Metro de Medellín Ltda.

Suscripción en nube, soporte y mantenimiento de plataforma de gestión del Centro Integrado de Seguridad y Emergencias – CISE

Especificaciones Técnicas

Versión 1.0

Tabla de Contenido

Tabla de Contenido 2
1. Introducción 5
2. Glosario 6
3. Antecedentes 7
3.1 Diseño actual CISE 8
3.1.1 Servicios de terceros integrados con CISE 9
3.1.2 Integración VMS 10
3.1.3 Integración ArcGIS 12
3.1.4 Integración Sistema Control de Acceso 14
3.1.5 Integración Message Bird - Integración de servicio de Envío de WhatsApp y correo electrónico con plataforma de gestión CISE 15
3.1.6 Integración datos abiertos 16
3.1.7 Integración SAP 18
3.2 Detalle técnico adicional de la plataforma CISE 18
3.3 Conectividad 21
3.3.1 WAF 21
3.3.2 AWS Control Tower 21
3.3.3 AWS Organizations 21
3.3.4 AWS Site-to-Site VPN 22
3.3.5 AWS Network Firewall 22
3.4 Arquitectura Backend 22
3.4.1 Diagrama 22
3.4.2 Servicio IAM 23
3.4.3 Servicio Amazon CloudWatch 23
3.4.4 Servicio AWS CloudTrail 24
3.4.5 Servicio SQS 24
3.4.6 AWS KMS 24
3.4.7 EKS 24
3.4.8 Amazon Managed Grafana 24

3.4.9 Amazon SES 24
3.4.10 Amazon S3 25
3.4.11 DynamoDB 25
3.4.12 Cognito 25
3.4.13 Lambda 25
3.4.14 Step Functions 25
3.4.15 API Gateway 25
3.4.16 Amazon SNS 26
3.4.17 Event Bridge 26
3.4.18 Amplify 26
3.5 Arquitectura Frontend 26
3.5.1 Diagrama 26
3.5.2 Servicio Amazon Athena 27
3.5.3 Grafana onCall 27
3.5.4 DynamoDB 28
3.5.5 Amazon Cognito 28
3.5.6 Diseño aplicado 28
4. Objeto 30
5. Alcance general 30
5.1 Servicios profesionales 30
5.2 El soporte 30
5.2.1 Niveles de soporte 30
5.2.2 Acuerdos de Nivel de Servicio (SLA) 31
5.2.3 Reportes 32
5.3 El mantenimiento 33
5.3.1 Suscripción mensual 33
5.3.2 Consumo de los servicios 33
5.3.3 Nuevas implementaciones 33
6. Alcance específico 34
6.1 Sostenimiento de la plataforma 34
6.2 Arquitectura CISE 35
6.3 Componente suscripción de servicios en nube de la solución de software del CISE 35
6.4 Personal contratista – Gestión CISE 37

6.5 Horas de configuración y desarrollo 38
6.6 Usuarios del CISE 40
6.7 Gestión y operación de recursos de nube 40
6.8 Gestión y operación de datos y reportes 41
6.9 Capacitación de la plataforma de gestión CISE 43
6.10 Documentación 43
6.10.1 Presentación de Informes 44
6.11 Garantía 44
6.12 Otros 46
6.13 Condiciones de trabajo especiales en las instalaciones del Metro de Medellín 46
7. Seguridad de la información 47
7.1 Garantía sobre el tratamiento de la información de La Empresa 47

1. Introducción

El presente documento describe las características técnicas y funcionales requeridas para la contratación del soporte, mantenimiento y atención requerimientos para la plataforma de gestión del Centro Integrado de Seguridad y Emergencias – CISE del Metro de Medellín, en adelante LA EMPRESA, que consiste en garantizar la continuidad de la suscripción de servicios implementados actualmente en nube AWS, atención de eventos sobre los desarrollos actuales, implementación de nuevos requerimientos sobre la plataforma por la modalidad de horas de desarrollo, así como la ejecución de ajustes o cambios requeridos en la plataforma para cumplir el alcance detallado en el presente documento.

Adicionalmente, se relacionan los aspectos operativos y algunos aspectos generales que regirán durante la ejecución del contrato.

2. Glosario

A continuación, presentamos un glosario de términos, como guía para el presente documento:

RPCC: Riesgo Público y Convivencia Ciudadana.

VMS: Video Manager System – Sistema de gestión de video vigilancia.

CISE: Centro Integrado de Seguridad y Emergencias. Desde donde se gestionan centralizadamente diferentes sistemas de seguridad electrónica y los procedimientos de atención de seguridad y emergencias de LA EMPRESA.

SOP: Standard Operating Procedure – procedimiento de atención de eventos que deberá ser desplegado sobre la plataforma de IOC o protocolo de operación, en CISE conocidos también como PARP (procedimiento atención de Riesgo Público).

PCC: Puesto Central de Control – Desde donde se gestiona la operación de los medios de transporte que opera LA EMPRESA.

PBEO: Patios Bello, instalación técnica ubicada en el municipio de Bello desde donde se realizan las principales actividades de mantenimiento de los trenes. Incluye edificio de Talleres, Sede Administrativa y Torre de Control.

Nube AWS: La provisión de servicios de la plataforma CISE se realizó en la nube AWS por lo que se requiere mantener en dicha nube.

Siglas de las líneas del sistema Metro:

- LTA: Línea de Tranvía de Ayacucho
- L1: Línea 1 de Buses
- LA: Línea A de Metro
- LB: Línea B de Metro
- LJ: Línea J de Metrocable
- LK: Línea K de Metrocable
- LL: Línea L de Metrocable
- LM: Línea M de Metrocable
- LH: Línea H de Metrocable
- LP: Línea P de Metrocable
- PMIR, TYC o T&C: Talleres y Cocheras del sistema Tranviario ubicada en la estación Miraflores.

Equipo de desarrollo o configuración en nube: Grupo de profesionales del CONTRATISTA que realizará actividades de configuración y desarrollo de software requeridas por LA EMPRESA.

Desarrollador: Profesional que integra el equipo de desarrollo del CONTRATISTA.

3. Antecedentes

La Empresa constantemente ejecuta acciones en los componentes de seguridad física, de infraestructura, electrónica, humano y procedimental tendientes a disminuir la probabilidad de ocurrencia y la severidad de eventos que alteren la seguridad y la convivencia en las instalaciones de LA EMPRESA.

En este sentido, LA EMPRESA cuenta con el Centro Integrado de Seguridad y Emergencias - CISE, donde confluyen diferentes sistemas utilizados con un enfoque proactivo, para atender los eventos de Riesgo Público y de Emergencias en todas sus instalaciones.

El CISE es operado por la Gerencia Social y de Servicio al Cliente a través de su personal de Riesgo Público y Convivencia Ciudadana – RPCC y su propósito principal es contribuir con una operación segura y sostenible.

Atendiendo las nuevas necesidades de la gestión de seguridad y atención de emergencias se implementó a finales del año 2023 en nube del proveedor AWS la plataforma de Gestión CISE, la cual integra diferentes sistemas de seguridad, tiene implementados los protocolos de atención para guiar paso a paso a los analistas en las acciones que se deben realizar y registrar para la atención de los eventos de seguridad y emergencia en los que participan.

Actualmente la plataforma de gestión CISE, tiene integración con la plataforma de Gestión de Video VMS Milestone, el sistema de mapas ArgGis, el ERP SAP, el sistema de control de acceso Insitel. Los servicios de nube AWS actualmente implementados permitieron la migración de datos de diferentes repositorios Metro, captura, limpieza, extracción de datos, almacenamiento de datos, gestión de usuarios, gestión de reportes, implementación de protocolos de operación PARP, gestión de la seguridad, así como las integraciones entre los diferentes sistemas Metro.

En este apartado se explicará la implementación realizada en AWS para que los proponentes realicen las estimaciones necesarias para valorar el soporte, mantenimiento y los nuevos requerimientos. Sin embargo, existe información como detalles de conectividad, datos de los eventos de seguridad y emergencias, mayor detalle de integraciones que son confidenciales para LA EMPRESA pero que estarán a disposición de EL CONTRATISTA para el cumplimiento del presente alcance.

Se presenta como anexo el manual de usuario funcional que detalla todas las características de la plataforma implementadas para los operadores CISE.

Los siguientes documentos anexos se aportan para la ampliación de la información técnica requerida para las valoraciones por parte de los interesados:

- ANEXO 1 - Message Broker.
- ANEXO 2 – Manual Usuario Funcional CISE

3.1 Diseño actual CISE

A continuación, se muestra una figura ilustrativa de la arquitectura base del CISE, la cual se detallará a lo largo del presente numeral:

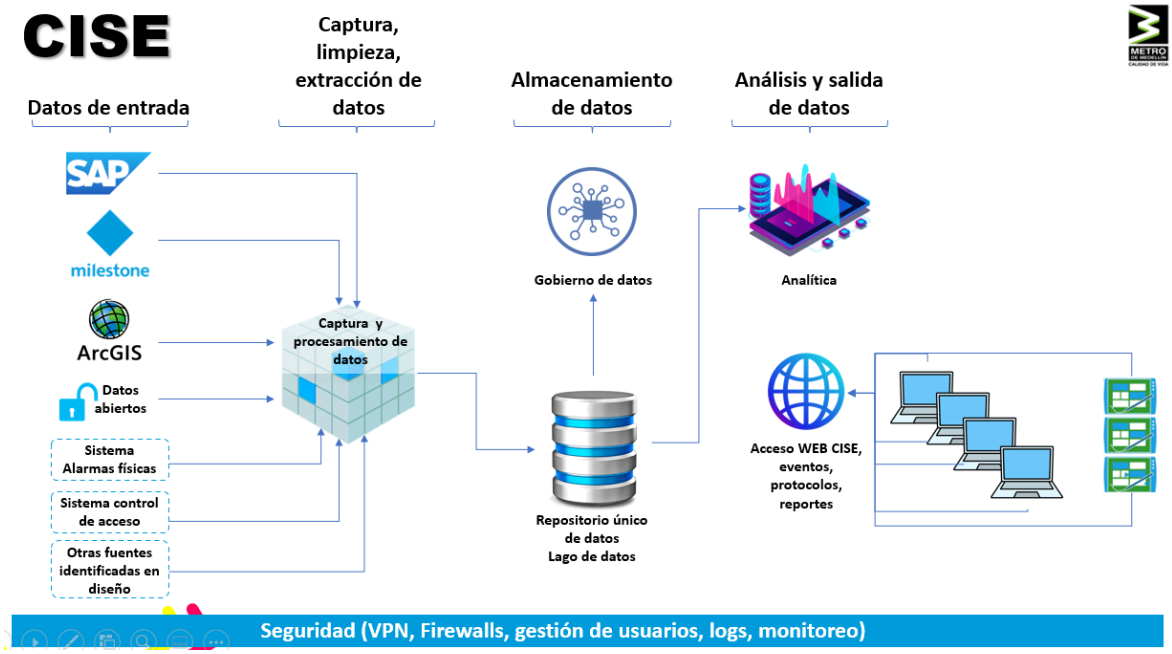

Imagen 1: Arquitectura básica CISE

La arquitectura implementada es 100% serverless (sin administración de servidores), lo que permite manejar los costos orientados a la transacción, en este caso el mensaje, sin costos adicionales por licenciamiento para El Metro.

3.1.1 Servicios de terceros integrados con CISE

Nombre	Descripción	Uso y limitantes	Acceso	Tipo
ArcGIS	Permite obtener mapas e información vía WS	Para adquirir información detallada sobre la ubicación de las estaciones y edificios del sistema Metro. Incluye el acceso a capas específicas creadas por el equipo de ArcGIS de Metro, como las estaciones del sistema, cámaras de vigilancia y las líneas del sistema.	REST Service	Transaccional y analítica
SAP	Obtener información de formularios que el personal de Metro diligencia desde las estaciones. Los hechos relevantes en la operación.	Requerida a nivel de transacciones cómo a nivel de analítica. Se realiza con el llamado de 2 WS expuestos por SAP o se obtendrá la información hasta de 2 tablas.	jdbc a una base de datos	Transaccional y analítica
VMS de sensores volumétricos.	Permite obtener información de los sensores volumétricos	Usando el SDK de Milestone se obtienen los eventos con cierta regularidad.	Vía SDK	Transaccional
Whatsapp	Envía mensaje de Whatsapp	Envía mensaje de Whatsapp vía http/rest que expone la red social, se publicarán hasta 20.000 mensajes al mes.	HTTP/REST	Transaccional
Enviar Correo	Envía email vía SMTP	Envía email vía SMTP, en AWS SES (simple email service) una cuenta de correo cise@metrodemedellin.gov.co para realizar el envío. Se enviarán hasta 100.000 correos al mes.	SMTP	Transaccional
Embeber VMS - CCTV	Permite que el operador tenga acceso al vídeo usando la consola	Seleccionar una cámara en el mapa y presentarla directamente en la consola del operador, para esto se usó javascript que permite embeber este contenido en la consola. Se asume el uso de máximo 5 llamadas al WS de Milestone simultáneas.	http o https	Transaccional

Nombre	Descripción	Uso y limitantes	Acceso	Tipo
		También permite traer en vivo y en directo ante la ocurrencia de un evento y publicar en el videowall la/las cámaras asociadas a eventos de video analítica de aquellas cámaras que lo tienen, ejemplo Patio de Bello con la integración de la fibra perimetral, PCC.		
Embeber correo	Permite al operador ver correos (filtrados) en la consola como eventos	Vía AWS SMS (Simple Email Service) se configura solo una cuenta de correo para mensajes entrantes y se configuraron hasta 5 filtros para solo crear los eventos importantes en la consola del operador.	SMTP	Transaccional
Control de acceso	Captura de eventos y reenviado a VMS después de presentado al operador en CISE	Se configuraron los siguientes eventos • Puerta mantenida abierta. • apertura forzada, • usuario no autorizado, • falla sistema	HTTP/REST o jdbc	Transaccional
Datos abiertos	Usar fuentes de datos abiertos para evaluar impacto a nivel de riesgo público.	Correlacionar eventos pasados cerca o dentro de las instalaciones de Metro, con el fin de evaluar información de interés, ya sea, sectores que necesiten refuerzo policial, mayor vigilancia por parte del sistema de cámaras o investigaciones policiales, para correlacionar víctimas, victimarios, elementos y acontecimientos.	https	Transaccional y analítica

3.1.2 Integración VMS

Dentro de los datos de entrada actuales se encuentra el VMS Milestone Corporate siendo el gestor de Video de LA EMPRESA.

VMS es un software que se utiliza para administrar, visualizar y almacenar vídeo y datos relacionados con la vigilancia por video en el Metro de Medellín. Permite a los usuarios monitorear múltiples cámaras de video en tiempo real, grabar y almacenar imágenes de video, gestionar la configuración de las cámaras, así como realizar análisis de video y búsqueda de eventos grabados.

Además, puede integrarse con otros sistemas de seguridad, como sistemas de control de acceso o sistemas de detección de intrusos, para proporcionar una solución de seguridad más completa y coordinada.

El analista puede visualizar desde la plataforma cualquier cámara implementada en el VMS, también verá de manera automática la reproducción del video que se active por alguna video analítica en cualquiera de las cámaras configuradas con esta función tanto en Patio Bello como en otras ubicaciones. Para lograr la visualización automática del video en vivo de las cámaras en la Plataforma de Gestión CISE desde el Sistema de Gestión de Video (VMS) cuando se detecte una alerta proveniente de la analítica de video o de la solución de fibra perimetral, se implementó un servicio en la Plataforma de Gestión CISE que consume el servicio web SOAP de Milestone, indicado de manera general a continuación:

Autenticación: El proceso de autenticación se inicia con una solicitud de acceso al Directorio Activo a través del protocolo NTLM. Se envían las credenciales requeridas para la autenticación, y el Directorio Activo procede a validar dichas credenciales. En caso de ser correctas, se genera y devuelve un token de autorización.

Integración con VMS mediante la biblioteca SOAP: Se estableció una conexión con el sistema de gestión de video (VMS) mediante la biblioteca SOAP. Posteriormente, se ejecutan consultas al VMS con el fin de obtener tanto el flujo de video de las cámaras como los registros de las alarmas.

Consumo de Servicios de Alarmas: El token de autorización obtenido en el proceso de autenticación se emplea para acceder a los servicios de alarmas proporcionados por el VMS. A continuación, la información de las alarmas se transfiere a una función lambda para su posterior procesamiento.

Función Lambda: La función lambda recibe los registros de alarmas provenientes del VMS. Luego, esta función se encarga de procesar los registros de manera adecuada y los envía al message broker para su distribución y gestión posterior.

Message Broker: El message broker recibe los registros de las alarmas enviados por la función lambda y se responsabiliza de su distribución a los diferentes consumidores, tales como la base de datos y otras aplicaciones. Posteriormente, los registros de las alarmas son almacenados en la base de datos, utilizando un esquema adecuado que garantiza una estructuración eficiente y segura de la información.

Recepción en la Plataforma CISE: La Plataforma CISE emplea el protocolo GraphQL para recibir los registros de las alarmas directamente desde la base de datos. Estos registros son procesados y presentados de manera apropiada en la interfaz de usuario de la aplicación, lo que asegura una visualización clara y comprensible de la información. Este proceso posibilita una integración eficaz entre el sistema de gestión de video (VMS) y la Plataforma CISE, lo que facilita la monitorización y gestión centralizada y eficiente de las alarmas.



Imagen 2: ejemplo visualización de cámaras desde plataforma CISE

3.1.3 Integración ArcGIS

ArcGIS es una plataforma líder en sistemas de información geográfica (SIG) desarrollada por Esri, en la actualidad Metro cuenta con un servidor privado y público en donde se encuentran las diferentes capas de la plataforma CISE.

Se encuentran los siguientes Map Servers

- Cise/Camaras_cise (MapServer)
  - Domo (6 id)
  - Domo y fijas (5 id)
  - Domo +360 (4 id)
  - Fija (3 id)
  - Interfono (2 id)
  - Redscan (1 id)

- Cise/Hidrantes_CentrosSalud (MapServer)
  - Centros de salud (0 id)

- Hidrante (1 id)
- Comunas (2 id)
- Barrios (3 id)

- Cise/Sistema Metro (MapServer)
  - Estaciones Sistema Metro (0 id)
  - Edificaciones Sistema Metro (1 id)
  - Líneas Sistema (2 id)

- Cise/Zonas Seguridad Física (MapServer)
  - Zonas RPCC Puntos (0 id)
  - Zonas RPCC Líneas (1 id)
  - Zonas RPCC (2 id)
  - Estructura Delincuencial (3)
  - Valle de Aburrá (4)
  - Barrios Sabaneta (5)
  - Barrios La Estrella (6)

Autenticación con el servidor ArcGis: utiliza OAuth 2.0 como un protocolo estándar para la autenticación y la autorización en sus servicios y aplicaciones. Aquí hay una explicación básica de cómo ArcGIS utiliza OAuth 2.0 para la autenticación:

El método que se emplea para acceder a los servicios de Arcgis es el de **Recepción del token de acceso**: Si la solicitud es válida, el servidor de autorización de ArcGIS responde con un token de acceso. Este token de acceso es un identificador que la aplicación puede utilizar para realizar solicitudes en nombre del usuario autenticado durante un período de tiempo limitado.



Imagen 3: Visualización de Capas en mapa

3.1.4 Integración Sistema Control de Acceso

La integración se realiza por un servicio web que permite filtrar elementos según un rango de fechas y número de página. El servicio web es llamado por una función lambda, la cual actúa como intermediario entre el sistema de control de acceso y la plataforma.

Esta función lambda realizará el filtrado de los elementos recibidos del Metro de Medellín y los enviará al message broker para su posterior procesamiento.

El message broker AWS se encargará de enviar los datos filtrados a una segunda función lambda, la cual tendrá la tarea de escribir estos datos en la tabla "Alarms" de la base de datos DynamoDB. Esta tabla almacena la información de las alarmas registradas en el sistema de control de acceso.

Para garantizar una actualización continua de la Plataforma CISE con la información más reciente sobre las alarmas, se utiliza el protocolo GraphQL. De esta manera, cada vez que se registre una nueva entrada en la tabla de la base de datos, la Plataforma CISE se actualizará automáticamente con estos datos.

En resumen, esta funcionalidad permite una integración fluida entre el sistema de control de acceso del Metro de Medellín y la plataforma CISE, asegurando que se está siempre al tanto de las alarmas y eventos relevantes para la operación del Metro.



Imagen 4: Visualización tabla alarmas del Sistema Control de Acceso

3.1.5 Integración Message Bird - Integración de servicio de Envío de WhatsApp y correo electrónico con plataforma de gestión CISE

La integración con Message Bird se realiza con el objetivo de utilizar las APIs oficiales de META para el envío de mensajes. En este proceso, la plataforma de gestión CISE genera un template para enviar mensajes a través de la API de notificaciones. Dicha API se comunica con una función Lambda que transmite el token y la solicitud a través de la API de Message Bird, lo que facilita el envío del template al número o grupo de números seleccionados.

Para llevar a cabo el envío de mensajes a través de WhatsApp, se registró un número específico en la cuenta de META de Metro de Medellín. Este número no requiere estar conectado constantemente a internet.

Para el envío de correos electrónicos, se utilizó el **servicio de Amazon SES**, y el registro se lleva a cabo a través de la consola de AWS. Una vez registrado en SES, Amazon envía una notificación al correo electrónico registrado para validar la suscripción. Es importante destacar que la suscripción no tiene ningún tipo de costo asociado. Además, el envío de correos electrónicos también se realiza a través de este servicio.

El envío de mensajes a WhatsApp puede dirigirse ya sea a un número específico o a un grupo de números asociados al rol de usuario correspondiente.

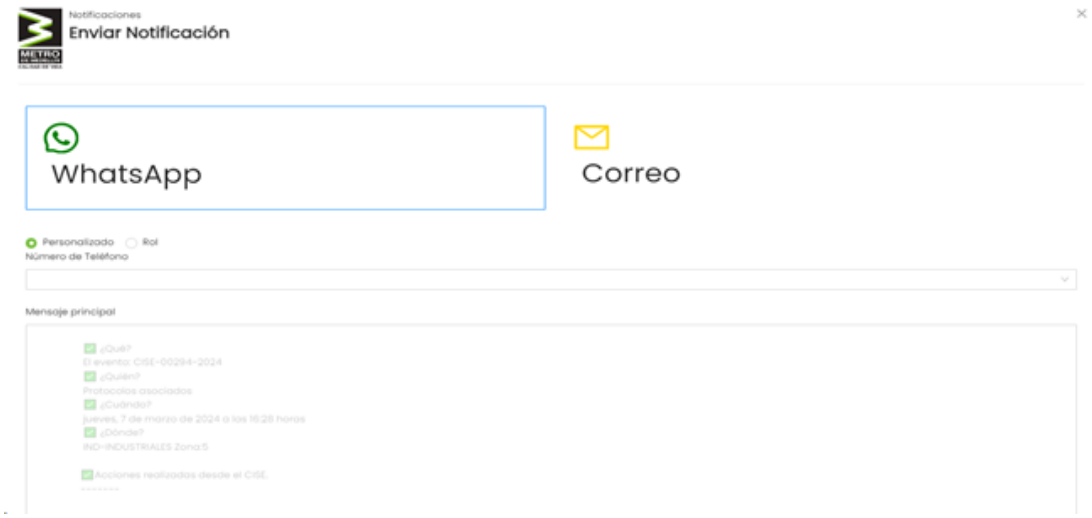

Imagen 5: Funcionalidad envío de WhatsApp

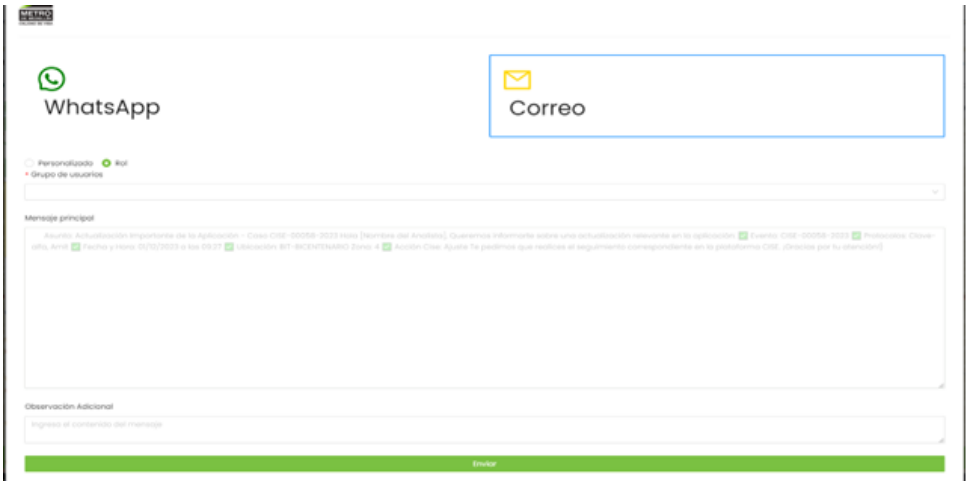

Imagen 6: Funcionalidad envío de Correo electrónico

3.1.6 Integración datos abiertos

Para el proyecto CISE 3, se especificó la necesidad de traer fuentes de datos abiertos para evaluar impacto a nivel de riesgo público, no solamente por parte de los sistemas de Metro de Medellín, sino también por organismos gubernamentales dedicados a la seguridad.

El impacto de los problemas de seguridad a nivel de extorsión y homicidio fueron los seleccionados para trabajar, mostrándose en el apartado de reportes de la aplicación de gestión CISE, para realizar este proceso se accede a la página de datos abiertos de Medellín de la Web de medata.gov.co. en donde se muestra la información recolectada y con georreferenciación.

Con la información recolectada, se cargó en el lago de datos, cabe aclarar que desde un principio esta ingesta debería ser automatizada; sin embargo, en el momento del desarrollo, medata, estaba actualizando la información y la gestión de sus APIs para ser consumidas, por lo que la información se encontraba disponible únicamente a través de una descarga directa de un archivo CSV publicado mes a mes por parte de medata. A continuación, las URL de la consulta realizada:

- https://medata.gov.co/
- Homicidios: https://medata.gov.co/dataset/1-027-23-000008
- Extorsión: https://medata.gov.co/dataset/1-027-23-000007

La visualización de los datos para el usuario final, le permitirá correlacionar eventos pasados cerca o dentro de las instalaciones de Metro, con el fin de evaluar información de interés, ya sea, sectores que necesiten refuerzo policial, mayor vigilancia por parte del sistema de cámaras o investigaciones policiales, para correlacionar víctimas, victimarios, elementos y acontecimientos.

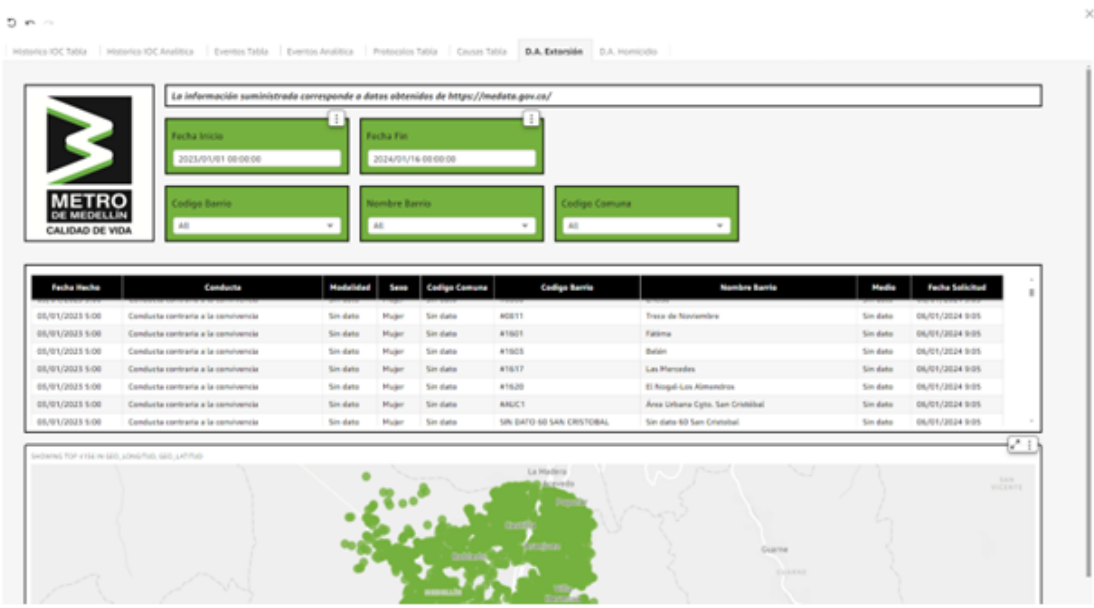

Imagen 7: Dashboard extorsión medata CISE AWS

5. Diagrama de secuencia funcional

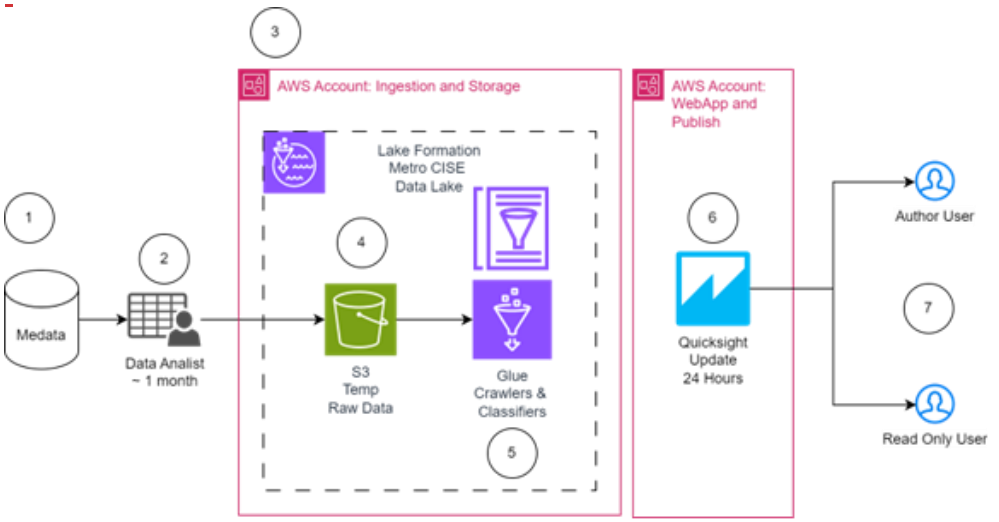

Imagen 8. Secuencia funcional

3.1.7 Integración SAP

CISE tiene integración con el ERP Corporativo SAP, con el fin de automatizar la actualización de informes de hechos relevantes IHR y generar eventos en la plataforma.

La integración desarrollada se construyó sobre una arquitectura de procesamiento de datos en AWS. La información se almacena en S3, se procesa mediante Glue Jobs, se consulta desde Athena y se visualiza en QuickSight. Como resultado, la información procesada permite alimentar la Plataforma de Gestión CISE y crear eventos automáticamente en el módulo correspondiente.

Componente	Rol en la solución	Resultado esperado
Amazon S3	Almacenamiento de archivos de entrada y datos procesados.	Información disponible para procesamiento y consulta.
AWS Glue Jobs	Procesamiento, preparación y transformación de la información.	Datos normalizados para explotación analítica y operativa.
Amazon Athena	Consulta de información procesada sobre los datos almacenados.	Base de consulta para reportes y tableros.
Amazon QuickSight	Visualización de la información mediante dashboards.	Tableros finales disponibles para consulta del equipo.
Plataforma CISE	Consumo de la información procesada para registrar eventos.	Eventos creados automáticamente en el módulo de Eventos.

La actualización de la información quedó configurada para ejecutarse diariamente a las 5:00 AM. Con esta actualización, la plataforma cuenta cada día con información procesada y disponible para la operación.

A partir de la información actualizada se crean eventos automáticamente en la Plataforma de Gestión CISE. Estos eventos quedan disponibles en el menú de Eventos, permitiendo al equipo consultar el registro generado y dar seguimiento operativo desde la plataforma.

Registro de eventos automático: En el módulo de Eventos se visualizan los registros creados automáticamente con base en la información procesada. La pantalla permite consultar eventos, ubicación, fecha de creación, tipo, riesgo, protocolos, asunto y estado.

Tablero de informes de hechos relevantes El tablero de informes de hechos relevantes fue implementado en QuickSight. La visualización permite revisar la lista de incidentes reportados, con datos como hora, ID, descripción, ubicación, reportador, tipo de riesgo y acciones inmediatas.

Adicionalmente, el tablero permite consultar la distribución por tipo de riesgo y un resumen cuantitativo de registros. Esta vista facilita el análisis operativo de los hechos relevantes registrados para el periodo seleccionado.

3.2 Detalle técnico adicional de la plataforma CISE

En AWS la plataforma de Gestión CISE está diseñada entorno a tres componentes principales: el Operation Center, el Message Broker y la Analítica Descriptiva. Estos elementos constituyen la columna vertebral de un sistema integral diseñado para optimizar y gestionar eficientemente diversas operaciones.

Arquitectura de alto nivel: A continuación, se muestran la forma cómo interactúa la arquitectura:

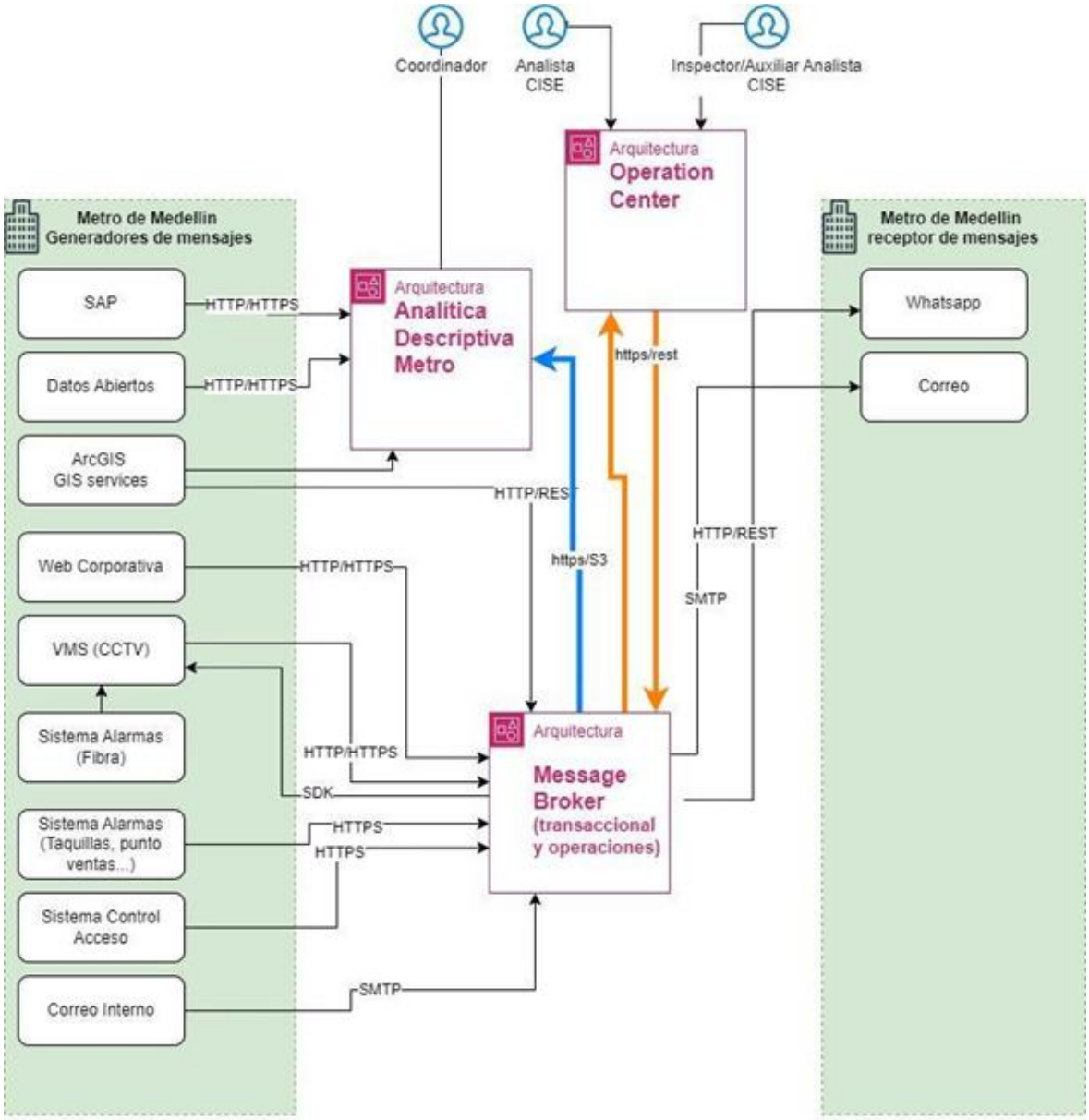

Imagen 9: Arquitectura de alto nivel CISE AWS

En este diagrama se presenta a la izquierda, los generadores de mensajes transaccionales relacionados con el centro de operaciones de Metro de Medellín, para cumplir con las mejores prácticas de integración empresarial, todos los mensajes son dirigidos al “Message Broker” que actúa como un bus de integraciones.

Metro de Medellín para el CISE implementó las siguientes premisas:

- Integraciones desacopladas.
- Un único punto de integración.

- Soluciones de código abierto.
- Servicios serverless nativos de nube.
- Uso protocolos comunes o estándar.
- Servicios administrados.

Adicionalmente se manejaron las integraciones relacionadas con analítica de las integraciones transaccionales propias de un Centro de Operaciones, esto permitió:

- Mejorar los tiempos de respuesta de los mensajes transaccionales (emergencias).
- Atomizar los mensajes transaccionales para evitar agruparlos.
- Optimizar el flujo de información histórica cómo analítica.
- Optimizar la carga de trabajo en las fuentes de información cuando no se requiere tiempo real.
- Organizar de manera separada el pipeline de analítica vs enrutamiento de mensajes transaccionales.
- Independizar los resultados: 1ro. En el caso de analítica es la generación de reportes, 2do. En caso de transacciones es el apoyo a la operación del CISE.

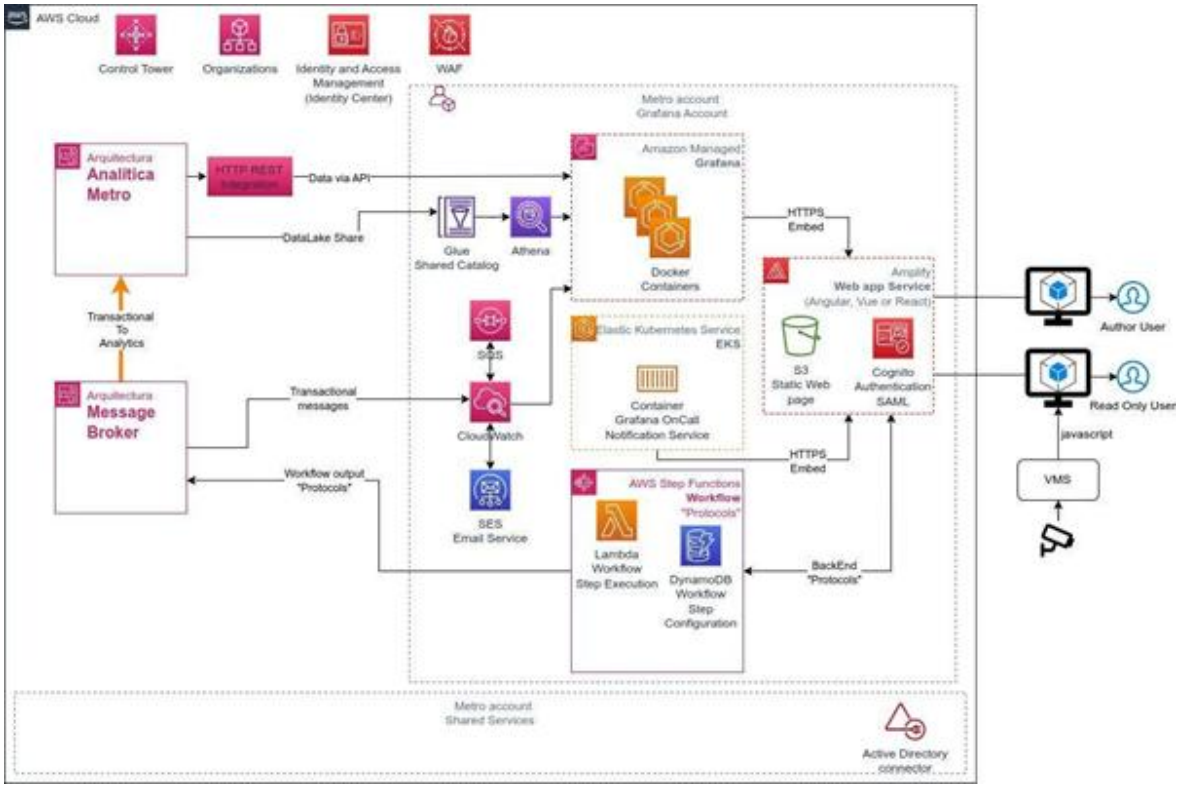

Imagen10: Detalle Arquitectura servicios AWS – CISE

3.3 Conectividad

La arquitectura CISE incluye los componentes (servicios AWS) para la gestión de la seguridad que se describen a continuación:

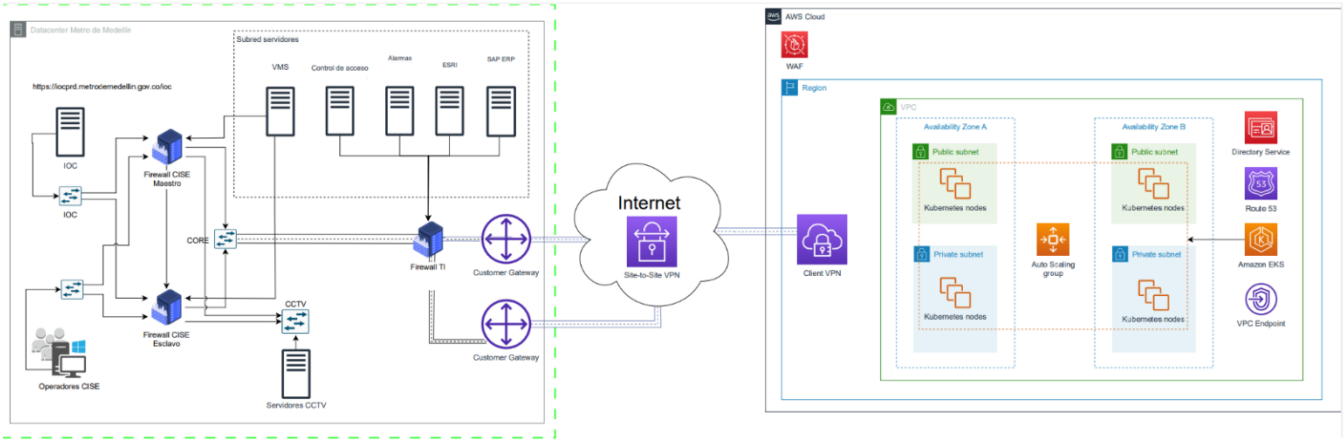

Imagen 11: Detalle arquitectura conectividad Metro – AWS

3.3.1 WAF

Web Application Firewall, permite monitorear los requerimientos HTTP y HTTPS que son atendidos por los recursos web protegidos. Para CISE, ayuda a proteger los servicios alojados en nube de técnicas comunes de ataque, como la inyección de código SQL y el scripting entre sitios (XSS). Adicionalmente, podrá crear reglas que bloquean ataques de agentes de usuarios específicos, bots malintencionados o extractores de contenido.

3.3.2 AWS Control Tower

Ofrece la forma más sencilla de configurar y controlar un entorno de AWS seguro y multicuenta. En la arquitectura diseñada para CISE, AWS Control Tower orquesta las capacidades de otros servicios de AWS incluidos AWS Organizations, AWS Service Catalog y AWS IAM Identity Center (sucesor de AWS Single Sign-On), para crear una zona de aterrizaje basada en modelos de prácticas recomendadas y permitir la gobernanza mediante controles que se pueden elegir de una lista preempaquetada.

3.3.3 AWS Organizations

Servicio de administración de cuentas que permite consolidar varias cuentas de AWS en una organización que puede crear y administrar de forma centralizada. Para este proyecto, se crearon cuentas en la organización y se invitaron a las cuentas existentes a unirse facilitando así la administración como un grupo.

3.3.4 AWS Site-to-Site VPN

Las soluciones de red privada virtual de AWS establecen conexiones seguras entre las redes del cliente en las instalaciones, las oficinas remotas, los dispositivos y la red global de AWS. AWS Site-to-Site VPN creará túneles cifrados entre la red de Metro de Medellín y los recursos de AWS, que hacen parte de la solución CISE, para que los usuarios puedan acceder experimentando los beneficios de alta disponibilidad, seguridad y rendimiento entre otros.

3.3.5 AWS Network Firewall

AWS Network Firewall es un servicio administrado de AWS que facilita la implementación de protecciones de red básicas para Amazon Virtual Private Clouds (VPC), como se observa en el diagrama. AWS Network Firewall está indicado para clientes que deseen inspeccionar y filtrar el tráfico hacia, desde o entre sus VPC de Amazon.

3.4 Arquitectura Backend

A continuación, se presenta la arquitectura y los servicios implementados en backend del CISE:

3.4.1 Diagrama

El siguiente diagrama presenta la arquitectura en bloques utilizada en CISE:

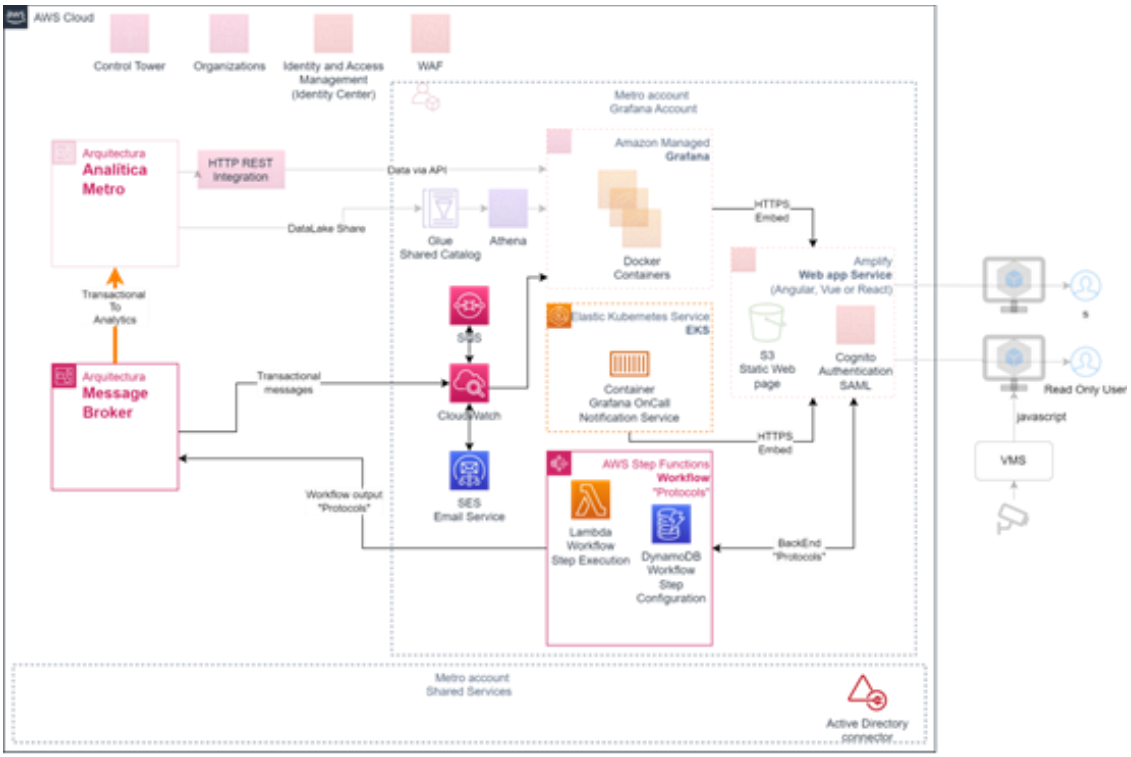

Imagen 72: Detalle Arquitectura backend CISE

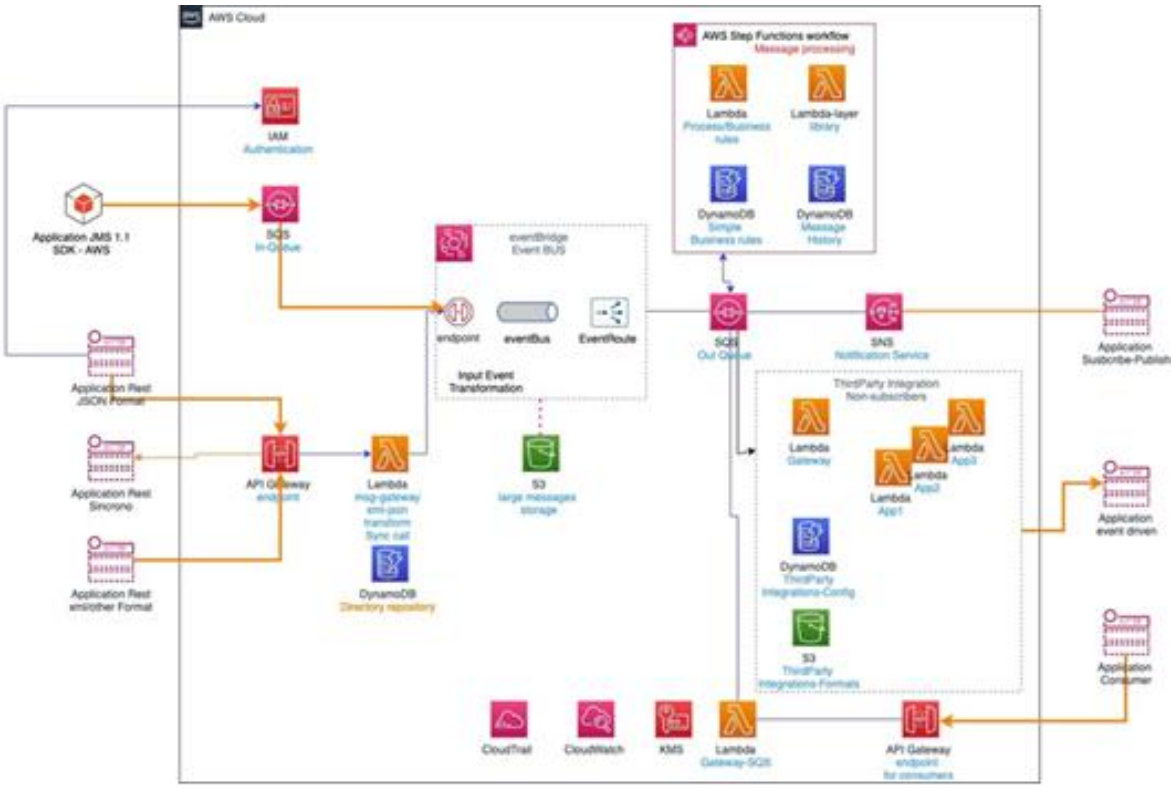

Imagen 83: Detalle 2 Arquitectura backend CISE

3.4.2 Servicio IAM

Aquellos usuarios administradores del Metro de Medellín que requieren acceder a AWS con el propósito de realizar modificaciones a los tableros de reportes, configuraciones básicas de reglas, o para seguimiento de los diferentes procesos con motivos de auditoría, tienen acceso a través de un usuario de IAM, también este servicio permite la definición de reglas de uso para diferentes servicios evitando problemas de configuración y borrado de elementos importantes.

Actualmente existen 3 usuarios administradores Metro; se usa una asignación de políticas least privileges y se debe tener acceso de tipo MFA para evitar la suplantación y acceso al desarrollo.

3.4.3 Servicio Amazon CloudWatch

CloudWatch permite tener un registro personalizado de la mayoría de los procesos llevados a cabo dentro de la plataforma del CISE, tales como fechas, formatos, usuarios, entre otros, la idea es que estos registros detallados ayudan a detectar problemas y hacer seguimiento de los procesos más complejos.

3.4.4 Servicio AWS CloudTrail

CloudTrail al igual que CloudWatch es una herramienta de monitoreo, en este caso para aquellas acciones realizadas directamente a alguno de los servicios de AWS, de esta forma se puede obtener un registro más detallado no solamente de información personalizada, sino también del servicio que se utilizó para esa parte del proceso en concreto y cuál fue su resultado.

3.4.5 Servicio SQS

Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos. Amazon SQS ofrece construcciones comunes como colas de caracteres muertos y etiquetas de asignación de costos. Proporciona una API de servicios web genérica a la que puede obtener acceso mediante cualquier lenguaje de programación compatible con el SDK de AWS.

3.4.6 AWS KMS

La protección de información sensible es importante a lo largo de diferentes procesos en toda la plataforma, esta información está presente en el caso de contraseñas, identificadores de elementos, información de terceros, entre otros, mediante KMS se encripta dicha información sensible que no debe ser accesible para externos.

3.4.7 EKS

Amazon EKS ayuda a ejecutar Kubernetes (software de código abierto que le permite implementar y administrar aplicaciones en contenedores a escala) en AWS sin instalar, operar ni mantener su propio plan de control Kubernetes. Amazon EKS aprovisiona y escala el plano de control de Kubernetes, incluidos los servidores API y la capa de persistencia de backend, en varias zonas de disponibilidad para obtener alta disponibilidad y tolerancia a errores.

3.4.8 Amazon Managed Grafana

Es actualmente la interfaz gráfica del CISE, del centro de operación. Los operadores de CISE podrán generar informes como se verá más adelante en este documento.

3.4.9 Amazon SES

Mediante Amazon SES es posible configurar diferentes tipos de mensajes de correo electrónico, tanto con anexos como sin ellos. En el momento que se requiera enviar la información acerca de un evento concreto por correo, para una tarea de seguimiento o como evidencia para algún proceso es posible hacer uso de Amazon SES.

3.4.10 Amazon S3

El almacenamiento de información es un ítem principal del CISE, mediante S3 se alberga diferentes configuraciones, tanto la plataforma CISE como aquellas integraciones con terceros de las cuales se debe tener en cuenta formatos, estructuras de datos entre otros.

La información de diferentes mensajes viaja a través del message bróker y en ocasiones puede llegar a exceder los límites de capacidad de AWS, es por ello por lo que una solución práctica es almacenar dicha información en S3 y mediante un procesamiento fraccionado completarlo.

3.4.11 DynamoDB

Dentro del proyecto están contempladas diferentes bases de datos con diferentes propósitos, ya que se adoptó una metodología basada en microservicios, cada uno de estos microservicios contará con una base de datos dedicada, dónde está la información de la plataforma, como eventos, protocolos, usuarios, notificaciones, actividades, entre otros. También existe una base de datos dedicada para aquellos procesos del message bróker que requieren información organizada.

3.4.12 Cognito

Cognito es la fuente de autenticación en la plataforma, se conecta con el directorio activo para permitir ingresar a los trabajadores fácilmente a la plataforma con nada más que un usuario y contraseña, Cognito también incluye métodos de autenticación personalizados por lo que es posible integrar procedimientos desencadenados mediante el inicio de sesión de un usuario en concreto o de un grupo. Actualmente los usuarios del Metro son locales.

3.4.13 Lambda

Lambda en el caso particular del CISE, es utilizada como el backend de la plataforma, donde mediante código estructurado, se realizan operaciones, búsquedas en bases de datos, creación automatizada de elementos, orquestación de servicios, entre otros, lambda es principalmente la herramienta de procesamiento del proyecto.

3.4.14 Step Functions

Tener un seguimiento claro del estado de los protocolos de forma práctica y sin complicaciones es posible gracias a Step Functions donde los protocolos son un proceso definido en pasos (actividades) estos pasos deben completarse para que el protocolo sea completado, con otro tipo de aproximaciones habría que tener en cuenta muchas variables, sin embargo con Step Functions es posible definir incluso gráficamente paso a paso un flujo robusto que puede quedar abierto hasta por un año en caso de que la información referente al protocolo tome tiempo en ser recolectada.

3.4.15 API Gateway

La plataforma de CISE cuenta con una arquitectura backend basada en microservicios, los cuales tendrá disponibles APIs, dicho grupo de APIs tendrá a disposición sus endpoints, documentación,

configuración y auditoría mediante API Gateway, en donde las API REST estarán disponibles para uso particular, y dentro de la plataforma para realizar los procedimientos comunes.

3.4.16 Amazon SNS

Existen diferentes formas de notificar acerca de eventos particulares, en caso de notificar alarmas o eventos que interesen solamente a un grupo específico de usuarios, es posible configurar suscripciones a temas de interés, así en el caso de que un analista de zona le interese solamente recibir notificaciones de un área específica, puede suscribirse a un grupo de notificaciones de solamente esa zona, dichos temas de interés (tópicos) son altamente personalizables y útiles para segregar la cantidad de información que realmente es relevante para el usuario.

3.4.17 Event Bridge

Con la cantidad de elementos que pueden interactuar dentro del CISE, es posible que sea complicado hacer un seguimiento y determinar reglas para cada uno de ellos de forma práctica y escalable, con Event Bridge es posible personalizar reglas y patrones comportamiento dependiendo del servicio que se desee, como obtener mensajes, alarmas, comunicación de cámaras, intercomunicadores y más, de forma práctica, y escalable haciendo que el tránsito de la información sea fiable y seguro.

3.4.18 Amplify

La plataforma tiene el hosting de su FrontEnd en Amplify, pero su habilidad no es solamente el hosting, Amplify provee una serie de herramientas para despliegue continuo y la integración de otros servicios de AWS de forma práctica, por lo que es posible configurar nativamente el uso de S3 para guardado de información, autenticación para tener un sistema integrado y seguro, y la personalización de pruebas End-to-End como parte del despliegue de una nueva versión de la plataforma.

3.5 Arquitectura Frontend

A continuación, se presenta la arquitectura y los servicios implementados en backend del CISE:

3.5.1 Diagrama

El siguiente diagrama presenta la arquitectura en utilizada en CISE:

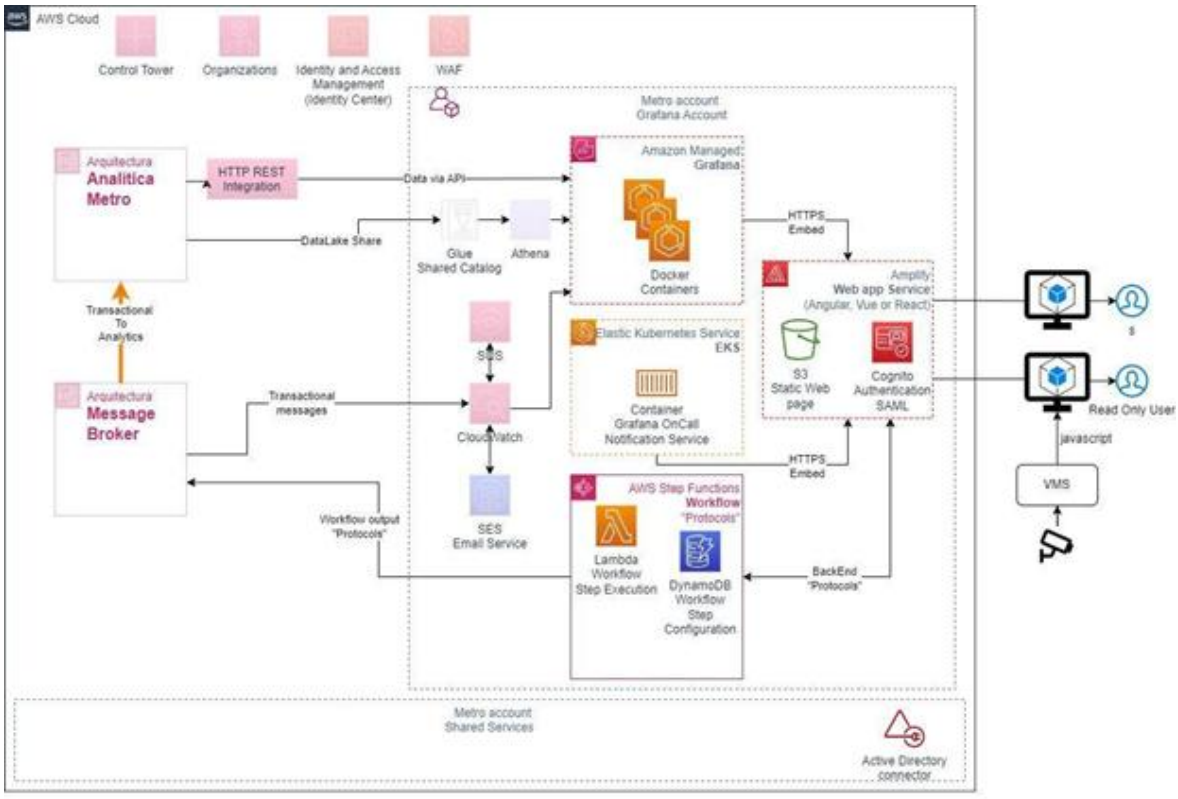

Imagen 94: Detalle Arquitectura frontend CISE

3.5.2 Servicio Amazon Athena

Selecciona la base de datos que contiene las tablas catalogadas por AWS Glue. Escribe consultas SQL estándar en Athena para analizar datos. Athena utiliza las definiciones de tablas del AWS Glue Data Catalog para entender la estructura de tus datos.

3.5.3 Grafana onCall

Es posible ejecutar notificaciones directamente desde Grafana en relación con la detección de alertas. Esto se logra a través de configuraciones que permiten el envío de alertas y notificaciones cuando ciertos umbrales o condiciones predefinidas son alcanzados por los datos visualizados en Grafana. Estas notificaciones pueden ser enviadas a través de diversos canales, como correos electrónicos, mensajes de texto u otros medios definidos por el usuario.

3.5.4 DynamoDB

Amazon DynamoDB se puede implementar eficientemente en un panel de control para almacenar y recuperar datos en tiempo real.

3.5.5 Amazon Cognito

Conectar con un directorio abierto para controlar el acceso a la plataforma de monitoreo.

3.5.6 Diseño aplicado

Los usuarios cuentan con un usuario y contraseña, propios para CISE que les permite con base en los permisos asignados, tener acceso a los servicios e información correspondiente. El ingreso se realiza a través del enlace https://www.cise.metrodemedellin.gov.co/. Para los usuarios Metro se cuenta con una integración al Directorio Activo Metro para facilitar los accesos.

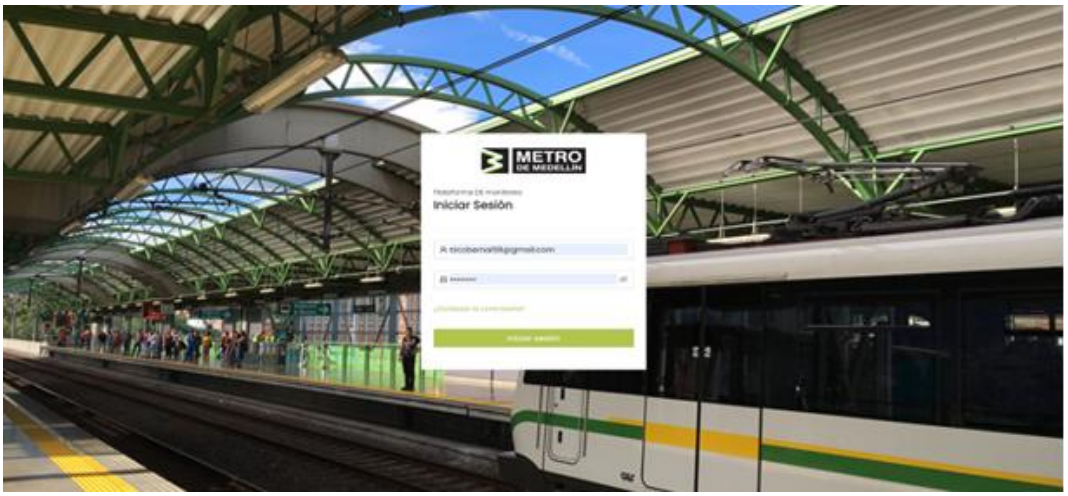

Imagen 105: Autenticación CISE

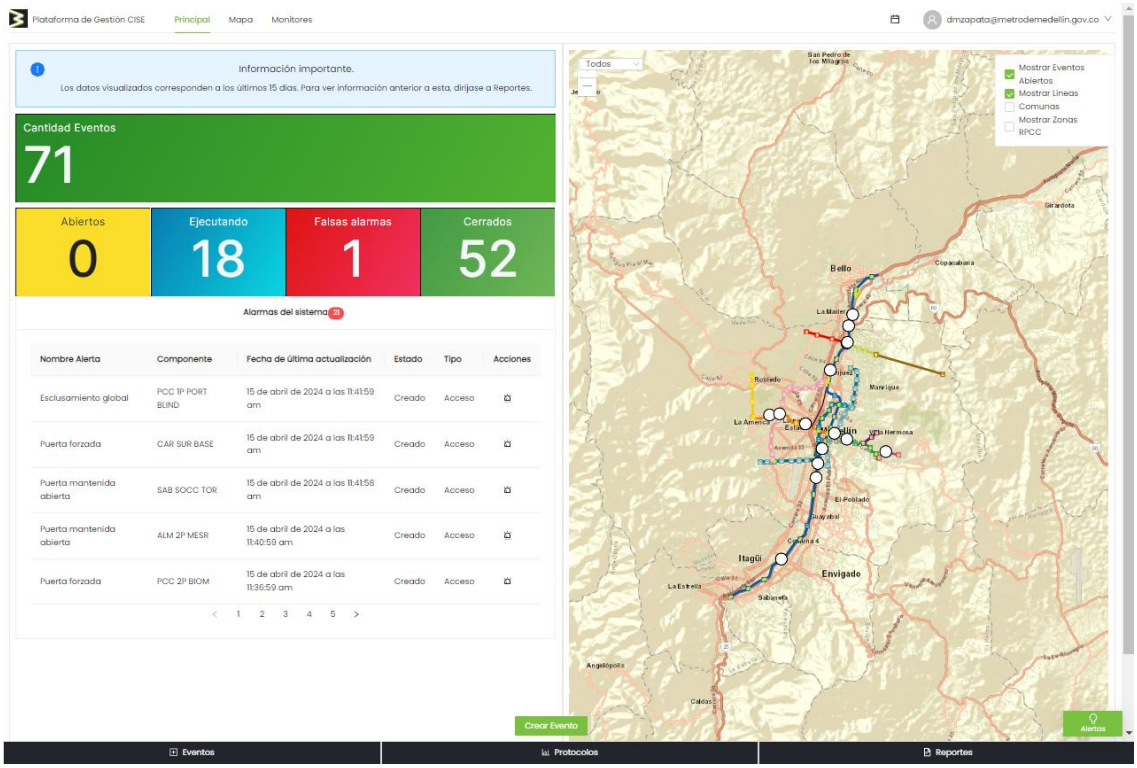

Imagen 116: Acceso principal CISE

El panel principal consta de un panel de control que ofrece contadores de eventos, gráficas que muestran el estado de las zonas, porcentajes de procedimientos ejecutados, un mapa con georreferenciación de la infraestructura del Metro, alarmas, eventos y cámaras en tiempo real.

Todo esto se complementa con herramientas de filtrado por ubicación, tipo de evento y protocolo PARP, calendario de eventos, así como opciones para exportar las gráficas.

La barra de herramientas superior muestra información del usuario, como su nombre e identificación, junto con la opción de "Ayuda" que brindará soporte. La barra de herramientas inferior se describe de la siguiente manera:

- Eventos: Crear y administrar eventos.
- Actividades: Gestionar protocolos asignados a los eventos.
- Reportes: Abrir formatos para análisis con Quicksight.

Se presenta como anexo el manual de usuario funcional que detalla todas las características de la plataforma implementadas para los operadores CISE.

4. Objeto

Mantener la suscripción de la plataforma del CISE sin interrupciones, además de brindar el soporte, mantenimiento y atención requerimientos para la plataforma de Gestión del Centro Integrado de Seguridad y Emergencias – CISE del Metro de Medellín sobre la nube AWS.

5. Alcance general

El alcance deberá ser implementado por un partner autorizado de Amazon Web Services – AWS en Colombia; a continuación, se indica lo requerido para LA EMPRESA:

5.1 Servicios profesionales

Los servicios profesionales, los profesionales que requiera EL CONTRATISTA para el mantenimiento y el soporte de la solución comprenden: atención de fallas, incidentes con la plataforma, desarrollo de nuevos requisitos, ajustar o implementar nuevos protocolos de operación (PARP), ajustar o implementar nuevos reportes de seguridad y emergencias, realizar capacitación al personal Metro cuando sea requerido de los cambios y nuevas implementaciones. Así mismo elaborar la documentación técnica, administrativa, legal, SST, ambiental necesaria durante la vigencia del contrato, realizar los reportes de gestión, gestionar la facturación y demás responsabilidades para cumplir con el alcance del contrato.

5.2 El soporte

Incluye la ejecución de las siguientes actividades por parte de EL CONTRATISTA:

5.2.1 Niveles de soporte

La atención inicial la realiza personal Metro del Área de Sistema Operativo, dentro de este contrato se solicita brindar soporte de nivel 1 y 2 por parte del partner AWS (EL CONTRATISTA) y nivel bussines de soporte de AWS, según los niveles de atención de servicios establecidos o cuando EL CONTRATISTA identifique alarmas que requiera este tipo de asistencia. Este soporte incluye, entre otras cosas, la creación y eliminación de usuarios, roles y permisos, así como la atención de incidentes o eventos que ocurran en la plataforma durante la gestión de eventos, reportes y otras actividades.

El soporte se proporcionará en modalidad 5x10 de lunes a viernes (de 8 a.m. a 6 p.m.) y durante 4 horas los sábados (de 8 a.m. a 12 p.m.). Para eventos que ocurran fuera de estos horarios y en casos de severidad alta, el contratista debe contar con una línea telefónica disponible para realizar reportes en un esquema de atención 7x24.

5.2.2 Acuerdos de Nivel de Servicio (SLA)

Severidad	**Alta**	**Media**	**Baja**
Tiempo de respuesta	1 hora	2 horas	3 días

Severidad alta: Es aquella anomalía que provoca indisponibilidad total en la solución y que requiere de atención inmediata. Esta severidad tendrá atención vía VPN dentro del esquema 7x24. Este tipo de casos serán determinados en conjunto con Metro de Medellín. Presentación de respuesta dentro de la 1ra hora, contada desde el momento en que se recibe llamada al número o plataforma web de atención que disponga EL CONTRATISTA; en todo caso la solución definitiva dentro de 4 horas.

Tendrá como excepción en tiempo de solución y respuesta, los casos que requieran apertura con soporte de fábrica. Dentro de estos se encuentran eventos como:

- **Falla crítica del sistema:** La plataforma experimenta una falla total que impide que los usuarios accedan a los servicios o realicen acciones importantes como crear eventos.

- **Pérdida masiva de acceso a los datos:** Se produce falla de acceso a una gran cantidad de datos críticos para el funcionamiento de la plataforma. En este caso, más de cinco (5) usuarios no pueden obtener información de las estaciones, cámaras, grabaciones, ubicaciones, acciones de uno o varios PARP.

- **Tiempo de inactividad prolongado**: La plataforma experimenta un período prolongado de tiempo de inactividad, lo que afecta significativamente la disponibilidad y el rendimiento de los servicios.

Severidad media: Es aquella anomalía que produce impacto en las funciones de la plataforma de gestión, pero que se puede seguir operando, así no se cuente con la misma calidad de servicio con la que se trabaja habitualmente. Esta severidad tendrá atención vía VPN dentro de la franja hábil (lunes a viernes de 8:00 a.m. a 6:00 p.m. y sábados de 8 a.m. a 12 p.m.). Este tipo de casos serán determinados en conjunto con Metro de Medellín. EL CONTRATISTA presentará un plan de solución de fallas dentro de 24 horas hábiles, considerados a partir de la notificación de la incidencia, un plazo máximo de solución definitiva de 48 horas. Tendrá como excepción en tiempo de solución y respuesta, los casos que requieran apertura con soporte de fábrica. En este caso se puede experimentar:

- **Problema de rendimiento moderado:** La plataforma experimenta una degradación del rendimiento que afecta la velocidad de respuesta de las aplicaciones, pero no impide por completo su funcionamiento.

- **Errores de funcionalidad no críticos**: Se identifican errores o problemas de funcionalidad en la plataforma que afectan a un grupo de menos de cinco (5) usuarios o algunas funciones, pero no tienen un impacto generalizado.

- **Fallas en la integración con terceros:** Se producen problemas de integración con servicios o sistemas de terceros que causan interrupciones temporales en algunas funcionalidades de la plataforma.

Severidad baja: es aquella anomalía que tiene bajo impacto en la funcionalidad de la solución y que da tiempo de espera en su atención. Esta severidad tendrá atención vía VPN dentro de la franja hábil (lunes a viernes de 8:00 a.m. a 6:00 p.m. y sábados de 8 a.m. a 12 p.m.). Este tipo de casos serán determinados en conjunto con Metro de Medellín. EL CONTRATISTA presentará un plan de solución de fallas dentro de 3 días hábiles, considerados a partir de la notificación de la incidencia, un plazo máximo de solución definitiva de 10 días. Tendrá como excepción en tiempo de solución y respuesta, los casos que requieran apertura con soporte de fábrica. Dentro de esta severidad se encuentran:

- **Mantenimiento programado:** Se lleva a cabo un mantenimiento programado en la plataforma durante un período de baja actividad para realizar tareas de optimización o actualización de infraestructura.

- **Notificaciones de rutina:** Se envían notificaciones de rutina a los usuarios sobre eventos o cambios menores en la plataforma, como actualizaciones de políticas, cambios en los términos de servicio, o recordatorios de eventos próximos.

- **Actividades de monitoreo y auditoría:** Se realizan actividades de monitoreo y auditoría regulares para verificar el rendimiento, la seguridad y la integridad de la plataforma, sin identificar problemas graves.

- **Solicitudes de soporte no críticas**: Los usuarios realizan solicitudes de soporte o asistencia técnica relacionadas con problemas menores que no impiden el uso normal de la plataforma.

- **Solicitudes de información**: Se generan consultas, por parte de los usuarios, de tipo informativo que no generan ningún tipo de acción sobre la plataforma.

5.2.3 Reportes

Entregar mensualmente reporte de los soportes requeridos por LA EMPRESA, con los indicadores y SLA, el análisis de los eventos, las recomendaciones y acciones de mejora realizadas.

5.3 El mantenimiento

El mantenimiento incluye la ejecución de las siguientes actividades por parte de EL CONTRATISTA:

5.3.1 Suscripción mensual

Mantener la suscripción mensual durante toda la vigencia del contrato de los servicios implementados en la nube AWS para garantizar la operatividad de la plataforma de Gestión, lo cual comprende:

a. Suscripción mensual de servicios en nube del proveedor de servicio de nube AWS.

b. La suscripción de los servicios de nube debe garantizar el correcto y completo funcionamiento de toda la solución actual realizada en la nube AWS, así como los servicios adicionales que puedan ser requeridos para atender los nuevos requerimientos que solicite LA EMPRESA durante la vigencia del contrato.

5.3.2 Consumo de los servicios

EL CONTRATISTA deberá presentar al Metro las mediciones del consumo que se tengan para cada uno de los servicios implementados para el CISE previo a cada facturación, así mismo deberá monitorear permanentemente este consumo y alertar con una periodicidad al menos semanal sobre los consumos de cada servicio, verificando si existen consumos irregulares, que correspondan con un funcionamiento anormal, un error de implementación de EL CONTRATISTA o si son un verdadero consumo por parte del Metro. Analizar las desviaciones presentadas en cada periodo y tomar las decisiones del consumo con personal Metro.

El Metro tomará como referencia los consumos y capacidades estimados establecidos en la oferta presentada por EL CONTRATISTA. En consecuencia, EL CONTRATISTA deberá implementar las medidas de control necesarias sobre las configuraciones, implementaciones y capacidades habilitadas por sus profesionales. Asimismo, únicamente podrá habilitar nuevos servicios o incrementar las capacidades de los servicios existentes en la nube AWS cuando medie un requerimiento oficial del Metro, por medio del supervisor del contrato.

5.3.3 Nuevas implementaciones

Se establecerá una bolsa de horas estimadas de desarrollo integral, las cuales serán utilizadas y pagadas bajo demanda acorde con los requerimientos oficiales que el Metro realice a EL CONTRATISTA por medio del supervisor del contrato y que sean completamente atendidos por EL CONTRATISTA y recibidos a satisfacción por LA EMPRESA.

EL CONTRATISTA deberá, en conjunto con el personal necesario de LA EMPRESA, realizar el levantamiento técnico detallado o caso de uso del requerimiento, valorar en horas de desarrollo y presentar a Metro para su aprobación previo a su implementación. Para lo anterior, se tendrá una bolsa de horas estimadas totales de 200 horas para atender todos los requerimientos durante la vigencia de este contrato.

Incluye entregar a LA EMPRESA el código fuente del software, cuando éste sea desarrollado exclusivamente para LA EMPRESA, con licencia para ser editado posteriormente por terceros.

6. Alcance específico

6.1 Sostenimiento de la plataforma

EL CONTRATISTA debe garantizar:

a. Sostenimiento de la Plataforma CISE, la implementación de protocolos de operación PARP o ajustes que LA EMPRESA requiera de estos, la gestión, cambios o ajustes de reportes actuales, implementación de nuevos reportes, mantener y mejorar las integraciones actuales que hay entre la plataforma CISE y otros sistemas Metro descritos en el presente documento.

b. La captura, limpieza, extracción de datos, mantenimiento del repositorio de almacenamiento de datos del CISE, así como las configuraciones necesarias sobre la nube pública y entre la nube pública y los sistemas de LA EMPRESA para garantizar el intercambio seguro de la información que sea requerida.

Durante la ejecución del contrato, EL CONTRATISTA debe realizar un levantamiento de requerimientos para lo cual convocará las reuniones necesarias con el personal Metro, creará y documentará los casos de uso de las necesidades que tenga LA EMPRESA frente a la Plataforma CISE para aprobación del Metro y valorará en tiempo y costo cada uno de ellos con el fin de que LA EMPRESA tome la decisión de implementar o no y el momento para realizarlo.

Por ningún motivo EL CONTRATISTA podrá desarrollar mejoras, o nuevas implementaciones a la plataforma, aumentar capacidades o consumos sin la autorización del supervisor del contrato debidamente oficializada. En caso de ocurrir, LA EMPRESA no autorizará pagos a EL CONTRATISTA por estos conceptos.

EL CONTRATISTA deberá detallar a LA EMPRESA la forma de cada integración entre la plataforma CISE y las plataformas existentes en el Metro (mediante web service, APIs, etc.), así mismo se deberá definir e implementar la manera de compartir información con entidades como externas como Bomberos, Policía y demás que se identifiquen en conjunto con LA EMPRESA en la etapa de diseño acorde con los convenios que LA EMPRESA pueda tener a la fecha de ejecución del contrato.

Aun cuando LA EMPRESA no comience a compartir información del CISE con entidades externas, está incluido dentro del alcance realizar las configuraciones, desarrollos, parametrización y documentación del lado Metro sobre la plataforma CISE para poder compartir información de la gestión del CISE a futuro con entidades externas.

6.2 Arquitectura CISE

EL CONTRATISTA deberá mantener la arquitectura implementada en CISE; sin embargo, si surge una propuesta de mejora o cambio deberá ser aprobada por el Supervisor del Contrato, en tal caso EL CONTRATISTA presentará las ventajas, costos y análisis de los cambios o nuevas introducciones de servicios para ser aprobado por LA EMPRESA antes de su implementación.

Todas las implementaciones en la nube AWS para el CISE deben ser soportadas por EL CONTRATISTA durante el tiempo de ejecución del contrato.

Durante los últimos 2 meses de ejecución del contrato, LA EMPRESA requerirá a EL CONTRATISTA para realizar diferentes reuniones, se le solicitará información, documentación técnica, sesiones de trabajo conjuntas y reportes de empalme para entregar toda la gestión de la plataforma CISE al futuro Contratista que resulte adjudicatario para iniciar el nuevo contrato de CISE.

Estas reuniones, sesiones de trabajo o informes se encuentran incluidas dentro del alcance del presente contrato como parte de las actividades técnicas y administrativas de EL CONTRATISTA.

6.3 Componente suscripción de servicios en nube de la solución de software del CISE

EL CONTRATISTA deberá desarrollar las interfaces gráficas lo más parecidas a las actuales o proponer nuevas interfaces mediante los servicios ofertados que solo podrán implementarse siempre que sean aprobadas previamente por LA EMPRESA a través del supervisor, contengan todas las funcionalidades actuales y las mejoras requeridas por LA EMPRESA o propuestas por EL CONTRATISTA, sean intuitivas y de fácil manejo para los operadores y la lógica de operación se mantenga lo más fiel posible para que se puedan replicar o mejorar la ejecución de los PARP establecidos. En todo caso LA EMPRESA deberá aprobar el diseño de implementación previamente.

La selección de los servicios en la nube necesarios para mantener la Plataforma CISE deberá realizarse involucrando tecnologías de la revolución 4.0 que permita a LA EMPRESA realizar como punto de partida el análisis de datos para una gestión más proactiva. Así como implementar nuevos servicios que faciliten la gestión de los eventos en el CISE, un ejemplo puede ser servicios tipo *speach to text*.

A continuación, se indican los requisitos mínimos de la suscripción de servicios AWS:

a. La suscripción debe realizarse sobre los servicios ofrecidos en la nube del proveedor de servicios de nube, AWS.

b. La suscripción de los servicios de nube deberá ser desde la orden de inicio, la plataforma debe mantenerse activa y disponible para LA EMPRESA durante el tiempo de ejecución sin interrupciones ya que el CISE opera en disponibilidad 7X24X365.

c. EL CONTRATISTA deberá registrar la consola de operación, administración y demás componentes requeridos para la solución a nombre de LA EMPRESA de Transporte Masivo del Valle de Aburrá – Metro de Medellín Ltda., tal como se hace en la actualidad y como recibirá para su gestión. De tal manera que LA EMPRESA quede en capacidad y libertad de solicitar a los distribuidores, partners autorizados de AWS que oferten para la prestación de servicio de soporte, mantenimiento y futuros crecimientos del sistema.

d. LA EMPRESA deberá contar con el usuario de administración, raíz o propietario, de tal manera que EL CONTRATISTA obtenga estos permisos en la nube seleccionada a partir de una asignación directa por parte de LA EMPRESA.

e. LA EMPRESA tendrá la potestad de determinar el nivel de acceso de los usuarios a las consolas de nube AWS.

f. EL CONTRATISTA deberá asignar y entregar los permisos de administración máximos que faculten a LA EMPRESA como el usuario final de la operación de nube.

g. Los artefactos, tanto de componentes de software como los datos que a partir de los procesos realizados sean obtenidos serán propiedad intelectual de LA EMPRESA en caso de aplicar, desde el código fuente, hasta los componentes analíticos generados, excepto cualquier servicio SaaS o PaaS propiedad de la nube AWS.

h. Actualmente existen protocolos PARP, los PARP y sus ajustes deberán implementarse sobre un servicio que permita ingresar y automatizar en donde sea posible la captura de los datos principales de un evento, como por ejemplo, lugar de ocurrencia del evento, tipo de evento, quien lo reporta, zona donde ocurre el evento, así mismo debe permitir que se asigne el protocolo de atención que corresponda con el evento a atender y guie y soporte de manera intuitiva y ágil al operador en el cumplimiento de dichos pasos.

i. Deberá mantener la trazabilidad existente en el sistema del cumplimiento de los pasos para la atención de los eventos y el registro del operador que los ejecutó y los detalles de la atención para que análisis en los reportes de gestión.

j. EL CONTRATISTA podrá sugerir cambios, mejoras, ajustes a los protocolos actuales los cuales serán sometidos a aprobación de LA EMPRESA a través del supervisor del contrato previo a cualquier implementación.

k. EL CONTRATISTA podrá sugerir cambios, mejoras, ajustes a cualquiera de los módulos de la plataforma (eventos, reportes, calendario, alertas, etc.) los cuales serán sometidos a aprobación de LA EMPRESA a través del supervisor del contrato previo a cualquier implementación.

l. Debe mantenerse el acceso a la plataforma CISE a través de la web donde se tiene la visión general de la Operación del Metro de Medellín respecto a los eventos de Seguridad y Emergencia.

m. Los operadores deben mantener la facilidad de poder crear y modificar eventos de seguridad y emergencia en múltiples dispositivos (PC, Tablet, Celular) independiente del lugar de ejecución, también se debe permitir la visualización georreferenciada en el mapa Metro y en tiempo real de los eventos, equipos de seguridad y emergencia (cámaras, sensores, equipos para atención de emergencia en las estaciones y paradas).

n. EL CONTRATISTA deberá habilitar para el CISE las capas de Centros de salud y Hospitales cercanos, instituciones como bomberos y policía cercanos a la ubicación de un evento dado. Todo lo anterior acorde como se apruebe por parte de LA EMPRESA y las capas suministradas por LA EMPRESA en ArcGis.

o. EL CONTRATISTA podrá proponer mejoras para los reportes y análisis de datos, indicadores críticos para la gestión de la seguridad y emergencias del Metro, los cuales serán sometidos a aprobación de LA EMPRESA a través del supervisor del contrato previo a cualquier implementación.

p. EL CONTRATISTA debe realizar mejoras a la gestión de datos abiertos implementados en la plataforma CISE acorde con su experiencia y la disponibilidad de datos en las entidades generadoras de dicha información, actualmente las fuentes consultadas por LA EMPRESA son las siguientes:

    - http://medata.gov.co
    - https://datosabiertos.metropol.gov.co

    Sin embargo, podrán surgir nuevas fuentes a analizar bien sugeridas por LA EMPRESA o por EL CONTRATISTA que puedan resultar importantes para la toma de decisiones que repercutan en la seguridad del sistema Metro.

q. EL CONTRATISTA deberá mantener la integración para compartir, entregar y recibir información hacia y del sistema ERP corporativo SAP.

6.4 Personal contratista – Gestión CISE

Se deben incluir, por parte de EL CONTRATISTA, los servicios profesionales necesarios para el soporte y mantenimiento de la plataforma CISE.

El personal profesional de EL CONTRATISTA en servicio al Contrato deberá tener conocimiento y certificaciones técnicas vigentes en servicios en la nube AWS, para tales efectos debe indicar nombre completo, número de identificación y el certificado en servicios de nube que tiene cada persona, indicando el tipo y código de certificado para ser validado por LA EMPRESA.

Se requieren tres (3) profesionales, cada uno de los cuales debe poseer al menos una de las siguientes certificaciones de Amazon Web Services (AWS), las cuales deben estar vigentes a la fecha de presentación de la oferta y durante toda la vigencia del Contrato:

- AWS Certified Solutions Architect
- AWS Certified Cloud Practitioner
- AWS Certified Developer

Experiencia: Mínimo dos (2) años de experiencia en mantenimiento, soporte y/o desarrollos de plataformas en nube. (PaaS)

EL CONTRATISTA deberá adicionalmente, presentar un (1) profesional con pregrado residente que estará localmente en cualquier ubicación dentro del Valle de Aburrá con disponibilidad para desplazarse a las instalaciones de LA EMPRESA cuando sea requerido dentro de las franjas de horario lunes- viernes 8:00 – 18:00 durante toda la vigencia del contrato.

NOTA: La información de los profesionales solicitados serán requisitos de ejecución, es decir se verificarán previo al acta de inicio del contrato. Una vez adjudicado el contrato, EL CONTRATISTA tendrá un plazo máximo de 10 días hábiles para proporcionar la información requerida de los profesionales.

6.5 Horas de configuración y desarrollo

LA EMPRESA requiere que EL CONTRATISTA ponga a su disposición un equipo de configuración de nube o desarrollo de software, según se requiera, en un modelo de bolsa de horas que LA EMPRESA podrá usar durante toda la vigencia del contrato bajo el modelo de solicitud de requerimientos.

Se aclara que se trata de bolsa de ejecución de nuevos requerimientos no para la atención de soportes ni mantenimientos regulares de la plataforma, la cual se pagará por la disponibilidad del personal y el consumo real de los servicios mensualmente.

A continuación, se describe el servicio solicitado:

Cantidad de horas: La Empresa requiere que EL CONTRATISTA cotice una bolsa de horas del equipo de configuración de nube y desarrollo de doscientas (200) horas. En el formulario de valor deberá consignar el valor unitario de las horas de desarrollo y en caso de que durante la vigencia del Contrato se finalicen las 200 horas de la bolsa inicial, LA EMPRESA estará en libertad de contratar horas adicionales teniendo como base el valor unitario presentado en la oferta el cual debe regir durante toda la vigencia del contrato.

Equipo de configuración de nube o configuración: para llevar a cabo actividades y requerimientos orientadas a las mejoras, ajustes o nuevas solicitudes de los servicios de nube AWS o cualquiera de los componentes de la plataforma CISE, EL CONTRATISTA debe considerar que el equipo debe ser asignado como grupo, es decir cada hora cotizada debe incluir la prestación del servicio del equipo de trabajo de **configuración en nube o de desarrollo** según sea necesario acorde con el requerimiento de LA EMPRESA y los recursos mínimos que los integran son:

Configuración Nube	Desarrollo
Líder técnico: con experiencia mínima 1 año, con asignación mínima del 20%, certificación de conocimiento AWS y Scrum vigentes a la fecha de presentación de la oferta las cuales deben permanecer vigentes durante toda la duración del contrato. • AWS Certified Associate Solutions Architect	**Líder técnico**: con asignación mínima del 30% y al menos 2 años de experiencia liderando proyectos de desarrollo, adicionalmente con acreditación Scrum vigente a la fecha de presentación de la oferta y debe permanecer vigente durante toda la duración del contrato.
Implementador 1: con experiencia mínima 1 año y certificación de proveedor de servicios de nube AWS básica que debe permanecer vigente durante toda la duración del contrato. • AWS Certified Associate Solutions Architect o AWS Certified Associate Developer • AWS Certified Cloud Practitioner	**Desarrollador 1:** con experiencia mínima 1 año en FrontEnd y/o BackEnd (lenguajes NodeJS o Python) • AWS Certified Associate Solutions Architect o AWS Certified Associate Developer • AWS Certified Cloud Practitioner
Implementador 2: con experiencia mínima 1 año y certificación de proveedor de servicios de nube AWS básica que debe permanecer vigente durante toda la duración del contrato. • AWS Certified Associate Solutions Architect o AWS Certified Associate Developer • AWS Certified Cloud Practitioner	**Desarrollador 2:** con experiencia mínima 1 año, en FrontEnd y/o BackEnd (lenguajes Node JS o Python) • AWS Certified Associate Solutions Architect o AWS Certified Associate Developer • AWS Certified Cloud Practitioner

Forma de solicitud de nuevos requerimientos para la plataforma de Gestión CISE:

Para el consumo de las horas de desarrollo, LA EMPRESA entregará a EL CONTRATISTA seleccionado un requerimiento que contiene las actividades a realizar sobre la Plataforma CISE, EL CONTRATISTA deberá evaluar el requerimiento, solicitar información necesaria adicional que considere pertinente, reunirse con el equipo Metro las veces necesarias hasta asegurar el entendimiento del

requerimiento y dimensionar la cantidad de horas integral a asignar del equipo de configuración de nube o desarrollo para solucionar y entregar satisfactoriamente el requerimiento. Posterior a esto, EL CONTRATISTA debe presentarle la valoración al supervisor del contrato para su aprobación.

EL CONTRATISTA deberá dar respuesta a LA EMPRESA máximo 10 días hábiles después de enviado el requerimiento. Metro de Medellín podrá elegir ejecutar o no las horas de acuerdo con la evaluación que realice el Supervisor del Contrato, Si El Supervisor del Contrato por parte del Metro de Medellín autoriza que la bolsa de horas sea utilizada en el requerimiento, EL CONTRATISTA seleccionado deberá asignar el equipo de configuración de nube y/o desarrollo en un plazo máximo de 10 días hábiles.

EL CONTRATISTA sólo ejecutará un requerimiento cuando esté oficialmente aprobado por el Supervisor del Contrato quien, una vez finalizada la ejecución del requerimiento, descontará la cantidad de horas usadas del saldo de la bolsa de horas. Cada hora presupuestada deben incluir el desarrollo, pruebas, despliegue, ajustes y capacitación a usuarios finales en caso de ser necesario.

Metodología: Se solicita a EL CONTRATISTA usar la metodología de desarrollo ágil SCRUM.

6.6 Usuarios del CISE

Se tienen usuarios con acceso web para personal de Riesgo Público y Convivencia Ciudadana RPCC (roles de operadores analistas CISE, inspectores CISE, analistas de Zona, Coordinadores CISE) y personal de Telemática. Todos pueden acceder de manera simultánea.

Se tienen tres (3) usuarios superadministradores de la Plataforma CISE y que a su vez son los usuarios para la gestión de las consolas de servicios AWS y Message bird.

Se cuenta con integración con el Directorio Activo DA Metro, la cual opera como proveedor SAML hacia la nube de AWS mediante el servicio AWS Cognito.

Esta integración permite que los usuarios autorizados ingresen al aplicativo CISE utilizando su correo corporativo, a través del mecanismo de autenticación administrado por Metro. AWS Cognito se sincroniza con el grupo de usuarios que tienen acceso a la aplicación configurada en el DA.

6.7 Gestión y operación de recursos de nube

La provisión de servicios de la plataforma CISE se realizó en la nube AWS por lo que se requiere mantener en dicha nube la implementación y atender sobre la misma y con los recursos de ella los nuevos requerimientos que surjan. Conservando las integraciones ya definidas o que se definan con los sistemas Metro On premises o en nube diferente.

La solución deberá estar implementada en nube pública AWS, la cual debe cumplir con los siguientes estándares:

a. Se deben conservar los servicios administrados o serverless, y así mismo si se implementan nuevos deberán ser serverless.

b. Todas las conexiones de las fuentes de datos y sistemas de LA EMPRESA deben ser privadas y seguras, a través de servicios tipo VPN.

c. La infraestructura utilizada por EL CONTRATISTA deberá ser parte de una región la cual contenga al menos 2 datacenters o zonas permitiendo la implementación de una arquitectura de alta disponibilidad.

d. En el caso de requerirse la utilización de instancias (máquinas virtuales) EL CONTRATISTA deberá tener la capacidad e incluir en la suscripción, crear dichas instancias con una customización de recursos (vCPU y Memoria), sin que esto represente costos adicionales para LA EMPRESA, diferentes al valor ofertado para ejecutar este contrato.

e. Se deberá presentar a LA EMPRESA dentro de los dos (2) primeros meses de ejecución del contrato el plan y estrategia de protección de datos de la Empresa ante delitos de ciberseguridad, demostrando la protección en el acceso y transmisión de la información. Este plan ejecutado hace parte de la solución y es requisito de aceptación de la implementación, debe ser presentado para aprobación al supervisor del Contrato.

f. LA EMPRESA durante toda la vigencia del contrato podrá solicitar a EL CONTRATISTA o realizar por su cuenta pruebas de hacking ético – scan de vulnerabilidades a la plataforma, sus servicios o cualquiera de sus componentes y EL CONTRATISTA deberá atender y cerrar las brechas de seguridad que sean detectadas y estén bajo su responsabilidad.

g. El Contratista deberá presentar mensualmente el dimensionamiento de los datos de la plataforma considerando como base la volumetría de datos y características de lo que contenga la plataforma, debe tomar en cuenta características como tamaño de bases de datos, tamaño de tablas en (MB, GB o TB), deltas de crecimiento, tipo de datos, esto para el repositorio de datos.

h) LA EMPRESA suministrará la información histórica de consumos base para la estimación de los recursos de nube requeridos por la plataforma CISE. (anexo de consumos actuales).

6.8 Gestión y operación de datos y reportes

Para gestionar los reportes, se deberá conservar y mejorar de ser necesario el Repositorio Único de datos o lago de datos actual del CISE como fuente única para alimentar los reportes necesarios para LA EMPRESA.

Si LA EMPRESA en marco del programa Metro Digital determina unificar lagos de datos se informará a EL CONTRATISTA y se acordará lo necesario técnicamente para proceder.

Debe cumplir los siguientes requisitos mínimos:

a. Deberá ser completamente serverless.

b. Debe poder escalar automáticamente en recursos de procesamiento y de almacenamiento.

c. Deberá ser altamente disponible, con SLA 99.99% uptime.

d. Los datos deberán replicarse entre distintas zonas para garantizar la confiabilidad y durabilidad del almacenamiento.

e. Los datos deberán estar encriptados tanto en tránsito como en reposo.

f. Los datos almacenados y en tránsito deberán ser propiedad de LA EMPRESA.

g. Deberá poder almacenar datos estructurados, semi-estructurados y geográficos.

h. Deberá integrarse con un catálogo de datos para el gobierno de los datos almacenados.

i. Deberá permitir aplicar políticas de acceso diferenciados de acuerdo con los roles a definir por LA EMPRESA.

j. Deberá contar con almacenamiento de datos para eficiencia de las consultas.

k. Deberá permitir almacenar datos en real-time y que estén disponibles para consultas inmediatamente.

l. Deberá poder obtener datos almacenados en otras nubes de forma sencilla sin tener que diseñar pipelines de datos, para análisis ad hoc. Deberá permitir la integración entre diferentes nubes públicas.

m. Deberá integrarse con el repositorio de datos AWS seleccionado para la plataforma Metro Digital y, si LA EMPRESA tiene nubes diferentes, permitirá su integración.

n. Deberá permitir a LA EMPRESA una forma de conexión estándar a su repositorio de datos para garantizar las integraciones que debe realizar LA EMPRESA. Por ejemplo, ofreciendo conectores como JDBC e interfaces en lenguajes estándar (no propietarios).

o. Deberá tener la capacidad de ocultar, visualizar dinámicamente aquellos datos considerados como sensibles por LA EMPRESA, y permitir su visualización, ocultamiento u ofuscación de acuerdo con la asignación de perfiles y roles que serán determinados por LA EMPRESA, lo anterior sin necesidad de duplicar información.

p. La conexión y la implementación del proceso ETL o ELT necesario para automatizar la ingesta de datos de las diferentes fuentes de datos hacia el repositorio centralizado (Repositorio Único de datos) es responsabilidad de EL CONTRATISTA.

q. EL CONTRATISTA deberá configurar, desarrollar, integrar e implementar lo necesario en la plataforma CISE para permitirle a LA EMPRESA mostrar indicadores críticos de la operación en tiempo real, acerca de los eventos de seguridad y emergencias registrados en el software de gestión.

r. Debe permitir también que los operadores puedan realizar consultas dinámicas a los datos gobernados por una capa semántica para facilitar la exploración de los datos. Esta capa semántica debe contar con control de versiones a través de un repositorio Git, y será manejada por los usuarios que administren el gobierno de los datos, por lo que debe permitir también que se controle el acceso a los datos diferenciado por atributos asignados a los usuarios finales.

s. Los reportes deben permitir ser compartidos para visualización y estar disponibles para ser extraídos del sistema al menos en formato Excel y PDF y ser compartidos vía email corporativo.

t. Se podrá consultar los eventos ocurridos en un rango de tiempo, ubicación del evento, consultar por palabra clave de la descripción, consultar por el identificador del evento u otros campos que deberán definirse entre EL CONTRATISTA y LA EMPRESA en la etapa de diseño mediante la toma de requerimientos que haga EL CONTRATISTA para configurar los reportes y en la cual se definirá todo el modelo de gestión y operación de los reportes entre EL CONTRATISTA y LA EMPRESA.

6.9 Capacitación de la plataforma de gestión CISE

EL CONTRATISTA debe realizar bajo demanda y acorde con las implementaciones o mejoras que se realicen en la plataforma, capacitaciones para personal Metro tanto para los usuarios funcionales como los administradores. El contenido, duración, material de apoyo y documentación será presentado al Supervisor del contrato para su aprobación.

Se tiene estimado inicialmente una formación periódica semestral para los usuarios funcionales y administradores donde se haga retroalimentación de cambios, fallas recurrentes y su solución y las nuevas implementaciones durante el periodo.

6.10 Documentación

Los documentos en su versión final, manuales técnicos, manuales de operación, planos y demás que apliquen deberán ser sometidos a revisión y deberán ser entregados a LA EMPRESA en formato digital como requisito para la aceptación final y deberá estar aceptada por LA EMPRESA por parte del Supervisor del Contrato.

La documentación para el presente alcance que debe ser suministrada mínimamente es:

a. Descripción detallada de los servicios implementados o modificados.

b. Diagramas y documentos relacionados.

c. Manuales de operación actualizados.

d. Manuales de administración actualizados.

e. Documentación técnica detallada de las integraciones actuales, las nuevas realizadas o los cambios sobre las mismas.

f. Códigos fuentes cuando aplique.

g. Detalle y configuración de los reportes actuales, nuevos implementados o ajustes realizados sobre los existentes.

h. Se debe suministrar información documentada sobre los procedimientos de backup y restauración del software intervenido o implementado, la revisión de logs, archivos de configuración y parametrizaciones implementadas.

i. Si existe un desarrollo específico para LA EMPRESA durante la ejecución del proyecto se deberá documentar técnicamente y entregar a LA EMPRESA además del código fuente, la documentación de especificación de requisitos y diseño aplicado.

6.10.1 Presentación de Informes

LA EMPRESA solicitará a EL CONTRATISTA los informes que a su juicio estime convenientes. Sin embargo, obligatoriamente se tienen los siguientes informes:

a. **Informes de avance:** Mensualmente se presentará a LA EMPRESA un informe de avance que detallará las labores ejecutadas en el período y los temas administrativos y financieros. Este informe es indispensable para la presentación de la facturación.

b. **Informe de avance implementaciones nuevas:** EL CONTRATISTA deberá reportar el porcentaje (%) de avance de las nuevas implementaciones, indicando el progreso de las implementaciones nuevas realizada. Este informe deberá detallar cada implementación completada, junto con su descripción y el estado de finalización. Además, se debe incluir una evaluación de los recursos utilizados y cualquier desviación significativa en el plan original, con sus respectivas justificaciones.

c. **Informes específicos:** Son los informes que a juicio LA EMPRESA le solicite sobre aspectos o problemas técnicos específicos surgidos durante el periodo.

6.11 Garantía

El soporte y garantía incluye el derecho de LA EMPRESA al uso de las suscripciones, servicios de terceros y demás componentes licenciados durante la vigencia del contrato, sin perjuicio de los derechos de propiedad intelectual y de uso, mantenimiento, modificación y entrega a terceros que

correspondan a LA EMPRESA sobre los desarrollos, configuraciones, integraciones y código fuente desarrollados durante la en ejecución del contrato.

El soporte deberá incluir los servicios de atenciones remota y en sitio, y consultas para recuperar los servicios ofrecidos en los tiempos establecidos en los Acuerdos de Nivel de Servicio.

Se requiere obligatoriamente la presencia de EL CONTRATISTA en el Área Metropolitana durante toda la vigencia del Contrato en una disponibilidad mínima de 5 días a la semana (lunes a viernes) 08:00 a 18:00 y en remoto en disponibilidad 7x24 para la atención de eventos y debe disponer de una línea telefónica para establecer las comunicaciones con el personal técnico de LA EMPRESA cuando se requiera y de acuerdo con lo descrito en el numeral **5.2.1** del presente documento.

EL CONTRATISTA, deberá informar durante el primer mes de ejecución del contrato, los canales de atención dispuestos para la atención de requerimientos; esto es, correos electrónicos, línea telefónica de atención y disponer o implementar a servicio del Contrato una herramienta web de reporte de las incidencias.

EL CONTRATISTA, en dicha herramienta llevará un registro o bitácora actualizada con las incidencias presentadas en la plataforma CISE (comportamientos no deseados o anómalos) y compartir el informe periódicamente con LA EMPRESA. En todo caso LA EMPRESA solicitará estadísticas, reportes e informes de las atenciones a las incidencias y sus soluciones en cualquier momento dentro de la ejecución de la solución. El registro o bitácora responsabilidad de EL CONTRATISTA debe contener como mínimo:

- Un identificador del caso o evento generado.
- Fecha y hora del evento.
- Datos del evento: ubicación y demás campos que apliquen.
- Clasificación y descripción del evento reportado.
- Severidad del evento
- El estado en que se encuentra el proceso de solución del problema, así:
    - solucionado
    - en espera de solución
- Fecha y hora de la solución.
- Elemento generador de la falla
- Solución de la falla
- Observaciones y recomendaciones.

EL CONTRATISTA debe otorgar una garantía técnica sobre todas las implementaciones, desarrollos, configuraciones, parametrizaciones, ajustes realizados por el término de tres (3) meses, contados a partir de la entrega para operación de todo el contrato.

Tipo	Quién	Duración	Alcance
Soporte y garantía	CONTRATISTA	Durante la implementación y seis (6) meses más a partir de la entrega a LA EMPRESA para operación de todo lo ejecutado.	Incluye soporte técnico remoto y en sitio que sea requerido, sobre las configuraciones, desarrollos e integraciones realizadas, así como en la infraestructura que tenga en la nube para soportarla. Incluye el derecho de LA EMPRESA al uso del software, la gestión del software, los reportes y todo lo que EL CONTRATISTA haya implementado en este alcance. Incluye el registro, seguimiento, atención, trazabilidad y solución de eventos o casos de soporte que sean solicitados por LA EMPRESA y su atención acorde con los SLA definidos. También incluye la implementación de actualizaciones de software, actualizaciones de los servicios, a las últimas versiones y parches de seguridad de la nube implementada sin necesidad de intervención de LA EMPRESA.

6.12 Otros

En este numeral se recogen a continuación una serie de requerimientos adicionales de carácter general, que EL CONTRATISTA deberá cumplir:

a. Se deberán acatar las normatividades aplicables para cada caso según las leyes colombianas.

b. EL CONTRATISTA deberá garantizar que todos los equipos de cómputo que utilice para el cumplimiento del alcance deberán contar con licenciamiento de sistema operativo legalizado y antivirus por suscripción actualizado.

6.13 Condiciones de trabajo especiales en las instalaciones del Metro de Medellín

EL CONTRATISTA debe disponer del personal idóneo, suficiente y necesario para la ejecución de todas las actividades requeridas dentro del presente alcance.

- Personal un arquitecto de software
- Un líder de base de datos

Horario de actividades: : Generalmente las actividades se desarrollan en horario laboral Lunes a viernes entre las 08:00 y 18:00 horas; sin embargo, es posible que en el desarrollo de las actividades del alcance existirán actividades que deberán hacerse en el horario nocturno (por ejemplo si implican interrupción total del sistema CCTV, del propio CISE, atenciones a eventos de seguridad informática que lo ameriten), inclusive después de la Operación comercial, por lo que en varios casos las actividades solo podrán realizarse entre 11:30pm a 3:30am, aproximadamente, estos trabajos son coordinados por la IOT (instrucción Operativa de trabajo) – reunión semanal donde se coordina la logística de los trabajos del Metro, reunión a la cual debe asistir EL CONTRATISTA en caso de requerirse. Para la mayoría de los casos se realizaría trabajo diurno.

7. Seguridad de la información

Metro de Medellín Ltda. reconoce la información como un activo valioso de la organización que permite la generación e incremento del valor. Por tanto, es exigencia que sus servicios se presten bajo un ambiente controlado que permita la mitigación de los riesgos asociados a este tipo de servicios. Con base a esto, es necesario que el servicio ofertado cuente con las siguientes características mínimas de seguridad:

7.1 Garantía sobre el tratamiento de la información de La Empresa

Toda la información y documentación relativa a LA EMPRESA que sea intercambiada entre las partes para la ejecución del contrato, así como la información transitada y almacenada en aplicativos o sistemas de información propiedad de EL CONTRATISTA, debe efectuarse con la finalidad exclusiva de la prestación de los servicios objeto del presente contrato y se debe realizar bajo el deber general de confidencialidad y secreto. EL CONTRATISTA asume el compromiso expreso de no utilizar la información y documentación suministrada para cualquier propósito distinto que no sea la prestación de los servicios objeto contratados.

Esta condición debe extenderse para los empleados de EL CONTRATISTA y están obligados al secreto profesional absoluto, a la neutralidad y máxima discreción frente a otros clientes o interesados en la solución.