red y verificaciones de estado evidencian un consumo controlado y sin afectaciones relevantes, lo que confirma la eficiencia del entorno y la correcta asignación de recursos.



La arquitectura implementada incorpora esquemas de escalabilidad que permiten ajustar la capacidad de cómputo, almacenamiento y red en función del crecimiento de los servicios, así como mecanismos de redundancia y recuperación que aseguran la disponibilidad continua del entorno, incluso ante eventos de falla. Esto incluye balanceadores de carga, zonas de disponibilidad independientes, políticas de recuperación automática ante StatusCheckFailed y la operación estable de la VPN híbrida que conecta la infraestructura on-premise con la nube. La compatibilidad con la infraestructura tecnológica existente se garantiza mediante la integración de redes privadas, túneles seguros, balanceo de tráfico y servicios gestionados que se adaptan

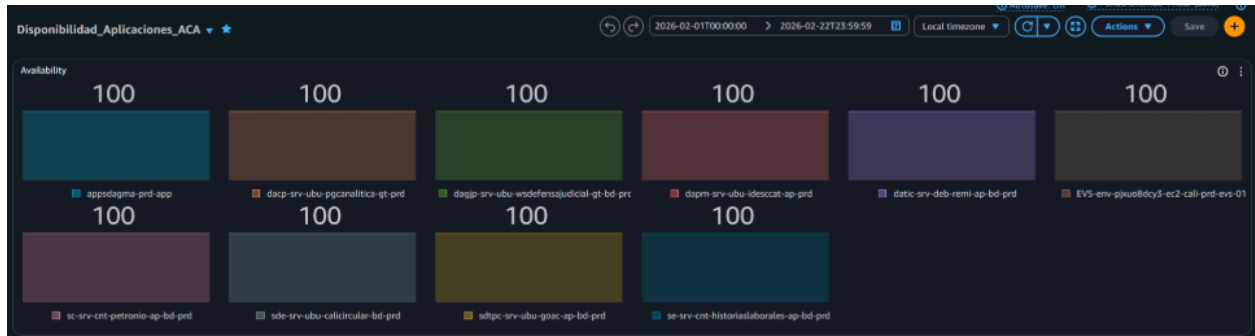
 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

al modelo operativo actual del Distrito.

Con este conjunto de prácticas, monitoreo constante y mecanismos de alta disponibilidad, se fortalece la plataforma tecnológica que soporta los sistemas de información transversales, permitiendo que la infraestructura permanezca operativa, segura, eficiente y preparada para soportar crecimiento, cargas variables y requerimientos institucionales, en concordancia con la descripción técnica del bien adquirido y los lineamientos contractuales establecidos.

Documento anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

26 Suministrar herramientas de monitoreo en tiempo real con métricas detalladas (uso de CPU, memoria, red, almacenamiento, etc.), garantizando la disponibilidad de históricos de monitoreo desde el inicio de operación y proveer reportes de optimización y desempeño de los servicios.



El proveedor dispuso herramientas de monitoreo en tiempo real mediante el uso de Amazon CloudWatch, servicio nativo de AWS que permite recopilar, visualizar y analizar métricas detalladas de la infraestructura, incluyendo uso de CPU, memoria, red, almacenamiento y estado de los recursos.

CloudWatch proporciona paneles personalizados (dashboards) y alarmas configurables, permitiendo supervisar el desempeño de los servicios y responder oportunamente ante cualquier desviación o incidente. Además, se garantiza la disponibilidad de históricos de monitoreo desde el inicio de la operación, facilitando el análisis de tendencias y la generación de reportes de desempeño.

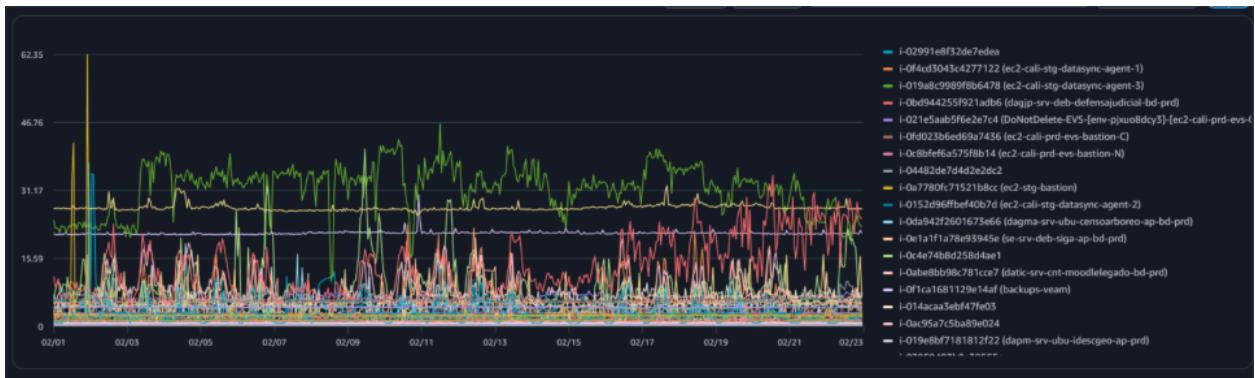
Como complemento, utilizó AWS Compute Optimizer, herramienta que analiza métricas

Este documento es propiedad de la Administración Central del Distrito de Santiago de Cali. Prohibida su alteración o modificación por cualquier medio, sin previa autorización del Alcalde.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

de uso reales y recomienda configuraciones óptimas de cómputo, almacenamiento y red, contribuyendo a la optimización continua del rendimiento y los costos de la infraestructura.

La disponibilidad y gestión de las soluciones tecnológicas desarrolladas se garantizan mediante el uso de herramientas nativas de AWS, principalmente a través de Amazon CloudWatch, que permite el monitoreo continuo de la infraestructura subyacente y de los servicios de virtualización. Esta herramienta proporciona visibilidad en tiempo real del rendimiento, uso de recursos y estado operativo de los componentes.



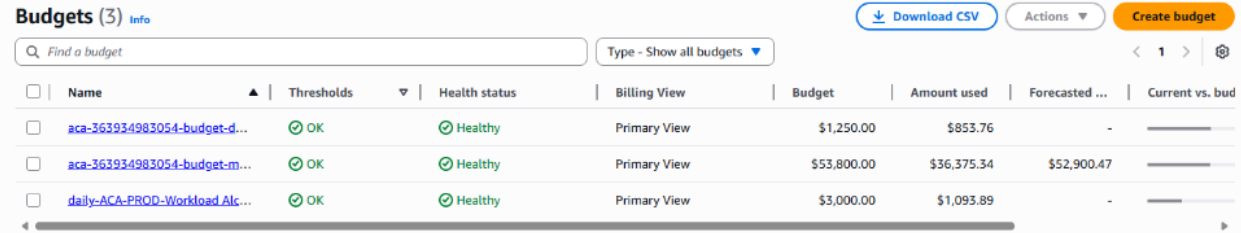
Métricas medidas para todos los recursos que se crean en aws a través del cliente de cloudwatch:

1. CPU Utilization: Porcentaje de capacidad de procesamiento de la instancia que se está utilizando. Un valor consistentemente alto indica que el servidor está bajo una carga de trabajo pesada.
2. StatusCheckFailed: Indicador general de que la instancia ha fallado una verificación automática de estado, requiriendo atención.
3. StatusCheckFailed_Instance: Falla a nivel de software o sistema operativo (ej., la aplicación no responde).
4. StatusCheckFailed_System: Falla detectada por AWS en el hardware físico subyacente, lo que normalmente requiere una recuperación automática o manual de la instancia.
5. DiskReadBytes: Cantidad de datos (en bytes) que la instancia lee desde sus discos. Alto volumen indica una intensa actividad de lectura de información.
6. DiskWriteBytes: Cantidad de datos (en bytes) que la instancia escribe en sus

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

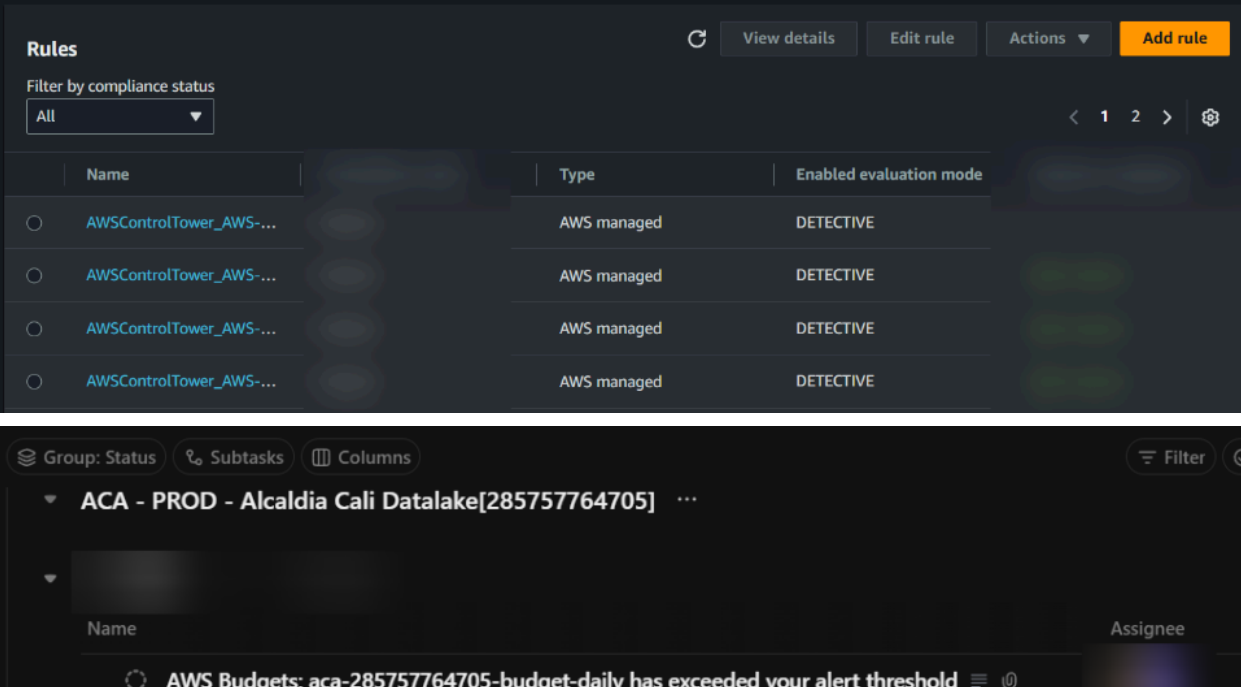
- discos. Alto volumen indica una intensa actividad de guardado o modificación de archivos.
7. DiskReadOps: Número de operaciones de lectura individuales que la instancia solicita a sus discos. Muchas operaciones pueden ser demandantes incluso si el volumen de datos es bajo.
 8. DiskWriteOps: Número de operaciones de escritura individuales que la instancia realiza en sus discos. Un recuento elevado es común en sistemas con bases de datos activas.
 9. NetworkIn: Volumen total de datos (en bytes) que la instancia recibe desde la red.
 10. NetworkOut: Volumen total de datos (en bytes) que la instancia envía a la red. Estas dos métricas reflejan el tráfico total de su aplicación.
 11. NetworkPacketsIn: Número de paquetes de datos individuales que la instancia recibe. Un número muy alto puede consumir recursos de CPU.
 12. NetworkPacketsOut: Número de paquetes de datos individuales que la instancia envía. Es útil para diagnosticar problemas de rendimiento de red o aplicaciones con mucho "chateo" (pequeñas comunicaciones frecuentes).

Adicionalmente se crean alertas con diferentes herramientas internas y externas de aws



<input type="checkbox"/>	Name	Thresholds	Health status	Billing View	Budget	Amount used	Forecasted ...	Current vs. bud
<input type="checkbox"/>	aca-363934983054-budget-d...	OK	Healthy	Primary View	\$1,250.00	\$853.76	-	<div style="width: 68%;"></div>
<input type="checkbox"/>	aca-363934983054-budget-m...	OK	Healthy	Primary View	\$53,800.00	\$36,375.34	\$52,900.47	<div style="width: 67%;"></div>
<input type="checkbox"/>	daily-ACA-PROD-Workload Alc...	OK	Healthy	Primary View	\$3,000.00	\$1,095.89	-	<div style="width: 36%;"></div>

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



The screenshot shows the AWS IAM console 'Rules' page. It features a table with columns for Name, Type, and Enabled evaluation mode. Below the table, a notification is visible for 'ACA - PROD - Alcaldia Cali Datalake[285757764705]' regarding an AWS Budgets alert.

Name	Type	Enabled evaluation mode
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE

Notification: AWS Budgets: aca-285757764705-budget-daily has exceeded your alert threshold

Documento Anexo: [Informe de monitoreo y disponibilidad Alcaldía de Cali](#)

27 Implementar mecanismos de cifrado y control de accesos, asegurando la integridad, disponibilidad y confidencialidad de la información financiera, lo anterior en cumplimiento de las normativas de seguridad establecidas.

Se cuenta con una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

La gestión de identidades y accesos se realiza mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permite administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

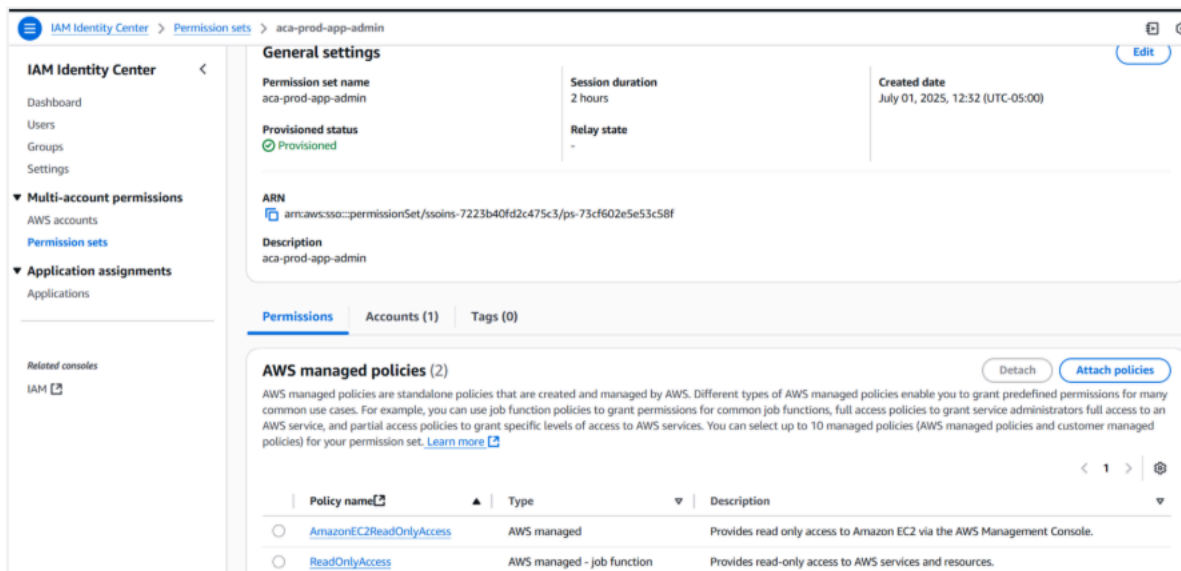
Como parte de la implementación de seguridad en AWS, el proveedor configuró un

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

- ACA -AppAdmin

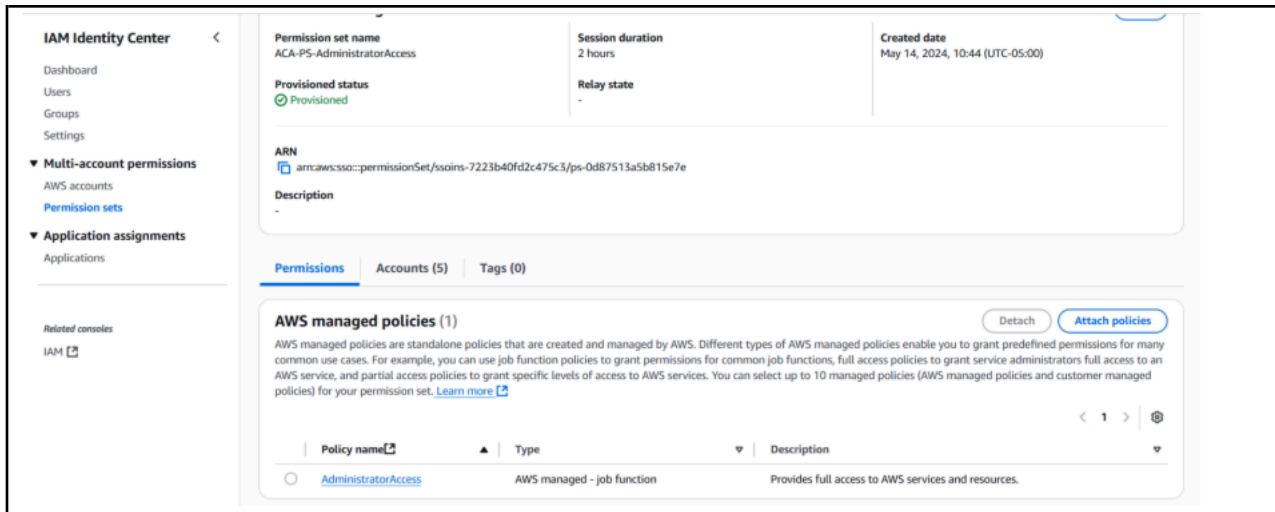
Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD -Workload Alcaldía Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.



- ACA – CloudAdmin

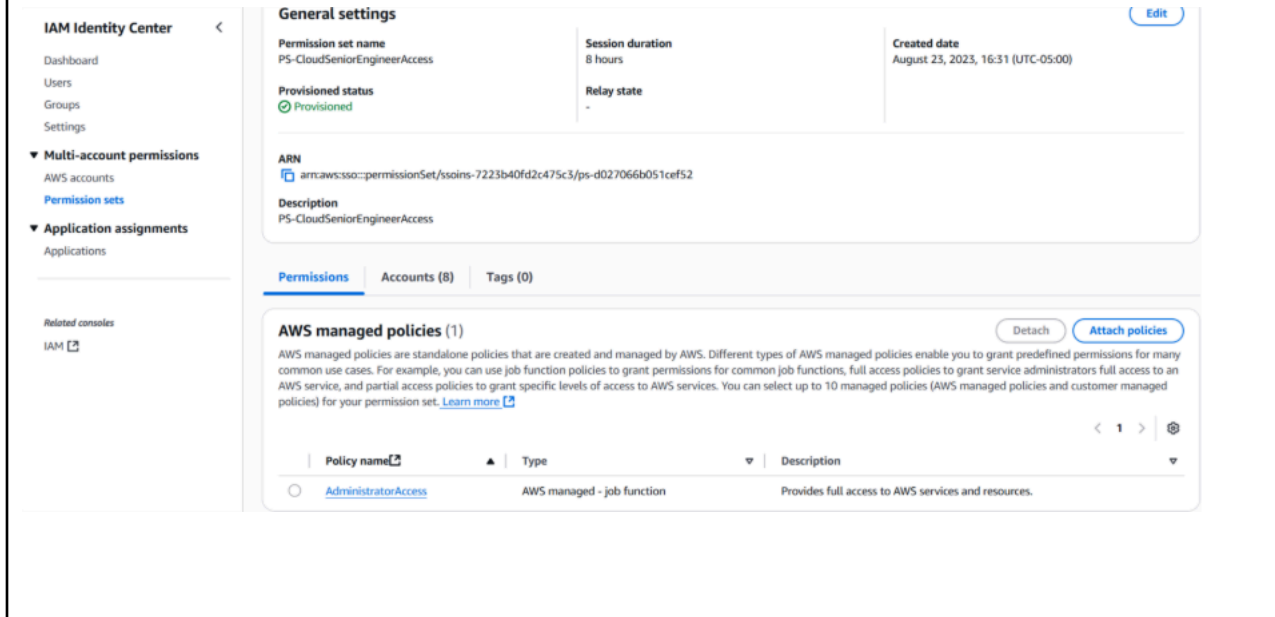
El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002



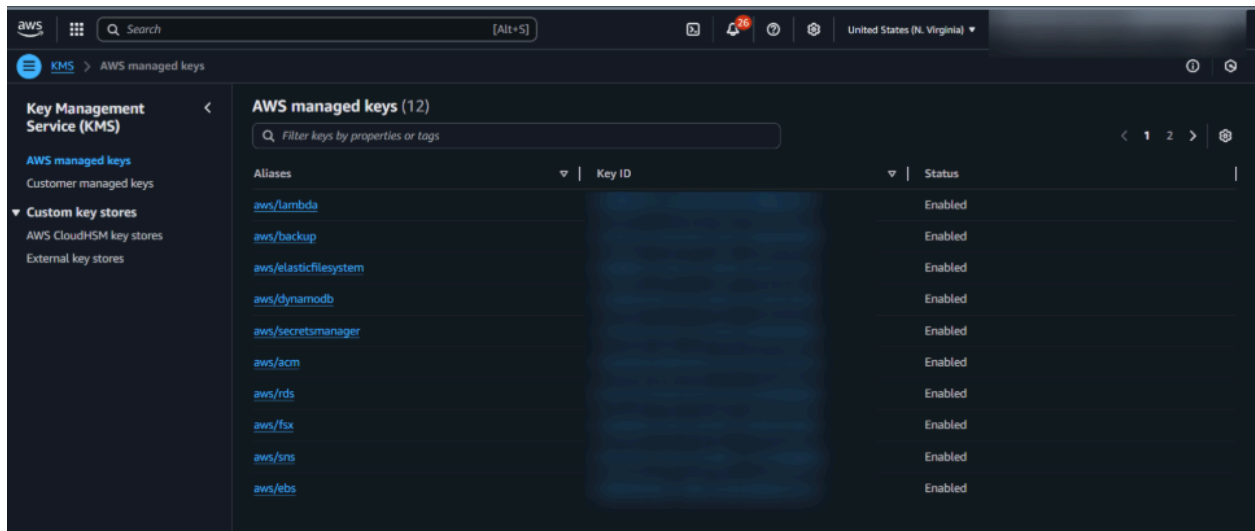
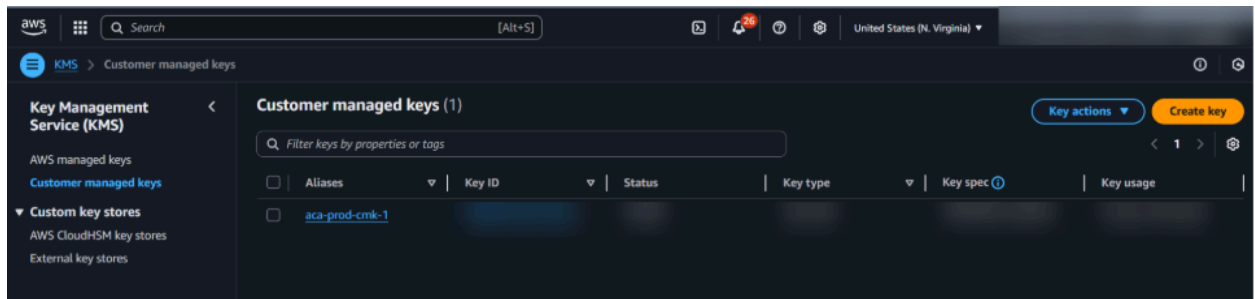
● NUVU – CLOUDCloudSeniorEngineer

Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Adicionalmente se manejan llaves KMS para encriptar todos los recursos de aws que se creen en las cuentas



Documento Anexo: Documentación Infraestructura AWS

28 Brindar un escenario que permita el desarrollo y automatización de copias de respaldo, bajo la política día, mes y año y con ello poder realizar la restauración en caso de falla o interrupción.

Como parte de la implementación del entorno AWS, el proveedor estableció un plan de respaldo para garantizar la protección y recuperación de los recursos migrados. El plan

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

plan-cali-prd-backup se configura mediante políticas con distintos periodos de retención y transición a almacenamiento frío-

plan-cali-prd-backup

[Delete](#) [View JSON](#)

Summary



Backup plan name plan-cali-prd-backup	Version ID Zjk2MWY2MGUtMmYxNi000 DhhLWJIM2EtZTFhNTJIYTAzY Tgy	Last modified July 30, 2025, 10:00:50 (UTC-05:00)	Last runtime September 12, 2025, 01:15:07 (UTC-05:00)
Backup plan ID e17d35df-91fd-4391-9311-33ac5c855379			

Los backups son gestionados a través del vault vault-cali-prd-backup.

vault-cali-prd-backup Info

[Manage vault lock](#) [Delete vault](#) [Edit access policy](#)

Summary

Vault name vault-cali-prd-backup	KMS encryption key ID 	Vault lock 🔒 Locked – Governance mode Vault lock is editable. Learn more
Vault type Backup vault	Creation date June 26, 2025, 14:48:16 (UTC-05:00)	Retention period for vault lock Minimum retention period: 6 days Maximum retention period: –
Vault ARN  arn:aws:backup:us-east-1:363934983054:backup-vault:vault-cali-prd-backup		

Políticas de retención implementadas:

- DailyBackup-7DayRetention: Frecuencia diaria con retención de 15 días.
- WeeklyBackup-1MonthRetention: Frecuencia semanal con retención de 1 mes.
- MonthlyBackup-1YearRetention: Frecuencia mensual con retención de 1 año, con transición a almacenamiento frío a los 3 meses (90 días).
- YearlyBackup-20YearRetention: Frecuencia anual con retención de 20 años, con transición a almacenamiento frío a los 3 meses (90 días).

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Backup rules (4) Edit Delete Add backup rule

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Name	Backup vault	Destination Backup vault
DailyBackup-15DayRetention	vault-cali-prd-backup	-
MonthlyBackup-1YearRetention	vault-cali-prd-backup	-
WeeklyBackup-1MonthRetention	vault-cali-prd-backup	-
YearlyBackup-20YearRetention	vault-cali-prd-backup	-

La asignación de recursos se realizó mediante la etiqueta "Backup - Enabled", utilizando el rol IAM role-cali-prd-backup para la ejecución automatizada de las copias de seguridad. Esta estrategia permitió cumplir con los requerimientos de recuperación ante incidentes, optimización de costos y políticas de compliance de la organización.

plan-cali-prd-backup-resources-selection Delete

Summary

Resource assignment name
plan-cali-prd-backup-resources-selection

IAM role
arn:aws:iam::363934983054:role/role-cali-prd-backup

Tags
Backup - Enabled

Los recursos cubiertos por las cuatro políticas de backups son los siguientes:

Resource ID	Resource type
file-system/fs-0967f438281ee1e78	EFS



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

instance/i-0ff91dad5f9352e5	EC2
instance/i-0ff8ef35f1871e677	EC2
instance/i-0f7f720eed4cdb558	EC2
instance/i-0f1ca1681129e14af	EC2
instance/i-0f16abff95586310d	EC2
instance/i-0e8c34a41b6c86ade	EC2
instance/i-0e7b96bc549ff0898	EC2
instance/i-0e5bab7e27d08ff0b	EC2
instance/i-0e1a1f1a78e93945e	EC2
instance/i-0da942f2601673e66	EC2
instance/i-0ccfa3f8c3b574c0d	EC2
instance/i-0c4e74b8d258d4ae1	EC2

Este documento es propiedad de la Administración Central del Distrito de Santiago de Cali. Prohibida su alteración o modificación por cualquier medio, sin previa autorización del Alcalde.



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

instance/i-0c427895e543ad95a	EC2
instance/i-0c235aa02cae57bb0	EC2
instance/i-0bf67840dd8dd4eec	EC2
instance/i-0bd944255f921adb6	EC2
instance/i-0bc591901eb7d3aa9	EC2
instance/i-0b7fc7de52d011a07	EC2
instance/i-0b444291b70de254c	EC2
instance/i-0ad841c9f7539cf4f	EC2
instance/i-0ac95a7c5ba89e024	EC2
instance/i-0abe8bb98c781cce7	EC2
instance/i-0a68d16a6d7cf54e1	EC2
instance/i-09f57f65953dcbbe9	EC2



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

instance/i-09daed7db5a91bb0e	EC2
instance/i-09c6b3858b15f90d4	EC2
instance/i-096f1f443330d321b	EC2
instance/i-092c20bbf14353f45	EC2
instance/i-0914776bdd46e8113	EC2
instance/i-08f030c4b0bad9c63	EC2
instance/i-080bc0076e766115d	EC2
instance/i-07fcf5c3bf586f4fb	EC2
instance/i-07d892e7c73ed3e42	EC2
instance/i-071b7ac828a68c668	EC2
instance/i-0713215fb793cf15e	EC2



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

instance/i-06a5a265833c118fe	EC2
instance/i-053306f51fb24c2ab	EC2
instance/i-04bfaa21b951e7d55	EC2
instance/i-047fc8d7b771cb5a0	EC2
instance/i-045b6c8d631a1933e	EC2
instance/i-03dd3e5f2b0ecf3bf	EC2
instance/i-03b3aeba5a89cc6df	EC2
instance/i-03b020eed552c3747	EC2
instance/i-03acb8e98633046e9	EC2
instance/i-03959403b0e38555e	EC2
instance/i-0393259ac7c75ded6	EC2
instance/i-02caec961eef45329	EC2



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO


MAJA01.04.03.P002.F003

VERSIÓN

002

instance/i-0256a7b9f2de6c2fc	EC2
instance/i-0245e6e2a42d81bef	EC2
instance/i-023cf71bccb8448d2	EC2
instance/i-01e2fd3f70af99abd	EC2
instance/i-019e8bf7181812f22	EC2
instance/i-014acaa3ebf47fe03	EC2
instance/i-012296a22fb19cb60	EC2
instance/i-005516784418bcbeb	EC2
instance/i-092c20bbf14353f45	EC2
instance/i-0045bcb36c2e9dba3	EC2
instance/i-001741585e5ab2a52	EC2
instance/i-0a7780fc71521b8cc	EC2

Este documento es propiedad de la Administración Central del Distrito de Santiago de Cali. Prohibida su alteración o modificación por cualquier medio, sin previa autorización del Alcalde.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

instance/i-04482de7d4d2e2dc2	EC2
instance/i-03bf30e6bcbaa7bd7	EC2
volume/vol-01a2926f544d54f9e	EBS
file-system/fs-067f7766e3ab13903	EFS

Para los buckets de S3 implementó un versionamiento como capa de protección de datos.

Resource name	Resource ID
s3-cali-prd-workspace	s3-cali-prd-workspace
s3-cali-prd-VMware-audit-logs	s3-cali-prd-VMware-audit-logs
s3-cali-prd-shared-vpc-audit-logs	s3-cali-prd-shared-vpc-audit-logs
s3-cali-prd-secretaria-turismo-audit-logs	s3-cali-prd-secretaria-turismo-audit-logs
s3-cali-prd-repository-01	s3-cali-prd-repository-01



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

s3-cali-prd-podmanbucket	s3-cali-prd-podmanbucket
s3-cali-prd-orfeo-storage	s3-cali-prd-orfeo-storage
s3-cali-prd-orfeo-bodega	s3-cali-prd-orfeo-bodega
s3-cali-prd-oraclerman	s3-cali-prd-oraclerman
s3-cali-prd-migrate-v5-audit-logs	s3-cali-prd-migrate-v5-audit-logs
s3-cali-prd-migrar-gce-VMware	s3-cali-prd-migrar-gce-VMware
s3-cali-prd-katana	s3-cali-prd-katana
s3-cali-prd-integratic	s3-cali-prd-integratic
s3-cali-prd-infra-mc	s3-cali-prd-infra-mc
s3-cali-prd-orfeo-bodega	s3-cali-prd-orfeo-bodega
s3-cali-prd-oraclerman	s3-cali-prd-oraclerman
s3-cali-prd-migrate-v5-audit-logs	s3-cali-prd-migrate-v5-audit-logs

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

s3-cali-prd-daruma-aplicacion	s3-cali-prd-daruma-aplicacion
s3-cali-prd-daruma-aplicacion	s3-cali-prd-daruma-aplicacion
s3-cali-prd-daisy-bkt	s3-cali-prd-daisy-bkt
s3-cali-prd-daas-audit-logs	s3-cali-prd-daas-audit-logs
s3-cali-prd-bckrman-pegasus	s3-cali-prd-bckrman-pegasus
s3-cali-prd-backups-piso15-alcaldiacali	s3-cali-prd-backups-piso15-alcaldiacali
s3-cali-prd-backup-dr-audit-logs	s3-cali-prd-backup-dr-audit-logs

Documento Anexo: Documentación Infraestructura AWS

29 Brindar soporte técnico Premium 24/7 mensual, a través de diversos canales (teléfono, correo electrónico, sistema de tiquetes), garantizando los tiempos de respuesta adecuados según la criticidad del servicio.

En el marco del servicio contratado proveedor brindó soporte técnico Premium 24/7, disponible a través de múltiples canales incluyendo teléfono, correo electrónico y sistema de tiquetes garantizando tiempos de respuesta acordes con la criticidad del servicio, conforme a los Acuerdos de Nivel de Servicio (ANS) establecidos con la Entidad. Este componente incluye la disponibilidad permanente de personal técnico especializado para atender incidentes, requerimientos y ajustes sobre la infraestructura

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

virtual contratada, así como acompañamiento directo durante ventanas de mantenimiento, actividades planificadas y cambios operativos que requieran soporte conjunto con los equipos de la Alcaldía de Santiago de Cali. El soporte incorpora diagnóstico, estabilización y acciones de continuidad para servicios críticos, asegurando el restablecimiento oportuno y la prevención de riesgos operativos.

La atención la realizó de manera articulada con los equipos de DATIC, promoviendo la transferencia de conocimiento y la apropiación tecnológica mientras se mantiene un registro detallado de cada intervención mediante bitácoras y trazabilidad dentro de la herramienta oficial de gestión de tickets HelpDesk. A través de esta plataforma, los usuarios autorizados pueden registrar y gestionar incidentes, solicitudes de información, solicitudes de cambio (RFC), requerimientos operativos y peticiones de administración de infraestructura, incluyendo creación o eliminación de recursos AWS tales como EC2, RDS, S3, EBS, Security Groups, Roles IAM, WAF y balanceadores; ajustes de configuración en VPC, redes o servidores; despliegue o modificación de máquinas virtuales en VMware; validación de conectividad híbrida y revisión de logs, costos, copias de seguridad o restauración de snapshots.

Para este proceso, el proveedor habilitó los usuarios designados por la entidad, quienes acceden al portal oficial de soporte mediante la URL: <https://helpdesk.ia.blend360.com/#login>, lo que garantizó que la gestión de solicitudes se realizará bajo un flujo formal de atención, con roles definidos, permisos adecuados y trazabilidad completa desde la creación hasta el cierre de cada ticket. Durante la ejecución del contrato se realizaron las habilitaciones necesarias de usuarios, se validó la correcta asignación de perfiles y se entregó el Manual de Usuario asociado a la herramienta, el cual explica los pasos de acceso, registro, consulta, actualización, escalamiento y seguimiento de solicitudes.

El comportamiento operativo registrado evidencia un volumen significativo de casos atendidos, principalmente asociados a administración de infraestructura, despliegues de ambientes, reglas de firewall, configuración de elementos de seguridad, soporte en redes, consultas técnicas y ajustes de permisos IAM. La mayoría de los casos presentan estados Cerrado, Entregado o Resuelto, demostrando cumplimiento de los tiempos de atención y efectividad en la gestión del soporte. Las solicitudes clasificadas con criticidad alta fueron atendidas de manera prioritaria, especialmente aquellas relacionadas con continuidad operativa o despliegues productivos, mientras que los casos en estado Aceptado, En entendimiento o Esperando respuesta continúan su

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

gestión conjunta según el flujo de trabajo acordado con DATIC.

Con estas acciones, garantizó un soporte técnico integral, continuo y especializado que asegura la disponibilidad de la infraestructura, la respuesta oportuna ante eventos críticos, la correcta ejecución de los requerimientos operativos y la trazabilidad total de todas las actividades técnicas, fortaleciendo la estabilidad y confiabilidad de la solución tecnológica implementada.

Durante el periodo analizado se registró un número significativo de solicitudes en la herramienta de soporte Help Desk por parte de la Alcaldía de Santiago de Cali, principalmente asociadas a gestión de infraestructura, despliegues de ambientes, reglas de firewall, administración de recursos en AWS y consultas operativas.

En términos generales, los casos presentan el siguiente comportamiento:

- Durante el periodo evaluado realizó la atención, gestión y seguimiento de un alto volumen de solicitudes técnicas asociadas a la operación, seguridad y modernización de la infraestructura tecnológica en AWS de la Alcaldía de Santiago de Cali.
- La mayoría de las solicitudes se encuentran cerradas o resueltas, evidenciando una gestión oportuna y efectiva, mientras que un número controlado permanece en estado de espera o diagnóstico, principalmente asociado a iniciativas de modernización en curso.
- Atendió las solicitudes relacionadas con seguridad de la infraestructura, incluyendo actualización y definición de reglas de firewall, configuración de controles de acceso, revisión de tráfico, mitigación de alertas de seguridad (SOC) y sesiones técnicas de AWS WAF.
- Ejecutó actividades de conectividad y redes, tales como configuración y seguimiento de VPN site-to-site, interconexión por Direct Connect, monitoreo de disponibilidad de interconnect y enrutamiento entre entornos AWS y OCI.
- Brindó soporte a la operación de servidores y servicios críticos, incluyendo revisiones de máquinas virtuales, configuración de agentes, snapshots, montaje de imágenes ISO, eliminación y creación de recursos, así como verificación de disponibilidad y alcanzabilidad.
- Avanzó en iniciativas de modernización de infraestructura en AWS, particularmente en la Modernización de Orfeo, el cambio de infraestructura del Portal de la Alcaldía de Cali y el Proyecto de Ecosistemas Digitales, actualmente en fase de ejecución y seguimiento.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

- Apoyó procesos de gestión de accesos e identidades, mediante la creación de usuarios IAM, asignación de políticas, accesos a plataformas institucionales y soporte a usuarios de la entidad.
- Elaboró y entregó informes técnicos y de gestión, incluyendo reportes de backups, seguimiento de interconectividad, información de ciberseguridad para la construcción del DRP y avances del informe de gestión contractual.

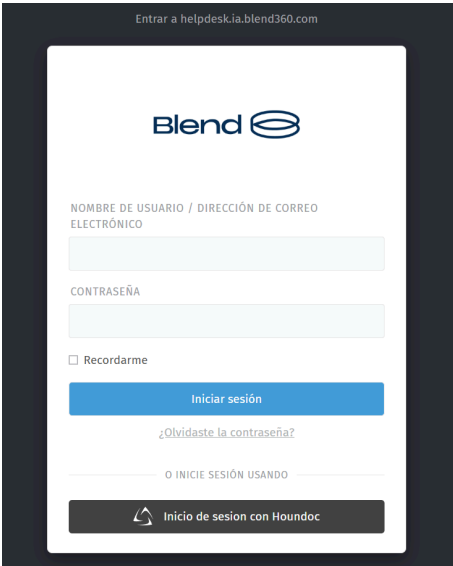
Documento Anexo: Informe mensual de casos

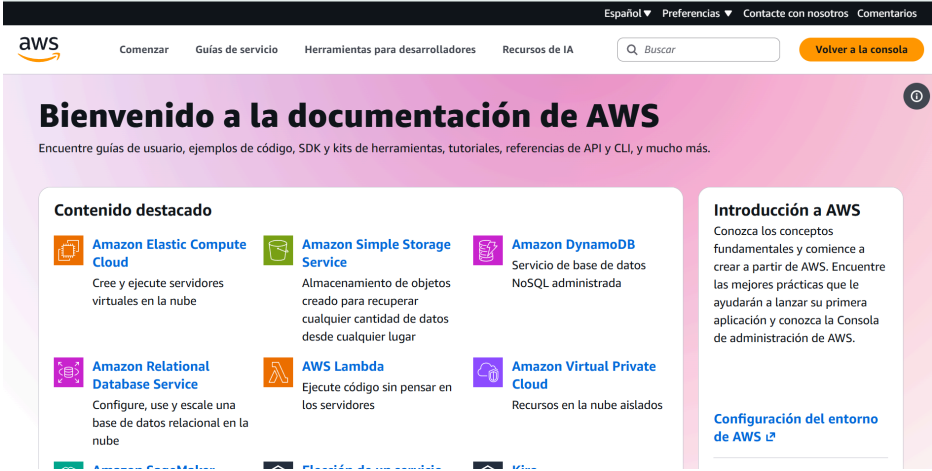
30 Mantener una base de conocimiento con documentación técnica y foros de consulta.

Como parte del cumplimiento de la presente obligación, el proveedor dispuso de un canal de soporte para la atención de solicitudes y consultas del equipo de la Alcaldía de Santiago de Cali (<https://helpdesk.ia.blend360.com/#login>), las cuales han sido atendidas de manera oportuna a través de los mecanismos definidos, incluyendo llamadas telefónicas y comunicación vía WhatsApp, de acuerdo con las necesidades operativas identificadas.

Adicionalmente, para el desarrollo de las actividades técnicas, la atención de requerimientos y como referencia para la operación, configuración y aplicación de buenas prácticas, se ha utilizado la documentación oficial de AWS disponible en https://docs.aws.amazon.com/es_es/, la cual se mantiene permanentemente actualizada. Esto permite asegurar que los lineamientos técnicos aplicados se encuentren alineados con las recomendaciones vigentes y los estándares definidos por AWS.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002





https://docs.aws.amazon.com/es_es/

4.31 Brindar documentación técnica de los procesos ejecutados para los sistemas generados y realizar transferencia de conocimiento entregando documentación detallada de la misma, tales como videos, manuales, guías y demás documentos requeridos por la entidad.

Este documento es propiedad de la Administración Central del Distrito de Santiago de Cali. Prohibida su alteración o modificación por cualquier medio, sin previa autorización del Alcalde.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

El proveedor avanzó en iniciativas de modernización de infraestructura en AWS, alineadas con los lineamientos técnicos y de seguridad definidos por la Alcaldía de Santiago de Cali. En este marco, se ejecutan actividades relacionadas con la modernización del sistema Orfeo, orientadas a mejorar su desempeño, disponibilidad y sostenibilidad tecnológica; la modernización del Portal Municipal de la Alcaldía, fortaleciendo su operación sobre infraestructura en la nube; y el despliegue de ecosistemas digitales, soportando la implementación de nuevas capacidades tecnológicas y servicios digitales para la entidad. Una vez finalizadas estas actividades, se realizará la entrega de manuales técnicos, guías, videos y demás documentos requeridos, así como la transferencia de conocimiento correspondiente a los equipos designados por la entidad.

4.32 Realizar la transferencia de conocimiento en la gestión y operación de la plataforma adquirida al equipo técnico de la Alcaldía de Santiago de Cali.

El proveedor en cumplimiento de la obligación de realizar la transferencia de conocimiento, llevó a cabo la transferencia de conocimiento dirigida a los colaboradores de la Alcaldía de Santiago de Cali, resaltando la importancia de la seguridad como un eje transversal en la operación y administración de las soluciones tecnológicas. En este contexto, realizó una jornada de capacitación enfocada en seguridad en la nube AWS, en la cual se abordaron los principios fundamentales de seguridad, la responsabilidad compartida y la necesidad de adoptar controles preventivos, detectivos y correctivos para la protección de la información y los servicios. Durante la sesión presentó el uso de AWS WAF para la protección de aplicaciones web frente a amenazas comunes, AWS Shield para la mitigación de ataques DDoS, AWS Config para el control y cumplimiento de configuraciones, Amazon CloudWatch para el monitoreo, análisis de métricas, logs y generación de alertas, así como otros servicios de seguridad como AWS IAM para la gestión de identidades y accesos, AWS CloudTrail para la trazabilidad y auditoría de acciones, Amazon GuardDuty para la detección de amenazas, y AWS Security Hub para la centralización del estado de seguridad y cumplimiento. Esta capacitación permitió sensibilizar al equipo sobre la relevancia de la seguridad en la nube y fortalecer sus capacidades para operar, administrar y proteger de manera adecuada las soluciones tecnológicas implementadas.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Revisión AWS Seguridad Blend

🕒 Vie 20/02/2026, de 9:00 AM a 11:00 AM

📍 <https://meet.google.com/koo-gemm-vjz>

👤 Paulo Cesar Guerrero Agudelo le ha invitado.
10 sin respuesta

☰ Revisión AWS Seguridad Blend Unirme con Google Meet: Paulo Cesar Guerrero Agudelo te ha invitado a asistir al evento llamado Revisión AWS Seguridad Blend el viernes 20 de feb...

Documento anexo: Sesión Revisión AWS Seguridad Blend

33 Garantizar que la solución cuente con mecanismos para bloquear ataques comunes (como inyección SQL, XSS y otros del OWASP Top 10) y protección frente a tráfico automatizado malicioso (bots), asegurando la integridad de las aplicaciones web institucionales.

El proveedor garantizó que las aplicaciones web institucionales, desplegadas sobre infraestructura en la nube de Amazon Web Services (AWS), cuenten con mecanismos de seguridad orientados a la prevención, detección y mitigación de ataques comunes, incluyendo aquellos definidos en el OWASP Top 10, así como con controles para la protección frente a tráfico automatizado malicioso (bots). Estos mecanismos permiten asegurar la integridad, disponibilidad y operación segura de las soluciones tecnológicas de la Alcaldía de Santiago de Cali.

Para el desarrollo de esta actividad, se ejecutan las siguientes acciones:

1. Protección a nivel de aplicación en AWS

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

<p>a. Implementación de AWS Web Application Firewall (WAF) integrado con los servicios expuestos en AWS (Load Balancers, CloudFront y/o API Gateway), permitiendo la inspección y filtrado del tráfico HTTP/HTTPS.</p> <p>b. Configuración de reglas administradas y personalizadas para mitigar ataques como inyección SQL, Cross-Site Scripting (XSS), exploración de vulnerabilidades, fuerza bruta y otros vectores del OWASP Top 10.</p> <p>2. Protección frente a tráfico automatizado malicioso (bots)</p> <p>a. Uso de reglas <i>rate-based</i> del WAF para detectar picos anómalos de solicitudes y comportamientos automatizados.</p> <p>b. Bloqueo de direcciones IP que superan los umbrales definidos, reduciendo el riesgo de ataques de denegación de servicio, scraping y abuso de las aplicaciones web.</p> <p>c. Administración de listas de control (whitelists y blacklists) a nivel de aplicación.</p> <p>3. Controles complementarios de seguridad en la infraestructura AWS</p> <p>a. Aplicación de controles de acceso a nivel de red mediante Security Groups, operando bajo el principio de <i>deny by default</i> y permitiendo únicamente el tráfico autorizado.</p> <p>b. Propagación rápida de reglas de seguridad dentro de la infraestructura AWS, garantizando tiempos de respuesta adecuados ante incidentes o alertas de seguridad.</p> <p>4. Monitoreo y operación segura</p> <p>a. Seguimiento continuo del tráfico y eventos de seguridad, permitiendo la identificación temprana de intentos de ataque o comportamientos anómalos.</p> <p>b. Atención de solicitudes de ajuste, bloqueo o habilitación de accesos conforme a los procedimientos definidos.</p> <p>5. Soporte documental</p>

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

a. Aplicación del Procedimiento de Gestión de IPs y Reglas de Seguridad, que documenta la administración de controles de seguridad en AWS, incluyendo el uso de AWS WAF y la gestión de reglas a nivel de red y aplicación, como soporte al cumplimiento de esta obligación.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.34 Permitir la gestión centralizada de reglas de seguridad, su despliegue automático a múltiples sitios mediante plantillas predefinidas, y su administración completa a través de APIs documentadas.

El proveedor con la solución implementada, permitió la gestión centralizada de las reglas de seguridad sobre la infraestructura tecnológica desplegada en AWS, facilitando su definición, control, actualización y propagación automática a múltiples aplicaciones, sitios o entornos. Esta gestión se apoya en el uso de plantillas predefinidas, mecanismos de automatización y APIs documentadas, asegurando consistencia, trazabilidad y eficiencia operativa en la administración de la seguridad.

Para el desarrollo de esta actividad, se ejecutan las siguientes acciones:

1. Gestión centralizada de reglas de seguridad

a. Administración centralizada de reglas de seguridad a nivel de red y aplicación, permitiendo aplicar políticas homogéneas sobre múltiples recursos y servicios.

b. Definición de reglas estándar y personalizadas que responden a los lineamientos de seguridad establecidos por la Alcaldía de Santiago de Cali.

2. Despliegue automático mediante plantillas predefinidas

a. Uso de plantillas y configuraciones reutilizables para la creación, actualización y despliegue de reglas de seguridad en distintos entornos (producción, pruebas, contingencia).

b. Aplicación automática de reglas a múltiples sitios o aplicaciones, reduciendo la

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

intervención manual y el riesgo de configuraciones inconsistentes.

c. Propagación rápida de cambios de seguridad en la infraestructura AWS, garantizando tiempos de respuesta adecuados ante nuevas necesidades o incidentes.

3. Administración a través de APIs documentadas

a. Posibilidad de integrar la gestión de seguridad con herramientas externas de automatización, monitoreo o gestión de servicios, conforme a las necesidades de la entidad.

b. Disponibilidad de documentación técnica que describe los flujos, parámetros y buenas prácticas para la administración de las reglas mediante APIs.

4. Trazabilidad y control operativo

a. Registro y seguimiento de los cambios realizados sobre las reglas de seguridad, permitiendo auditoría y control de configuraciones.

b. Capacidad de validar el estado y la correcta aplicación de las reglas desplegadas en los diferentes sitios o recursos.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.35 Garantizar que el sistema registre solicitudes en tiempo real, incluyendo detalles como IP, geolocalización, URI, agente de usuario y referenciadores, integrándose con las plataformas de monitoreo de la entidad.

El proveedor garantiza el registro en tiempo real de las solicitudes realizadas a las aplicaciones web mediante el uso de servicios nativos de AWS, específicamente Amazon CloudWatch Logs Insights y VPC Flow Logs. A través de estos mecanismos se capturan y analizan datos como dirección IP, geolocalización, URI solicitada, agente de usuario y referenciadores, permitiendo la trazabilidad del tráfico, el monitoreo operativo y el soporte a la identificación de eventos de seguridad y desempeño, asegurando la integridad y control de las aplicaciones web institucionales.



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

Los siguientes servicios tuvieron un comportamiento estable.

Service	RSS	Today	4 Feb	3 Feb	2 Feb	1 Feb	31 Jan	30 Jan
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

Service	RSS	9 Feb	8 Feb	7 Feb	6 Feb	5 Feb	4 Feb	3 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted



ALCALDÍA DE
SANTIAGO DE CALI

GESTIÓN JURÍDICO
ADMINISTRATIVA
GESTIÓN CONTRACTUAL

MODELO INTEGRADO DE
PLANEACIÓN Y GESTIÓN
(MIPG)

INFORME DE SUPERVISIÓN DE
CONTRATO

MAJA01.04.03.P002.F003

VERSIÓN

002

Service	RSS	16 Feb	15 Feb	14 Feb	13 Feb	12 Feb	11 Feb	10 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted

Service	RSS	Today	22 Feb	21 Feb	20 Feb	19 Feb	18 Feb	17 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted

Documento Anexo: [Informe de monitoreo y disponibilidad Alcaldía de Cali](#)

4.36 Administración de listas de IP anónimas, así como la rápida propagación de las reglas de seguridad definidas, con tiempos de actualización que no superen los cinco minutos en entornos productivos

El proveedor permite la administración de listas de IP anónimas mediante el uso de

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

AWS Web Application Firewall (AWS WAF) sobre la infraestructura desplegada en AWS. A través de este servicio, gestionamos listas de bloqueo automático (blacklists) y listas de permitidos, así como reglas *rate-based* que permiten identificar y mitigar comportamientos anómalos o tráfico malicioso, incluyendo accesos automatizados y picos inusuales de solicitudes. Las reglas de seguridad definidas se propagan de forma automática a los entornos productivos, con tiempos de actualización inferiores a cinco minutos, garantizando una respuesta oportuna ante eventos de seguridad y asegurando la protección continua de las aplicaciones web institucionales de la Alcaldía de Santiago de Cali.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.37 Disponibilidad de canal Interconnect 1000 Mbps

En el marco de la infraestructura tecnológica implementada para la Alcaldía de Santiago de Cali, el proveedor habilitó un esquema de conectividad híbrida que garantiza la disponibilidad, continuidad y resiliencia del canal Interconnect de 1000 Mbps establecido entre la infraestructura local de la entidad y los servicios desplegados en AWS.

Este diseño contempla la integración entre el enlace AWS Direct Connect, configurado sobre uno de los canales de Internet institucional, con el fin de asegurar la continuidad operativa ante cualquier evento de indisponibilidad o degradación del enlace principal.

1. Integración del Canal Direct Connect 1000 Mbps

El enlace Direct Connect correspondiente a la cuenta de networking de la Alcaldía ha sido:

- Desplegado y configurado conforme a los lineamientos de arquitectura definidos para la solución.
- Integrado con las VPC y servicios de AWS que soportan las cargas de trabajo del proyecto.
- Validado a nivel de operación, rutas, propagación BGP y performance.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG) INFORME DE SUPERVISIÓN DE CONTRATO	MAJA01.04.03.P002.F003	
		VERSIÓN	002

Según el estado registrado en la consola, el recurso Direct Connect se encuentra activo, estable y funcional, operando como canal principal de intercambio de datos entre la infraestructura local y la plataforma cloud.

2. Arquitectura de Alta Disponibilidad: Activo-Activo / Activo-Pasivo

Estos canales operan bajo un esquema de alta disponibilidad, permitiendo:

- Modo Activo-Activo: Cuando la arquitectura requiere balanceo de carga o distribución dinámica del tráfico.
- Modo Activo-Pasivo con Failover Automático: Mecanismo que detecta anomalías y conmuta inmediatamente hacia la VPN sin afectar las conexiones ni los servicios.

El sistema de enrutamiento supervisa permanentemente:

- Pérdida de conectividad.
- Incremento inusual de latencia.
- Interrupciones o degradaciones del Direct Connect.

Ante cualquier evento, el tráfico se desvía automáticamente hacia la VPN, asegurando continuidad sin intervención manual.

3. Garantía de Redundancia y Resiliencia Operacional

La configuración combinada de Direct Connect proporciona una infraestructura de comunicación robusta y alineada con las buenas prácticas de arquitectura híbrida:

- Redundancia: Dos canales independientes operando como rutas principales y de contingencia.
- Resiliencia: Recuperación sin interrupciones ante fallas del enlace dedicado.
- Estabilidad: Mantiene operativos los sistemas críticos incluso en escenarios adversos.
- Seguridad: Ambos canales funcionan bajo cifrado y estándares de seguridad compatibles con AWS y con la normativa institucional.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

Este esquema permite asegurar la disponibilidad continua de:

- Servicios cloud estratégicos.
- Cargas virtualizadas y aplicaciones institucionales.
- Procesos misionales del Distrito que dependen de la interconexión híbrida.

tgw-rtb-03f2b8b2696919c22 / tgwrt-cali-prd-direct-connect [info](#) Actions

Details

Transit gateway route table ID tgw-rtb-03f2b8b2696919c22	State Available	Default association route table No	Default propagation route table No
---	--------------------	---------------------------------------	---------------------------------------

Transit gateway ID
[tgw-0af543d46cb6941a9](#)

Associations | Propagations | Prefix list references | **Routes** | Tags

Filter routes by CIDR (2)

Exact CIDR: | Longest prefix match: | Supernet of match: | Subnet of match:

Routes (9)

CIDR	Attachment ID	Resource ID	Resour...	Route t...	Route st...	Prefix list ID
<input type="checkbox"/> 10.10.14.0/24	tgw-attach-025a988473581ad1	vpc-0f362e7b77050c398	VPC	Propagated	Active	-
<input type="checkbox"/> 10.10.15.0/24	tgw-attach-00c7b53fbb55bab6d	vpc-0dcaad1778984a574	VPC	Propagated	Active	-
<input type="checkbox"/> 10.130.0.0/22	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
<input type="checkbox"/> 10.30.104.0/21	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a427f721a0	VPC	Propagated	Active	-
<input type="checkbox"/> 10.30.80.0/24	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
<input type="checkbox"/> 10.98.0.0/16	tgw-attach-01118378fe1bd73c	vpc-0577102c2eb4b5892	VPC	Propagated	Active	-
<input type="checkbox"/> 172.18.0.0/16	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a427f721a0	VPC	Static	Active	-
<input type="checkbox"/> 172.18.26.0/27	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a427f721a0	VPC	Static	Active	-
<input type="checkbox"/> 172.18.8.0/24	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a427f721a0	VPC	Static	Active	-

Documento Anexo: Informe de Estado Direct Connect ACA

OBSERVACIONES AL INFORME TÉCNICO: Vencido el plazo de ejecución de la Orden de Compra, se deja constancia de que el contratista cumplió con las obligaciones principales derivadas del objeto contractual y desarrolladas en los estudios previos, correspondientes a los ítems definidos en la Orden de Compra. No obstante lo anterior, continúan vigentes las obligaciones postcontractuales relacionadas con los servicios de infraestructura, soporte y modernización tecnológica, por el término establecido contractualmente, durante el cual el proveedor deberá atender solicitudes, generar reportes de monitoreo y garantizar la continuidad operativa de la solución implementada.

 ALCALDÍA DE SANTIAGO DE CALI GESTIÓN JURÍDICO ADMINISTRATIVA GESTIÓN CONTRACTUAL	MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)	MAJA01.04.03.P002.F003	
	INFORME DE SUPERVISIÓN DE CONTRATO	VERSIÓN	002

6. RECOMENDACIONES PARA EL CONTRATISTA

No se reportan recomendaciones

7. FIRMAS RESPONSABLES

 <hr/> PAULO CESAR GUERRERO AGUDELO Supervisor	 <hr/> RODOLFO TEJADA NAVEROS Contratista - Apoyo a la Supervisión - Rol Técnico
 <hr/> HECTOR FABIO MORENO MUÑOZ Contratista - Apoyo a la Supervisión - Rol Jurídico	 <hr/> ANDREA LUCIA CALDERON SERRATO Contratista - Apoyo a la Supervisión - Rol Financiero

Fecha de suscripción del informe de supervisión: Santiago de Cali Distrito Especial, 15 de marzo de 2026

Alcaldía de Cali

ORDEN DE COMPRA No. 151305

Informe de ejecución cuota 3 OC 151305



**ALCALDÍA DE
SANTIAGO DE CALI**

CONTROL DE CAMBIOS

Versión	Fecha	Responsable	Descripción
1.0	14/03/2026	Kelly Carbonell	Creación del documento



1. Introducción	4
2. Objetivos.....	5
2.1. Objetivo general	5
2.2. Objetivos específicos	5
3. Detalle Orden de Compra 151305.....	6
4. Ejecución del contrato OC 151305.....	11
5. Obligaciones contractuales estudios previos OC 151305.....	11
4.1 Cumplir los requerimientos establecidos en las especificaciones técnicas, estudios previos, oferta económica y demás documentos que hagan parte del proceso de contratación.	11
4.2 Entregar un plan de trabajo de la ejecución del contrato, donde se contemple como mínimo las actividades de diseño y arquitectura base de cada solución tecnológica, la configuración de la herramienta de virtualización, la replicación de la data previamente conciliada con el supervisor, las pruebas y la puesta en marcha de los modelos y soluciones tecnológicas. En este plan de trabajo se deberán visualizar con claridad, en su estructura de descomposición de trabajo las líneas y actividades del contrato, así como sus recursos y el avance actual de cada una de ellas.....	12
4.3 Elaborar y entregar informes periódicos de actividades, en el cual se evidencie el desarrollo y avance del objeto contratado, siendo potestad del supervisor designado solicitarlo en cualquier momento de la ejecución del contrato, de acuerdo con las fases de ejecución del contrato.....	12
4.4 Garantizar que las soluciones tecnológicas desplegadas sean compatibles con la operación del modelo de datos almacenado por la Alcaldía del Distrito de Santiago de Cali.....	13
4.5 Realizar la gestión de la infraestructura bajo una cuenta designada por la entidad o conforme a las políticas establecidas por esta, utilizando etiquetas (tags) normalizadas para cada recurso (nombre del proyecto, entorno, responsable, criticidad, centro de costo), que faciliten la trazabilidad técnica y financiera de los mismos.....	13
4.6 Ocuparse de la gestión de administración de la infraestructura de servicios de virtualización, de manera que asegure la disponibilidad de dicha infraestructura en al menos en 99.9% (ANS).....	14
4.7 Habilitar y configurar un canal de comunicación alternativo mediante VPN, utilizando uno de los canales de Internet proporcionados por la entidad. Esta VPN deberá estar correctamente integrada con el canal Direct Connect (o su equivalente), y ambas conexiones deberán operar bajo un esquema de alta disponibilidad, ya sea en configuración activo-activo o, como mínimo, en activo-pasivo con conmutación automática (failover automático), garantizando la continuidad del servicio ante fallos de conectividad.	15
4.8 Monitorear y reportar mensualmente el consumo de la infraestructura (almacenamiento, cómputo, tráfico, etc.), incluyendo recomendaciones de optimización y alertas sobre posibles desviaciones presupuestales, asegurando la eficiencia del uso de los recursos contratados.....	16

4.9 Implementar política de acceso basada en roles (IAM), que permita controlar, limitar y auditar el acceso a los recursos de la nube, conforme a los principios de menor privilegio y segregación de funciones, entregando a la entidad los registros de acceso generados durante la ejecución del contrato.17

4.10 Gestionar y mantener actualizadas las copias de seguridad (backups) de los sistemas, datos y configuraciones relacionados con la solución contratada, en los servicios de almacenamiento y respaldo habilitados en la nube de AWS o equivalentes. Las copias de seguridad deberán incluir mecanismos de recuperación (snapshots, volcados de bases de datos, archivos de configuración, etc.), y se deberá realizar al menos una prueba de restauración por trimestre calendario, dejando constancia de los resultados en un informe técnico que deberá ser entregado a la entidad. Para asegurar la portabilidad de la información, los backups deberán estar disponibles en formato descargable. En el caso de servicios gestionados (máquinas nativas o bases de datos nativas), el contratista deberá garantizar la exportación de los datos (por ejemplo, mediante mysqldump, pg_dump u otro método adecuado) y almacenarlos en Amazon S3 u otro repositorio que permita su descarga directa. Al finalizar el contrato, el contratista deberá entregar la totalidad de las copias de seguridad vigentes en el medio de almacenamiento que disponga la Alcaldía Distrital en su momento, asegurando la integridad, trazabilidad y disponibilidad de la información durante el proceso de entrega.....19

4.11 Garantizar la disponibilidad de herramientas digitales de administración y gestión de las soluciones tecnológicas desarrolladas, que cuente con acceso a la infraestructura subyacente, permitiendo el monitoreo de todos los servicios de virtualización.....21

4.12 Realizar la gestión del proyecto, asegurando la planificación y el seguimiento adecuado de la ejecución del contrato22

4.13 Llevar a cabo la transferencia de conocimiento dirigida a los colaboradores de la Alcaldía de Santiago de Cali sobre el funcionamiento, uso y administración de las soluciones tecnológicas desarrolladas.....23

4.14 Prestar el servicio especializado para la implementación de las soluciones tecnológicas, durante la vigencia del contrato.25

4.15 Cumplir con las áreas principales del modelo de computación en los servicios digitales, como lo son: despliegue de servicios, orquestación de servicios, administración de los servicios digitales, privacidad y seguridad. Lo anterior en concordancia con lo establecido en la Guía Técnica de Computación en la nube de MinTIC y las versiones que lo modifiquen.....26

4.16 Designar un delegado para participar en las mesas de trabajo establecidas por el supervisor del contrato y atender las medidas que allí sean tomadas con el fin de soportar los requerimientos y que los mismo se lleven a cabo de manera articulada.27

4.17 Elaborar, suscribir y presentar al Distrito de Santiago de Cali - Departamento Administrativo de Tecnologías de la Información y las Comunicaciones las respectivas actas e informes correspondientes a la ejecución de la contratación. Estos documentos deberán ser aprobados por el Supervisor del Contrato.28

4.18 Dar cumplimiento a la normatividad de protección de datos personales y de confidencialidad de la información, donde garantice una adecuada definición de los niveles de seguridad para no generar accesos no autorizados a datos confidenciales de propiedad de la Entidad.....28

4.19 Garantizar que siempre la Entidad tendrá la propiedad y el control de su información, así como disponible un mecanismo para el borrado seguro de los datos, si llegare a ocurrir una terminación anticipada, según el modelo computacional.30

4.20 Entregar los códigos, manuales, tutoriales y/o instructivos asociados a las soluciones tecnológicas brindadas. También debe entregar los accesos a los aplicativos y a herramientas de monitoreo para acceder por parte del personal de DATIC.32

4.21 Garantizar que los servicios a proveer cumplan con estándares de calidad con las normas vigentes relativas al servicio la infraestructura digital, ISO 9901-ISO 27001 –ISO 27017 –ISO27018 – SOC1 –SOC2 – SOC3 –CSA -FEDRAMP.....32

4.22 Atender las sugerencias que el Distrito de Santiago de Cali - Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones, considere convenientes y pertinentes para la ejecución del objeto del contrato.....34

4.23 Asegurar el manejo del acceso a las soluciones tecnológicas, con el fin de evitar manejos múltiples de administradores y así evitar fraudes y robos de información, migración de datos e información, actualizaciones de aplicaciones personales, aplicaciones adicionales y gestión de sus datos personales35

4.24 Ejecutar un plan de reversibilidad al finalizar el contrato, que contemple la desactivación de servicios, transferencia de recursos, entrega de accesos y documentación, eliminación segura de configuraciones y recursos desplegados, asegurando que la entidad no incurra en costos residuales o innecesarios posteriores a la finalización contractual.....36

4.25 Garantizar la implementación y el fortalecimiento de la plataforma tecnológica que soporta los sistemas de información transversales con su respectiva disponibilidad, seguridad y eficiencia, así mismo asegurar la compatibilidad con la infraestructura tecnológica existente y proveer capacidad de escalabilidad y redundancia, según la descripción detallada del bien adquirido.37

4.26 Suministrar herramientas de monitoreo en tiempo real con métricas detalladas (uso de CPU, memoria, red, almacenamiento, etc.), garantizando la disponibilidad de históricos de monitoreo desde el inicio de operación y proveer reportes de optimización y desempeño de los servicios.38

4.27 Implementar mecanismos de cifrado y control de accesos, asegurando la integridad, disponibilidad y confidencialidad de la información financiera, lo anterior en cumplimiento de las normativas de seguridad establecidas..... 40

4.28 Brindar un escenario que permita el desarrollo y automatización de copias de respaldo, bajo la política día, mes y año y con ello poder realizar la restauración en caso de falla o interrupción.....43

4.29 Brindar soporte técnico Premium 24/7 mensual, a través de diversos canales (teléfono, correo electrónico, sistema de tiquetes), garantizando los tiempos de respuesta adecuados según la criticidad del servicio.....47

4.30 Mantener una base de conocimiento con documentación técnica y foros de consulta..... 49

4.31 Brindar documentación técnica de los procesos ejecutados para los sistemas generados y realizar transferencia de conocimiento entregando documentación detallada de la misma, tales como videos, manuales, guías y demás documentos requeridos por la entidad..... 49

4.32 Realizar la transferencia de conocimiento en la gestión y operación de la plataforma adquirida al equipo técnico de la Alcaldía de Santiago de Cali. 49

4.33 Garantizar que la solución cuente con mecanismos para bloquear ataques comunes (como inyección SQL, XSS y otros del OWASP Top 10) y protección frente a tráfico automatizado malicioso (bots), asegurando la integridad de las aplicaciones web institucionales. 53

4.34 Permitir la gestión centralizada de reglas de seguridad, su despliegue automático a múltiples sitios mediante plantillas predefinidas, y su administración completa a través de APIs documentadas..... 55

4.35 Garantizar que el sistema registre solicitudes en tiempo real, incluyendo detalles como IP, geolocalización, URI, agente de usuario y referenciadores, integrándose con las plataformas de monitoreo de la entidad. 56

4.36 Administración de listas de IP anónimas, así como la rápida propagación de las reglas de seguridad definidas, con tiempos de actualización que no superen los cinco minutos en entornos productivos 57

4.37 Disponibilidad de canal Interconnect 1000 Mbps 58

1. Introducción

En cumplimiento de la OC No. 151305, celebrado entre HIGH TECH SOFTWARE S.A.S. (Blend 360) y el Departamento Administrativo de Tecnologías de la Información y Comunicaciones (DATIC) de la Alcaldía de Santiago de Cali, presentó este informe consolidado correspondiente a la ejecución del contrato correspondiente a la cuota 3.

El objeto del contrato es suministrar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali.

La ejecución contractual se enmarca en el objeto de contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, orientada a garantizar la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información del Distrito, de acuerdo con lo dispuesto en los Estudios Previos y el Requerimiento Técnico del proceso contractual. Asimismo, se atiende lo dispuesto en el Plan de Trabajo de Ejecución del Proyecto, el cual estructura las actividades, entregables, roles y mecanismos de seguimiento asociados a la implementación de la solución tecnológica contratada. Este informe presenta de manera detallada la realización de las actividades ejecutadas, las acciones técnicas y administrativas adelantadas, y la trazabilidad de cumplimiento frente a cada una de las obligaciones contractuales, con el fin de permitir al supervisor validar el cumplimiento correspondiente para la autorización del tercer desembolso, equivalente al 20% del valor total del contrato, de acuerdo con el esquema de pagos establecido.

2. Objetivos

2.1. Objetivo general


Evidenciar el avance alcanzado en la ejecución del contrato durante la tercera cuota demostrando el cumplimiento de las obligaciones contractuales definidas para el proyecto, conforme a lo establecido en el Plan de Trabajo, Estudios Previos, Especificaciones Técnicas y demás documentos que hacen parte integral del proceso contractual.

2.2. Objetivos específicos

- Describir las actividades técnicas, administrativas y operativas ejecutadas durante la tercera cuota del contrato, en correspondencia con el cronograma y el alcance establecido.

- Verificar y documentar el cumplimiento de cada una de las obligaciones contractuales, presentando la evidencia de su ejecución y/o avance.
- Garantizar la trazabilidad y transparencia en el cumplimiento de las actividades realizadas, en concordancia con los principios y lineamientos de gestión pública establecidos por DATIC.

3. Detalle Orden de Compra 151305



ALCALDIA MUNICIPIO SANTIAGO DE CALI - DEPARTAMENTO ADMINISTRATIVO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
N.I.T. 890399011
ORDEN DE COMPRA

Hightech Software S.A.S.
N.I.T. 900718336
Calle 56 # 36 A - 09
Bogotá, Bogotá, Distrito Capital
Atte: Karen Arandia
ad@nuvu.cc
Teléfono: +57 1 7703250

<p>Número de Orden: 151305 No de Instrumento: Instrumento agregación: IAD Software por Catalogo II Fecha de Emisión: 05/09/25 Fecha de Vencimiento: 15/03/26 Comprador: Andres Olaya Perdomo Ordenador del gasto: Alexander Mondragon Valencia Supervisor: Ermilson Diaz Martinez Teléfono: 3113216186 Detalle de Entrega:</p>	<p>Gravámenes adicionales: Pro-Desarrollo 3,5% Pro-Univalle 2% Pro-Hospital 1% Pro UniPacífico 0,5% Pro-Cultura 1% Pro-Adulto Mayor 2% Justicia Familiar 2% Pro-Deporte y Recreación 2% Impuesto del Timbre 0,5%</p>
<p>Justificación: Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali.</p>	

Enviar a
ALCALDÍA MUNICIPIO SANTIAGO DE CALI - DEPARTAMENTO ADMINISTRATIVO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Facturar a
ALCALDÍA MUNICIPIO SANTIAGO DE CALI - DEPARTAMENTO ADMINISTRATIVO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Línea	Presupuesto	Descripción	Cant.	Unidad	Precio	Total
1	CDP 3600011684	sxc02---NUV-HOU-03-01-Software General-Otro-High Tech Software S.A.S - N/A-SAAS-N/A-N/A-Dolar-N/A-Mensual-Houndoc	1353642.0	Unidad	4.736,00	6.410.848.512,00
2	VF 6000000210	sxc02---NUV-HOU-01-05-Software General-Otro-High Tech Software S.A.S - N/A-SAAS-N/A-N/A-Unidad-N/A-Mensual-Houndoc	15.0	Unidad	238.189.032,00	3.572.835.480,00
3	CDP 3600011684	sxc02---IT-SW-09-02-Software General-Otro-High Tech Software S.A.S - N/A-N/A-Remota-Profesional-Hora-Todas las zonas-N/A-Configuración y parametrización de los Productos	3006.0	Unidad	140.716,00	422.992.296,00
4	CDP 3600011684	sxc02---IT-SW-02-03-Software General-Otro-High Tech Software S.A.S - N/A-N/A-Presencial-Profesional-Mes-3-N/A-Soporte técnico en sitio	17.0	Unidad	16.455.673,00	279.746.441,00
5	CDP 3600011684	sxc02---IVA	1.0	Unidad	133.520.360,00	133.520.360,00
10.819.943.089,00 COP						

A continuación, se presentan los componentes asociados a las líneas presupuestales derivadas de la Orden de Compra No. 151305, indicando su alcance, propósito y estado de ejecución.

- **Línea 1: sxc02---NUV-HOU-03-01 Software General – Otro – High Tech Software S.A.S-N/A-N/A-Dolar-N/A-Mensual-Houndoc**

Este componente corresponde al uso y operación de la infraestructura virtual desplegada en AWS, necesaria para soportar los sistemas de información institucionales del Distrito. Incluye los costos variables asociados al consumo de:

- Recursos de cómputo (instancias, núcleos virtuales y procesamiento)
- Almacenamiento distribuido y en capas (EBS, S3, EFS)
- Servicios de red y transferencia de datos (interconexión, VPN y tráfico interno/externo)
- Capacidades nativas de seguridad, respaldo, auditoría y monitoreo

La infraestructura fue configurada bajo un modelo de alta disponibilidad, con mecanismos de recuperación ante fallos y herramientas de monitoreo continuo, permitiendo garantizar continuidad operativa y estabilidad de los servicios institucionales.

Adicionalmente, se implementó un proceso para el monitoreo y optimización permanente del gasto, el cual incluye:

- Etiquetado estandarizado para trazabilidad por cuenta, servicio y entorno
- Revisión continua de consumos y proyecciones
- Alertas automáticas de desbordamiento presupuestal
- Recomendaciones de optimización
- Reporte mensual de costos, uso y eficiencia

En virtud de lo establecido en la Orden No. 151303, cuyo objeto es *“Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali”*, realiza entrega de un certificado de la bolsa de recursos cloud a la entidad, destinado al consumo de los servicios de infraestructura cloud asociados a esta solución durante la vigencia del contrato.

Documento Anexo: Certificación bolsa de recursos Cloud Alcaldía de Cali

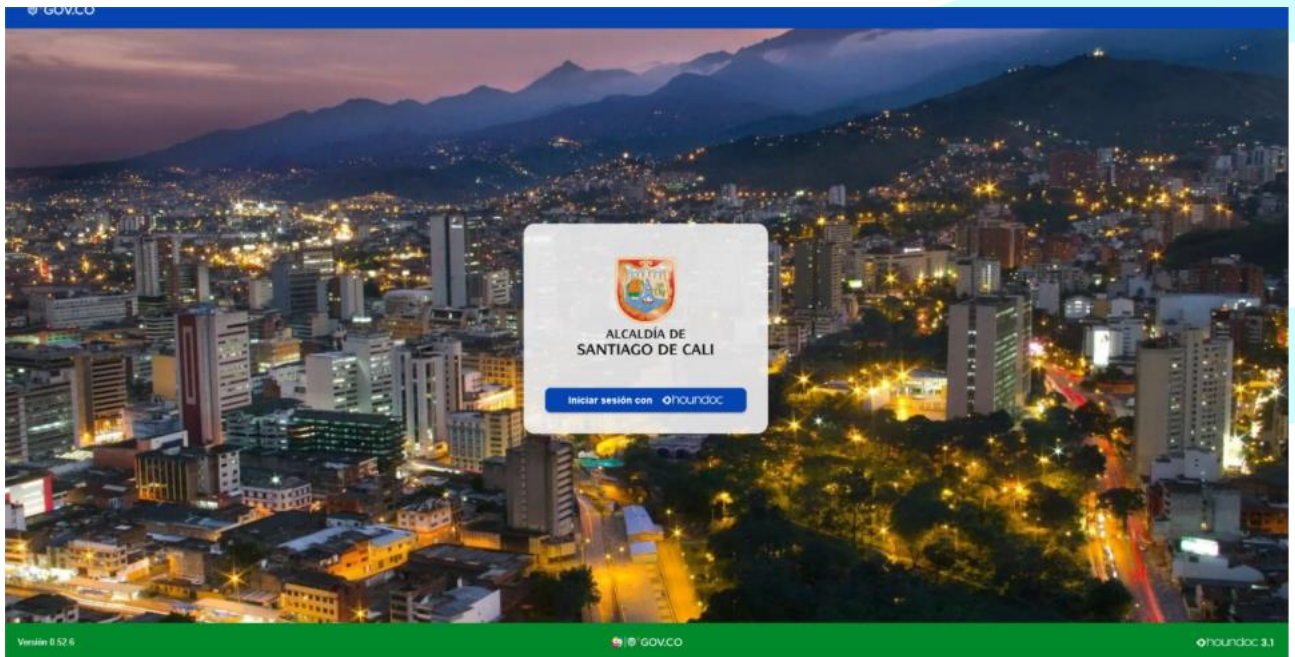
- **Línea 2: sxc02---NUV-HOU-01-05 Software General – Otro – High Tech Software S.A.S-N/A-SAAS-N/A-N/A-Unidad-N/A-Houndoc**

Se hace entrega del licenciamiento de la plataforma tecnológica Houndoc, que consolida la información sobre la licencia otorgada para su uso y garantiza que la Alcaldía de Cali cuente con los accesos y derechos necesarios

Información del licenciamiento:

- Licenciante: High Tech Software S.A.S.

- Licenciatario: Santiago de Cali Distrito Especial- Departamento Administrativo de Tecnologías de La Información y las Comunicaciones.
- Modalidad: SaaS exclusiva y no transferible, territorio Colombia.
- Usuarios: Hasta 1000 usuarios nombrados.
- Versión: Houndoc v0.52.6.
- Vigencia: Hasta 31 de diciembre de 2026.
- Orden de compra: No. 151305
- Acceso: se encuentra desplegado en la nube, en portal web: <https://app.ia.cali.gov.co/> en productivo para usuarios de Alcaldía Cali.



La plataforma centraliza:

- Caracterización del Ciudadano (Integración de datos de beneficiarios de programas sociales).
- Observatorio Educación (Integración de datos para la gestión educativa).
- Chatbot y Agente Experto en Trámites, con métricas de uso y monitoreo interactivo.
- Agente Cognitivo de Infraestructura en AWS, orientado a la operación y observación de cargas de procesamiento en nube.
- Geocodificador, para localización de la ubicación geográfica de direcciones en el mapa de la ciudad.
- Dashboard de Costos de Soluciones en la Nube, para trazabilidad financiera y control de consumo por cada caso de uso implementado.
- Métricas de uso de Houndoc, para análisis de adopción y desempeño de la plataforma.

Como parte de los entregables del contrato, se realizó la entrega del licenciamiento de la plataforma Houndoc a la Alcaldía de Santiago de Cali, cumpliendo con las condiciones técnicas y administrativas definidas.

Documento Anexo: Certificación licenciamiento houndoc Alcaldia de Cali-proyecto Visualización

- **Línea 3: sxc02---IT-SW-09-02 Software General – Otro – High Tech Software S.A.S-N/A-N/A-Remota-Profesional-Hora-Todas las zonas-N/A-Configuración y parametrización de los Productos**

Este componente corresponde a la configuración y parametrización de los productos asociados a la solución contratada. Como parte de esta entrega, se presenta la certificación emitida en virtud de lo establecido en la Orden No. 151303, cuyo objeto es:

“Contratar una solución tecnológica integral de virtualización de la infraestructura tecnológica institucional, que incorpore capacidades inteligentes para la gestión optimizada de recursos computacionales, garantizando la alta disponibilidad, continuidad operativa, escalabilidad y seguridad de los sistemas de información transversales del Distrito de Santiago de Cali”.

En este sentido, se certifica que, en el marco del servicio contratado, la entidad cuenta con una bolsa de 3.006 horas de servicios profesionales, destinadas a la creación, personalización e implementación asociadas a virtualización objeto del contrato que permitirá garantizar el acompañamiento técnico especializado necesario para el desarrollo progresivo de los distintos componentes de la solución, en articulación con los requerimientos funcionales y operativos definidos por la Entidad.

Asimismo, dichas horas serán utilizadas para el acompañamiento técnico en los procesos de modernización de las aplicaciones de la Alcaldía, incluyendo la evaluación y ejecución de cambios de arquitectura, con el fin de asegurar su adecuada evolución, estabilidad, seguridad y alineación con las buenas prácticas tecnológicas y los lineamientos institucionales.

Documento Anexo: Certificación servicios profesionales OC 151305

- **Línea 4: sxc02—IT-SW-02-03 Software General – Otro – High Tech Software S.A.S – N/A – N/A – Presencial – Profesional – Mes – 3 – N/A – Soporte técnico en sitio**

Como parte de la presente entrega, se incorpora el certificado correspondiente a los servicios de soporte el cual respalda la disponibilidad de personal técnico especializado para la atención, acompañamiento y operación de la infraestructura virtual contratada por la Alcaldía de Santiago de Cali. Este componente cubre la prestación del servicio de soporte, que incluye el acompañamiento operativo en incidentes, requerimientos y ajustes, el soporte directo durante ventanas de mantenimiento y cambios planificados, y las actividades de diagnóstico, estabilización y continuidad de servicios críticos. Asimismo, contempla la interacción permanente con los equipos de DATIC para asegurar la transferencia de conocimiento y la apropiación tecnológica durante todo el proceso de operación.

Las actividades desarrolladas se ejecutan bajo los Acuerdos de Nivel de Servicio (ANS) definidos con la entidad, respetando horarios, mecanismos de atención y manteniendo registros trazables en bitácoras de soporte. La gestión se realiza a través de la herramienta oficial Zammad, mediante la cual los usuarios habilitados pueden registrar, modificar y cerrar solicitudes de incidentes, solicitudes de cambio (RFC) y requerimientos de información (RFI). Esta plataforma permite, además, solicitar la creación o eliminación de recursos AWS (EC2, RDS, S3, EBS, Security Groups, IAM Roles, WAF, Load Balancers), gestionar configuraciones en servidores, redes VPC o balanceadores, modificar o desplegar máquinas virtuales en VMware, validar conectividad híbrida, revisar logs, realizar análisis de costos, gestionar copias de seguridad y ejecutar restauraciones. La solución también genera reportes técnicos y operativos que permiten el seguimiento integral de cada caso atendido.

Durante el periodo correspondiente se mantuvo la operación de Zammad con los usuarios oficiales de la Alcaldía de Santiago de Cali debidamente habilitados, quienes disponen del portal <https://helpdesk.ia.blend360.com/#login> para el registro, consulta y seguimiento de solicitudes. Adicionalmente, se entregó y socializó el Manual de Usuario, asegurando el conocimiento operativo para el uso adecuado de la plataforma y garantizando la trazabilidad de incidentes, solicitudes de información y solicitudes de cambio gestionadas en el marco del

servicio contratado. Los reportes consolidados evidencian un número considerable de solicitudes relacionadas con infraestructura, despliegues, configuración de reglas de firewall, administración de recursos AWS y validaciones operativas, la mayoría clasificadas con criticidad alta y atendidas dentro de los tiempos definidos por los ANS.

Documento Anexo: Certificación servicios de soporte OC 151305

4. Ejecución del contrato OC 151305

En cumplimiento de la OC N.º 151305 y de los documentos contractuales se presenta el avance técnico y administrativo correspondiente al segundo hito de ejecución, con el cual se soporta la verificación del Pago N.º 3 La ejecución se orienta al objeto contractual de entregar una solución tecnológica integral de virtualización con alta disponibilidad, continuidad operativa, escalabilidad y seguridad, según alcance y lineamientos definidos por DATIC. Detalle alcance del contrato:

- Diseño e implementación de una arquitectura virtual escalable, que permita consolidar los entornos tecnológicos actuales y facilitar su expansión futura según la demanda operativa.
- Aprovisionamiento de recursos computacionales virtuales, incluyendo núcleos de procesamiento, almacenamiento distribuido y redes internas de alta eficiencia, configurados bajo esquemas de alta disponibilidad y recuperación ante fallos.
- Incorporación de capacidades de inteligencia artificial aplicada a la gestión de la infraestructura, tales como ajuste automático de recursos, clasificación de cargas, recomendaciones de configuración y detección anticipada de eventos críticos.
- Integración de mecanismos avanzados de protección, orientados a la defensa de aplicaciones y servicios virtualizados frente a amenazas cibernéticas, mediante reglas adaptativas, monitoreo continuo y control de accesos basado en roles.
- Administración centralizada de los entornos virtualizados, con capacidades de supervisión técnica, segmentación lógica, gestión automatizada de recursos y generación de reportes operativos para auditoría y control.
- Transferencia de conocimiento y acompañamiento técnico especializado, que garantice la correcta adopción de la solución por parte del equipo institucional, asegurando su sostenibilidad técnica y operativa.

5. Obligaciones contractuales estudios previos OC 151305

Con el fin de garantizar el cumplimiento del contrato y en coherencia con el objetivo de implementar una solución, se procederá a describir en detalle cada

una de las obligaciones contractuales correspondientes a la tercera cuota, junto con las actividades técnicas ejecutadas por el equipo de trabajo.

4.1 Cumplir los requerimientos establecidos en las especificaciones técnicas, estudios previos, oferta económica y demás documentos que hagan parte del proceso de contratación.

En cumplimiento de lo establecido en la obligación contractual que busca asegurar, demostrar y documentar que todas las obligaciones técnicas y contractuales con lo solicitado en los Estudios Previos de la OC 151305. Para lograrlo, se creó una Matriz de Trazabilidad de Requisitos (MTR) establecidos en los estudios previos, donde se listan uno por uno todos los requisitos técnicos, funcionales y administrativos del proyecto, indicando:

- Obligaciones del contrato.
- Qué entregable o evidencia lo demuestra.
- La periodicidad con la que se entregará

Adicionalmente, se elaboró un documento donde se detallan las obligaciones del contrato y la periodicidad de entrega que permitirá revisar el cumplimiento de cada obligación se esté cumpliendo de manera verificable, transparente y acorde con lo estipulado en el contrato.

Documento Anexo: Matriz de Trazabilidad de Requisitos verificable contra estudios previos

4.2 Entregar un plan de trabajo de la ejecución del contrato, donde se contemple como mínimo las actividades de diseño y arquitectura base de cada solución tecnológica, la configuración de la herramienta de virtualización, la replicación de la data previamente conciliada con el supervisor, las pruebas y la puesta en marcha de los modelos y soluciones tecnológicas. En este plan de trabajo se deberán visualizar con claridad, en su estructura de descomposición de trabajo las líneas y actividades del contrato, así como sus recursos y el avance actual de cada una de ellas.

En cumplimiento de las obligaciones contractuales, se elaboró y entregó a la entidad el Plan de Trabajo de Ejecución del Contrato, documento que consolida la hoja de ruta técnico–metodológica para la implementación de la solución tecnológica integral objeto del contrato. Dicho plan fue estructurado siguiendo los lineamientos estratégicos de DATIC y las directrices técnicas definidas en los Estudios Previos y en el Requerimiento Técnico.

El Plan de Trabajo contempla una estructura de descomposición de actividades (EDT/WBS) que permite visualizar de manera clara y secuencial cada fase del proyecto, sus actividades asociadas, los responsables, los recursos técnicos y humanos involucrados, y el avance estimado para cada componente.

Documento Anexo: Plan de trabajo

4.3 Elaborar y entregar informes periódicos de actividades, en el cual se evidencie el desarrollo y avance del objeto contratado, siendo potestad del supervisor designado solicitarlo en cualquier momento de la ejecución del contrato, de acuerdo con las fases de ejecución del contrato.

En cumplimiento de lo establecido en la obligación contractual referente a la entrega de informes periódicos de actividades, se ha estructurado un mecanismo formal de seguimiento y reporte que permite evidenciar el avance técnico y operativo del proyecto, así como el estado de cumplimiento del objeto contratado.

Durante la ejecución del contrato se elaboran y presentan Informes de Ejecución de acuerdo con las fases definidas en el Plan de Trabajo y conforme a los requerimientos del supervisor del contrato, quien podrá solicitar estos informes en cualquier momento para efectos de verificación, trazabilidad y control de avance.

Cada informe incluirá:

- Descripción detallada de las actividades ejecutadas en el periodo.
- Estado de avance frente a las obligaciones contractuales.
- Evidencias documentales y técnicas que soportan el cumplimiento.

Documento Anexo: Informes de ejecución mensual

4.4 Garantizar que las soluciones tecnológicas desplegadas sean compatibles con la operación del modelo de datos almacenado por la Alcaldía del Distrito de Santiago de Cali.

En cumplimiento de esta obligación, garantizamos que las soluciones tecnológicas desplegadas son diseñadas e implementadas de manera compatible con el modelo de datos institucional de la Alcaldía del Distrito de Santiago de Cali. Para ello, realizamos la revisión y entendimiento del modelo de datos existente, sus estructuras, reglas de negocio y lineamientos técnicos, asegurando que las soluciones respetaran la integridad, coherencia y operación de la información. Adicionalmente, validamos la correcta integración y funcionamiento de las soluciones con los sistemas existentes, ejecutando pruebas de compatibilidad y documentando los resultados, de tal forma que se garantizara una operación estable, segura y alineada con los estándares definidos por la entidad.

4.5 Realizar la gestión de la infraestructura bajo una cuenta designada por la entidad o conforme a las políticas establecidas por esta, utilizando etiquetas (tags) normalizadas para cada recurso (nombre del proyecto, entorno, responsable, criticidad, centro de costo), que faciliten la trazabilidad técnica y financiera de los mismos.

En cumplimiento de esta obligación, se realiza la gestión integral de la infraestructura tecnológica dentro de la cuenta designada por la entidad, aplicando estrictamente las políticas de etiquetado definidas para garantizar la trazabilidad técnica, operativa y financiera de todos los recursos implementados. Para ello, se utiliza la política de tagging establecida por Blend, en la que se definen las etiquetas obligatorias y opcionales que deben ser incorporadas en cada recurso desplegado en la nube. Estas etiquetas incluyen el nombre del recurso (Name), el entorno de despliegue (Env), la aplicación o producto asociado (App), el identificador del proyecto (ProjectId) y el cliente (Client), todas categorías obligatorias conforme a la política oficial, así como la etiqueta opcional Component cuando se requiere especificar el rol del recurso, ya sea front, back u otro tipo de componente.

Cada etiqueta se aplica siguiendo las reglas de nomenclatura formal descritas en la política: nombres completamente en minúsculas para los recursos, entornos en mayúsculas con siglas normalizadas, aplicaciones alineadas al maestro de productos y un ProjectId estandarizado que inicia con la letra P seguida de cuatro dígitos. Este modelo de etiquetado permite identificar de manera precisa el propósito, el entorno, la responsabilidad técnica, la criticidad operativa y el centro de costo asociado a cada recurso, lo que asegura un control adecuado en procesos de facturación, auditoría, asociabilidad financiera y gestión operativa de la infraestructura.

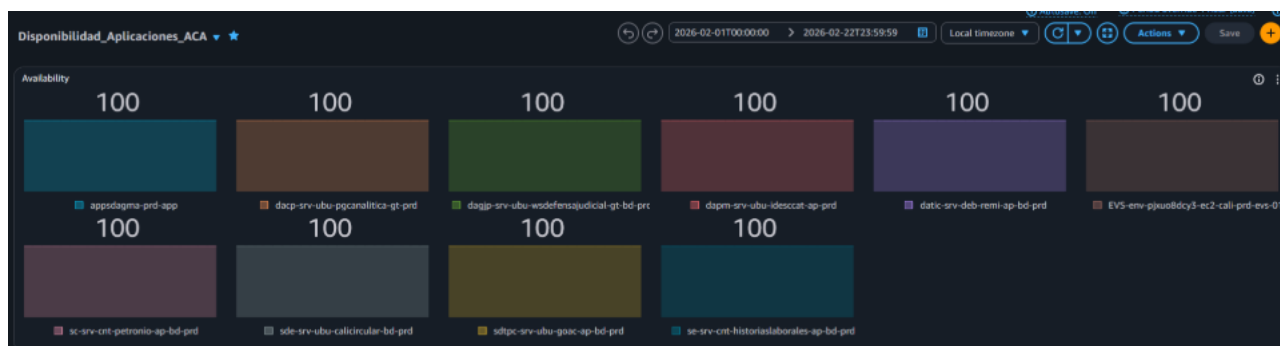
La administración de los recursos bajo esta política garantiza que la entidad cuente con una infraestructura ordenada, estandarizada y completamente trazable, facilitando la identificación de consumos, la depuración de costos, la administración de responsabilidades y la alineación del inventario tecnológico con las necesidades de operación del Distrito de Santiago de Cali. Con la aplicación consistente de estas etiquetas, se asegura el cumplimiento de las políticas internas de la entidad, la transparencia en el uso de la infraestructura y la capacidad de dar seguimiento técnico y financiero al ciclo de vida de cada recurso cloud.

Documento Anexo: Política de etiquetado

4.6 Ocuparse de la gestión de administración de la infraestructura de servicios de virtualización, de manera que asegure la disponibilidad de dicha infraestructura en al menos en 99.9% (ANS).

En cumplimiento de la obligación, se realiza la administración integral de la infraestructura de virtualización garantizando una disponibilidad mínima del 99.9%. El equipo mantiene un monitoreo continuo sobre los componentes críticos cómputo, almacenamiento, red, balanceadores y conectividad—utilizando métricas de rendimiento y disponibilidad que permiten identificar anomalías, atender incidentes de manera oportuna y asegurar la estabilidad del servicio. De forma permanente se aplican acciones de optimización,

autosanación, recuperación y ajuste de plataformas, lo que permite preservar la continuidad operativa y la estabilidad del entorno tecnológico. La disponibilidad alcanzada y las actividades de operación se consolidan en informes periódicos que evidencian el nivel de servicio comprometido.



Documento Anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.7 Habilitar y configurar un canal de comunicación alternativo mediante VPN, utilizando uno de los canales de Internet proporcionados por la entidad. Esta VPN deberá estar correctamente integrada con el canal Direct Connect (o su equivalente), y ambas conexiones deberán operar bajo un esquema de alta disponibilidad, ya sea en configuración activo-activo o, como mínimo, en activo-pasivo con conmutación automática (failover automático), garantizando la continuidad del servicio ante fallos de conectividad.

En la infraestructura implementada para la Alcaldía de Santiago de Cali se habilitó y configuró un canal de comunicación alternativo mediante una VPN establecida sobre uno de los canales de Internet suministrados por la entidad, con el fin de garantizar continuidad operativa ante cualquier evento de conectividad. Esta VPN se encuentra correctamente integrada con el enlace Direct Connect que opera en la cuenta de networking de la organización, el cual ha sido desplegado, configurado y validado para soportar el intercambio de datos entre la infraestructura local y los servicios de AWS. Conforme al estado del recurso registrado, el Direct Connect se encuentra activo y funcional, mientras que la VPN actúa como un enlace de respaldo plenamente operativo ante posibles fallas o degradaciones del servicio principal.

tgw-rtb-03f2b8b2696919c22 / tgwrt-cali-prd-direct-connect [info](#) Actions

Details

Transit gateway route table ID: tgw-rtb-03f2b8b2696919c22 State: Available Default association route table: No Default propagation route table: No

Transit gateway ID: tgw-0af543d456cb6941a9

Associations | Propagations | Prefix list references | **Routes** | Tags

Filter routes by CIDR (2)

Exact CIDR: Longest prefix match: Supernet of match: Subnet of match:

Routes (9) [info](#) Actions Create static route

Find route by attribute or tag

CIDR	Attachment ID	Resource ID	Resourc...	Route L...	Route st...	Prefix list ID
<input type="checkbox"/> 10.10.14.0/24	tgw-attach-025a988473581add1	vpc-0f362e7b77050c398	VPC	Propagated	Active	-
<input type="checkbox"/> 10.10.15.0/24	tgw-attach-00c7b51db55bab6e4	vpc-0dcaad1778984a574	VPC	Propagated	Active	-
<input type="checkbox"/> 10.130.0.0/22	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
<input type="checkbox"/> 10.30.104.0/21	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Propagated	Active	-
<input type="checkbox"/> 10.30.80.0/24	tgw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
<input type="checkbox"/> 10.98.0.0/16	tgw-attach-01118378cfe1bd73c	vpc-0577102c2eb4b5892	VPC	Propagated	Active	-
<input type="checkbox"/> 172.18.0.0/16	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-
<input type="checkbox"/> 172.18.26.0/27	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-
<input type="checkbox"/> 172.18.8.0/24	tgw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-

Ambos canales operan bajo un esquema de alta disponibilidad, lo que permite su funcionamiento en configuración activo-activo cuando la arquitectura lo requiere, o como mínimo en un modelo activo-pasivo con conmutación automática (failover) para garantizar que el tránsito del tráfico continúe sin interrupciones ante una caída del enlace principal. El mecanismo de enrutamiento detecta automáticamente pérdidas de conectividad, latencias atípicas o fallos en el Direct Connect, activando de inmediato el túnel VPN como ruta alternativa sin afectar los servicios ni los sistemas que dependen de esta comunicación híbrida.

Esta configuración integrada asegura redundancia, resiliencia y estabilidad en la conectividad entre los sistemas de la Alcaldía y la nube, permitiendo mantener la operación continua de las cargas de trabajo, servicios críticos y procesos institucionales, incluso ante fallos de infraestructura o interrupciones externas. Con ello, se garantiza un modelo de comunicación robusto, seguro y alineado con las buenas prácticas de arquitectura híbrida y los requerimientos establecidos por la entidad.

Documento Anexo: Informe de Estado Direct Connect ACA

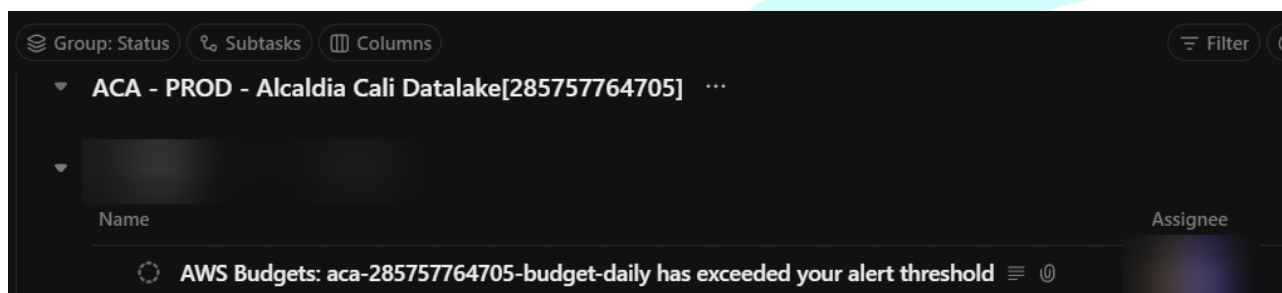
4.8 Monitorear y reportar mensualmente el consumo de la infraestructura (almacenamiento, cómputo, tráfico, etc.), incluyendo recomendaciones de optimización y alertas sobre posibles desviaciones presupuestales, asegurando la eficiencia del uso de los recursos contratados.

Realizamos el monitoreo continuo del consumo de la infraestructura tecnológica y consolidamos esta información en los reportes mensuales de consumo de infraestructura, en los cuales se presenta el uso de recursos de cómputo, almacenamiento, tráfico y servicios asociados. En dichos reportes incluimos el análisis del comportamiento del consumo, recomendaciones de optimización orientadas a la eficiencia en el uso de los recursos, así como alertas tempranas sobre posibles

desviaciones presupuestales, con el fin de apoyar el control, seguimiento y la toma de decisiones por parte de la Alcaldía del Distrito de Santiago de Cali.

Se cuenta con procesos establecidos de gestión financiera operativa que permiten monitorear y optimizar el consumo de la infraestructura en la nube. Estos procesos incluyen el etiquetado (tagging) sistemático de recursos para mantener trazabilidad del gasto por cuenta, entorno o proyecto, facilitando el análisis detallado del uso y los costos asociados.

Con esta información se crean alarmas específicas para cada cuenta en el que se indica y se informa a través de la plataforma de click up cuando un promedio de budget sobrepasa su umbral correspondiente



Estas alarmas se verifican de manera diaria y se da una razón y justificación para el aumento de este costo, y se subsana realizando modificaciones en la alarma si es un nuevo despliegue que se haya realizado o se realizan los ajustes necesarios en el recurso que aumentó su costo para disminuirlo

De igual forma se realizará un informe mensual en el que se registren los costos de cada servicio de ese mes y cualquier tipo de cambio o hallazgo que se deba tener en cuenta para informarlo, junto con su respectiva solución para trazabilidad.

Documento Anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.9 Implementar política de acceso basada en roles (IAM), que permita controlar, limitar y auditar el acceso a los recursos de la nube, conforme a los principios de menor privilegio y segregación de funciones, entregando a la entidad los registros de acceso generados durante la ejecución del contrato.

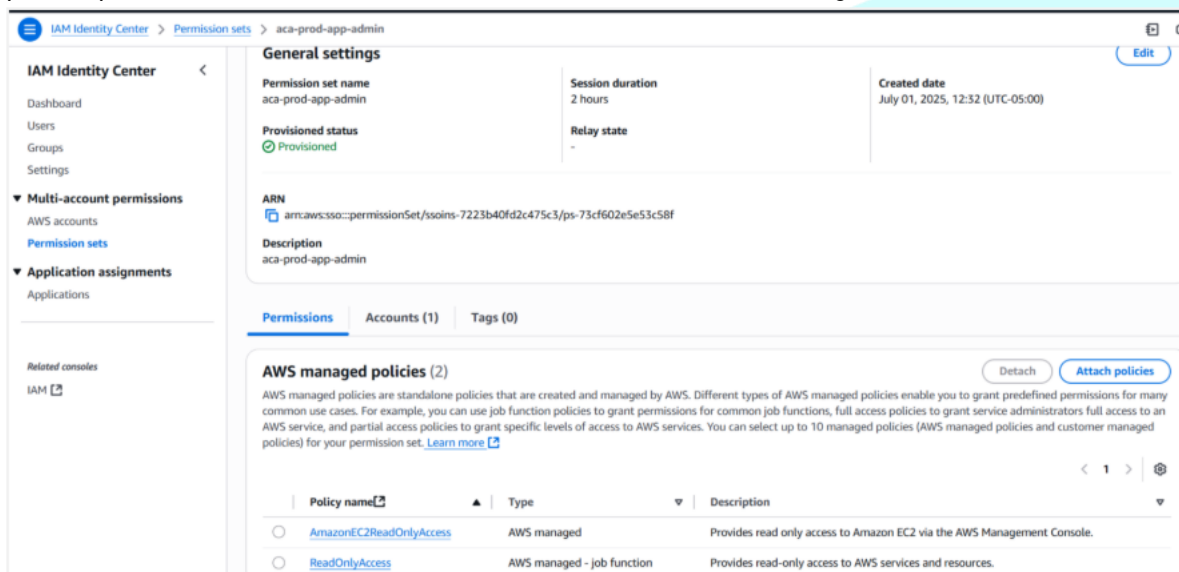
Se cuenta con una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

La gestión de identidades y accesos se realiza mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permite administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

Como parte de la implementación de seguridad en AWS, se configuró un conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

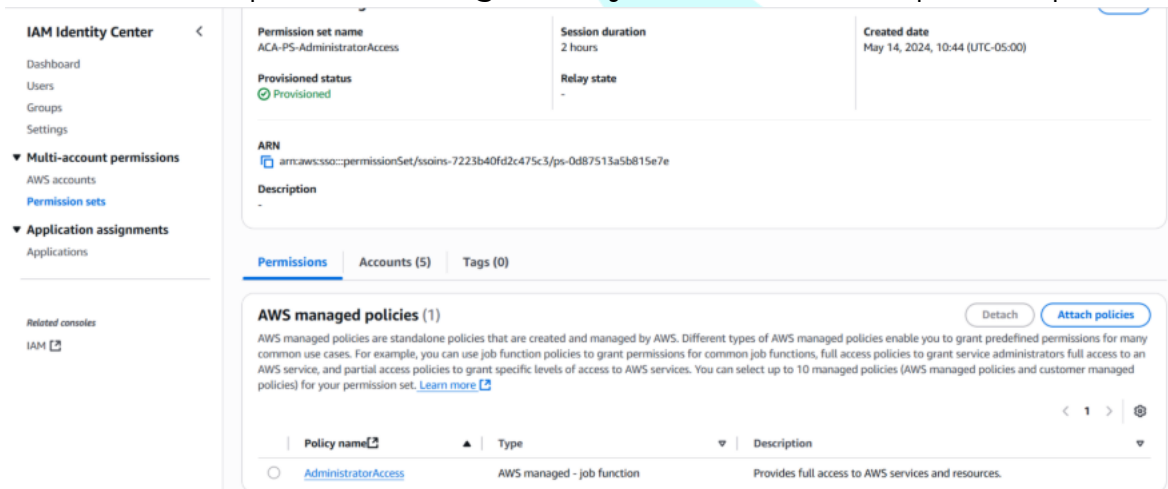
- ACA -AppAdmin

Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD -Workload Alcaldia Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.



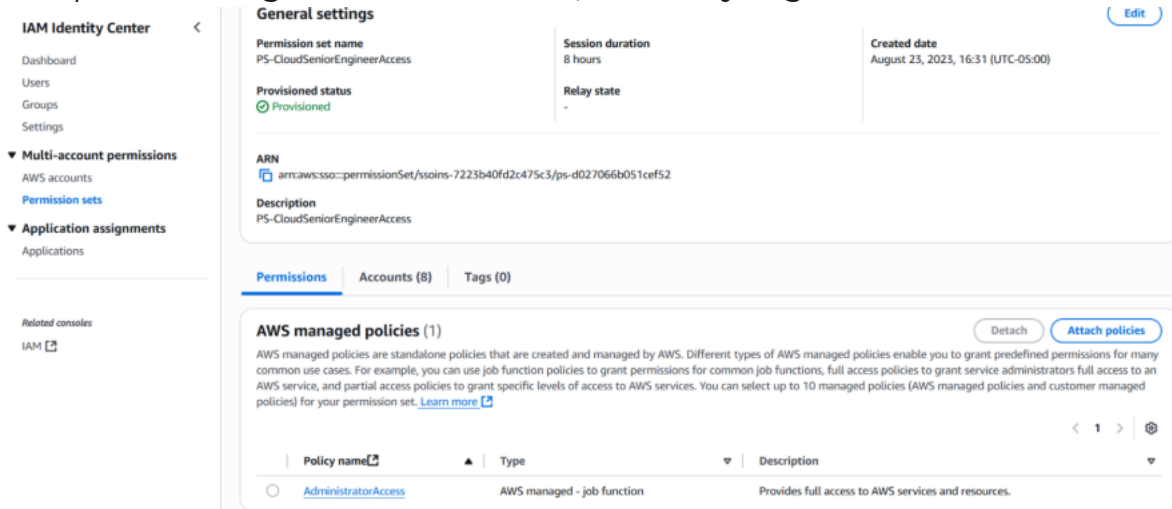
- ACA – CloudAdmin

El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.



- NUVU – CLOUDCloudSeniorEngineer

Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



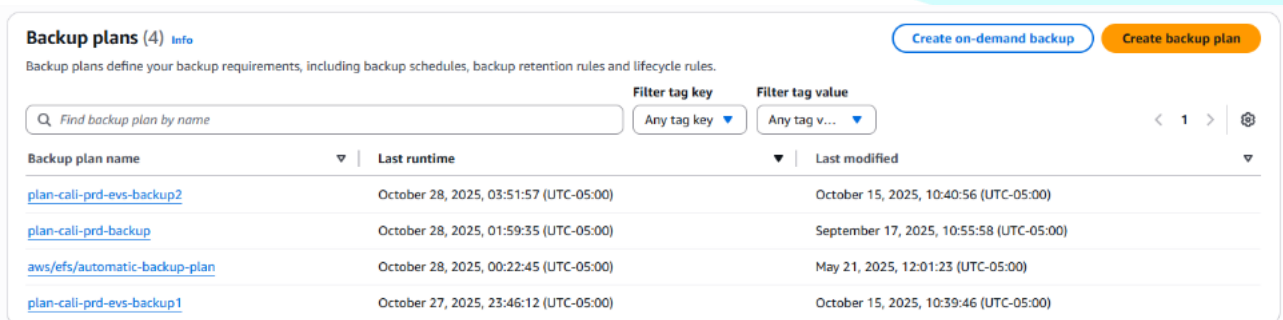
The screenshot shows the AWS IAM console interface for a permission set named 'PS-CloudSeniorEngineerAccess'. The 'General settings' section includes:

- Permission set name:** PS-CloudSeniorEngineerAccess
- Session duration:** 8 hours
- Created date:** August 23, 2023, 16:31 (UTC-05:00)
- Provisioned status:** Provisioned (indicated by a green checkmark)
- Relay state:** -
- ARN:** arn:aws:iam:::permissionSet/ssoins-7223b40fd2c475c3/ps-d027066b051cef52
- Description:** PS-CloudSeniorEngineerAccess

Below the general settings, there are tabs for 'Permissions', 'Accounts (8)', and 'Tags (0)'. The 'Permissions' tab is active, showing 'AWS managed policies (1)'. A table lists the policy 'AdministratorAccess' with the type 'AWS managed - job function' and the description 'Provides full access to AWS services and resources.'.

Documento Anexo: Documentación Infraestructura AWS

4.10 Gestionar y mantener actualizadas las copias de seguridad (backups) de los sistemas, datos y configuraciones relacionados con la solución contratada, en los servicios de almacenamiento y respaldo habilitados en la nube de AWS o equivalentes. Las copias de seguridad deberán incluir mecanismos de recuperación (snapshots, volcados de bases de datos, archivos de configuración, etc.), y se deberá realizar al menos una prueba de restauración por trimestre calendario, dejando constancia de los resultados en un informe técnico que deberá ser entregado a la entidad. Para asegurar la portabilidad de la información, los backups deberán estar disponibles en formato descargable. En el caso de servicios gestionados (máquinas nativas o bases de datos nativas), el contratista deberá garantizar la exportación de los datos (por ejemplo, mediante mysqldump, pg_dump u otro método adecuado) y almacenarlos en Amazon S3 u otro repositorio que permita su descarga directa. Al finalizar el contrato, el contratista deberá entregar la totalidad de las copias de seguridad vigentes en el medio de almacenamiento que disponga la Alcaldía Distrital en su momento, asegurando la integridad, trazabilidad y disponibilidad de la información durante el proceso de entrega.



The screenshot shows the AWS Backup console interface. At the top, there are buttons for 'Create on-demand backup' and 'Create backup plan'. Below this, there is a search bar and filter options for 'Filter tag key' and 'Filter tag value'. A table lists the backup plans:

Backup plan name	Last runtime	Last modified
plan-cali-prd-ews-backup2	October 28, 2025, 03:51:57 (UTC-05:00)	October 15, 2025, 10:40:56 (UTC-05:00)
plan-cali-prd-backup	October 28, 2025, 01:59:35 (UTC-05:00)	September 17, 2025, 10:55:58 (UTC-05:00)
aws/efs/automatic-backup-plan	October 28, 2025, 00:22:45 (UTC-05:00)	May 21, 2025, 12:01:23 (UTC-05:00)
plan-cali-prd-ews-backup1	October 27, 2025, 23:46:12 (UTC-05:00)	October 15, 2025, 10:39:46 (UTC-05:00)

Jobs

In jobs, you can monitor the status and other details of backup, restore, and copy activity.

[Backup jobs](#) | [Restore jobs](#) | [Copy jobs](#)

Backup jobs (306+) Info
Stop backup job Create report Last 14 days ▾

Records of your scheduled or on-demand backups.

302 matches

Status = Completed Clear filters

Backup job ID	Status	Resource name	Message category	Resource ID	Resource type
1DC42716-0627-39C5-546B-02AC4DABD080	Completed	altar	Success	vm/vm-0000478549D2A7FF5	VMware virtual m
7764C3D8-22E9-F143-2366-B4FD4A99E3E8	Completed	SEMNTITAAPPEDPT01	Success	vm/vm-0000694BD1A774B04	VMware virtual m
013BC9AF-6A00-2EC5-D29F-FADADCC00BC7	Completed	nfs-oracderman	Success	vm/vm-000075EC6FD687278	VMware virtual m
FAAA9F52-25A3-820B-B3EE-4322A79BA752	Completed	Contratacion-Portal-DB-ENIATO	Success	vm/vm-00005D95A511843E7	VMware virtual m
6273B6FE-F192-2748-4F1E-386D73C9808F	Completed	GestionDocumental	Success	vm/vm-000051FE935A15DF1	VMware virtual m
912681E4-B1F3-7E77-F3AB-5536EAB0F8F4	Completed	SiCali-DB-QUIMBAYA	Success	vm/vm-000040869ACOFF332	VMware virtual m
ED743C04-E88D-FF62-AE22-2454BCDFC8A3	Completed	CATASTRO-DataQuality-PRD-App-ESTIGIA	Success	vm/vm-00005E54D34CBBC10	VMware virtual m
9C8A27D6-137E-669B-8BFA-A60279C730AB	Completed	Datic Zimbra mail	Success	vm/vm-00005CAFC4F1BC8B4	VMware virtual m
7B2225DA-556A-E4F5-D52A-CE15AE91E083	Completed	Concejo PRE-PRD Procesos y Apache	Success	vm/vm-00004C396D0A783DA	VMware virtual m
69C3DB12-1303-1F99-E731-8C94694C41F7	Completed	calieducadigital_MYSQL2	Success	vm/vm-000059EB390E535D2	VMware virtual m

Actualmente tenemos implementado un sistema robusto de copias de seguridad en AWS Backup que protege toda la infraestructura crítica de la solución contratada.

El sistema cuenta con 4 planes de backup activos que respaldan más de 500 recursos, incluyendo 450 máquinas virtuales, 50+ instancias EC2, volúmenes EBS, sistemas de archivos EFS y buckets S3. Todos los backups se almacenan en 4 vaults configurados con cifrado KMS y políticas de retención apropiadas.

El vault principal "vault-cali-prd-backup" contiene 3,429 puntos de recuperación y está configurado con bloqueo de seguridad. Las ejecuciones son diarias y automáticas.

Los sistemas respaldados incluyen todas las bases de datos críticas (PostgreSQL, Oracle, MySQL), servidores de aplicaciones (GlassFish, Wildfly), sistemas de gestión documental, infraestructura de red, servidores de correo Zimbra, y sistemas ERP y catastro.

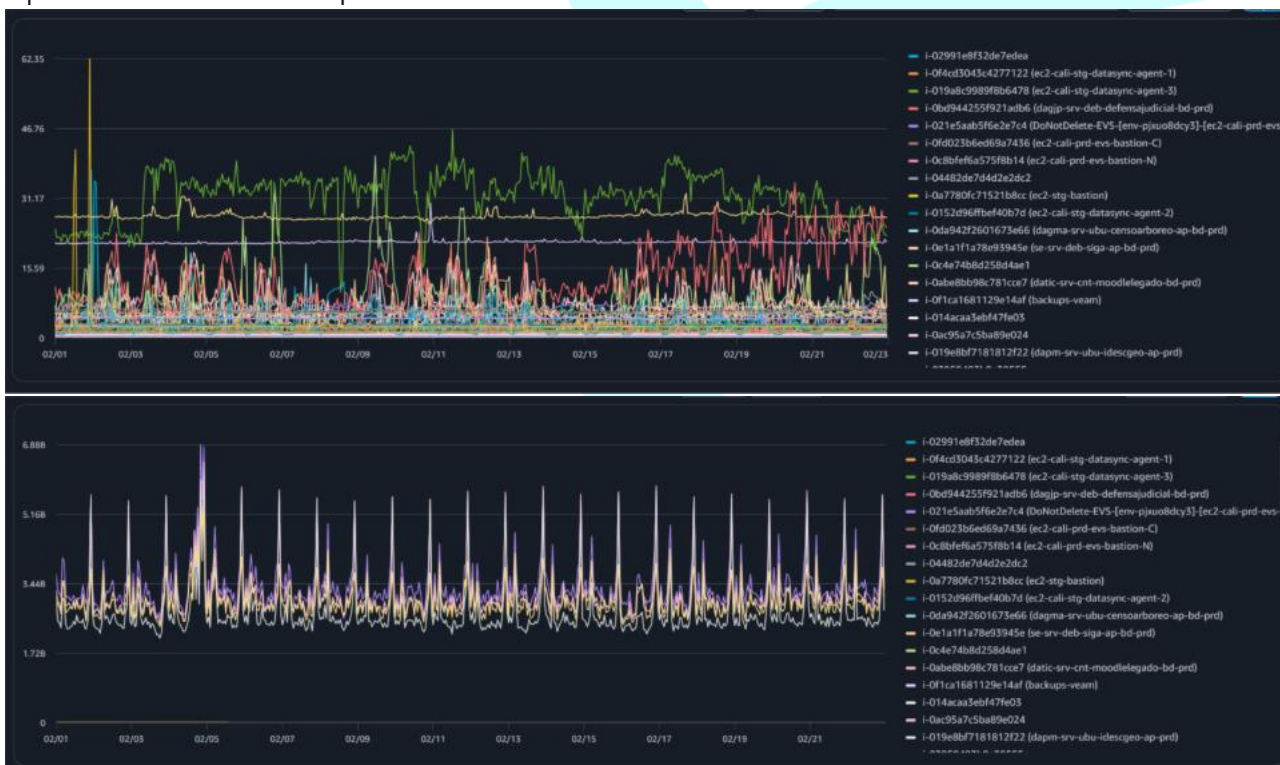
En casos de restauración se ha realizado para la máquina datic-srv-win-directorioactivo-gt-prd para la cual se solicitó una eliminación a través del portal de la mesa de servicio de Blend y posteriormente una restauración a través del mismo servicio a una copia que se tenía gracias a los planes de backup que se encuentran activos



Documento Anexo: Documentación Infraestructura AWS

4.11 Garantizar la disponibilidad de herramientas digitales de administración y gestión de las soluciones tecnológicas desarrolladas, que cuente con acceso a la infraestructura subyacente, permitiendo el monitoreo de todos los servicios de virtualización.

La disponibilidad y gestión de las soluciones tecnológicas desarrolladas se garantizan mediante el uso de herramientas nativas de AWS, principalmente a través de Amazon CloudWatch, que permite el monitoreo continuo de la infraestructura subyacente y de los servicios de virtualización. Esta herramienta proporciona visibilidad en tiempo real del rendimiento, uso de recursos y estado operativo de los componentes.



Métricas medidas para todos los recursos que se creen en aws a través del cliente de cloudwatch:

1. CPU Utilization: Porcentaje de capacidad de procesamiento de la instancia que se está utilizando. Un valor consistentemente alto indica que el servidor está bajo una carga de trabajo pesada.

2. **StatusCheckFailed:** Indicador general de que la instancia ha fallado una verificación automática de estado, requiriendo atención.
3. **StatusCheckFailed_Instance:** Falla a nivel de software o sistema operativo (ej., la aplicación no responde).
4. **StatusCheckFailed_System:** Falla detectada por AWS en el hardware físico subyacente, lo que normalmente requiere una recuperación automática o manual de la instancia.
5. **DiskReadBytes:** Cantidad de datos (en bytes) que la instancia lee desde sus discos. Alto volumen indica una intensa actividad de lectura de información.
6. **DiskWriteBytes:** Cantidad de datos (en bytes) que la instancia escribe en sus discos. Alto volumen indica una intensa actividad de guardado o modificación de archivos.
7. **DiskReadOps:** Número de operaciones de lectura individuales que la instancia solicita a sus discos. Muchas operaciones pueden ser demandantes incluso si el volumen de datos es bajo.
8. **DiskWriteOps:** Número de operaciones de escritura individuales que la instancia realiza en sus discos. Un recuento elevado es común en sistemas con bases de datos activas.
9. **NetworkIn:** Volumen total de datos (en bytes) que la instancia recibe desde la red.
10. **NetworkOut:** Volumen total de datos (en bytes) que la instancia envía a la red. Estas dos métricas reflejan el tráfico total de su aplicación.
11. **NetworkPacketsIn:** Número de paquetes de datos individuales que la instancia recibe. Un número muy alto puede consumir recursos de CPU.
12. **NetworkPacketsOut:** Número de paquetes de datos individuales que la instancia envía. Es útil para diagnosticar problemas de rendimiento de red o aplicaciones con mucho "chateo" (pequeñas comunicaciones frecuentes).

Documento Anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.12 Realizar la gestión del proyecto, asegurando la planificación y el seguimiento adecuado de la ejecución del contrato

Realizamos la gestión del proyecto, asegurando la adecuada planificación y el seguimiento de la ejecución del contrato. Para ello, elaboramos un plan de trabajo en el cual se definieron las actividades a ejecutar y llevamos a cabo un seguimiento continuo y coordinado con el cliente a las solicitudes y requerimientos presentados. Adicionalmente, compartimos de manera periódica los reportes mensuales de avance, los cuales permitieron evidenciar el estado de la ejecución del contrato, los avances realizados y el apoyo brindado ante cualquier requerimiento técnico u operativo, garantizando así el cumplimiento de los objetivos contractuales.

Documento Anexo: Plan de trabajo

4.13 Llevar a cabo la transferencia de conocimiento dirigida a los colaboradores de la Alcaldía de Santiago de Cali sobre el funcionamiento, uso y administración de las soluciones tecnológicas desarrolladas.

En cumplimiento de la obligación de realizar la transferencia de conocimiento, se lleva a cabo un proceso estructurado de capacitación dirigido a los colaboradores de la Alcaldía de Santiago de Cali, enfocado en el funcionamiento, uso, buenas prácticas y administración de las soluciones tecnológicas implementadas en la infraestructura de virtualización y servicios cloud. Como parte de este proceso, se realizó un Workshop técnico presencial, desarrollado en conjunto entre AWS y Blend360, en el cual se presentaron los conceptos clave necesarios para que el equipo de la Alcaldía pueda operar, administrar y comprender adecuadamente los servicios utilizados.

Durante la sesión, se utilizó la presentación oficial del workshop, en la cual se abordaron los siguientes módulos fundamentales del ecosistema AWS:

Visión General de Servicios AWS

Se explicó la estructura global y regional de AWS, sus tipos de servicios y cómo se distribuyen entre componentes globales (IAM, Route 53, CloudFront, WAF) y regionales (EC2, RDS, S3, Lambda, entre otros).

EC2 – Elastic Compute Cloud

- Concepto de servidores virtuales escalables.
- Creación y configuración de instancias.
- AMI, Security Groups, Key Pairs y consideraciones de seguridad.
- Cómo escalar en función de la demanda.

VPC – Virtual Private Cloud

- Funcionamiento de redes virtualizadas en AWS.
- Subredes públicas y privadas.
- Internet Gateway, tablas de enrutamiento y conectividad.
- Aislamiento, segmentación y control del tráfico.

IAM – Identity and Access Management

- Gestión centralizada de usuarios y roles.
- Principio de mínimo privilegio.
- Buenas prácticas de seguridad.

S3 – Simple Storage Service

- Concepto de almacenamiento global/regional.
- Buckets, objetos y nomenclatura global.
- Usos, integración y políticas.

Práctica Guiada en la Consola AWS

- Acceso seguro al entorno del workshop.
- Ejercicios prácticos en EC2, IAM, VPC y S3.
- Validación de configuración y despliegue.



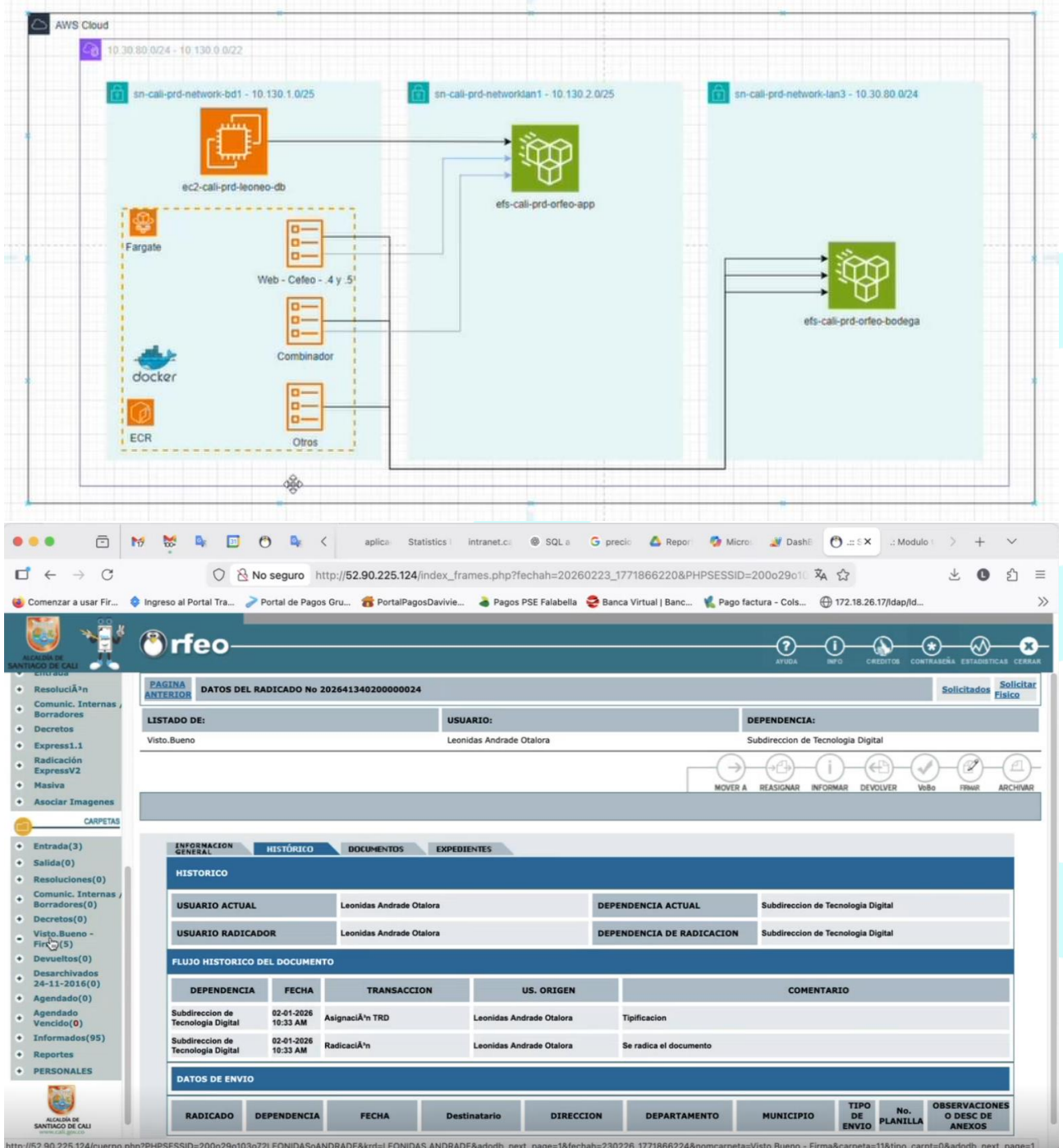
Se realizó la transferencia de conocimiento al equipo de la Alcaldía de Santiago de Cali mediante un workshop técnico desarrollado conjuntamente con AWS y Blend360. Durante la sesión se abordaron los servicios fundamentales utilizados en la solución,

incluyendo EC2, VPC, IAM y S3, así como la arquitectura de servicios regionales y globales. La capacitación permitió fortalecer las capacidades del personal en el uso, operación y administración de la infraestructura cloud, brindando herramientas prácticas y conceptuales para garantizar la adecuada gestión de los servicios implementados. La presentación oficial del workshop fue utilizada como soporte del proceso formativo.

Documento Anexo: Reporte Capacitación ACA

4.14 Prestar el servicio especializado para la implementación de las soluciones tecnológicas, durante la vigencia del contrato.

Como parte de esta obligación contractual, durante la vigencia de esta cuota del contrato se ha brindado acompañamiento técnico y operativo en las iniciativas de modernización de infraestructura en AWS definidas por la Alcaldía de Santiago de Cali. Como parte de esta actividad, se han avanzado en la modernización del sistema Orfeo, la modernización del Portal Municipal de la Alcaldía, así como en el despliegue de ecosistemas digitales, asegurando que las soluciones a modernizar se encuentren alineadas con los lineamientos técnicos, de seguridad y de operación establecidos, y contribuyan a la mejora de la disponibilidad, escalabilidad y sostenibilidad de la infraestructura tecnológica de la entidad.



The screenshot displays an AWS Cloud environment with three Availability Zones. The first zone (sn-cali-prd-network-bd1) contains an Amazon EC2 instance (ec2-cali-prd-leoneo-db) and a VPC. The second zone (sn-cali-prd-networklan1) contains an Amazon EFS instance (efs-cali-prd-orfeo-app). The third zone (sn-cali-prd-network-lan3) contains another Amazon EFS instance (efs-cali-prd-orfeo-bodega). A VPC peering connection links the first two zones. Below the AWS console, a web browser shows the 'rfeo' application interface. The page title is 'DATOS DEL RADICADO No 20264134020000024'. The interface includes a navigation menu on the left, a top navigation bar with 'rfeo' logo and user profile, and a main content area with tabs for 'INFORMACION GENERAL', 'HISTORICO', 'DOCUMENTOS', and 'EXPEDIENTES'. The 'HISTORICO' tab is active, showing a table of document history.

DEPENDENCIA	FECHA	TRANSACCION	US. ORIGEN	COMENTARIO
Subdireccion de Tecnologia Digital	02-01-2026 10:33 AM	Asignaci3n TRD	Leonidas Andrade Otalora	Tipificacion
Subdireccion de Tecnologia Digital	02-01-2026 10:33 AM	Radicaci3n	Leonidas Andrade Otalora	Se radica el documento

4.15 Cumplir con las 3reas principales del modelo de computaci3n en los servicios digitales, como lo son: despliegue de servicios, orquestaci3n de servicios, administraci3n de los servicios digitales, privacidad y seguridad. Lo anterior en concordancia con lo establecido en la Gu3a T3cnica de Computaci3n en la nube de MinTIC y las versiones que lo modifiquen.

En cumplimiento de lo establecido en la Gu3a T3cnica de Computaci3n en la Nube del MinTIC, se garantiza que la soluci3n implementada opera bajo las 3reas fundamentales del modelo de computaci3n aplicable a los servicios digitales de la entidad. Para ello, se ejecutan procesos estructurados de despliegue, orquestaci3n, administraci3n,

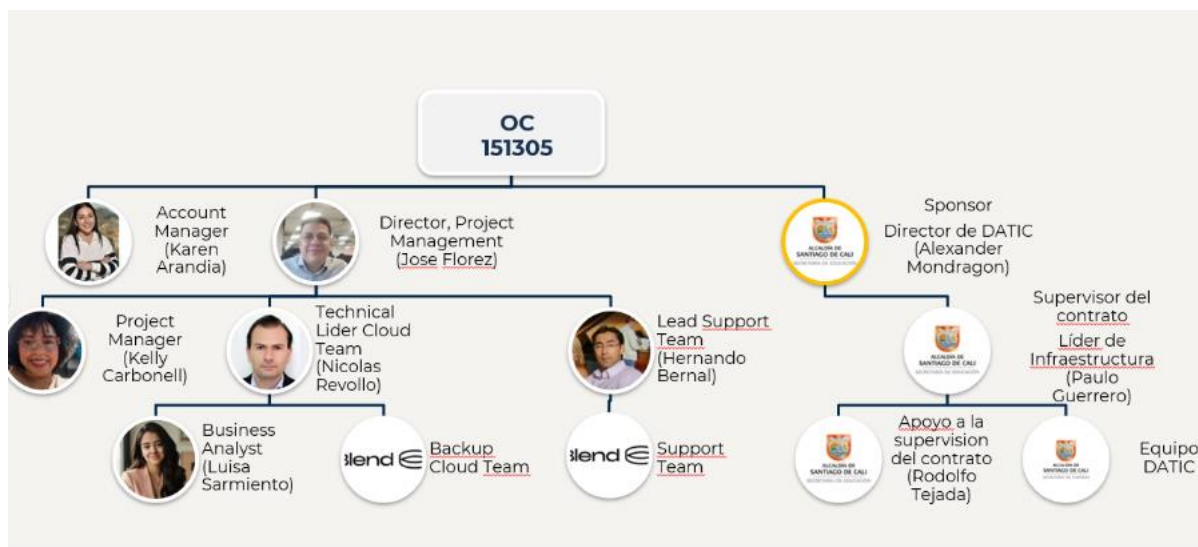
privacidad y seguridad, asegurando que cada uno de estos componentes se integre de manera coherente dentro de la infraestructura tecnológica de la Alcaldía de Santiago de Cali. El despliegue de los servicios se realiza a través de procedimientos estandarizados que permiten implementar máquinas virtuales, configuraciones de red y servicios complementarios de forma consistente, utilizando plantillas, configuraciones predefinidas y mecanismos que aseguran uniformidad, trazabilidad y estabilidad operativa. Paralelamente, la orquestación de los servicios permite coordinar los distintos recursos de cómputo, red y almacenamiento, integrando la automatización de tareas, el escalamiento de recursos según la demanda, la operación asincrónica y la comunicación segura entre los distintos componentes, garantizando así un funcionamiento unificado y eficiente de los servicios digitales. El proceso de administración se desarrolla de manera continua mediante actividades de supervisión, monitoreo, mantenimiento, gestión de incidencias y optimización, asegurando el rendimiento, la disponibilidad y la estabilidad de la infraestructura. Esto incluye el seguimiento permanente de métricas críticas, la aplicación de ajustes preventivos y correctivos, la operación ininterrumpida de los servicios virtualizados y la gestión completa del ciclo de vida de los recursos. En materia de privacidad, se aplica un tratamiento responsable de la información mediante controles de acceso basados en el principio de mínimo privilegio, segmentación de redes, cifrado en tránsito y en reposo, y mecanismos que aseguran que los datos sensibles se mantengan protegidos durante todo su ciclo de uso. Finalmente, la seguridad se garantiza a través de políticas de control, firewalls, monitoreo de eventos, prácticas de fortalecimiento de sistemas, rutas seguras de comunicación y medidas que protegen la integridad, disponibilidad y confidencialidad de los servicios digitales. Todo lo anterior asegura que la infraestructura y los servicios implementados se encuentren alineados con los lineamientos, principios y estándares definidos por el MinTIC, cumpliendo con las mejores prácticas nacionales para la prestación segura, confiable y eficiente de servicios digitales en entornos de computación en la nube.

Documento Anexo: Servicios de AWS Para el Cumplimiento de Modelos de Computación y Estándares Normativos (ACA)

4.16 Designar un delegado para participar en las mesas de trabajo establecidas por el supervisor del contrato y atender las medidas que allí sean tomadas con el fin de soportar los requerimientos y que los mismo se lleven a cabo de manera articulada.

En cumplimiento de esta disposición, se designa formalmente a la Gerente de Proyectos Kelly Carbonell Ramos como representante responsable de participar en las mesas de trabajo convocadas por el supervisor del contrato. Esta designación se encuentra establecida dentro del plan de trabajo y garantiza la articulación permanente entre las decisiones adoptadas en dichas sesiones y la ejecución técnica y operativa del proyecto. La delegada asiste de manera activa a los espacios definidos, atiende las directrices impartidas por el supervisor y asegura que cada medida, requerimiento o ajuste acordado sea incorporado oportunamente dentro del desarrollo de las actividades. Adicionalmente, el proyecto cuenta con un equipo técnico de apoyo que respalda la gestión de la Gerente de Proyectos, permitiendo una correcta interpretación de los requerimientos, una respuesta oportuna a las necesidades planteadas y una ejecución articulada entre la coordinación, la operación y los frentes técnicos involucrados. Este

esquema de trabajo garantiza la trazabilidad de las decisiones, la alineación entre las partes y el cumplimiento eficiente de los objetivos del contrato.



4.17 Elaborar, suscribir y presentar al Distrito de Santiago de Cali - Departamento Administrativo de Tecnologías de la Información y las Comunicaciones las respectivas actas e informes correspondientes a la ejecución de la contratación. Estos documentos deberán ser aprobados por el Supervisor del Contrato.

En cumplimiento de lo establecido para la adecuada ejecución contractual, se elaboran y presentan al Distrito de Santiago de Cali – Departamento Administrativo de Tecnologías de la Información y las Comunicaciones los informes de ejecución mensual, en los cuales se documenta de manera detallada el avance del proyecto y el cumplimiento de las obligaciones a cargo del contratista. Estos informes se generan con la periodicidad definida en los estudios previos y en el plan de trabajo, es decir, de forma mensual, consolidando las actividades realizadas, los resultados obtenidos, la trazabilidad de los entregables y los soportes correspondientes. Cada informe es remitido al Supervisor del Contrato para su revisión y aprobación, asegurando transparencia, seguimiento oportuno y alineación con los objetivos técnicos y administrativos establecidos por la entidad.

Documento Anexo: Informes de ejecución mensual

4.18 Dar cumplimiento a la normatividad de protección de datos personales y de confidencialidad de la información, donde garantice una adecuada definición de los niveles de seguridad para no generar accesos no autorizados a datos confidenciales de propiedad de la Entidad.

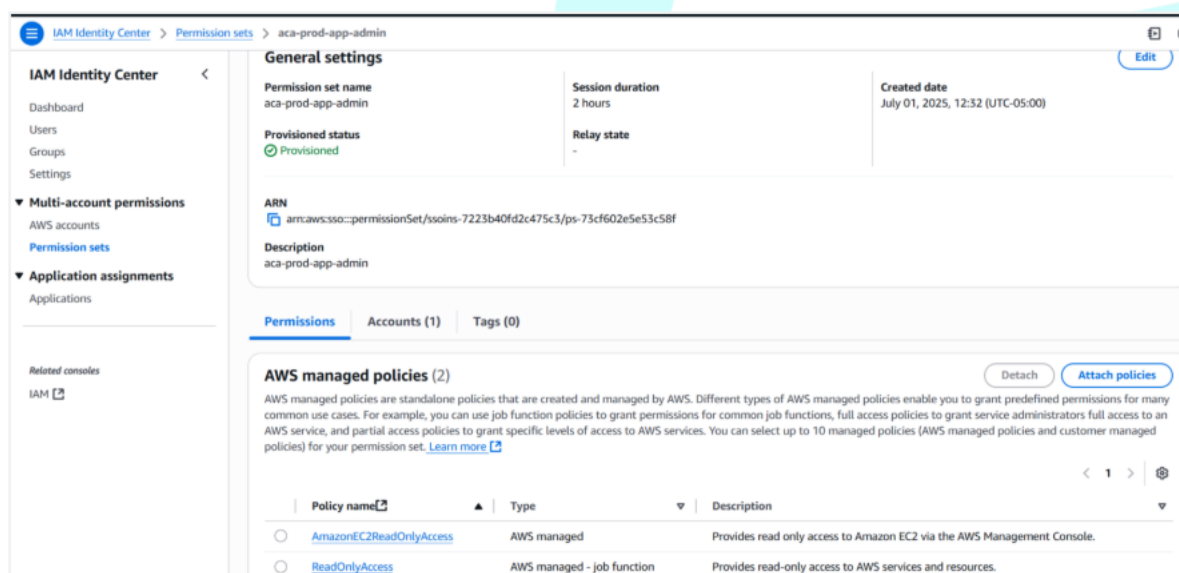
Se cuenta con una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

La gestión de identidades y accesos se realiza mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permite administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

Como parte de la implementación de seguridad en AWS, se configuró un conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

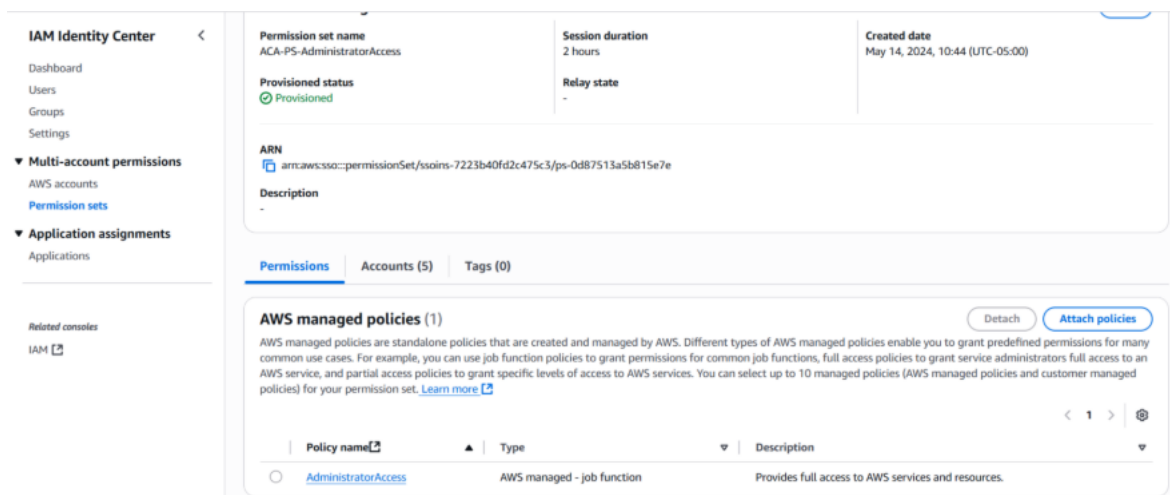
- ACA -AppAdmin

Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD - Workload Alcaldia Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.



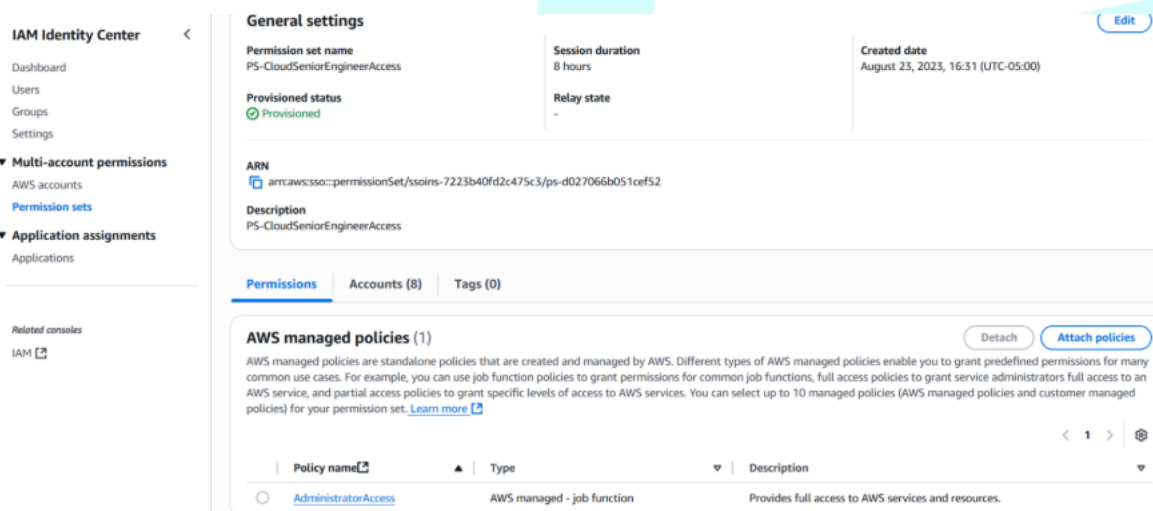
- ACA – CloudAdmin

El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.



- NUVU – CLOUDCloudSeniorEngineer

Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



Documento Anexo: Informe de Políticas de Acceso Para la Organización de ACA

4.19 Garantizar que siempre la Entidad tendrá la propiedad y el control de su información, así como disponible un mecanismo para el borrado seguro de los datos, si llegare a ocurrir una terminación anticipada, según el modelo computacional.

En cumplimiento de esta disposición, se garantiza que la Entidad mantiene en todo momento la propiedad, titularidad y control absoluto sobre toda su información, independientemente de que los datos se encuentren procesados, almacenados o respaldados dentro de los servicios de AWS. Toda la arquitectura y operación de la infraestructura se implementa respetando este principio, asegurando que el acceso,

tratamiento, administración y gestión de los datos se realiza exclusivamente bajo las directrices y autorizaciones de la Entidad. Con el fin de reforzar este control y asegurar la disponibilidad, integridad y recuperación de la información institucional, se implementa una política robusta de respaldos que forma parte del modelo computacional aplicado en la nube. Esta estrategia se encuentra configurada en AWS mediante el plan plan-cali-prd-backup, el cual administra los respaldos a través del vault vault-cali-prd-backup y se ejecuta mediante el rol IAM role-cali-prd-backup, asegurando que todas las copias de seguridad se generen de manera automatizada, controlada y sin intervención de terceros no autorizados.

plan-cali-prd-backup

[Delete](#) [View JSON](#)

Summary

Backup plan name plan-cali-prd-backup	Version ID Zjk2MWY2MGUtMmYxNi00O DhhLWJiM2EtZTFhNTJlYTAzY Tgy	Last modified July 30, 2025, 10:00:50 (UTC-05:00)	Last runtime September 12, 2025, 01:15:07 (UTC-05:00)
Backup plan ID e17d35df-91fd-4391-9311-33ac5c855379			

vault-cali-prd-backup Info

[Manage vault lock](#) [Delete vault](#) [Edit access policy](#)

Summary

Vault name vault-cali-prd-backup	KMS encryption key ID [Redacted]	Vault lock 🔒 Locked – Governance mode Vault lock is editable. Learn more
Vault type Backup vault	Creation date June 26, 2025, 14:48:16 (UTC-05:00)	Retention period for vault lock Minimum retention period: 6 days Maximum retention period: –
Vault ARN 📄 arn:aws:backup:us-east-1:363934983054:backup-vault:vault-cali-prd-backup		

Backup rules (4)

Backup rules specify the backup schedule, backup window, and lifecycle rules.

[Edit](#) [Delete](#) [Add backup rule](#)

Name	Backup vault	Destination Backup vault
DailyBackup-15DayRetention	vault-cali-prd-backup	-
MonthlyBackup-1YearRetention	vault-cali-prd-backup	-
WeeklyBackup-1MonthRetention	vault-cali-prd-backup	-
YearlyBackup-20YearRetention	vault-cali-prd-backup	-

La política incluye ciclos de retención diarios, semanales, mensuales y anuales, con períodos que van desde 15 días hasta 20 años, y contempla la transición automática a almacenamiento frío según corresponda, optimizando costos sin comprometer la disponibilidad ni la trazabilidad de los respaldos. Los recursos sujetos a esta estrategia son identificados mediante la etiqueta “Backup – Enabled”, lo que permite garantizar una administración ordenada y consistente del proceso de protección de datos. Esta estructura de respaldos no solo respalda la continuidad operativa, sino que también constituye un mecanismo seguro de preservación y restauración de información, permitiendo atender incidentes, garantizar cumplimiento normativo y mantener la integridad de los datos institucionales.

De igual forma, y en concordancia con el modelo computacional adoptado, se dispone de un mecanismo de borrado seguro para el caso en que se presente una terminación

anticipada del contrato. Este mecanismo asegura que, una vez la Entidad lo solicite, toda la información almacenada en los servicios de AWS pueda ser eliminada de manera definitiva mediante procedimientos certificados que imposibilitan su recuperación posterior, salvaguardando así la confidencialidad y los derechos de propiedad de la Entidad sobre su información. Con esta combinación de control, respaldo y eliminación segura, se garantiza el manejo responsable de los datos durante toda la vigencia contractual y después de su finalización, manteniendo siempre la soberanía y protección de los activos de información de la Alcaldía de Santiago de Cali.

4.20 Entregar los códigos, manuales, tutoriales y/o instructivos asociados a las soluciones tecnológicas brindadas. También debe entregar los accesos a los aplicativos y a herramientas de monitoreo para acceder por parte del personal de DATIC.

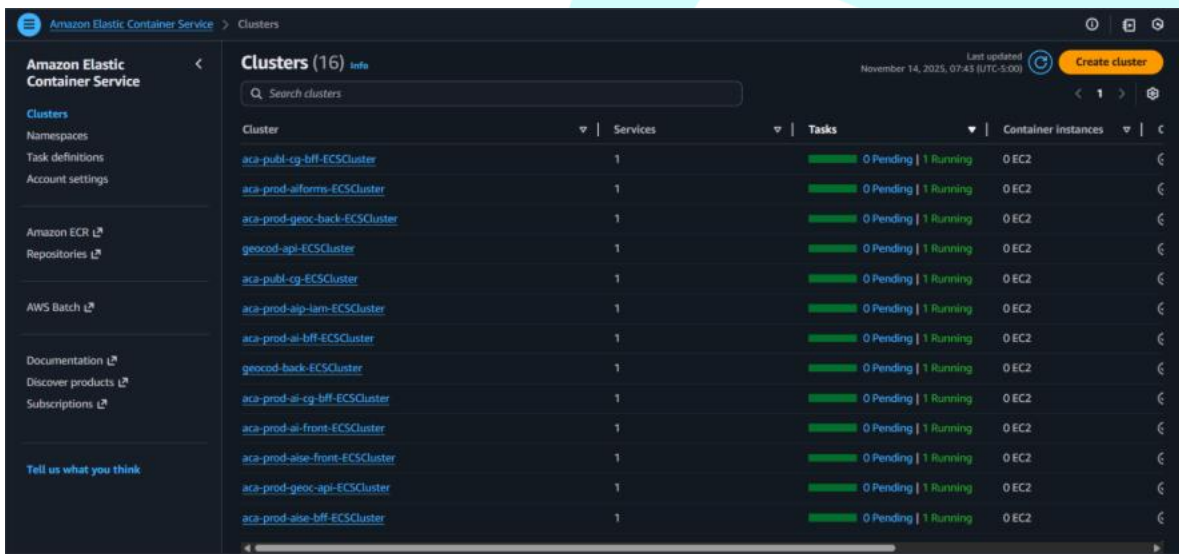
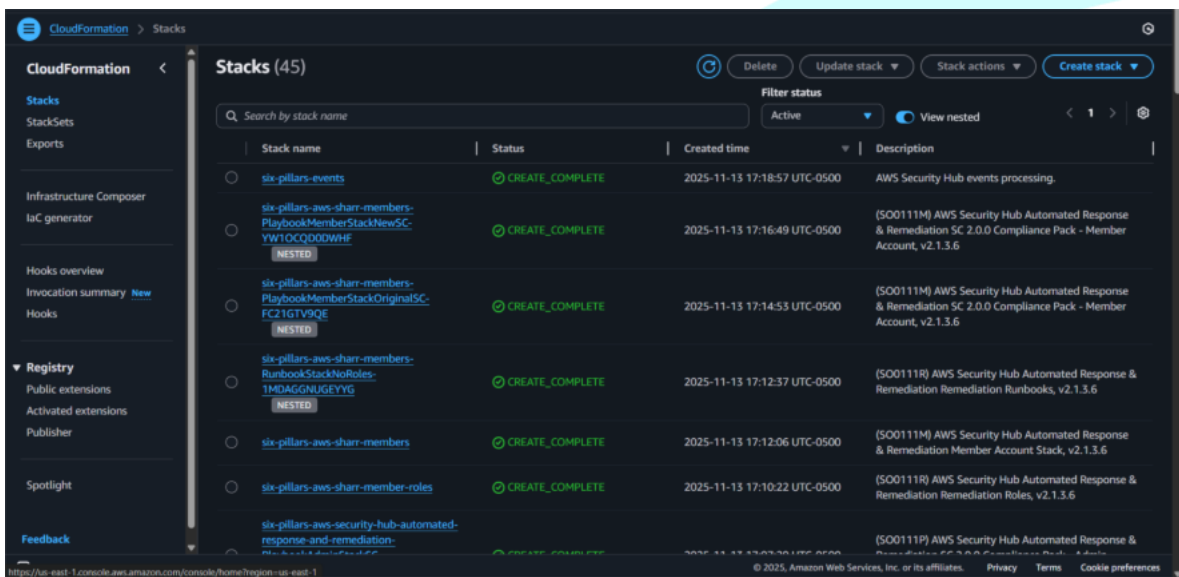
En el marco del cumplimiento de la obligación consistente en entregar los códigos, manuales, tutoriales y/o instructivos asociados a las soluciones tecnológicas brindadas, así como los accesos a los aplicativos y a las herramientas de monitoreo para el personal de DATIC, actualmente se encuentran en ejecución las actividades asociadas a la modernización del sistema Orfeo, del Portal Municipal de la Alcaldía y al despliegue de ecosistemas digitales.

Estas actividades se desarrollan con el objetivo de asegurar que las soluciones tecnológicas a intervenir se alineen progresivamente con los lineamientos técnicos, de seguridad y de operación establecidos por la Entidad, y que contribuyan a la mejora de la disponibilidad, escalabilidad y sostenibilidad de la infraestructura tecnológica institucional. A medida que se consoliden los avances, se realizará la entrega gradual de los documentos, códigos, manuales y accesos correspondientes, como soporte del cumplimiento de la obligación contractual.

4.21 Garantizar que los servicios a proveer cumplan con estándares de calidad con las normas vigentes relativas al servicio la infraestructura digital, ISO 9901-ISO 27001 –ISO 27017 –ISO27018 – SOC1 –SOC2 – SOC3 –CSA -FEDRAMP.

En la prestación de los servicios se garantiza que toda la infraestructura y los componentes tecnológicos implementados cumplen con los estándares internacionales de calidad y seguridad definidos para servicios digitales y entornos de computación en la nube, incluyendo ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, CSA y FEDRAMP. Este cumplimiento se respalda en la adopción de servicios nativos de AWS que han sido diseñados para operar bajo estos marcos normativos y cuyo funcionamiento, certificaciones y controles se encuentran plenamente alineados con las mejores prácticas globales. Tal como se describe en el documento de referencia, los servicios utilizados para despliegue, orquestación, administración, privacidad y seguridad entre ellos CloudFormation, ECS, EC2, Lambda, Organizations, Control Tower, CloudWatch, CloudTrail, Systems Manager, Config, Trusted Advisor, IAM, IAM Identity Center, KMS, ACM, WAF, GuardDuty y Shield permiten asegurar que la infraestructura funciona bajo políticas estrictas de gobierno, protección, auditoría, cifrado, autenticación y gestión de incidentes, cumpliendo así los lineamientos establecidos por los estándares normativos mencionados.

La arquitectura desplegada incorpora controles técnicos y procedimentales que garantizan la protección de los datos, la segregación de funciones, la trazabilidad, la privacidad, la gestión segura de identidades, el cumplimiento de políticas de seguridad y el aseguramiento de ambientes operativos confiables, todo dentro del marco de certificaciones globales que AWS mantiene permanentemente auditadas. De esta manera, los servicios provistos no solo se ajustan a las normas vigentes aplicables a la infraestructura digital de la Entidad, sino que operan bajo un modelo de cumplimiento sustentado, verificable y acorde a los estándares internacionales más exigentes, asegurando la calidad, integridad y seguridad del servicio durante toda la vigencia del contrato.



Documento Anexo: Servicios de AWS Para el Cumplimiento de Modelos de Computación y Estándares Normativos (ACA)

4.22 Atender las sugerencias que el Distrito de Santiago de Cali - Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones, considere convenientes y pertinentes para la ejecución del objeto del contrato.

En el marco de la ejecución del contrato se atienden de manera oportuna, integral y continua todas las sugerencias, recomendaciones y solicitudes emitidas por el Distrito de Santiago de Cali, a través del Departamento Administrativo de Tecnologías de la Información y las Comunicaciones, garantizando que cada requerimiento planteado sea incorporado y gestionado dentro del ciclo operativo de la infraestructura tecnológica. Este proceso se desarrolla mediante la mesa de servicios y el uso de la plataforma Service Center, en la cual se registran las solicitudes que la entidad considera pertinentes para fortalecer, ajustar o validar aspectos relacionados con la operación del entorno cloud y los servicios implementados. Tal como se evidencia en el Informe Mensual de Casos correspondiente al mes, durante dicho periodo se procesaron múltiples solicitudes asociadas a ajustes de infraestructura de red, validaciones de seguridad, configuración de recursos, despliegue de instancias, actualizaciones de reglas de seguridad y verificación de conectividad, todas ellas derivadas de necesidades y sugerencias planteadas por los equipos de DATIC.

Cada una de estas solicitudes fue analizada y gestionada conforme a su criticidad y prioridad, registrando avances, resultados y estados de cierre que demuestran la atención efectiva de las recomendaciones realizadas por la entidad. De acuerdo con el informe, todas las solicitudes presentadas durante el periodo fueron gestionadas adecuadamente y culminaron en su correcta implementación o resolución, evidenciando una respuesta alineada con las directrices de la entidad y una integración permanente entre los equipos técnicos de Blend360 y DATIC. Este proceso de atención continúa asegura que cualquier sugerencia relacionada con ajustes, mejoras, validaciones, fortalecimiento de seguridad o necesidades operativas sea incorporada de inmediato en la ejecución contractual, permitiendo una operación articulada, coherente y plenamente alineada con los objetivos estratégicos y técnicos definidos por la Alcaldía de Santiago de Cali.

En el desarrollo del contrato se atienden de manera oportuna todas las sugerencias, recomendaciones y observaciones que el Distrito de Santiago de Cali, a través del Departamento Administrativo de Tecnologías de la Información y las Comunicaciones, considera pertinentes para la correcta ejecución del objeto contractual. Cada indicación emitida por el supervisor o por los equipos técnicos de la Entidad es analizada, incorporada y gestionada dentro del proceso operativo, asegurando que las actividades, entregables y ajustes necesarios se realicen de forma articulada y alineada con las necesidades institucionales. Este mecanismo de respuesta permanente garantiza que el proyecto se mantenga en coherencia con los lineamientos estratégicos de DATIC, facilite la mejora continua de las soluciones implementadas y permita que las decisiones tomadas en conjunto fortalezcan la calidad, funcionalidad y alcance de los servicios entregados.

Documento Anexo: ACA - Informe de Mensual de Casos

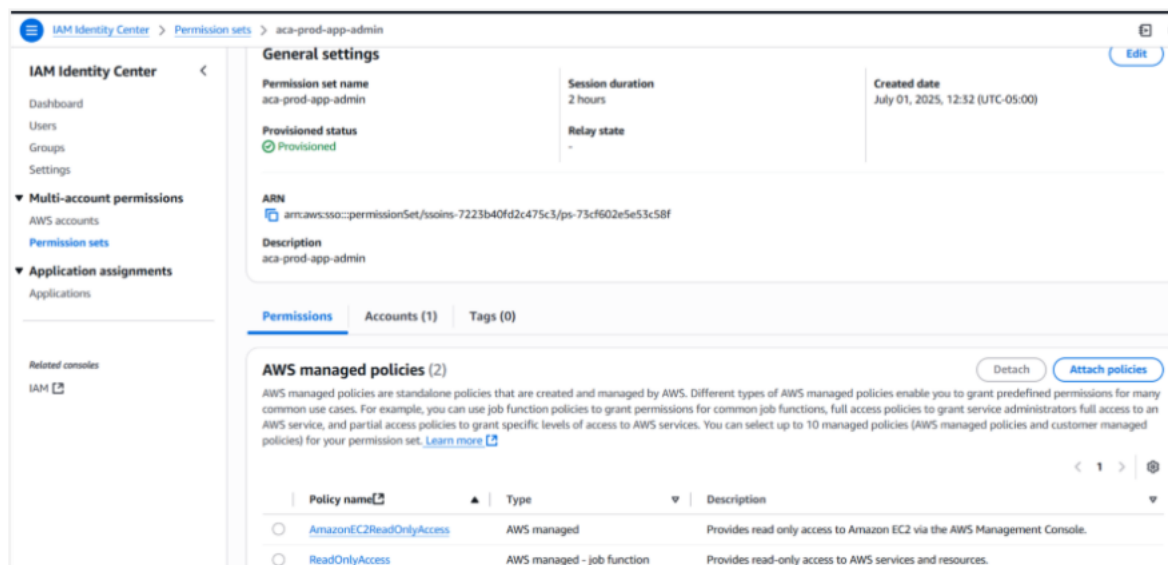
4.23 Asegurar el manejo del acceso a las soluciones tecnológicas, con el fin de evitar manejos múltiples de administradores y así evitar fraudes y robos de información, migración de datos e información, actualizaciones de aplicaciones personales, aplicaciones adicionales y gestión de sus datos personales

Para asegurar el manejo adecuado del acceso a las soluciones tecnológicas y evitar múltiples administradores, fraudes, robos de información, migraciones no autorizadas de datos, instalación de aplicaciones personales o manipulación indebida de información institucional, se implementa un modelo de control de accesos basado en políticas estrictas, roles claramente delimitados y el principio de mínimo privilegio. Conforme a las políticas de acceso definidas para la organización, la administración del entorno se realiza mediante grupos, perfiles y permisos configurados en AWS Identity Center, garantizando que cada usuario cuente únicamente con las capacidades estrictamente necesarias para sus funciones. El documento de políticas de acceso consolida esta estructura, detallando los grupos disponibles y sus responsabilidades: el rol ACA-AppAdmin, destinado a funcionarios de la Alcaldía y Nexura, permite únicamente permisos de lectura sobre aplicaciones y recursos EC2 en la cuenta de producción, evitando cualquier tipo de modificación directa; el grupo ACA-CloudAdmin, asignado a personal de DATIC, otorga capacidades de administración controlada sobre cuentas específicas, manteniendo restricciones explícitas sobre los ambientes sensibles, como la cuenta de producción del proceso de migración; y el grupo NUVU-CLOUDCloudSeniorEngineer, asignado exclusivamente a personal de infraestructura de Blend360, quien posee permisos avanzados necesarios para la gestión de cambios, monitoreo y soporte especializado sobre la plataforma.

Este esquema segmentado de accesos garantiza que no existan administradores múltiples sin control, previene configuraciones no autorizadas, evita la manipulación o extracción indebida de información, impide la instalación de aplicaciones personales o ajenas a la operación institucional y protege la integridad de los datos y servicios. Adicionalmente, toda la actividad de acceso se mantiene trazada y auditada a través de los servicios de seguridad de AWS, asegurando visibilidad total sobre las acciones ejecutadas por cada usuario. Con esta arquitectura de control se establece un modelo seguro, ordenado y alineado con las mejores prácticas de gobernanza digital, garantizando la protección del entorno tecnológico y la gestión responsable de los datos de la Alcaldía de Santiago de Cali.

Se garantiza un manejo controlado y seguro del acceso a las soluciones tecnológicas implementadas, con el propósito de evitar la existencia de múltiples administradores y reducir los riesgos asociados a fraudes, uso indebido de credenciales, robos de información, manipulaciones no autorizadas y alteraciones en los servicios. Para ello, se aplica un esquema centralizado de gestión de identidades y permisos que permite definir perfiles, roles y niveles de acceso estrictamente necesarios para cada usuario, eliminando privilegios excesivos y asegurando que las acciones de administración se limiten exclusivamente al personal autorizado. Este modelo de control también evita la instalación o actualización de aplicaciones personales, la incorporación de software no permitido, manipulaciones de datos no autorizadas y cualquier intento de migración irregular de información. Todo el proceso se encuentra respaldado por políticas de

auditoría, monitoreo continuo y registro de actividades, lo que garantiza trazabilidad completa, protección de los datos institucionales y cumplimiento de los estándares de seguridad exigidos por la Entidad.



Documento Anexo: Informe de Políticas de Acceso Para la Organización de ACA

4.24 Ejecutar un plan de reversibilidad al finalizar el contrato, que contemple la desactivación de servicios, transferencia de recursos, entrega de accesos y documentación, eliminación segura de configuraciones y recursos desplegados, asegurando que la entidad no incurra en costos residuales o innecesarios posteriores a la finalización contractual.

En relación con la Obligación, se deja indicado en el informe de facturación que su cumplimiento se ejecutará al cierre del consumo de la bolsa de recursos de nube actualmente disponible, es decir, una vez finalicen dichos recursos y se adelante el proceso de cierre operativo, momento en el cual se realizará la desactivación ordenada de los servicios, la transferencia de recursos y accesos, y la entrega de documentación, dejando constancia formal mediante el Acta de entrega de infraestructura.

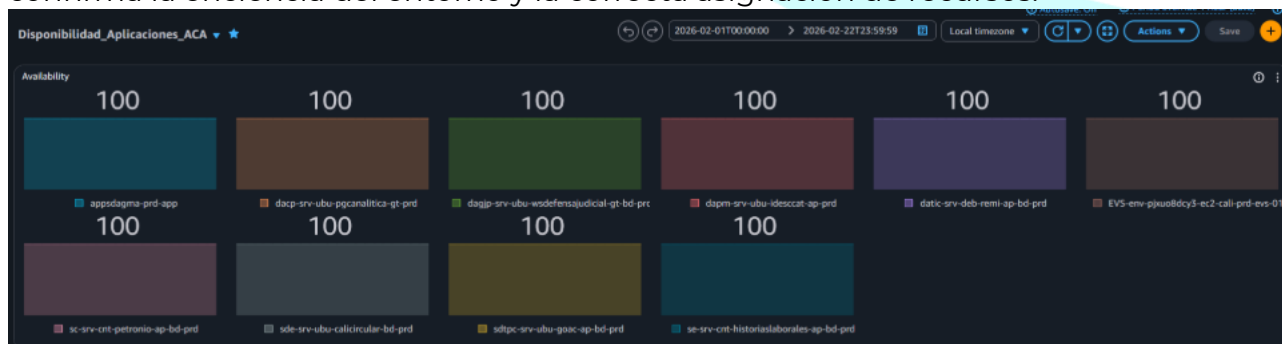
- Para garantizar un cierre controlado y que la Entidad no asuma costos residuales o innecesarios posteriores, efectuaremos las siguientes acciones:
- Inventario final de los recursos desplegados y dependencias (servicios, ambientes, redes, almacenamiento, reglas/políticas y componentes asociados).
- Transferencia de control y accesos a la Entidad: entrega/rotación de credenciales, cuentas, roles y permisos; actualización de responsables y trazabilidad.
- Entrega integral de documentación: arquitectura y configuración “as-is”, procedimientos operativos, respaldos/plantillas aplicables, y guías de continuidad/cierre.
- Plan de desactivación con ventana acordada, validación de impactos y verificación posterior de apagado/corte según corresponda.

- Eliminación segura de configuraciones y recursos: revocación de accesos temporales, rotación de llaves/secretos, cierre de endpoints y borrado seguro cuando aplique.
- Control y verificación de costos post-cierre: revisión de consumos, identificación de recursos huérfanos, alarmas y confirmación del estado de facturación esperado.
- Suscripción del Acta de entrega de infraestructura, con evidencia de accesos entregados, recursos desactivados/eliminados y medidas adoptadas para evitar consumos posteriores.

De esta manera, el informe final dejará claramente trazado que el plan de reversibilidad será cumplido en su integridad al finalizar el consumo de los recursos, asegurando una transición ordenada, documentada y sin impactos financieros posteriores para la Entidad.

4.25 Garantizar la implementación y el fortalecimiento de la plataforma tecnológica que soporta los sistemas de información transversales con su respectiva disponibilidad, seguridad y eficiencia, así mismo asegurar la compatibilidad con la infraestructura tecnológica existente y proveer capacidad de escalabilidad y redundancia, según la descripción detallada del bien adquirido.

Se garantiza la implementación, operación y fortalecimiento continuo de la plataforma tecnológica que soporta los sistemas de información transversales de la Alcaldía de Santiago de Cali, asegurando su disponibilidad, seguridad, eficiencia y compatibilidad con la infraestructura tecnológica existente. La solución desplegada se encuentra construida sobre servicios de AWS que, según el análisis presentado en el Informe de Monitoreo y Disponibilidad, han mantenido un comportamiento estable y sin interrupciones durante el periodo evaluado, reflejando niveles de disponibilidad adecuados para los sistemas institucionales. El monitoreo realizado durante el mes de noviembre demuestra que componentes críticos como EC2, EFS, ELB, VPC, Elastic Disaster Recovery y Site-to-Site VPN operaron sin incidentes, garantizando continuidad en la ejecución de aplicaciones, conectividad segura y acceso persistente a los datos. Asimismo, las métricas de CPU, lectura y escritura en disco, tráfico de red y verificaciones de estado evidencian un consumo controlado y sin afectaciones relevantes, lo que confirma la eficiencia del entorno y la correcta asignación de recursos.



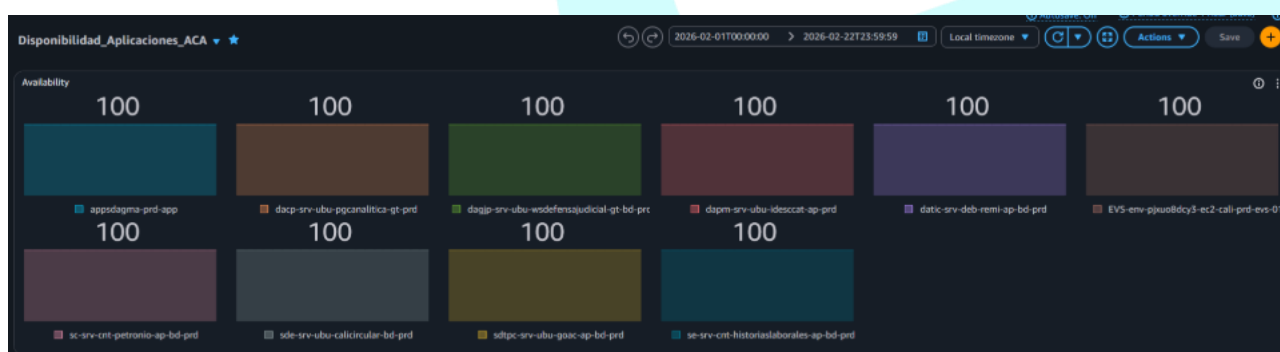
La arquitectura implementada incorpora esquemas de escalabilidad que permiten ajustar la capacidad de cómputo, almacenamiento y red en función del crecimiento de los servicios, así como mecanismos de redundancia y recuperación que aseguran la

disponibilidad continua del entorno, incluso ante eventos de falla. Esto incluye balanceadores de carga, zonas de disponibilidad independientes, políticas de recuperación automática ante `StatusCheckFailed` y la operación estable de la VPN híbrida que conecta la infraestructura on-premise con la nube. La compatibilidad con la infraestructura tecnológica existente se garantiza mediante la integración de redes privadas, túneles seguros, balanceo de tráfico y servicios gestionados que se adaptan al modelo operativo actual del Distrito.

Con este conjunto de prácticas, monitoreo constante y mecanismos de alta disponibilidad, se fortalece la plataforma tecnológica que soporta los sistemas de información transversales, permitiendo que la infraestructura permanezca operativa, segura, eficiente y preparada para soportar crecimiento, cargas variables y requerimientos institucionales, en concordancia con la descripción técnica del bien adquirido y los lineamientos contractuales establecidos.

Documento anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.26 Suministrar herramientas de monitoreo en tiempo real con métricas detalladas (uso de CPU, memoria, red, almacenamiento, etc.), garantizando la disponibilidad de históricos de monitoreo desde el inicio de operación y proveer reportes de optimización y desempeño de los servicios.



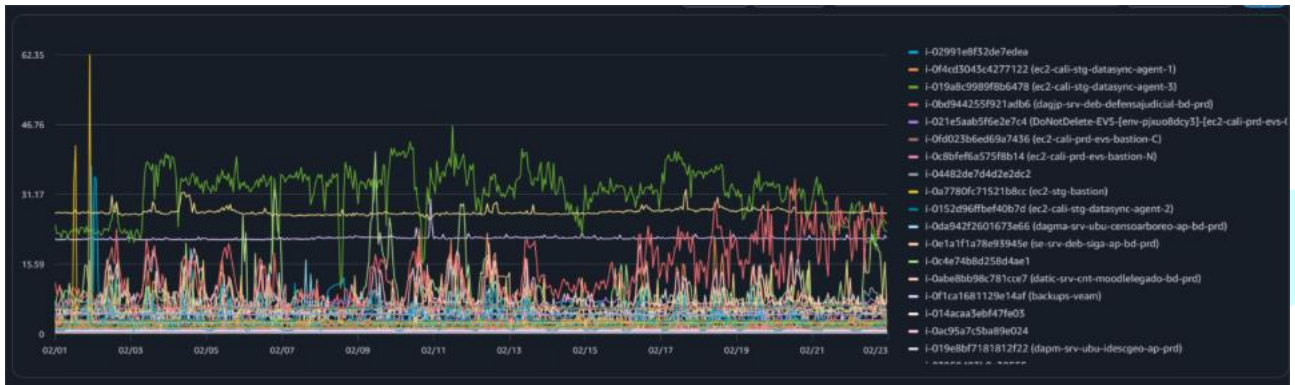
Se dispone de herramientas de monitoreo en tiempo real mediante el uso de Amazon CloudWatch, servicio nativo de AWS que permite recopilar, visualizar y analizar métricas detalladas de la infraestructura, incluyendo uso de CPU, memoria, red, almacenamiento y estado de los recursos.

CloudWatch proporciona paneles personalizados (dashboards) y alarmas configurables, permitiendo supervisar el desempeño de los servicios y responder oportunamente ante cualquier desviación o incidente. Además, se garantiza la disponibilidad de históricos de monitoreo desde el inicio de la operación, facilitando el análisis de tendencias y la generación de reportes de desempeño.

Complementariamente, se utiliza AWS Compute Optimizer, herramienta que analiza métricas de uso reales y recomienda configuraciones óptimas de cómputo, almacenamiento y red, contribuyendo a la optimización continua del rendimiento y los costos de la infraestructura.

La disponibilidad y gestión de las soluciones tecnológicas desarrolladas se garantizan mediante el uso de herramientas nativas de AWS, principalmente a través de Amazon CloudWatch, que permite el monitoreo continuo de la infraestructura subyacente y de los servicios de virtualización. Esta herramienta

proporciona visibilidad en tiempo real del rendimiento, uso de recursos y estado operativo de los componentes.

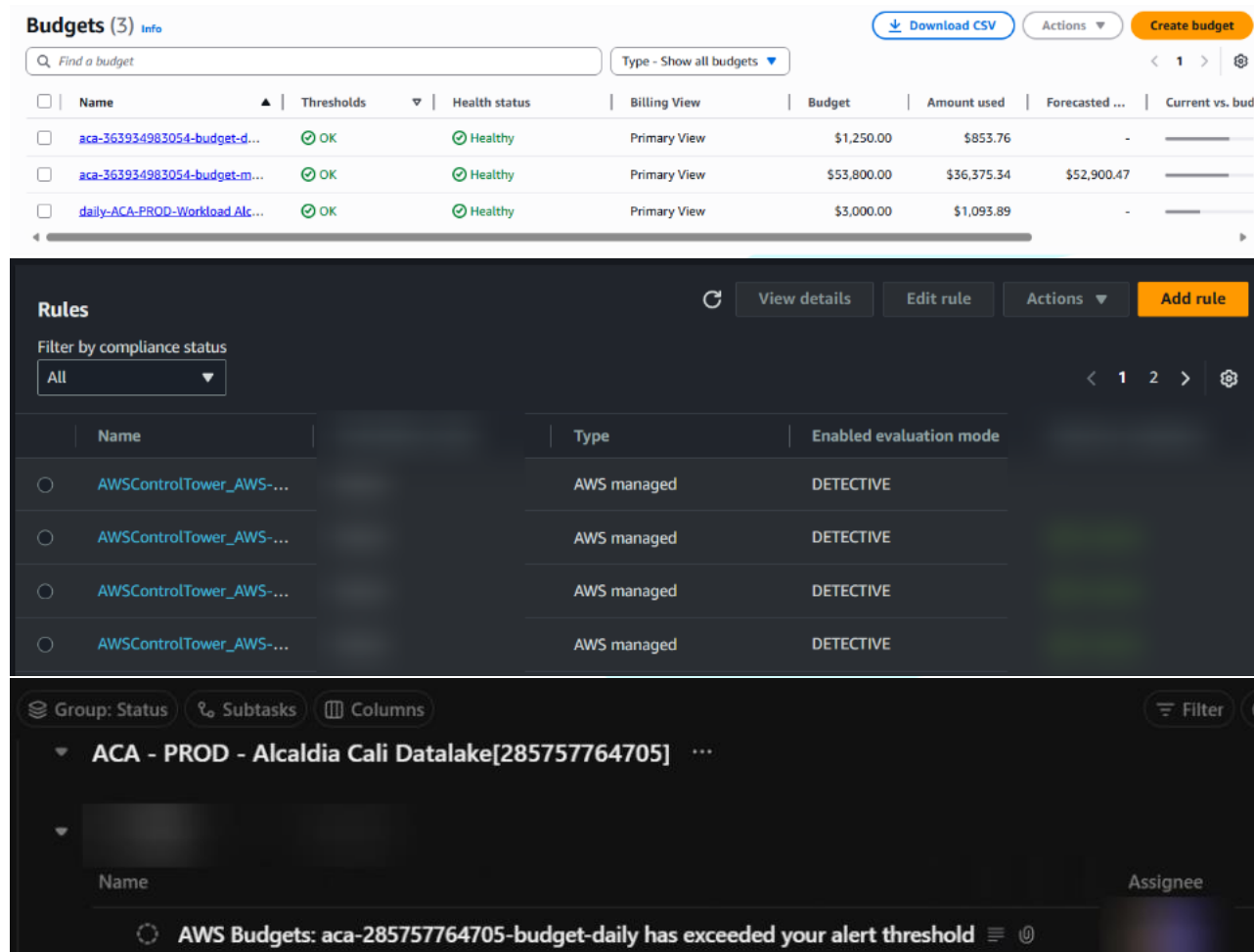


Métricas medidas para todos los recursos que se crean en aws a través del cliente de cloudwatch:

1. CPU Utilization: Porcentaje de capacidad de procesamiento de la instancia que se está utilizando. Un valor consistentemente alto indica que el servidor está bajo una carga de trabajo pesada.
2. StatusCheckFailed: Indicador general de que la instancia ha fallado una verificación automática de estado, requiriendo atención.
3. StatusCheckFailed_Instance: Falla a nivel de software o sistema operativo (ej., la aplicación no responde).
4. StatusCheckFailed_System: Falla detectada por AWS en el hardware físico subyacente, lo que normalmente requiere una recuperación automática o manual de la instancia.
5. DiskReadBytes: Cantidad de datos (en bytes) que la instancia lee desde sus discos. Alto volumen indica una intensa actividad de lectura de información.
6. DiskWriteBytes: Cantidad de datos (en bytes) que la instancia escribe en sus discos. Alto volumen indica una intensa actividad de guardado o modificación de archivos.
7. DiskReadOps: Número de operaciones de lectura individuales que la instancia solicita a sus discos. Muchas operaciones pueden ser demandantes incluso si el volumen de datos es bajo.
8. DiskWriteOps: Número de operaciones de escritura individuales que la instancia realiza en sus discos. Un recuento elevado es común en sistemas con bases de datos activas.
9. NetworkIn: Volumen total de datos (en bytes) que la instancia recibe desde la red.
10. NetworkOut: Volumen total de datos (en bytes) que la instancia envía a la red. Estas dos métricas reflejan el tráfico total de su aplicación.
11. NetworkPacketsIn: Número de paquetes de datos individuales que la instancia recibe. Un número muy alto puede consumir recursos de CPU.
12. NetworkPacketsOut: Número de paquetes de datos individuales que la instancia envía. Es útil para diagnosticar problemas de rendimiento de red.

o aplicaciones con mucho "chateo" (pequeñas comunicaciones frecuentes).

Adicionalmente se crean alertas con diferentes herramientas internas y externas de aws



The image shows two screenshots from the AWS console. The top screenshot displays the 'Budgets (3)' page with a table of budget details:

Name	Thresholds	Health status	Billing View	Budget	Amount used	Forecasted ...	Current vs. bud
aca-363934983054-budget-d...	OK	Healthy	Primary View	\$1,250.00	\$853.76	-	
aca-363934983054-budget-m...	OK	Healthy	Primary View	\$53,800.00	\$36,375.34	\$52,900.47	
daily-ACA-PROD-Workload Alc...	OK	Healthy	Primary View	\$3,000.00	\$1,093.89	-	

The bottom screenshot shows the 'Rules' configuration page, filtered by 'All' compliance status. It lists several rules:

Name	Type	Enabled evaluation mode
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE
AWSControlTower_AWS-...	AWS managed	DETECTIVE

Below the rules list, a notification is visible: 'AWS Budgets: aca-285757764705-budget-daily has exceeded your alert threshold'.

Documento Anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.27 Implementar mecanismos de cifrado y control de accesos, asegurando la integridad, disponibilidad y confidencialidad de la información financiera, lo anterior en cumplimiento de las normativas de seguridad establecidas.

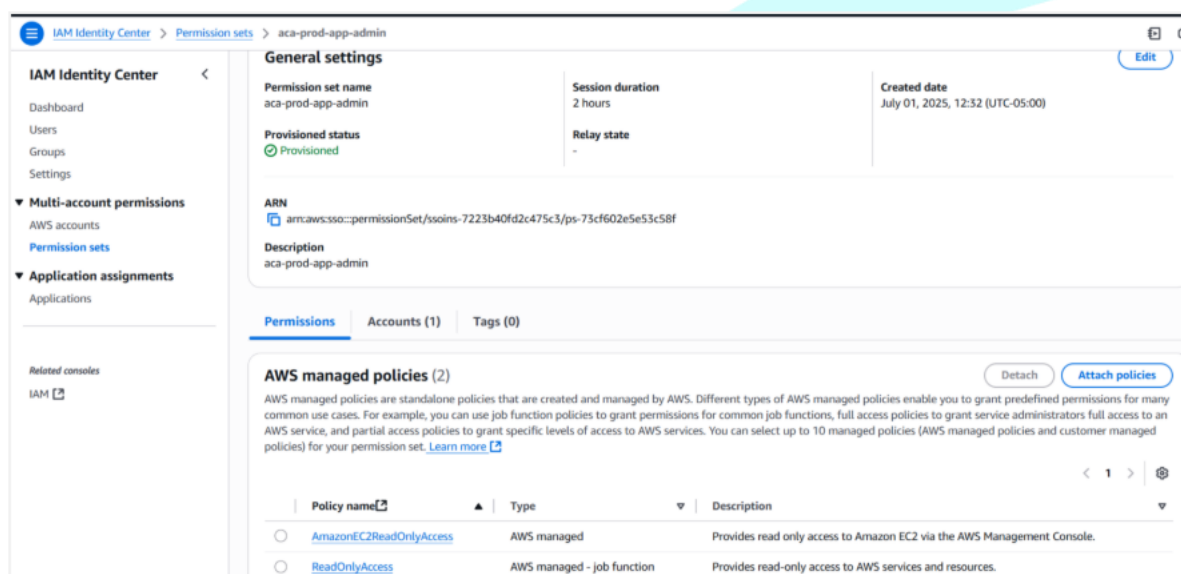
Se cuenta con una política de acceso basada en roles (IAM) alineada con los principios de menor privilegio y segregación de funciones, lo que permite controlar, limitar y auditar el acceso a los recursos de la nube de manera centralizada y segura.

La gestión de identidades y accesos se realiza mediante AWS Identity Center, siguiendo las prácticas recomendadas de centralización de identidad y autenticación federada. Esto permite administrar usuarios, roles y grupos desde un punto único de control, integrando el acceso con los directorios corporativos de la entidad y simplificando la aplicación de políticas consistentes.

Como parte de la implementación de seguridad en AWS, se configuró un conjunto de usuarios IAM con políticas de acceso específicas que siguen el principio de mínimo privilegio. Estos usuarios permiten el acceso seguro y controlado a los recursos del entorno para los diferentes equipos técnicos.

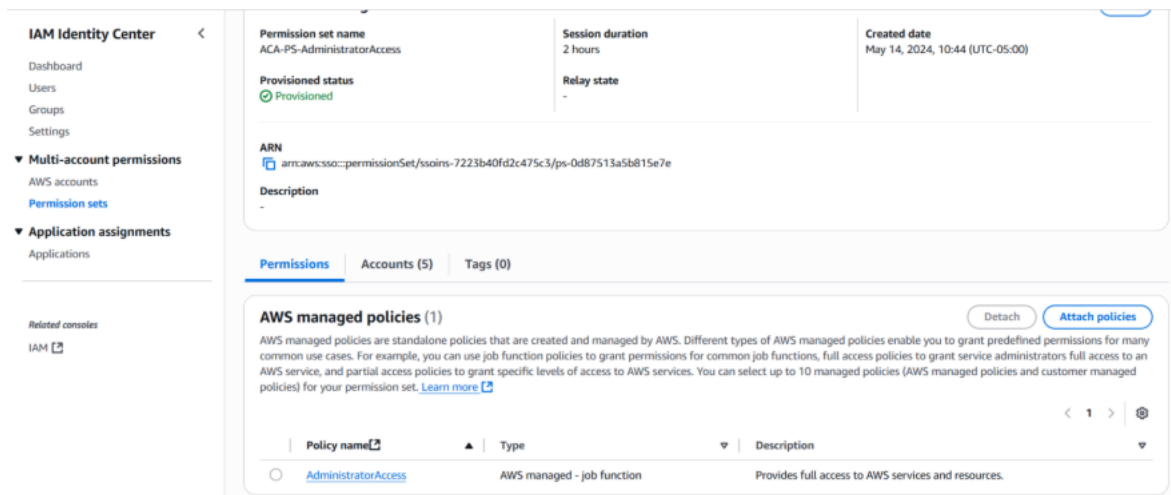
- ACA -AppAdmin

Este grupo permite a los usuarios solo tener permisos de lectura sobre las diferentes aplicaciones de EC2 en la cuenta ACA - PROD -Workload Alcaldía Cali. De esta manera, pueden entrar a revisar configuraciones y métricas de las máquinas sin el riesgo de una modificación. Este permiso está centrado principalmente sobre los funcionarios de la Alcaldía y de Nexura.



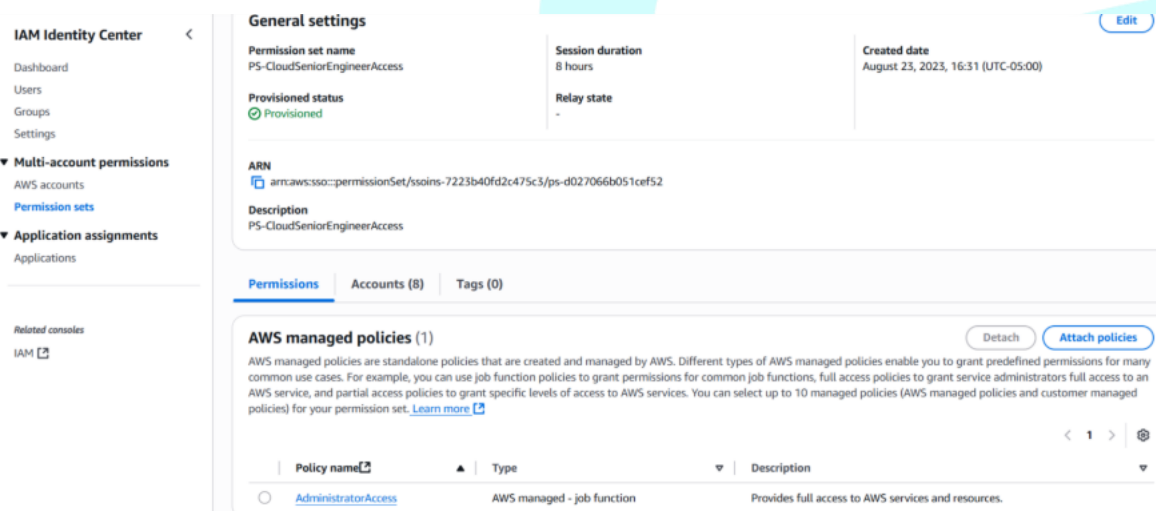
- ACA – CloudAdmin

El siguiente permiso establece que únicamente funcionarios autorizados del equipo DATIC de la Alcaldía de Santiago de Cali podrán contar con permisos administrativos sobre las diferentes cuentas de la plataforma. Se exceptúa la cuenta de producción, la cual mantiene un esquema de acceso restringido, conforme a las políticas de seguridad y control definidas para la operación.

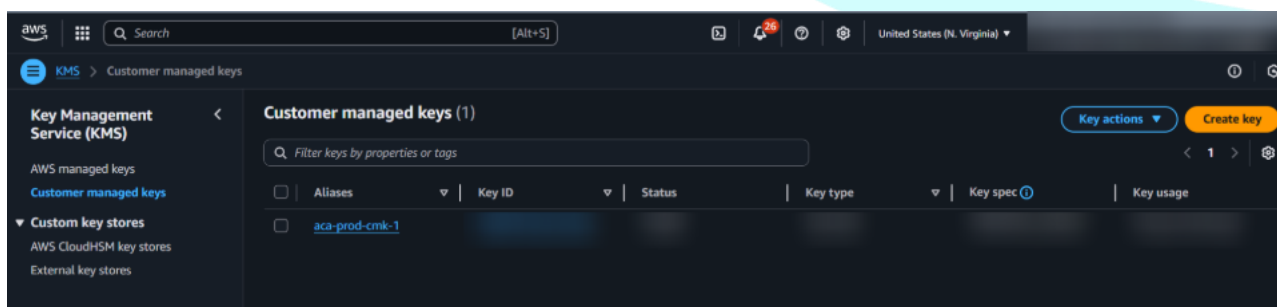


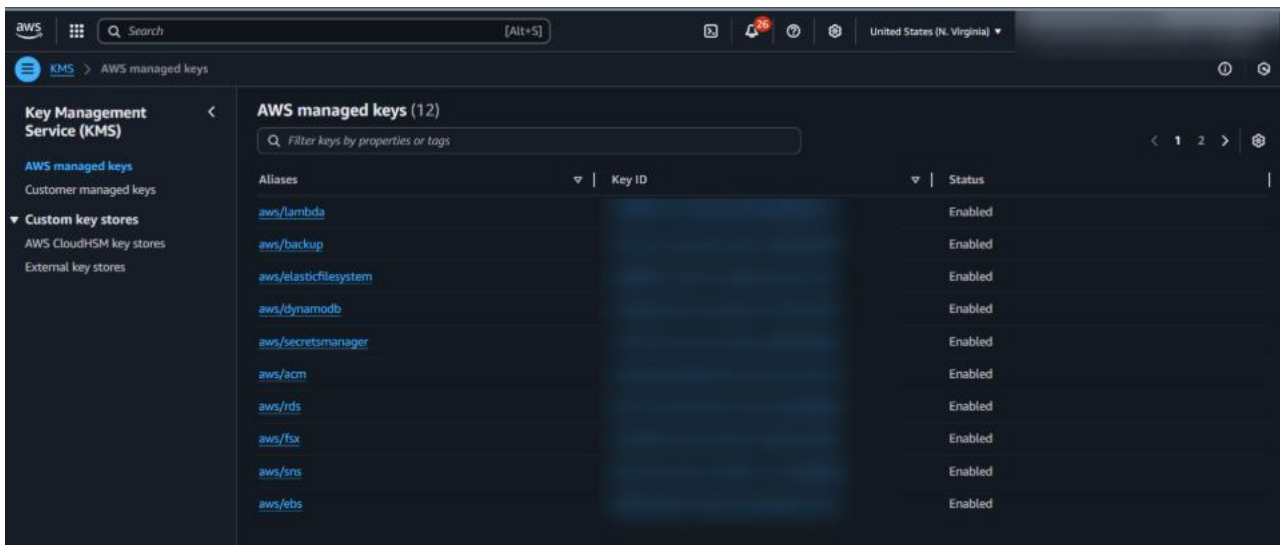
- NUVU – CLOUDCloudSeniorEngineer

Del lado de Blend, solo las personas del equipo de infraestructura de AWS pueden también tener permisos administrativos sobre la organización para tener la capacidad de gestión de cambios, revisión y seguimiento.



Adicionalmente se manejan llaves KMS para encriptar todos los recursos de aws que se creen en las cuentas





Documento Anexo: Documentación Infraestructura AWS

4.28 Brindar un escenario que permita el desarrollo y automatización de copias de respaldo, bajo la política día, mes y año y con ello poder realizar la restauración en caso de falla o interrupción.

Como parte de la implementación del entorno AWS, se estableció un plan de respaldos para garantizar la protección y recuperación de los recursos migrados. El plan plan-cali-prd-backup se configura mediante políticas con distintos periodos de retención y transición a almacenamiento frío-

plan-cali-prd-backup Delete View JSON

Summary

Backup plan name plan-cali-prd-backup	Version ID Zjk2MWY2MGUtMmYxNi000 DhhLWJiM2EtZTFhNTJlYTAzY Tgy	Last modified July 30, 2025, 10:00:50 (UTC-05:00)	Last runtime September 12, 2025, 01:15:07 (UTC-05:00)
Backup plan ID e17d35df-91fd-4391-9311-33ac5c855379			

Los backups son gestionados a través del vault vault-cali-prd-backup.

vault-cali-prd-backup Info Manage vault lock Delete vault Edit access policy

Summary

Vault name vault-cali-prd-backup	KMS encryption key ID arn:aws:kms:us-east-1:363934983054:key:12345678-9012-3456-7890-123456789012	Vault lock 🔒 Locked – Governance mode Vault lock is editable. Learn more
Vault type Backup vault	Creation date June 26, 2025, 14:48:16 (UTC-05:00)	Retention period for vault lock Minimum retention period: 6 days Maximum retention period: –
Vault ARN arn:aws:backup:us-east-1:363934983054:backup-vault:vault-cali-prd-backup		

Políticas de retención implementadas:

- DailyBackup-7DayRetention: Frecuencia diaria con retención de 15 días.
- WeeklyBackup-1MonthRetention: Frecuencia semanal con retención de 1 mes.
- MonthlyBackup-1YearRetention: Frecuencia mensual con retención de 1 año, con transición a almacenamiento frío a los 3 meses (90 días).
- YearlyBackup-20YearRetention: Frecuencia anual con retención de 20 años, con transición a almacenamiento frío a los 3 meses (90 días).

Backup rules (4) Edit Delete Add backup rule

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Name	Backup vault	Destination Backup vault
DailyBackup-15DayRetention	vault-cali-prd-backup	-
MonthlyBackup-1YearRetention	vault-cali-prd-backup	-
WeeklyBackup-1MonthRetention	vault-cali-prd-backup	-
YearlyBackup-20YearRetention	vault-cali-prd-backup	-

La asignación de recursos se realiza mediante la etiqueta "Backup - Enabled", utilizando el rol IAM role-cali-prd-backup para la ejecución automatizada de las copias de seguridad. Esta estrategia permite cumplir con los requerimientos de recuperación ante incidentes, optimización de costos y políticas de compliance de la organización.

plan-cali-prd-backup-resources-selection

Delete

Summary

Resource assignment name

plan-cali-prd-backup-resources-selection

IAM role

arn:aws:iam::363934983054:role/role-cali-prd-backup

Tags

Backup - Enabled

Los recursos cubiertos por las cuatro políticas de backups son los siguientes:

Resource ID	Resource type
file-system/fs-0967f438281ee1e78	EFS
instance/i-0ff91dad5f9352e5	EC2
instance/i-0ff8ef35f1871e677	EC2
instance/i-0f7f720eed4cdb558	EC2
instance/i-0f1ca1681129e14af	EC2
instance/i-0f16abff95586310d	EC2
instance/i-0e8c34a41b6c86ade	EC2
instance/i-0e7b96bc549ff0898	EC2
instance/i-0e5bab7e27d08ff0b	EC2

instance/i-0e1a1f1a78e93945e	EC2
instance/i-0da942f2601673e66	EC2
instance/i-0ccfa3f8c3b574c0d	EC2
instance/i-0c4e74b8d258d4ae1	EC2
instance/i-0c427895e543ad95a	EC2
instance/i-0c235aa02cae57bb0	EC2
instance/i-0bf67840dd8dd4eec	EC2
instance/i-0bd944255f921adb6	EC2
instance/i-0bc591901eb7d3aa9	EC2
instance/i-0b7fc7de52d011a07	EC2
instance/i-0b444291b70de254c	EC2
instance/i-0ad841c9f7539cf4f	EC2
instance/i-0ac95a7c5ba89e024	EC2
instance/i-0abe8bb98c781cce7	EC2
instance/i-0a68d16a6d7cf54e1	EC2
instance/i-09f57f65953dcbbe9	EC2
instance/i-09daed7db5a91bb0e	EC2
instance/i-09c6b3858b15f90d4	EC2
instance/i-096f1f443330d321b	EC2

instance/i-092c20bbf14353f45	EC2
instance/i-0914776bdd46e8113	EC2
instance/i-08f030c4b0bad9c63	EC2
instance/i-080bc0076e766115d	EC2
instance/i-07fcf5c3bf586f4fb	EC2
instance/i-07d892e7c73ed3e42	EC2
instance/i-071b7ac828a68c668	EC2
instance/i-0713215fb793cf15e	EC2
instance/i-06a5a265833c118fe	EC2
instance/i-053306f51fb24c2ab	EC2
instance/i-04bfaa21b951e7d55	EC2
instance/i-047fc8d7b771cb5a0	EC2
instance/i-045b6c8d631a1933e	EC2
instance/i-03dd3e5f2b0ecf3bf	EC2
instance/i-03b3aeba5a89cc6df	EC2
instance/i-03b020eed552c3747	EC2
instance/i-03acb8e98633046e9	EC2

instance/i-03959403b0e38555e	EC2
instance/i-0393259ac7c75ded6	EC2
instance/i-02caec961eef45329	EC2
instance/i-0256a7b9f2de6c2fc	EC2
instance/i-0245e6e2a42d81bef	EC2
instance/i-023cf71bccb8448d2	EC2
instance/i-01e2fd3f70af99abd	EC2
instance/i-019e8bf7181812f22	EC2
instance/i-014acaa3ebf47fe03	EC2
instance/i-012296a22fb19cb60	EC2
instance/i-005516784418bcbeb	EC2
instance/i-092c20bbf14353f45	EC2
instance/i-0045bcb36c2e9dba3	EC2
instance/i-001741585e5ab2a52	EC2
instance/i-0a7780fc71521b8cc	EC2
instance/i-04482de7d4d2e2dc2	EC2
instance/i-03bf30e6bcbaa7bd7	EC2
volume/vol-01a2926f544d54f9e	EBS
file-system/fs-067f7766e3ab13903	EFS

Para los buckets de S3 se implementó versionamiento como capa de protección de datos.

Resource name	Resource ID
s3-cali-prd-workspace	s3-cali-prd-workspace
s3-cali-prd-VMware-audit-logs	s3-cali-prd-VMware-audit-logs
s3-cali-prd-shared-vpc-audit-logs	s3-cali-prd-shared-vpc-audit-logs
s3-cali-prd-secretaria-turismo-audit-logs	s3-cali-prd-secretaria-turismo-audit-logs
s3-cali-prd-repository-01	s3-cali-prd-repository-01
s3-cali-prd-podmanbucket	s3-cali-prd-podmanbucket
s3-cali-prd-orfeo-storage	s3-cali-prd-orfeo-storage
s3-cali-prd-orfeo-bodega	s3-cali-prd-orfeo-bodega
s3-cali-prd-oraclerman	s3-cali-prd-oraclerman
s3-cali-prd-migrate-v5-audit-logs	s3-cali-prd-migrate-v5-audit-logs
s3-cali-prd-migrar-gce-VMware	s3-cali-prd-migrar-gce-VMware
s3-cali-prd-katana	s3-cali-prd-katana
s3-cali-prd-integratic	s3-cali-prd-integratic

s3-cali-prd-infra-mc	s3-cali-prd-infra-mc
s3-cali-prd-orfeo-bodega	s3-cali-prd-orfeo-bodega
s3-cali-prd-oraclerman	s3-cali-prd-oraclerman
s3-cali-prd-migrate-v5-audit-logs	s3-cali-prd-migrate-v5-audit-logs
s3-cali-prd-daruma-aplicacion	s3-cali-prd-daruma-aplicacion

s3-cali-prd-daruma-aplicacion	s3-cali-prd-daruma-aplicacion
s3-cali-prd-daisy-bkt	s3-cali-prd-daisy-bkt
s3-cali-prd-daas-audit-logs	s3-cali-prd-daas-audit-logs
s3-cali-prd-bckrman-pegasus	s3-cali-prd-bckrman-pegasus
s3-cali-prd-backups-piso15-alcaldiacali	s3-cali-prd-backups-piso15-alcaldiacali
s3-cali-prd-backup-dr-audit-logs	s3-cali-prd-backup-dr-audit-logs

Documento Anexo: Documentación Infraestructura AWS

4.29 Brindar soporte técnico Premium 24/7 mensual, a través de diversos canales (teléfono, correo electrónico, sistema de tiquetes), garantizando los tiempos de respuesta adecuados según la criticidad del servicio.

En el marco del servicio contratado se brinda soporte técnico Premium 24/7, disponible a través de múltiples canales incluyendo teléfono, correo electrónico y sistema de tiquetes garantizando tiempos de respuesta acordes con la criticidad del servicio, conforme a los Acuerdos de Nivel de Servicio (ANS) establecidos con la Entidad. Este componente incluye la disponibilidad permanente de personal técnico especializado para atender incidentes, requerimientos y ajustes sobre la infraestructura virtual contratada, así como acompañamiento directo durante ventanas de mantenimiento, actividades planificadas y cambios operativos que requieran soporte conjunto con los equipos de la Alcaldía de Santiago de Cali. El soporte incorpora diagnóstico, estabilización y acciones de continuidad para servicios críticos, asegurando el restablecimiento oportuno y la prevención de riesgos operativos.

La atención se realiza de manera articulada con los equipos de DATIC, promoviendo la transferencia de conocimiento y la apropiación tecnológica mientras se mantiene un registro detallado de cada intervención mediante bitácoras y trazabilidad dentro de la herramienta oficial de gestión de tickets HelpDesk. A través de esta plataforma, los usuarios autorizados pueden registrar y gestionar incidentes, solicitudes de información, solicitudes de cambio (RFC), requerimientos operativos y peticiones de administración de infraestructura, incluyendo creación o eliminación de recursos AWS tales como EC2, RDS, S3, EBS, Security Groups, Roles IAM, WAF y balanceadores; ajustes de configuración en VPC, redes o servidores; despliegue o modificación de máquinas virtuales en VMware; validación de conectividad híbrida y revisión de logs, costos, copias de seguridad o restauración de snapshots.

Para este proceso, se encuentran habilitados los usuarios designados por la entidad, quienes acceden al portal oficial de soporte mediante la URL: <https://helpdesk.ia.blend360.com/#login>, lo que garantiza que la gestión de solicitudes se realice bajo un flujo formal de atención, con roles definidos, permisos adecuados y trazabilidad completa desde la creación hasta el cierre de cada ticket. Durante la ejecución del contrato se realizaron las habilitaciones necesarias de usuarios, se validó la correcta asignación de perfiles y se entregó el Manual de Usuario asociado a la herramienta, el cual explica los pasos de acceso, registro, consulta, actualización, escalamiento y seguimiento de solicitudes.

El comportamiento operativo registrado evidencia un volumen significativo de casos atendidos, principalmente asociados a administración de infraestructura, despliegues de ambientes, reglas de firewall, configuración de elementos de seguridad, soporte en redes, consultas técnicas y ajustes de permisos IAM. La mayoría de los casos presentan estados Cerrado, Entregado o Resuelto, demostrando cumplimiento de los tiempos de atención y efectividad en la gestión del soporte. Las solicitudes clasificadas con criticidad alta fueron atendidas de manera prioritaria, especialmente aquellas relacionadas con continuidad operativa o despliegues productivos, mientras que los casos en estado Aceptado, En entendimiento o Esperando respuesta continúan su gestión conjunta según el flujo de trabajo acordado con DATIC.

Con estas acciones, se garantiza un soporte técnico integral, continuo y especializado que asegura la disponibilidad de la infraestructura, la respuesta oportuna ante eventos críticos, la correcta ejecución de los requerimientos operativos y la trazabilidad total de todas las actividades técnicas, fortaleciendo la estabilidad y confiabilidad de la solución tecnológica implementada.

Durante el periodo analizado se registró un número significativo de solicitudes en la herramienta de soporte Help Desk por parte de la Alcaldía de Santiago de Cali, principalmente asociadas a gestión de infraestructura, despliegues de ambientes, reglas de firewall, administración de recursos en AWS y consultas operativas.

En términos generales, los casos presentan el siguiente comportamiento:

- Durante el periodo evaluado se realizó la atención, gestión y seguimiento de un alto volumen de solicitudes técnicas asociadas a la operación, seguridad y modernización de la infraestructura tecnológica en AWS de la Alcaldía de Santiago de Cali.
- La mayoría de las solicitudes se encuentran cerradas o resueltas, evidenciando una gestión oportuna y efectiva, mientras que un número controlado permanece en estado de espera o diagnóstico, principalmente asociado a iniciativas de modernización en curso.
- Se atendieron solicitudes relacionadas con seguridad de la infraestructura, incluyendo actualización y definición de reglas de firewall, configuración de controles de acceso, revisión de tráfico, mitigación de alertas de seguridad (SOC) y sesiones técnicas de AWS WAF.
- Se ejecutaron actividades de conectividad y redes, tales como configuración y seguimiento de VPN site-to-site, interconexión por Direct Connect, monitoreo de disponibilidad de interconnect y enrutamiento entre entornos AWS y OCI.

- Se brindó soporte a la operación de servidores y servicios críticos, incluyendo revisiones de máquinas virtuales, configuración de agentes, snapshots, montaje de imágenes ISO, eliminación y creación de recursos, así como verificación de disponibilidad y alcanzabilidad.
- Se avanzó en iniciativas de modernización de infraestructura en AWS, particularmente en la Modernización de Orfeo, el cambio de infraestructura del Portal de la Alcaldía de Cali y el Proyecto de Ecosistemas Digitales, actualmente en fase de ejecución y seguimiento.
- Se apoyaron procesos de gestión de accesos e identidades, mediante la creación de usuarios IAM, asignación de políticas, accesos a plataformas institucionales y soporte a usuarios de la entidad.
- Se elaboraron y entregaron informes técnicos y de gestión, incluyendo reportes de backups, seguimiento de interconectividad, información de ciberseguridad para la construcción del DRP y avances del informe de gestión contractual.

Documento Anexo: Informe mensual de casos

4.30 Mantener una base de conocimiento con documentación técnica y foros de consulta.

Como parte del cumplimiento de la presente obligación, se dispuso de un canal de soporte para la atención de solicitudes y consultas del equipo de la Alcaldía de Santiago de Cali (<https://helpdesk.ia.blend360.com/#login>), las cuales han sido atendidas de manera oportuna a través de los mecanismos definidos, incluyendo llamadas telefónicas y comunicación vía WhatsApp, de acuerdo con las necesidades operativas identificadas.

Adicionalmente, para el desarrollo de las actividades técnicas, la atención de requerimientos y como referencia para la operación, configuración y aplicación de buenas prácticas, se ha utilizado la documentación oficial de AWS disponible en https://docs.aws.amazon.com/es_es/, la cual se mantiene permanentemente actualizada. Esto permite asegurar que los lineamientos técnicos aplicados se encuentren alineados con las recomendaciones vigentes y los estándares definidos por AWS.

Entrar a helpdesk.ia.blend360.com



NOMBRE DE USUARIO / DIRECCIÓN DE CORREO ELECTRÓNICO

CONTRASEÑA

Recordarme

Iniciar sesión

[¿Olvidaste la contraseña?](#)

O INICIE SESIÓN USANDO



Inicio de sesión con Houndoc

Bienvenido a la documentación de AWS

Encuentre guías de usuario, ejemplos de código, SDK y kits de herramientas, tutoriales, referencias de API y CLI, y mucho más.

Contenido destacado



Amazon Elastic Compute Cloud

Cree y ejecute servidores virtuales en la nube



Amazon Simple Storage Service

Almacenamiento de objetos creado para recuperar cualquier cantidad de datos desde cualquier lugar



Amazon DynamoDB

Servicio de base de datos NoSQL administrada



Amazon Relational Database Service

Configure, use y escale una base de datos relacional en la nube



AWS Lambda

Ejecute código sin pensar en los servidores



Amazon Virtual Private Cloud

Recursos en la nube aislados

Introducción a AWS

Conozca los conceptos fundamentales y comience a crear a partir de AWS. Encuentre las mejores prácticas que le ayudarán a lanzar su primera aplicación y conozca la Consola de administración de AWS.

[Configuración del entorno de AWS](#)

https://docs.aws.amazon.com/es_es/

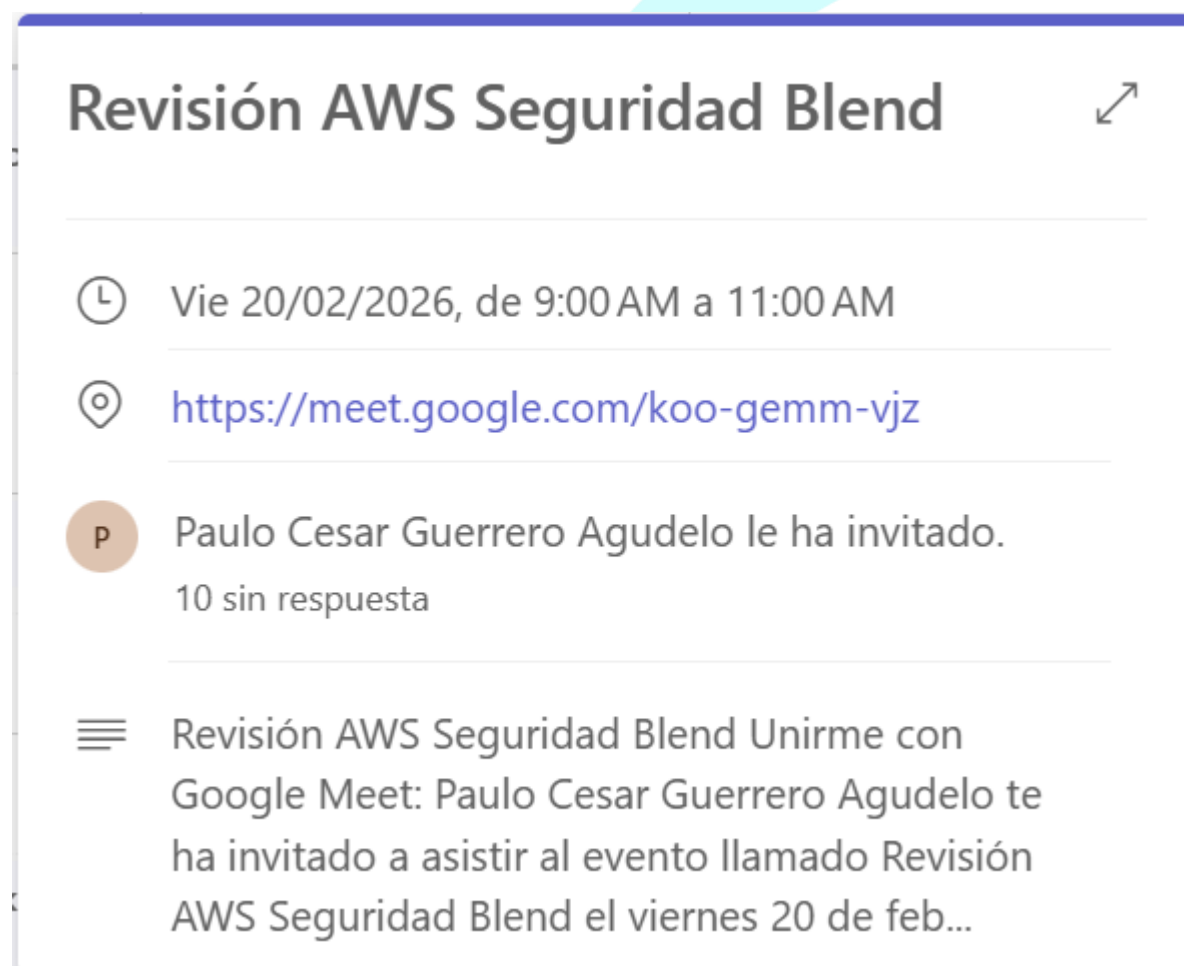
4.31 Brindar documentación técnica de los procesos ejecutados para los sistemas generados y realizar transferencia de conocimiento entregando documentación detallada de la misma, tales como videos, manuales, guías y demás documentos requeridos por la entidad.

Actualmente, nos encontramos en proceso de ejecución de las actividades asociadas a la modernización de las soluciones tecnológicas, por lo cual la elaboración y entrega de la documentación técnica detallada y la transferencia de conocimiento se realizarán una vez dichas iniciativas sean concluidas. Actualmente, avanzamos en iniciativas de modernización de infraestructura en AWS, alineadas con los lineamientos técnicos y de seguridad definidos por la Alcaldía de Santiago de Cali. En este marco, se ejecutan actividades relacionadas con la modernización del sistema Orfeo, orientadas a mejorar su desempeño, disponibilidad y sostenibilidad tecnológica; la modernización del Portal Municipal de la Alcaldía, fortaleciendo su operación sobre infraestructura en la nube; y el despliegue de ecosistemas digitales, soportando la implementación de nuevas capacidades tecnológicas y servicios digitales para la entidad. Una vez finalizadas estas actividades, se realizará la entrega de manuales técnicos, guías, videos y demás documentos requeridos, así como la transferencia de conocimiento correspondiente a los equipos designados por la entidad.

4.32 Realizar la transferencia de conocimiento en la gestión y operación de la plataforma adquirida al equipo técnico de la Alcaldía de Santiago de Cali.

En cumplimiento de la obligación de realizar la transferencia de conocimiento, se lleva a cabo un proceso llevamos a cabo la transferencia de conocimiento dirigida a los colaboradores de la Alcaldía de Santiago de Cali, resaltando la importancia de la seguridad como un eje transversal en la operación y administración de las soluciones tecnológicas. En este contexto, el día viernes se realizó una jornada de capacitación

enfocada en seguridad en la nube AWS, en la cual se abordaron los principios fundamentales de seguridad, la responsabilidad compartida y la necesidad de adoptar controles preventivos, detectivos y correctivos para la protección de la información y los servicios. Durante la sesión se presentó el uso de AWS WAF para la protección de aplicaciones web frente a amenazas comunes, AWS Shield para la mitigación de ataques DDoS, AWS Config para el control y cumplimiento de configuraciones, Amazon CloudWatch para el monitoreo, análisis de métricas, logs y generación de alertas, así como otros servicios de seguridad como AWS IAM para la gestión de identidades y accesos, AWS CloudTrail para la trazabilidad y auditoría de acciones, Amazon GuardDuty para la detección de amenazas, y AWS Security Hub para la centralización del estado de seguridad y cumplimiento. Esta capacitación permitió sensibilizar al equipo sobre la relevancia de la seguridad en la nube y fortalecer sus capacidades para operar, administrar y proteger de manera adecuada las soluciones tecnológicas implementadas.



Revisión AWS Seguridad Blend

Vie 20/02/2026, de 9:00 AM a 11:00 AM

<https://meet.google.com/koo-gemm-vjz>

Paulo Cesar Guerrero Agudelo le ha invitado.
10 sin respuesta

Revisión AWS Seguridad Blend Unirme con Google Meet: Paulo Cesar Guerrero Agudelo te ha invitado a asistir al evento llamado Revisión AWS Seguridad Blend el viernes 20 de feb...

Documento anexo: Sesión Revisión AWS Seguridad Blend

4.33 Garantizar que la solución cuente con mecanismos para bloquear ataques comunes (como inyección SQL, XSS y otros del OWASP Top 10) y protección frente a tráfico automatizado malicioso (bots), asegurando la integridad de las aplicaciones web institucionales.

Se garantiza que las aplicaciones web institucionales, desplegadas sobre infraestructura en la nube de Amazon Web Services (AWS), cuenten con mecanismos de seguridad orientados a la prevención, detección y mitigación de ataques comunes, incluyendo aquellos definidos en el OWASP Top 10, así como con controles para la protección frente a tráfico automatizado malicioso (bots). Estos mecanismos permiten asegurar la integridad, disponibilidad y operación segura de las soluciones tecnológicas de la Alcaldía de Santiago de Cali.

Para el desarrollo de esta actividad, se ejecutan las siguientes acciones:

1. Protección a nivel de aplicación en AWS
 - a. Implementación de AWS Web Application Firewall (WAF) integrado con los servicios expuestos en AWS (Load Balancers, CloudFront y/o API Gateway), permitiendo la inspección y filtrado del tráfico HTTP/HTTPS.
 - b. Configuración de reglas administradas y personalizadas para mitigar ataques como inyección SQL, Cross-Site Scripting (XSS), exploración de vulnerabilidades, fuerza bruta y otros vectores del OWASP Top 10.
2. Protección frente a tráfico automatizado malicioso (bots)
 - a. Uso de reglas *rate-based* del WAF para detectar picos anómalos de solicitudes y comportamientos automatizados.
 - b. Bloqueo de direcciones IP que superan los umbrales definidos, reduciendo el riesgo de ataques de denegación de servicio, scraping y abuso de las aplicaciones web.
 - c. Administración de listas de control (whitelists y blacklists) a nivel de aplicación.
3. Controles complementarios de seguridad en la infraestructura AWS
 - a. Aplicación de controles de acceso a nivel de red mediante Security Groups, operando bajo el principio de *deny by default* y permitiendo únicamente el tráfico autorizado.
 - b. Propagación rápida de reglas de seguridad dentro de la infraestructura AWS, garantizando tiempos de respuesta adecuados ante incidentes o alertas de seguridad.
4. Monitoreo y operación segura
 - a. Seguimiento continuo del tráfico y eventos de seguridad, permitiendo la identificación temprana de intentos de ataque o comportamientos anómalos.
 - b. Atención de solicitudes de ajuste, bloqueo o habilitación de accesos conforme a los procedimientos definidos.
5. Soporte documental

- a. Aplicación del Procedimiento de Gestión de IPs y Reglas de Seguridad, que documenta la administración de controles de seguridad en AWS, incluyendo el uso de AWS WAF y la gestión de reglas a nivel de red y aplicación, como soporte al cumplimiento de esta obligación.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.34 Permitir la gestión centralizada de reglas de seguridad, su despliegue automático a múltiples sitios mediante plantillas predefinidas, y su administración completa a través de APIs documentadas.

Se garantiza que la solución implementada permita la gestión centralizada de las reglas de seguridad sobre la infraestructura tecnológica desplegada en AWS, facilitando su definición, control, actualización y propagación automática a múltiples aplicaciones, sitios o entornos. Esta gestión se apoya en el uso de plantillas predefinidas, mecanismos de automatización y APIs documentadas, asegurando consistencia, trazabilidad y eficiencia operativa en la administración de la seguridad.

Para el desarrollo de esta actividad, se ejecutan las siguientes acciones:

1. Gestión centralizada de reglas de seguridad

- a. Administración centralizada de reglas de seguridad a nivel de red y aplicación, permitiendo aplicar políticas homogéneas sobre múltiples recursos y servicios.
- b. Definición de reglas estándar y personalizadas que responden a los lineamientos de seguridad establecidos por la Alcaldía de Santiago de Cali.

2. Despliegue automático mediante plantillas predefinidas

- a. Uso de plantillas y configuraciones reutilizables para la creación, actualización y despliegue de reglas de seguridad en distintos entornos (producción, pruebas, contingencia).
- b. Aplicación automática de reglas a múltiples sitios o aplicaciones, reduciendo la intervención manual y el riesgo de configuraciones inconsistentes.
- c. Propagación rápida de cambios de seguridad en la infraestructura AWS, garantizando tiempos de respuesta adecuados ante nuevas necesidades o incidentes.

3. Administración a través de APIs documentadas

- a. Posibilidad de integrar la gestión de seguridad con herramientas externas de automatización, monitoreo o gestión de servicios, conforme a las necesidades de la entidad.

- b. Disponibilidad de documentación técnica que describe los flujos, parámetros y buenas prácticas para la administración de las reglas mediante APIs.

4. Trazabilidad y control operativo

























































- a. Registro y seguimiento de los cambios realizados sobre las reglas de seguridad, permitiendo auditoría y control de configuraciones.
- b. Capacidad de validar el estado y la correcta aplicación de las reglas desplegadas en los diferentes sitios o recursos.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.35 Garantizar que el sistema registre solicitudes en tiempo real, incluyendo detalles como IP, geolocalización, URI, agente de usuario y referenciadores, integrándose con las plataformas de monitoreo de la entidad.

Garantizamos el registro en tiempo real de las solicitudes realizadas a las aplicaciones web mediante el uso de servicios nativos de AWS, específicamente Amazon CloudWatch Logs Insights y VPC Flow Logs. A través de estos mecanismos se capturan y analizan datos como dirección IP, geolocalización, URI solicitada, agente de usuario y referenciadores, permitiendo la trazabilidad del tráfico, el monitoreo operativo y el soporte a la identificación de eventos de seguridad y desempeño, asegurando la integridad y control de las aplicaciones web institucionales.

Los siguientes servicios tuvieron un comportamiento estable.

Service	RSS	Today	4 Feb	3 Feb	2 Feb	1 Feb	31 Jan	30 Jan
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

Service	RSS	9 Feb	8 Feb	7 Feb	6 Feb	5 Feb	4 Feb	3 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted

Service	RSS	16 Feb	15 Feb	14 Feb	13 Feb	12 Feb	11 Feb	10 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted

Service	RSS	Today	22 Feb	21 Feb	20 Feb	19 Feb	18 Feb	17 Feb
Amazon Elastic Compute Cloud (N. Virginia)								
Amazon Elastic Container Service (N. Virginia)								
Amazon Elastic File System (N. Virginia)								
Amazon Elastic Load Balancing (N. Virginia)								
Amazon Virtual Private Cloud (N. Virginia)								
AWS Elastic Disaster Recovery (N. Virginia)								
AWS Site-to-Site VPN (N. Virginia)								

[View post-event summaries](#)

Operating normally Impacted Degraded Disrupted

Documento Anexo: Informe de monitoreo y disponibilidad Alcaldía de Cali

4.36 Administración de listas de IP anónimas, así como la rápida propagación de las reglas de seguridad definidas, con tiempos de actualización que no superen los cinco minutos en entornos productivos

Garantizamos la administración de listas de IP anónimas mediante el uso de AWS Web Application Firewall (AWS WAF) sobre la infraestructura desplegada en AWS. A través de este servicio, gestionamos listas de bloqueo automático (blacklists) y listas de permitidos, así como reglas *rate-based* que permiten identificar y mitigar comportamientos anómalos o tráfico malicioso, incluyendo accesos automatizados y picos inusuales de solicitudes. Las reglas de seguridad definidas se propagan de forma automática a los entornos productivos, con tiempos de actualización inferiores a cinco minutos, garantizando una respuesta oportuna ante eventos de seguridad y asegurando la protección continua de las aplicaciones web institucionales de la Alcaldía de Santiago de Cali.

Documento Anexo: ACA - Procedimiento de Gestión de IPs y Reglas

4.37 Disponibilidad de canal Interconnect 1000 Mbps

En el marco de la infraestructura tecnológica implementada para la Alcaldía de Santiago de Cali, se habilitó un esquema de conectividad híbrida que garantiza la disponibilidad, continuidad y resiliencia del canal Interconnect de 1000 Mbps establecido entre la infraestructura local de la entidad y los servicios desplegados en AWS.

Este diseño contempla la integración entre el enlace AWS Direct Connect, configurado sobre uno de los canales de Internet institucional, con el fin de asegurar la continuidad operativa ante cualquier evento de indisponibilidad o degradación del enlace principal.

1. Integración del Canal Direct Connect 1000 Mbps

El enlace Direct Connect correspondiente a la cuenta de networking de la Alcaldía ha sido:

- Desplegado y configurado conforme a los lineamientos de arquitectura definidos para la solución.
- Integrado con las VPC y servicios de AWS que soportan las cargas de trabajo del proyecto.
- Validado a nivel de operación, rutas, propagación BGP y performance.

Según el estado registrado en la consola, el recurso Direct Connect se encuentra activo, estable y funcional, operando como canal principal de intercambio de datos entre la infraestructura local y la plataforma cloud.

2. Arquitectura de Alta Disponibilidad: Activo-Activo / Activo-Pasivo

Estos canales operan bajo un esquema de alta disponibilidad, permitiendo:

- Modo Activo-Activo: Cuando la arquitectura requiere balanceo de carga o distribución dinámica del tráfico.
- Modo Activo-Pasivo con Failover Automático: Mecanismo que detecta anomalías y conmuta inmediatamente hacia la VPN sin afectar las conexiones ni los servicios.

El sistema de enrutamiento supervisa permanentemente:

- Pérdida de conectividad.
- Incremento inusual de latencia.
- Interrupciones o degradaciones del Direct Connect.

Ante cualquier evento, el tráfico se desvía automáticamente hacia la VPN, asegurando continuidad sin intervención manual.

3. Garantía de Redundancia y Resiliencia Operacional

La configuración combinada de Direct Connect proporciona una infraestructura de comunicación robusta y alineada con las buenas prácticas de arquitectura híbrida:

- Redundancia: Dos canales independientes operando como rutas principales y de contingencia.
- Resiliencia: Recuperación sin interrupciones ante fallas del enlace dedicado.
- Estabilidad: Mantiene operativos los sistemas críticos incluso en escenarios adversos.
- Seguridad: Ambos canales funcionan bajo cifrado y estándares de seguridad compatibles con AWS y con la normativa institucional.

Este esquema permite asegurar la disponibilidad continua de:

- Servicios cloud estratégicos.
- Cargas virtualizadas y aplicaciones institucionales.
- Procesos misionales del Distrito que dependen de la interconexión híbrida.

The screenshot shows the AWS console interface for a transit gateway route table. The top section displays details for the route table 'tgw-rtb-03f2b8b2696919c22', including its ID, state (Available), and default association and propagation route tables. Below this, there are tabs for 'Associations', 'Propagations', 'Prefix list references', 'Routes', and 'Tags'. The 'Routes' tab is active, showing a filter section for 'Filter routes by CIDR (2)' with input fields for 'Exact CIDR', 'Longest prefix match', 'Supernet of match', and 'Subnet of match'. The main area displays a table of 9 routes with columns for CIDR, Attachment ID, Resource ID, Resource type, Route type, Route status, and Prefix list ID.

CIDR	Attachment ID	Resource ID	Resource...	Route...	Route st...	Prefix list ID
10.10.14.0/24	igw-attach-025a988472581add1	vpc-0f362e7b77050c398	VPC	Propagated	Active	-
10.10.15.0/24	igw-attach-00c7b53fbb55ba664	vpc-0dcaad1778984a574	VPC	Propagated	Active	-
10.130.0.0/22	igw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
10.30.104.0/21	igw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Propagated	Active	-
10.30.80.0/24	igw-attach-0386dc1a552706c26	vpc-0cf54cc1645db5b7d	VPC	Propagated	Active	-
10.98.0.0/16	igw-attach-01118378cfe1bd73c	vpc-0577102c2eb4b5892	VPC	Propagated	Active	-
172.18.0.0/16	igw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-
172.18.26.0/27	igw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-
172.18.8.0/24	igw-attach-063ac2c006bb3925b	vpc-0cbf0e3a42f7f21a0	VPC	Static	Active	-

Documento Anexo: Informe de Estado Direct Connect ACA



HIGH TECH SOFTWARE S.A.S
 NIT 900.718.336-7
 CARRERA 7 # 71-21 TORRE A PISO
 12
 Tel: (601) 7703250
 Bogotá - Colombia
 administrativocol@Blend360.com
 nuvu.cc



Factura electrónica de venta
 No. EHTS 2196

Señores	SANTIAGO DE CALI DISTRITO ESPECIAL DEPORTIVO CULTURAL TURISTICO EMPRESARIAL Y DE SERVICIOS		
NIT	890.399.011-3	Teléfono	(000) 6531063
Dirección	AV 2 NORTE 10 70 CEN ADMINISTRATIVO MUNICIPAL CAM TO ALCALDI ACALI	Ciudad	Cali - Colombia

Fecha y hora Factura	
Generación	23/02/2026, 14:56
Expedición	23/02/2026, 15:06
Vencimiento	25/03/2026

Ítem	Descripción	Cantidad	Vr. Unitario	Valor desc.	Vr. Bruto	Impto. Cargo
1	[P0375] sxc02--NUV-HOU-03-01-Software General-Otro-High Tech Software S.A.S - N/A-SAAS-N/A-N/A-Unidad-N/A-Mensual-Houndoc	306,043.40	4,736.00	0.00	1,449,421,542.40	0 %
2	[P0375] sxc02--NUV-HOU-01-05-Software General-Otro-High Tech Software S.A.S - N/A-SAAS-N/A-N/A-Unidad-N/A-Mensual-Houndoc	3.00	238,189,032.00	0.00	714,567,096.00	0 %

Total items: 2

Total Bruto	2,163,988,638.40
Total a Pagar	2,163,988,638.40

Valor en Letras:

Dos mil ciento sesenta y tres millones novecientos ochenta y ocho mil seiscientos treinta y ocho pesos m/cte con cuarenta cent.

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2026-03-25 por \$ 2,163,988,638.40

Observaciones:

OC 151305
 Gran Contribuyente para ICA en Bogotá Res. DDI-029334 de 31 de octubre de 2025.

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764098636526 aprobado en 20250915 prefijo EHTS desde el número 2001 al 10000 Vigencia: 24 Meses**

Responsable de IVA - Actividad Económica 6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Tarifa 9.66
CUFE: 45c5cd872ed60602838e6a989dd8b5d9ca1bc445a0b3733440c53903f94739df68799e4d73e5da78d37623a1b4a39b6a



HIGH TECH
SOFTWARE
S.A.S
NIT
900.718.336-7
Calle 56 #36A-
09
Tel: (601)
3215050286
Bogotá -
Colombia



Nota Crédito
No. 2 372

Señores	SANTIAGO DE CALI DISTRITO ESPECIAL DEPORTIVO CULTURAL TURISTICO EMPRESARIAL Y DE SERVICIOS		
NIT	890.399.011-3	Teléfono	(000) 6531063
Dirección	AV 2 NORTE 10 70 CEN ADMINISTRATIVO MUNICIPAL CAM TO ALCALDI ACALI	Ciudad	Cali - Colombia

Fecha Nota Crédito	2026-02-23
Factura de Venta	EHTS-2196
Generación	23/02/2026, 19:58
Expedición	23/02/2026, 19:58
Vencimiento	25/03/2026

Ítem	Descripción	Cantidad	Vr. Total
1	Ajuste al peso	1.00	0.40

Total items: 1

Valor en Letras:

pesos m/cte con cuarenta cent.

Condiciones de Pago:

Instrumento de pago no definido - Cruce de vencimiento - Cuota No. \$ 0.40
001 vence el 2026-03-25 por

Total Bruto	0.40
Total	0.40

Observaciones:

OC 151305
Gran Contribuyente para ICA en Bogotá Res. DDI-029334 de 31 de octubre de 2025

CUDE: 150f59966ed7041607e770d2a06c125beb615037227da26cf6d2a6e4568ba0c45e47ccea8285409b7d6fb40474f6a0a2

CUFE factura:

45c5cd872ed60602838e6a989dd8b5d9ca1bc445a0b3733440c53903f94739df68799e4d73e5da78d37623a1b4a39b6a

Informe del Revisor Fiscal

NUVUCER089

A la Administración de High Tech Software S.A.S

13 de febrero del 2026

En mi calidad de Revisor Fiscal de **High Tech Software S.A.S** identificada con Nit. 900.718.336-7 he efectuado los procedimientos de revisión que se detallan a continuación con el propósito de verificar los pagos efectuados por la Compañía por concepto de aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), durante el semestre comprendido entre el mes de agosto del 2025 y el mes de enero del 2026. El pago de dichos aportes es responsabilidad de la Administración de la Compañía como parte de su gestión. Mi responsabilidad de acuerdo con lo establecido en la regulación colombiana es emitir un informe sobre el cumplimiento de tales obligaciones.

Los procedimientos de revisión realizados fueron los siguientes:

1. Indagación con el personal del área responsable, en relación con los procedimientos utilizados para la identificación y pago de los aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).
2. Obtención del listado de liquidación de aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), preparado por la Compañía para el semestre comprendido entre el mes de agosto del 2025 y el mes de enero del 2026.
3. Comparación del listado obtenido según se menciona en el numeral anterior, con los documentos soporte de los respectivos pagos efectuados por la Compañía.

Con base en el resultado de los procedimientos enumerados anteriormente, informo que, durante el semestre comprendido entre el mes de agosto del 2025 y el mes de enero del 2026, la Compañía efectuó los pagos de los aportes de sus empleados a los sistemas de salud, pensiones y riesgos laborales y a las cajas de

compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Este informe se expide por solicitud de la Administración de la Compañía, para ser entregado dentro de sus procesos de licitación y legalización de contratos con terceros, y no debe ser utilizado para propósitos diferentes, ni distribuido a otros terceros.




Tatiana Prada Mejía
TP- 140139-T
Revisora Fiscal Designada
Cube Consultores S.A.S.

República de Colombia
Ministerio de Comercio Industria y Turismo

JUNTA CENTRAL DE CONTADORES
TARJETA PROFESIONAL
DE CONTADOR PÚBLICO

140139-T

**YERRY TATIANA
PRADA MEJIA**
C.C. 40330919
RESOLUCION INSCRIPCION 10 FECHA 12/02/2009
UNIVERSIDAD COOPERATIVA DE COLOMBIA


PRESIDENTE 

LUIS ALONSO COLMENARES RODRIGUEZ 150468

USO EXCLUSIVO DE HIGH TECH SOFTWARE S. A. S

PRIMA COPIA 63636

Esta tarjeta es el único documento que lo acredita como
CONTADOR PÚBLICO de acuerdo con lo establecido en
la Ley 43 de 1990.
Agradecemos a quien encuentre esta tarjeta devolverla
al Ministerio de Comercio Industria y Turismo - Junta Central
de Contadores.



UNIDAD
ADMINISTRATIVA
ESPECIAL

**JUNTA CENTRAL
DE CONTADORES**



Certificado No:

A 6 7 9 9 0 8 7 2 8 8 8 6 7 1 0

**LA REPUBLICA DE COLOMBIA
MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
UNIDAD ADMINISTRATIVA ESPECIAL
JUNTA CENTRAL DE CONTADORES**

**CERTIFICA A:
QUIEN INTERESE**

Que el contador público **YERRY TATIANA PRADA MEJIA** identificado con CÉDULA DE CIUDADANÍA No 40330919 de VILLAVICENCIO (META) Y Tarjeta Profesional No 140139-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de Inscripción.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS *****

Dado en BOGOTA a los 9 días del mes de Diciembre de 2025 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.


SANDRA MILENA BARRIOS PULIDO
DIRECTOR GENERAL

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web www.jcc.gov.co digitando el número del certificado



INDICE DERECHO

FECHA DE NACIMIENTO **10-MAR-1984**

BUCARAMANGA
(SANTANDER)

LUGAR DE NACIMIENTO

1.57
ESTATURA

O+
G.S. RH

F
SEXO

04-JUL-2002 VILLAVICENCIO
FECHA Y LUGAR DE EXPEDICION


REGISTRADORA NACIONAL
ALMABEATRIZ RENGIFO LOPEZ



A-5200100-69144511-F-0040330919-20060130

07740 06027A 02 185924841

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL

CEDULA DE CIUDADANIA

40.330.919

NUMERO


PRADA MEJIA

APELLIDOS

YERRY TATIANA

NOMBRES




FIRMA

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

1.090.394.391

NUMERO

VILLAMIZAR BOHORQUEZ

APELLIDOS

DIANA CAROLINA

NOMBRES



Diana C Villamizar B

FIRMA



INDICE DERECHO

FECHA DE NACIMIENTO 01-JUL-1988

CUCUTA
(NORTE DE SANTANDER)

LUGAR DE NACIMIENTO

1.68

ESTATURA

A+

G.S. RH

F

SEXO

25-AGO-2006 CUCUTA

FECHA Y LUGAR DE EXPEDICION

Almabeatriz Rengifo Lopez
REGISTRADORA NACIONAL
ALMABEATRIZ RENGIFO LOPEZ



P-2500100-57153272-F-1090394391-20061020

0142706292B 02 220276254

2. Concepto Actualización

4. Número de formulario

141231606801



(415)7707212489984(8020) 000014123160680 1

5. Número de Identificación Tributaria (NIT)

9 0 0 7 1 8 3 3 6

6. DV

7

12. Dirección seccional

Impuestos de Bogotá

14. Buzón electrónico

3 2

IDENTIFICACIÓN

24. Tipo de contribuyente

Persona jurídica

25. Tipo de documento

1

26. Número de Identificación

Lugar de expedición

28. País

29. Departamento

30. Ciudad/Municipio

31. Primer apellido

32. Segundo apellido

33. Primer nombre

34. Otros nombres

35. Razón social

HIGH TECH SOFTWARE S. A. S

36. Nombre comercial

37. Sigla

UBICACIÓN

38. País

COLOMBIA

1 6 9

39. Departamento

Bogotá D.C.

1 1

40. Ciudad/Municipio

Bogotá, D.C.

0 0 1

41. Dirección principal

CR 7 71 21 TO A P 12

42. Correo electrónico

administrativocol@Blend360.com

43. Código postal

44. Teléfono 1

6 0 1 7 7 0 3 2 5 0

45. Teléfono 2

3 0 0 2 4 1 2 2 2 6

CLASIFICACIÓN

Actividad económica

Ocupación

Actividad principal		Actividad secundaria		Otras actividades		51. Código	52. Número establecimientos
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código	1		
6 2 0 1	2 0 1 4 0 2 2 7	6 2 0 9	2 0 1 4 0 2 2 7	6 3 1 1	6 3 1 2		

Responsabilidades, Calidades y Atributos

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
53. Código	5	7	9	1	0	1	4	4	1	4	2	4	8	5	2	5	5								

05- Impto. renta y compl. régimen ordinario 48- Impuesto sobre las ventas - IVA

07- Retención en la fuente a título de renta 52 - Facturador electrónico

09- Retención en la fuente en el impuesto 55 - Informante de Beneficiarios Finales

10- Obligado aduanero

14- Informante de exógena

41- Declaración anual de activos en el extranjero

42- Obligado a llevar contabilidad

Usuarios aduaneros

Exportadores

1	2	3	4	5	6	7	8	9	10	55. Forma	56. Tipo	Servicio	1	2	3
54. Código	2	2	3							3	3	57. Modo	2		
	11	12	13	14	15	16	17	18	19			58. CPC	9	7	

IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación

Para uso exclusivo de la DIAN

59. Anexos

SI NO

60. No. de Folios:

0

La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012.

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

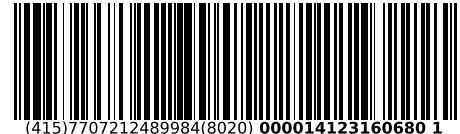
984. Nombre VILLAMIZAR BOHORQUEZ DIANA CAROLINA

985. Cargo Representante legal Certificado

Espacio reservado para la DIAN

4. Número de formulario

141231606801



(415)7707212489984(8020) 000014123160680 1

5. Número de Identificación Tributaria (NIT)

9 0 0 7 1 8 3 3 6

6. DV

7

12. Dirección seccional

Impuestos de Bogotá

14. Buzón electrónico

3 2

Características y formas de las organizaciones

62. Naturaleza

2

63. Formas asociativas

1 2

64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados

67. Sociedades y organismos extranjeros

70. Beneficio

1

65. Fondos

66. Cooperativas

68. Sin personería jurídica

69. Otras organizaciones no clasificadas

Constitución, Registro y Última Reforma

Composición del Capital

Documento	1. Constitución	2. Reforma	
71. Clase	0 4	0 4	82. Nacional 1 0 0 %
72. Número		1	83. Nacional público 0 . 0 %
73. Fecha	2 0 1 4 0 2 1 3	2 0 1 4 0 8 0 8	84. Nacional privado 1 0 0 . 0 %
74. Número de notaría			85. Extranjero 0 %
75. Entidad de registro	0 3	0 3	86. Extranjero público 0 . 0 %
76. Fecha de registro	2 0 1 4 0 2 2 7	2 0 1 4 0 9 1 0	87. Extranjero privado 0 . 0 %
77. No. Matrícula mercantil	0 2 4 2 0 3 3 6	0 2 4 2 0 3 3 6	
78. Departamento	1 1	1 1	
79. Ciudad/Municipio	4	4	
Vigencia			
80. Desde			
81. Hasta			

Entidad de vigilancia y control

88. Entidad de vigilancia y control

Superintendencia de Sociedades

5

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	8 0	2 0 1 6 0 8 0 4		-
2				-
3				-
4				-
5				-

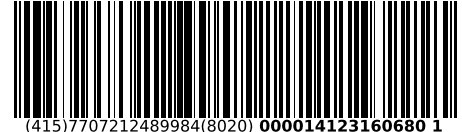
Vinculación económica

93. Vinculación económica	94. Nombre del grupo económico y/o empresarial	95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.
97. Nombre o razón social de la matriz o controlante			
170. Número de identificación tributaria otorgado en el exterior	171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP			

Espacio reservado para la DIAN

4. Número de formulario

141231606801



(415)7707212489984(8020) 000014123160680 1

5. Número de Identificación Tributaria (NIT) 9 0 0 7 1 8 3 3 6	6. DV 7	12. Dirección seccional Impuestos de Bogotá	14. Buzón electrónico 3 2
---	------------	--	------------------------------

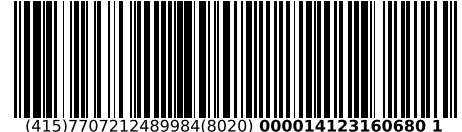
Representación

1	98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 2 5 0 7 0 1
	100. Tipo de documento Cédula de Ciudadaní	1 3	101. Número de identificación 1 0 9 0 3 9 4 3 9 1
	104. Primer apellido VILLAMIZAR	105. Segundo apellido BOHORQUEZ	106. Primer nombre DIANA
	107. Otros nombres CAROLINA	108. Número de Identificación Tributaria (NIT)	109. DV
2	98. Representación REPRS LEGAL SUPL	1 9	99. Fecha inicio ejercicio representación 2 0 2 5 0 7 3 1
	100. Tipo de documento Cédula de Ciudadan	1 3	101. Número de identificación 1 0 7 7 1 4 8 2 9 0
	104. Primer apellido ARANDIA	105. Segundo apellido CASALLAS	106. Primer nombre KAREN
	107. Otros nombres TATIANA	108. Número de Identificación Tributaria (NIT)	109. DV
3	98. Representación		99. Fecha inicio ejercicio representación
	100. Tipo de documento		101. Número de identificación
	104. Primer apellido	105. Segundo apellido	106. Primer nombre
	107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV
4	98. Representación		99. Fecha inicio ejercicio representación
	100. Tipo de documento		101. Número de identificación
	104. Primer apellido	105. Segundo apellido	106. Primer nombre
	107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV
5	98. Representación		99. Fecha inicio ejercicio representación
	100. Tipo de documento		101. Número de identificación
	104. Primer apellido	105. Segundo apellido	106. Primer nombre
	107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV

Espacio reservado para la DIAN

4. Número de formulario

141231606801



(415)7707212489984(8020) 000014123160680 1

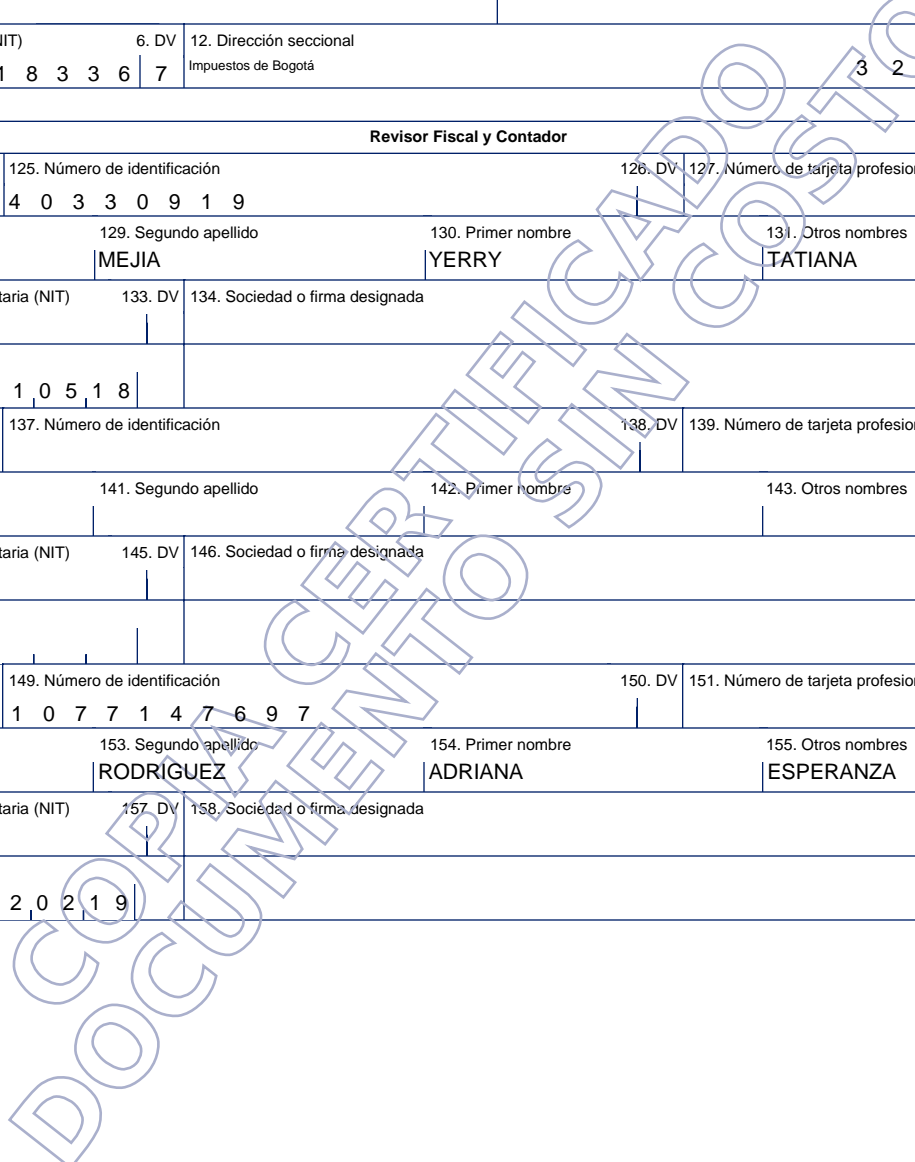
5. Número de Identificación Tributaria (NIT) 9 0 0 7 1 8 3 3 6	6. DV 7	12. Dirección seccional Impuestos de Bogotá	14. Buzón electrónico 3 2
---	------------	--	------------------------------

Revisor Fiscal y Contador

124. Tipo de documento Cédula de Ciudadanía 1 3	125. Número de identificación 4 0 3 3 0 9 1 9	126. DV	127. Número de tarjeta profesional 1 4 0 1 3 9 T
128. Primer apellido PRADA	129. Segundo apellido MEJIA	130. Primer nombre YERRY	131. Otros nombres TATIANA
132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada	
135. Fecha de nombramiento 2 0 2 1 0 5 1 8			

136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional
140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres
144. Número de Identificación Tributaria (NIT)	145. DV	146. Sociedad o firma designada	
147. Fecha de nombramiento			

148. Tipo de documento Cédula de Ciudadanía 1 3	149. Número de identificación 1 0 7 7 1 4 7 6 9 7	150. DV	151. Número de tarjeta profesional 2 3 2 8 1 4 T
152. Primer apellido CASTIBLANCO	153. Segundo apellido RODRÍGUEZ	154. Primer nombre ADRIANA	155. Otros nombres ESPERANZA
156. Número de Identificación Tributaria (NIT)	157. DV	158. Sociedad o firma designada	
159. Fecha de nombramiento 2 0 2 2 0 2 1 9			



BANCO SCOTIABANK COLPATRIA

NIT 860.034.594-1

CERTIFICA QUE

La empresa **HIGH TECH SOFTWARE S.A.S.** Con NIT **9007183367** Se encuentra vinculado en el banco a través de la **Cuenta Corriente No 1007047386**, Abierta desde el 26 de diciembre del 2018, la cual se encuentra en estado **Activo**.

La presente certificación se expide en Bogotá a los 13 días de febrero de 2026

Cordialmente,

Scotiabank Colpatria



Línea de Atención

Bogotá: 6017561616 - Cali: 6024891616 - Medellín: 6046041616 - Barranquilla: 6053851616 - Ibagué: 6082771616
Pereira: 6063401616 - Cartagena: 6056931616 - Neiva: 6088631616 - Bucaramanga: 6076971616 - Cúcuta: 6075955195
Santa Marta: 6054365966 - Villavicencio: 6086836126 - Valledupar: 6055898480 - Popayán: 6028353735
Resto del país: 018000522222

