Empresa de Transporte Masivo del Valle de Aburrá Limitada

Especificaciones técnicas

Especificaciones técnicas para contratar la prestación del servicio de conversión y migración de la plataforma ERP SAP ECC 6.0 EHP 8 a S/4 HANA en SAP RISE.

Gestión de Tecnologías de Información

Gerencia Administrativa

Bello, mayo de 2026

Contenido

1. OBJETO 3
2. GLOSARIO 3
3. ALCANCE 4
   3.1 Ejecutar todas las fases necesarias para la conversión técnica completa del ERP SAP ECC 6.0 EHP8 a la versión ERP SAP S/4HANA más actualizada al momento de iniciar la implementación en la modalidad Brownfield en la nube de AWS bajo la modalidad RISE. 4
   3.2 Migración de las interfaces que tenga el ERP SAP con otros sistemas de información de la Empresa a través de BTP (Business Technology Platform) Integration Suite. 5
   3.3 Implementación del módulo SAP S/4HANA Cash Management Private Edition 5
   3.4 Implementación del módulo SAP S/4HANA Cloud Supply Chain for Extended Warehouse Management. 8
   3.5 Implementación del módulo SAP S/4HANA Document and Reporting Compliance. 8
   3.6 Transferencia de conocimiento a usuarios técnicos y usuarios finales junto con el manejo del cambio. 8
   3.7 Documentación 9
   3.8 Garantías sobre los resultados de la consultoría 10
   3.9 Seguridad de la información 10
4. LICENCIAMIENTO SAP S/4HANA RISE 11
5. EXPERIENCIA Y PERSONAL REQUERIDO 11
   5.1 Experiencia de la empresa 11
   5.2 Experiencia y certificaciones del Recurso Humano 12
6. OTRAS OBLIGACIONES DEL CONTRATISTA 13
7. ANTECEDENTES INFRAESTRUCTURAS 14
   7.1 Sistema SAP 14
8. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN PARA COMPRA DE BIENES Y/O SERVICIOS 16
9. REQUISITOS ESPECÍFICOS PARA SOFTWARE COMO SERVICIO, WEB SERVICES Y APLICACIONES WEB 19

ANEXO DE ESPECIFICACIONES TÉCNICAS

Servicios profesionales para la conversión y migración de la plataforma ERP SAP ECC 6.0 EHP 8 a S/4 HANA en SAP RISE.

El presente documento establece los lineamientos mínimos que deberá tener en cuenta EL CONTRATISTA para desarrollar el objeto del contrato. No obstante, EL CONTRATISTA tendrá en cuenta que en la ejecución del contrato deberá aplicar sus conocimientos y experiencia para lograr llevar a cabo, y a entera satisfacción, el objeto contractual.

1. OBJETO

Contratar los servicios profesionales para la prestación del servicio de conversión y migración de la plataforma ERP SAP ECC 6.0 EHP 8 a S/4 HANA bajo la modalidad RISE en la nube de AWS.

2. GLOSARIO

ERP: Enterprise Resource Planning. Es una solución de software que integra y automatiza los procesos centrales de una empresa.

S/4HANA: Nueva generación de los sistemas de información fabricados por el proveedor SAP que se caracterizan por almacenar la información en la base de datos HANA.

HANA: High-performance ANalytic Appliance. Es una plataforma de base de datos en memoria, orientada a columnas, que permite el procesamiento de transacciones y análisis en tiempo real a alta velocidad.

SAP RISE: Es una oferta integral de transformación empresarial como servicio que combina software (S/4HANA), infraestructura en la nube, servicios gestionados y herramientas de inteligencia de procesos bajo un único contrato de suscripción.

BASE DE DATOS IN-MEMORY: Bases de datos que utilizan memoria interna (RAM) para el almacenamiento, ofreciendo un acceso mucho más rápido que los discos SSD o magnéticos.

CONVERSIÓN BROWNFIELD: es un método para migrar los sistemas SAP ERP (ECC) existentes a SAP S/4HANA mediante la actualización del sistema actual. Permite a las empresas conservar datos históricos, procesos personalizados y configuraciones, lo que reduce el tiempo de implementación y la complejidad en comparación con un enfoque desde cero.

DESARROLLOS Z: Son personalizaciones y programas a medida creados para adaptar el sistema a las necesidades específicas de la empresa, diferenciándose de las funcionalidades estándar. Estos programas,

que siempre comienzan con la letra Z o Y, incluyen transacciones, reportes y módulos diseñados para procesos únicos.

INTERFACES: Son puntos de conexión críticos que permiten el intercambio de datos entre sistemas SAP y aplicaciones externas (no SAP), facilitando procesos como la consolidación financiera o la automatización de la cadena de suministro.

AWS: Amazon Web Services. Plataforma de computación en la nube.

SAP BTP: SAP Business Technology Platform. es una plataforma en la nube unificada que combina datos, analíticas, IA, desarrollo de aplicaciones, automatización e integración. Diseñada para entornos SAP y no-SAP, permite extender aplicaciones, automatizar procesos y conectar sistemas para impulsar la transformación digital y la innovación con agilidad.

FPS: De sus siglas en ingles Feature Pack Stacks. Son actualizaciones semestrales o trimestrales que dispone SAP para S/4HANA Private Cloud, las cuales introducen nuevas funcionalidades opcionales, mejoras de experiencia de usuario (Fiori) y correcciones de errores.

Clean core: Estrategia de transformación que mantiene el núcleo del ERP SAP S/4HANA libre de modificaciones personalizadas (código Z), utilizando procesos estándar y extensiones en la nube (SAP BTP).

3. ALCANCE

3.1 Ejecutar todas las fases necesarias para la conversión técnica completa del ERP SAP ECC 6.0 EHP8 a la versión ERP SAP S/4HANA más actualizada al momento de iniciar la implementación en la modalidad Brownfield en la nube de AWS bajo la modalidad RISE.

EL CONTRATISTA deberá realizar la Conversión a S/4HANA RISE de los actuales ambientes del ERP (DEV, QAS, PRD).

EL CONTRATISTA debe analizar los desarrollos (Z) realizados a la medida en LA EMPRESA y asegurar el correcto funcionamiento una vez se realice la conversión a S/4HANA RISE.

EL CONTRATISTA deberá contar con una herramienta con capacidades de Inteligencia Artificial (IA) y certificada por SAP (incluida en SAP Store / Marketplace) para la migración a SAP S/4HANA. Esta herramienta debe acelerar el proceso de migración, analizar las personalizaciones sin perderlas y aprovechar las innovaciones de SAP, que permita automatizar mínimo un 95% de la conversión técnica de los custom code del ERP SAP ECC 6.0.8. Esta herramienta deberá ejecutar las fases PRE-SUM y POST-SUM, asegurando un mayor alcance de automatización técnica y una significativa reducción de tiempos, riesgos y esfuerzo manuales en proyectos de conversión como el que requiere LA EMPRESA, brindar FPS (Feature Pack Stacks) de SAP, upgrades y una herramienta de monitoreo del clean core. EL CONTRATISTA

deberá indicar la herramienta de conversión a S/4HANA RISE que será utilizada en el proyecto la cual no debe ser del tipo open source y debe tener soporte empresarial.

EL CONTRATISTA deberá indicar los tiempos y esfuerzos necesarios para realizar la conversión a S/4HANA RISE dentro del estimado que ha realizado la entidad. Deberá incluir un cronograma o plan de trabajo, detallando las fases y actividades a realizar durante el proyecto sin superar diez meses antes de la salida en vivo.

EL CONTRATISTA debe configurar y realizar la migración a Business Partners para la conversión a S/4 HANA RISE, ya que es prerrequisito de la migración a la versión S/4HANA.

EL CONTRATISTA debe realizar los respectivos análisis de pre-conversión, para lo cual hará uso de la herramienta proporcionada por SAP denominada Readiness Check, la cual ayudará a minimizar los riesgos y garantizar una adecuada transición hacia la nueva versión.

EL CONTRATISTA deberá disponer de especialistas SAP ABAP, para el ajuste manual de los desarrollos o personalizaciones que se requiera pasar a SAP S/4HANA RISE y que no hayan sido convertidos de forma automática con la herramienta de inteligencia artificial usada por EL CONTRATISTA.

EL CONTRATISTA deberá asegurar la actualización de la matriz de roles y perfiles SAP con base en la nueva versión ERP SAP S/4HANA entregando una estrategia de roles y perfiles con un enfoque orientado a mantener el tallaje de licenciamiento definido para LA EMPRESA (XS en RISE).

EL CONTRATISTA deberá acompañar el proceso de pruebas de funcionamiento en cada una de las etapas de la conversión garantizando la cobertura de principio a fin (E2E) sobre procesos SAP y no SAP. Realizar las recomendaciones que considere cruciales para garantizar el éxito de la conversión y la posterior administración de los sistemas SAP. EL CONTRATISTA deberá disponer de una herramienta certificada por SAP (incluida en SAP Store / Marketplace y que no sea del tipo open source) que permita automatizar el proceso completo de pruebas durante todo el proceso de implementación. EL CONTRATISTA deberá asegurar la trazabilidad y gestión de las pruebas mediante herramientas como Cloud ALM.

3.2 Migración de las interfaces que tenga el ERP SAP con otros sistemas de información de la Empresa a través de BTP (Business Technology Platform) Integration Suite.

EL CONTRATISTA deberá garantizar el correcto funcionamiento de las conexiones de las integraciones actuales entre el ERP SAP y los demás sistemas de la Empresa tanto internos como externos, entre otros. Las interfaces actuales son detalladas en este documento en el ítem 7.

3.3 Implementación del módulo SAP S/4HANA Cash Management Private Edition

A continuación, se detallan las necesidades que se deben tener en cuenta para la implementación de este módulo:

Automatización y gestión de pagos

- Generar un único formato de archivo de pagos XML como insumo para el intermediario (Proveedor ECS), quien se encargará de transformarlo y enviarlo a cada entidad bancaria. Este mismo flujo aplicará para archivos de respuesta, recaudos y extractos bancarios (Multicash).
- Validar automáticamente los archivos de respuesta del banco; en caso de rechazo, generar la anulación automática del documento de pago y notificar al usuario responsable, lo anterior deberá ser visible y gestionable a través de monitores.
- Agrupar automáticamente las órdenes de pago por banco, fecha, moneda, monto y otros criterios definidos.
- Validar propuestas de pagos mediante reglas de control como firmas autorizadas, límites jerárquicos y cuentas bancarias permitidas.
- Gestionar los pagos de nómina a empleados, proveedores de bienes y servicios, entidades bancarias, entre otros, validando cuentas bancarias asociadas y garantizando pagos en tiempo y forma.
- Controlar la retransmisión de propuestas de pago desde un monitor para evitar duplicidad.
- Permitir la descarga segura de archivos mediante encriptación en ruta SFTP definida para la comunicación bancaria.
- Envió de correspondencia para traslados bancarios entre cuentas de Metro de Medellín
- Desde la transacción F-110 se debe continuar la gestión de los demás pagos que no se transmiten con archivos XML.

Flujos de aprobación y trazabilidad

- Configurar las firmas digitales en SAP para las autorizaciones internas de pagos, de acuerdo con los niveles jerárquicos y los montos previamente establecidos. Estas firmas deberán generar el input necesario para habilitar la comunicación bancaria y permitir la ejecución efectiva del pago desde las distintas sucursales. En otras palabras, todo el proceso de aprobación se realizará dentro del sistema ERP SAP, y únicamente los pagos autorizados serán enviados al banco para su ejecución.
- Configurar un WorkFlow de aprobación multinivel, con opciones de aprobación o rechazo y motivo parametrizable, dejando trazabilidad completa de cada decisión.
- Gestionar sustitutos para usuarios aprobadores, garantizando continuidad operativa.
- Visualizar en tiempo real el estado de las aprobaciones desde una consola centralizada.
- Monitoreo y trazabilidad en tiempo real.
- Implementar un monitor que permita visualizar el estado de los pagos en tiempo real, incluyendo: fecha y hora de la propuesta, banco, estado, motivo, aprobadores y respuesta de la entidad bancaria por cada registro.
- Incluir una consola de monitoreo para el cargue de extractos bancarios.
- Incluir una consola de monitoreo para el estado de los recaudos en tiempo real, con campos como: fecha, NIT del pagador, concepto, entidad bancaria y monto.
- Identificar en el sistema los pagos rechazados o pendientes de confirmación para su gestión oportuna.
- Los pagos rechazados deben generar la opción de anulación (semiautomática) del comprobante de compensación o egreso.

Automatización de procesos contables y de recaudo

- Realizar la compensación automática de las partidas abiertas asociadas a los recaudos, una vez el pago haya sido identificado. Aunque actualmente no se cuenta con una llave conciliatoria definida por parte de la entidad bancaria para facilitar esta identificación, será necesario diseñar y construir el modelo de comunicación con las entidades financieras que permita la recepción estructurada y detallada de la información del pago, garantizando así su correcta aplicación en el sistema SAP.
- Revertir de forma automatizada los asientos contables en los casos aplicables.

Notificaciones y validaciones automatizadas

- Enviar notificaciones por correo electrónico a proveedores con respuesta de pago exitosa, con la información tomada del maestro de proveedores. El envío debe quedar registrado en una tabla de log.
- Programar Jobs de validación periódica para garantizar que los archivos de respuesta bancaria estén disponibles en la ruta SFTP y, por ende, actualizados en el sistema.

Carga de extractos para conciliación bancaria (multicash)

Cargar diariamente en SAP los extractos bancarios generados por el banco y depositados en la ruta SFTP establecida. La validación de cada extracto por cuenta bancaria se realizará a través del monitor de extractos del módulo Cash Management. En caso de errores durante la carga, se habilitará un proceso de post-procesamiento que permitirá reintentar la importación una vez se hayan corregido los errores correspondientes en el sistema SAP ERP.

- Contar con un monitor de extractos: este monitor es parte de la solución estándar Cash Management.
- Generar la conciliación bancaria: la conciliación bancaria se deberá poder consultar desde el monitor de extracto.

Reportes y seguimiento

- Generar informes de seguimiento por banco, sociedad, estatus de pago, fechas y montos, con opción de exportación y filtrado según necesidades operativas o de auditoría.
- Integración técnica y documentación.
- Utilizar el componente SAP BTP Integration Suite para la conexión con entidades bancarias.
- Entregar manuales técnicos de configuración del componente SAP Cash Management.
- Entregar manuales de usuario funcional paso a paso, con rutas claras y pantallas de ejemplo.

Formación, acompañamiento y soporte

- Brindar capacitación técnica y funcional a usuarios clave y usuarios finales.
- Acompañar la salida a producción, con resolución de incidencias durante el período de estabilización.

3.4 Implementación del módulo SAP S/4HANA Cloud Supply Chain for Extended Warehouse Management.

A continuación, se detallan las necesidades que se deben tener en cuenta para la implementación de este módulo:

- Realizar cobros en tiempo real. Es decir, que se genere el documento con la respectiva reserva y que el auxiliar del almacén pueda confirmar las cantidades a descargar del inventario al momento de retirar el bien de la ubicación.
- Se requiere que la herramienta le permita al auxiliar de recepción indicarle el estado de las ubicaciones disponibles además de la confirmación de la ubicación cuando este disponga de alguna de estas.
- Poder realizar traslados en tiempo real de elementos entre ubicaciones por medio de dispositivos móviles.
- Poder generar documentos para generar inventarios aleatorios donde se puedan bloquear códigos y/o ubicaciones específicas, además del cargue de la información generada en el conteo en estas mismas y que al final de cada conteo se genere un archivo de Excel que muestre la cantidad de códigos inventariados por cada funcionario.
- Poder realizar traslados entre almacenes, es decir, generar documento de traslado entre almacenes y solicitar confirmación de la mercancía trasladada.
- Poder generar reposición automática de los bienes por cada uno de los almacenes y zonas.
- Se requiere la trazabilidad de la entrega con confirmación de recepción de los bienes entregados.
- Que las herramientas se puedan cargar a los funcionarios a sus carteras y se haga control de tiempo del préstamo.
- Poder cargar por medio del código de los productos químicos la opción de las hojas de seguridad, por medio de un QR o código de barras.
- Llevar trazabilidad de fechas de vencimiento para los productos que cuentan con ella.
- Llevar trazabilidad de números de serie para productos que cuentan con estos.

El detalle de estas necesidades y el contexto de la administración actual de los almacenes de LA EMPRESA puede consultarse en el anexo “Información General para Implementación WMS V1.pdf”.

3.5 Implementación del módulo SAP S/4HANA Document and Reporting Compliance.

Los requisitos específicos para este módulo y el contexto actual de las interfaces que tiene LA EMPRESA con la DIAN pueden consultarse en el anexo “Especificaciones técnicas Implementación DRC.pdf”.

3.6 Transferencia de conocimiento a usuarios técnicos y usuarios finales junto con el manejo del cambio.

EL CONTRATISTA debe diseñar y ejecutar el plan de transferencia de conocimiento del nuevo sistema SAP S/4HANA RISE a los colaboradores que determine LA EMPRESA, así como el entrenamiento para la administración de usuarios, roles y perfiles en SAP al personal especializado de LA EMPRESA.

El servicio debe asegurar una transición eficiente y efectiva a la nueva versión ERP SAP S/4HANA garantizando sus integraciones y el correcto funcionamiento con otros sistemas de la Empresa y los datos requeridos para gestionar los procesos que operan.

El OFERENTE deberá comprometer un número de horas de formación para cada uno de los cuatro (4) componentes del proyecto. Las horas deben estar desagregadas por tipo de usuario: (i) técnico o administrador del sistema, (ii) super usuario funcional (usuario clave por proceso de negocio), y (iii) usuario final.

El OFERENTE deberá comprometer horas de soporte técnico-funcional dedicado a la Empresa durante los meses once (11) y doce (12) del contrato, es decir, el periodo posterior al go-live de la plataforma S/4HANA. Este soporte tiene como propósito el acompañamiento en la resolución de dudas operativas, incidentes funcionales y el refuerzo del conocimiento del equipo técnico y funcional interno de la Empresa.

Este criterio es independiente de la garantía contractual por defectos, que es una obligación del OFERENTE por derecho propio. El propósito será fortalecer la autonomía del equipo interno de la Empresa en la administración del sistema migrado.

3.7 Documentación

EL CONTRATISTA entregará a LA EMPRESA la documentación técnica, funcional y comercial que de conformidad con la naturaleza del objeto del contrato requiera LA EMPRESA durante su desarrollo. LA EMPRESA podrá hacer uso de toda la información entregada por EL CONTRATISTA con motivo del contrato, sin ninguna restricción, con propósitos de operación de las soluciones entregadas.

El OFERENTE deberá presentar un cronograma detallado del proyecto alineado con la metodología SAP Activate. El cronograma debe cumplir simultáneamente las siguientes condiciones verificables:

- Contener las seis (6) fases de la metodología SAP Activate: Discover, Prepare, Explore, Realize, Deploy y Run.
- No exceder diez (10) meses calendario desde la fecha de la orden de inicio hasta la salida en vivo (go-live).
- Contemplar de forma diferenciada los cuatro (4) componentes del proyecto: (i) migración ECC → S/4HANA, (ii) Cash Management, (iii) EWM y (iv) DRC.
- Identificar los hitos de entrega y las dependencias entre actividades.

El OFERENTE deberá presentar el cronograma en formato Gantt o equivalente, con las siguientes columnas mínimas: fase de SAP Activate, actividad, entregable o hito asociado, fecha de inicio, fecha de fin, dependencia y componente del proyecto al que pertenece (migración / Cash / EWM / DRC).

3.8 Garantías sobre los resultados de la consultoría

EL CONTRATISTA deberá atender por garantía los requerimientos que surjan hasta un plazo de seis (6) meses después del recibo a satisfacción de los servicios solicitados en los ítems 3.1 a 3.7 de este alcance y que sean atribuibles a EL CONTRATISTA.

3.9 Seguridad de la información

El 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:

- Políticas de seguridad

Será responsabilidad de EL CONTRATISTA la administración del usuario y clave asignada para acceder remotamente a las redes de la Empresa de Transporte Masivo del Valle de Aburra Limitada, por lo que en equipos portátiles no deberá almacenar la guía de acceso y tomar medidas de precaución que eviten en caso de que de que el portátil sea utilizado por terceros diferentes a las personas del contrato, la información de la Empresa esté segura. Todos los cambios que se realicen a los sistemas corporativos deben ser realizados siguiendo las políticas de ambientes de desarrollo, calidad y producción definidas por LA EMPRESA. El supervisor del contrato será quien defina el paso de los cambios a los sistemas de Producción acorde a las necesidades de operación de LA EMPRESA. EL CONTRATISTA deberá reportar a LA EMPRESA los eventos o incidentes de seguridad que afecten o tengan el potencial de afectar la prestación del servicio contratado, la información intercambiada entre las partes, los sistemas de información de LA EMPRESA o la información alojada en estos, y todas aquellas situaciones de alto riesgo que sean detectadas por los sistemas de monitoreo y control o en auditorías que realiza EL CONTRATISTA. De la misma forma deberá informar a LA EMPRESA los planes de remediación aplicados o por aplicar.

- Garantía sobre el tratamiento de la información de LA EMPRESA:

Toda la información y/o 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/o documentación suministrada para cualquier propósito distinto que no sea la prestación de los servicios objeto contratados. Esta condición debe ser extensiva para los empleados de EL CONTRATISTA y están obligados, no sólo al secreto profesional absoluto, sino también a la neutralidad y máxima discreción frente a otros clientes o interesados en la solución.

- Protección de datos personales:

EL CONTRATISTA y su servicio se encontrarán obligados al cumplimiento de la ley estatutaria 1581 de 2012 y el Decreto 1377 del 27 de junio de 2013, vigentes en Colombia.

4. LICENCIAMIENTO SAP S/4HANA RISE

A continuación, la lista de productos (BOM: Bill Of Materials) que LA EMPRESA tiene en proceso de adquisición. Este contiene el detalle por cada período:

Fase	ID Prod.	Descripción	Inicio	Fin	Cant.	Unidad
1	8019361	SAP Cloud ERP Private	1/10/2026	31/3/2027	60	1 Full Use Equivalent
1	8013803	SAP S/4HANA Cld for cash mgt, priv ed	1/10/2026	31/3/2027	3	1 User
1	8013668	SAP Doc a Rep Comp for S/4H Cld, priv ed	1/10/2026	31/3/2027	1	1 Object
1	8008783	SAP Payroll Processing, pce	1/10/2026	31/3/2027	500	1 User
1	8008910	SAP Core HCM Cld, priv ed	1/10/2026	31/3/2027	500	1 User
1	8008911	SAP Time Track Cld, priv ed	1/10/2026	31/3/2027	500	1 User
1	8017519	SAP S/4H Cld Sup Chain for EWM, priv ed	1/10/2026	31/3/2027	3	600.000 Document
1	8019164	SAP AI Unit	1/10/2026	31/3/2027	25	100 Capacity Unit
1	8008794	SAP Addit File Storage, priv cld ed	1/10/2026	31/3/2027	14	128 Gigabyte
1	8011727	SAP Cld, mem ext f. non-prd, Priv Ed	1/10/2026	31/3/2027	1	256 Gigabyte
1	8011367	SAP Additional Dbase Storage priv cld ed	1/10/2026	31/3/2027	2	128 Gigabyte
1	8008690	S/4 Cld, addt non-prod tier, priv ed (S)	1/10/2026	31/3/2027	1	1 Tenant
1	8013784	SAP S/4HANA Cld for TRM, priv ed	1/10/2026	31/3/2027	1	US$118.050.000
2	8019361	SAP Cloud ERP Private	1/4/2027	30/9/2031	180	1 Full Use Equivalent
2	8020297	SAP S/4HANA Cld, Digital Access, priv ed	1/4/2027	30/9/2031	500	1.000 Document
2	8013803	SAP S/4HANA Cld for cash mgt, priv ed	1/4/2027	30/9/2031	5	1 User
2	8013668	SAP Doc a Rep Comp for S/4H Cld, priv ed	1/4/2027	30/9/2031	1	1 Object
2	8008783	SAP Payroll Processing, pce	1/4/2027	30/9/2031	2500	1 User
2	8008910	SAP Core HCM Cld, priv ed	1/4/2027	30/9/2031	2500	1 User
2	8008911	SAP Time Track Cld, priv ed	1/4/2027	30/9/2031	2500	1 User
2	8017519	SAP S/4H Cld Sup Chain for EWM, priv ed	1/4/2027	30/9/2031	3	600.000 Document
2	8019164	SAP AI Unit	1/4/2027	30/9/2031	25	100 Capacity Unit
2	8011726	SAP Cld, mem ext f. prod tiers, priv ed	1/4/2027	30/9/2031	2	256 Gigabyte
2	8018022	SAP App Server Lynux Cld Prv Ed, add prd	1/4/2027	30/9/2031	1	1 Tenant
2	8011727	SAP Cld, mem ext f. non-prd, Priv Ed	1/4/2027	30/9/2031	2	256 Gigabyte
2	8011367	SAP Additional Dbase Storage priv cld ed	1/4/2027	30/9/2031	4	128 Gigabyte
2	8013784	SAP S/4HANA Cld for TRM, priv ed	1/4/2027	30/9/2031	3	US$118.050.000

5. EXPERIENCIA Y PERSONAL REQUERIDO

5.1 Experiencia de la empresa

EL CONTRATISTA deberá acreditar experiencia en migraciones del sistema SAP ERP ECC 6.0.X a las nuevas versiones del ERP S/4HANA en al menos dos (2) contratos finalizados en los últimos 24 meses.

Implementaciones del módulo Cash Management en la versión S/4HANA en al menos un (1) contrato finalizado en los últimos 24 meses.

Implementaciones del módulo WM o EWM (Extended Warehouse Management) en la versión S/4HANA, en al menos un (1) contrato finalizado en los últimos 24 meses.

Las experiencias en las migraciones y las implementaciones de los módulos descritos no necesariamente deben ser en un mismo proyecto, pero si deben acreditarse al menos las cantidades indicadas para la migración y para cada módulo.

La experiencia debe ser acreditada mediante constancia escrita, expedida por la empresa o entidad que recibió el servicio.

EL CONTRATISTA debe aparecer en el Partner Finder de SAP (https://www.sap.com/partners/find.html) como partner de Consultoría e Implementación de la solución SAP Cloud ERP Private con certificación PE Service vigente y emitida por SAP Colombia.

5.2 Experiencia y certificaciones del Recurso Humano

EL CONTRATISTA debe garantizar los siguientes perfiles para el proyecto de implementación:

- Gerente de proyecto.
- Arquitecto de solución.
- Experto en datos.
- Consultor Basis especialista en migración.
- Consultor ABAP especialista en Custom Code.
- Consultor especialista en Integraciones (BTP/CPI).
- Consultor especialista en Roles, perfiles y segregación de funciones.
- Consultor Basis especialista en CloudALM (Application LifeCycle Management).
- Consultor en Workflow/Fiori.
- Consultor FI-GL: Procesos financieros.
- Consultor FI-AM: Activos fijos.
- Consultor FI-CO: Costos.
- Consultor FI-TRM: Treasury and Risk Management.
- Consultor MM: Administración de Materiales.
- Consultor SD: Ventas y Distribución.
- Consultor PM: Mantenimiento de Planta
- Consultor HR: Recursos humanos, Nomina y administración de tiempos.
- Consultor PS: Sistema de Proyectos.
- Consultor PSM: Presupuesto Sector Publico.
- Consultor EWM: Administración extendida de almacenes.
- Consultor BCM/Cash Management.
- Consultor DRC: Document and Reporting Compliance
- Consultor experto en migración a Business Partner.

- Consultor experto en automatización de pruebas.
- Consultor experto en Gestión del Cambio.
- Consultor experto en procesos de negocio.

EL CONTRATISTA se obliga para con LA EMPRESA a garantizar, durante toda la vigencia del contrato la disponibilidad de cada uno de los perfiles. EL CONTRATISTA debe garantizar el nivel de dedicación de cada perfil para el cumplimiento del cronograma definido para el proyecto.

EL CONTRATISTA seleccionado deberá entregar la siguiente documentación para cada uno de los perfiles requeridos en un máximo de cinco (5) días hábiles, contados a partir de la adjudicación del contrato:

- Hoja de vida.
- Fotocopia del diploma o acta de grado que lo acredite como profesional graduado.
- Experiencia certificada en las actividades que serán su responsabilidad dentro del proyecto en, mínimo, dos (2) proyectos ya finalizados.

LA EMPRESA se reserva el derecho de revisar y validar las hojas de vida presentadas, solicitar aclaraciones, ajustes o reemplazos, rechazar perfiles que no cumplan con lo solicitado.

El incumplimiento en la presentación oportuna de la información del recurso humano que hará parte de la implementación podrá afectar el inicio de la operación del servicio, sin que ello genere: ampliación de plazos, reclamaciones contractuales ni reconocimientos económicos a favor de EL CONTRATISTA.

La validación de las hojas de vida no exime a EL CONTRATISTA de su responsabilidad sobre la idoneidad y permanencia del personal durante toda la vigencia del contrato.

Si por fuerza mayor debidamente sustentada, el profesional designado por EL CONTRATISTA no puede realizar las labores objeto del contrato, EL CONTRATISTA deberá poner a consideración de LA EMPRESA el personal sustituto, el cual deberá contar como mínimo con la experiencia y certificación acreditada del profesional a sustituir, **reservándose** LA EMPRESA la facultad discrecional de aprobar dicho cambio en caso de que éste no cumpla con lo requerido. Para tales efectos, EL CONTRATISTA deberá informar anticipadamente, y en un término de quince (15) días hábiles antes del cambio, quién será el nuevo profesional asignado para la ejecución del contrato.

6. OTRAS OBLIGACIONES DEL CONTRATISTA

EL CONTRATISTA se obliga para con LA EMPRESA a prestar la atención y soporte relacionada en el alcance del contrato, de forma virtual, en días laborales de lunes a viernes, en un horario comprendido entre las 07:30 y las 17:30.

Debido a la naturaleza de este contrato EL CONTRATISTA deberá realizar la ejecución de al menos el 30% del proyecto en sitio incluyendo: gerencia del proyecto, acompañamiento funcional, gestión del cambio y ejecución de pruebas con los usuarios.

Teniendo en cuenta que entre LA EMPRESA y el personal del CONTRATISTA no se crea ningún vínculo laboral ni administrativo, EL CONTRATISTA deberá entregar todos los medios necesarios para que el consultor realice las actividades requeridas para el cumplimiento del objeto contractual.

EL CONTRATISTA se obliga a asignar a su personal consultor un equipo de cómputo portátil completamente operativo y con el software debidamente licenciado, el cual debe incluir Sistema Operativo Windows Profesional y Office para la conexión a la red. Adicionalmente, EL CONTRATISTA deberá garantizar que este equipo portátil aprobará todos los protocolos implementados por LA EMPRESA para la seguridad de la información.

Estos protocolos son:

a. EL CONTRATISTA deberá presentar la factura de la legalidad del licenciamiento que tiene instalado en el equipo, tanto el sistema operativo como el demás software que tenga instalado en él. Si no presenta la factura, EL CONTRATISTA podrá traer una carta firmada por el representante legal de la compañía donde certifique la legalidad del software.

b. Si el equipo de cómputo de EL CONTRATISTA sólo se conecta a través de VPN y no al dominio Metro, debe garantizar que es un equipo de cómputo seguro, que no tiene virus y que tiene un antivirus instalado.

7. ANTECEDENTES INFRAESTRUCTURAS

7.1 Sistema SAP

Los sistemas SAP del Metro de Medellín Ltda. tienen como propósito soportar y automatizar los procesos básicos de LA EMPRESA y apoyar la gestión estratégica, a continuación, se relacionan los sistemas que actualmente tiene instalados la Empresa.

SAP ERP EHP8

Para el apoyo a la gestión de los procesos se tiene el sistema SAP ERP 6.08 con los siguientes módulos configurados:

FI CO Controlling.
FI GL Contabilidad General, incluye New General Leadger.
FI TR Tesorería.
FI TRM Tesorería Avanzada
FI AM Activos fijos.
PSM Control presupuestal para el sector público.
MM Manejo de materiales.
SD Ventas y distribución.
PS Project System.
HR Human Resources.

PY Nomina.
BC Basis/Workflow/Interface/B.D.
PM Plant Maintenance.

Sistema SAP Netweaver BW (Bodegas de datos)

Apoya a LA EMPRESA en los procesos de monitoreo y adecuación de la estrategia empresarial. Actualmente BW - Business Warehouse se encuentra en la versión 7.5.

Sistema SAP Solution Manager

Aporta al monitoreo de la infraestructura y consolidación de todos los sistemas SAP que posee LA EMPRESA, se encuentra implementado en la versión 7.2.

Landscape

A continuación, se relaciona el esquema de sistemas vigentes en la Empresa:

Solución	Versión	Ambiente	Sistema Operativo	Base de datos	Netweaver
SAP ERP 6.08	SAP ERP 6.08	DEV	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.5
	SAP ERP 6.08	PRD	Windows Server 2022 Estándar Enterprise-Cluster	Oracle 19.23.0.0.0	7.5
	SAP ERP 6.08	QAS	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.5
	SAP ERP 6.08	SANDBOX	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.5
SAP BW 7.5	SAP BW 7.5	DEV	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.5
	SAP BW 7.5	PRD	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.5
SAP SOLUTION MANAGER	Solution Manager 7.2	PRD	Windows Server 2022 Estándar	Oracle 19.23.0.0.0	7.4

Interfaces del ERP SAP con otros sistemas de LA EMPRESA a través de web services

Success Factors

- Replica de datos organizativos
- Servicio de confirmación
- Replicación de datos de PA

Suplos (Sistema de aprovisionamiento estratégico)

- Validación de documentos presupuestales
- Facturación de pedidos
- Ejecución contractual

Cívica (Gestión de medio de pago)

- Contabilización de usos de Cívica a SAP
- Contabilización de ajustes de Cívica a SAP
- Interfaz de recargas de Cívica a SAP
- Carga masiva de dinero desde SAP a Cívica
- Traslado de tiquetes desde SAP a Cívica
- Aprobaciones tiquetes desde Cívica a SAP
- Cargas Maquinas de Recarga Automática desde Cívica a SAP
- Conciliación Ventas desde Cívica a SAP y su compensación automática
- Partidas abiertas de las deudas de los deudores de SAP a Cívica
- Traslado de tarjetas recargadas desde Cívica a SAP
- Traslado ventas tarjetas costeadas desde Cívica a SAP
- Consulta de stocks y movimientos de material de tarjetas de SAP a Cívica
- Gestión de Afluencia de Pasajeros (Transacción ZPAS)

SAI (Sistema de Activos Inmobiliarios)

- Consulta de activos fijos.
- Consulta de valor neto de activos fijos.
- Consulta de datos básicos de acreedores.
- Consulta de datos de facturación de espacios comerciales.
- Consulta de avisos de mantenimiento asociados a espacios comerciales.

8. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN PARA COMPRA DE BIENES Y/O SERVICIOS

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 la compra de bienes y servicios para La Empresa se realice con CONTRATISTAS comprometidos con la protección de la información tanto propia como de terceros que los contratan, asimismo, con el cumplimiento de la normatividad de protección de datos personales vigente.

A continuación, se presentan los requisitos generales de seguridad de la información que deben cumplir todos los CONTRATISTAS. Además, los requisitos específicos para software como servicio, web services y aplicaciones web.

- **Políticas de Seguridad de la Información:** EL CONTRATISTA O ALIADO DE NEGOCIO debe contar con políticas de seguridad de la información implementadas al interior de su empresa debidamente publicadas y aprobadas por la alta dirección y sus empleados deben contar con el conocimiento y apropiación de estas.

- **Formación del personal:** EL CONTRATISTA O ALIADO DE NEGOCIO debe capacitar a su personal en el adecuado manejo y reserva de la información y bases de datos personales a las que tiene acceso, asimismo, en el cumplimiento de las políticas de seguridad de la información y la detección y respuesta ante eventos e incidentes.

- **Seguridad de los equipos de cómputo y legalidad de software:** EL CONTRATISTA O ALIADO DE NEGOCIO debe garantizar que la información intercambiada con LA EMPRESA o recolectada bajo su autorización será procesada o almacenada en equipos de cómputo y servidores autorizados, que cuenten con sistema operativo legal y actualizado a sus últimas versiones estables y con soporte técnico del fabricante y que tengan instalado software antivirus de uso corporativo, completamente actualizado y con soporte del fabricante. Asimismo, debe demostrar que posee y ha adquirido de manera legal la licencia o la autorización para el uso de los programas, software, aplicativos y hardware que utilizará para el desarrollo del objeto contractual.

- **Conexión de equipos a las redes de LA EMPRESA:** en caso de que EL CONTRATISTA o ALIADO DE NEGOCIO para cumplir con el objeto contractual requiera tener acceso autorizado al sistema, red o a algún recurso tecnológico de LA EMPRESA, se obliga a observar y a cumplir la política de seguridad de la información establecida, asimismo, acepta los controles de ciberseguridad implementados, entre los cuales se resaltan mas no se limita a los siguientes:

    - **Para equipos de CONTRATISTAS o ALIADOS DE NEGOCIO que requieren conexión directa a las redes de La Empresa:**
        - Instalación antivirus corporativo de LA EMPRESA en los equipos de contratistas en sitio.
        - Monitoreo y control de uso del servicio de internet corporativo.
        - Monitoreo y protección mediante dispositivos de seguridad perimetral.
        - Control del inventario de hardware y software.
        - Seguimiento periódico al uso de software legal.
        - Control de acceso mediante controlador de dominio.
        - Políticas de seguridad a nivel de red.
        - Intervenciones de hardware y software controlados por la mesa de servicios de La Empresa.
        - Borrado seguro de la información de LA EMPRESA y formateo del equipo al finalizar la relación contractual.

        .
    - **Para equipos de CONTRATISTAS o ALIADOS DE NEGOCIO que requieren conexión a través de software de conexión remota o a través de VPN a los sistemas de información o redes de La Empresa:**

- Software de conexión remota debe ser licenciado para uso corporativo.
- Se verifica el cumplimiento de los requisitos de Seguridad de los equipos de cómputo y legalidad de software por parte de LA EMPRESA para conexiones VPN.
- Instalación de cliente VPN de LA EMPRESA una vez autorizada la conexión.
- Monitoreo y protección de las conexiones VPN mediante dispositivos de seguridad perimetral.
- Control de acceso mediante dispositivos de seguridad perimetral.
- Políticas de seguridad a nivel de red.
- Borrado seguro de la información de LA EMPRESA al finalizar la relación contractual.

- **Gestión de eventos e incidentes de seguridad y privacidad de la información:** EL CONTRATISTA O ALIADO DE NEGOCIO debe reportar a LA EMPRESA los eventos o incidentes de seguridad que afecten o tengan el potencial de afectar la entrega de los bienes o la prestación del servicio contratado, afectar las bases de datos a su cargo, la información intercambiada entre las partes, los sistemas de información de LA EMPRESA o la información alojada en estos, y todas aquellas situaciones de alto riesgo que sean reportadas por sus empleados y aliados de negocio, detectadas por sus sistemas de monitoreo y control o a través de las auditorías que realiza. El correo electrónico al cual deben reportarse los eventos o incidentes de seguridad de la información es seguridaddigital@metrodemedellin.gov.co.

  EL CONTRATISTA O ALIADO DE NEGOCIO debe informar a LA EMPRESA cual será el correo electrónico oficial desde el cual se generarán estos reportes el cual será el mismo al que LA EMPRESA reportará aquellas situaciones de riesgo para él.

- **Almacenamiento e intercambio seguro de información:** En caso de requerirse el intercambio de información entre LA EMPRESA y EL CONTRATISTA o ALIADO DE NEGOCIO, deberá realizarse utilizando mecanismos seguros que minimicen el riesgo de acceso no autorizado, alteración, pérdida o fuga de esta. Asimismo, debe contar con mecanismos que garanticen la confidencialidad e integridad de la información a la que por objeto del contrato se le haya dado acceso o tenga almacenada en sus equipos y sistemas de información y garantizar que el acceso a esta únicamente estará disponible para personal autorizado y capacitado para su adecuado manejo y custodia.

- **Correo electrónico para comunicación con LA EMPRESA:** EL CONTRATISTA o ALIADO DE NEGOCIO debe contar con sus propios correos electrónicos para su personal durante la vigencia de los contratos. El correo debe ser de un dominio asociado a la empresa contratista o aliada, ejemplo, pepitoperez@empresa.com. No se admite el uso de correos electrónicos en dominios gratuitos como Gmail, Hotmail, Outlook, Yahoo!, entre otros. Estos dominios pueden ser bloqueados por las plataformas de seguridad dado que suelen ser usados para campañas maliciosas y envío de spam. Se debe evitar el envío de correos masivos o spam hacia cuentas de correo de La Empresa para evitar ser bloqueados por las plataformas de seguridad, afectando la comunicación necesaria para la ejecución del contrato.

  EL CONTRATISTA O ALIADO DE NEGOCIO debe configurar adecuadamente sus plataformas de correo para evitar ser víctima de suplantaciones de identidad o que los correos sean bloqueados por las plataformas de seguridad de LA EMPRESA, afectando las comunicaciones durante la ejecución contractual.

- **Capacitaciones de seguridad de la información citadas por LA EMPRESA**: EL CONTRATISTA o ALIADO DE NEGOCIO debe asistir a las capacitaciones que en materia de seguridad de la información LA EMPRESA realice y que a través de los supervisores de contrato se dan a conocer.

Para cumplir con los requisitos de seguridad generales descritos anteriormente, EL CONTRATISTA debe aportar a LA EMPRESA un documento firmado por el representante legal o su delegado, en el que los acepte e indique cómo cumple con cada uno de ellos.

9. REQUISITOS ESPECÍFICOS PARA SOFTWARE COMO SERVICIO, WEB SERVICES Y APLICACIONES WEB

Alojamiento de la información: La aplicación debe estar alojada en un centro de datos de alta disponibilidad que cumpla altos estándares de fiabilidad, escalabilidad y seguridad. Además, deberá contar como mínimo con las certificaciones en seguridad de la información ISO 27001:2013, SOC 1, SOC 2, SOC 3 y PCI DSS (en caso de que el servicio o aplicación se requiera para transmitir, procesar o almacenar información de tarjetas de pago).

Seguridad de la aplicación: EL CONTRATISTA o ALIADO DE NEGOCIO debe garantizar la seguridad del aplicativo y la infraestructura de hardware y software que lo soporta, cumpliendo como mínimo con las mejores prácticas descritas en ISO27001:2013, ISO 27032, NIST, u otros estándares y marcos de referencia, en cuanto al manejo de usuarios, contraseñas, puertos abiertos, servicios habilitados, separación de ambientes, definición de permisos, versiones actualizadas, (endurecimientos de hardware y software).

Desarrollo Seguro de la Aplicación o Servicio: EL CONTRATISTA O ALIADO DE NEGOCIO debe garantizar que el servicio o aplicación ofrecida y sus componentes, utiliza metodologías o buenas prácticas para el desarrollo seguro de software. A continuación, algunas de las más utilizadas:

- Proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés)
- Ciclo de vida de desarrollo de seguridad de Microsoft (Microsoft SDL, por sus siglas en inglés).
- Modelo de Madurez para Aseguramiento de Software (SAMM, por sus siglas en inglés).

Independencia de la Información: EL CONTRATISTA o ALIADO DE NEGOCIO debe garantizar que la información que bajo responsabilidad de LA EMPRESA sea almacenada en sus sistemas de información o bases de datos, se encuentra separada de la información de otros clientes o empresas.

Separación de ambientes: EL CONTRATISTA o ALIADO DE NEGOCIO debe garantizar que los ambientes productivos se encuentran separados de manera física o lógica de otros ambientes como calidad, desarrollo o pruebas.

Seguridad aplicaciones web: EL CONTRATISTA o ALIADO DE NEGOCIO debe tener implementados controles técnicos de seguridad de la información, por ejemplo, un cortafuegos para aplicaciones web (WAF, por sus siglas en inglés), que reduzcan la posibilidad de que se exploten vulnerabilidades críticas como las mencionadas en el top 10 del Open Web Application Security Project (OWASP).

Logs del servicio: El software, servicio o aplicación web debe mantener un registro de las actividades realizadas por los usuarios con un periodo de retención mínima de 30 días. Estos registros deben poder ser accesibles por EL CONTRATISTA cuando LA EMPRESA así lo solicite en el marco de procesos de auditoría, atención de eventos o incidentes.

Navegación segura: El software, servicio o aplicación web proporcionado por EL CONTRATISTA o ALIADO DE NEGOCIO debe contar con certificado SSL emitido por una entidad certificadora con validez internacional, para proporcionar a los clientes acceso seguro a la aplicación mediante https. Es responsabilidad de EL CONTRATISTA o ALIADO DE NEGOCIO mantener actualizado y vigente el certificado SSL.

Navegación segura con dominio web propio de LA EMPRESA: El software, servicio o aplicación web debe soportar la configuración de dominio o subdominio propio de LA EMPRESA, así como la instalación del respectivo certificado SSL para navegación segura mediante https. EL CONTRATISTA O ALIADO DE NEGOCIO debe configurar el sistema para que soporte esta funcionalidad.

Entrega de los datos almacenados: En caso de finalización del contrato o alianza por vencimiento del tiempo contratado u otros motivos, EL CONTRATISTA o ALIADO DE NEGOCIO debe entregar toda la información y datos personales propiedad de LA EMPRESA que se encuentre almacenada en las bases de datos de sus sistemas de información. EL CONTRATISTA o ALIADO DE NEGOCIO debe especificar el formato del archivo que sería entregado con el fin de que la información que contenga sea completamente accesible por LA EMPRESA. El plazo máximo para la entrega de la información será acordado entre LA EMPRESA y EL CONTRATISTA o ALIADO DE NEGOCIO y no podrá exceder los treinta (30) días calendario tras la finalización del contrato o alianza.

Destrucción de la información almacenada: Una vez finalizada la relación contractual y después de entregar a LA EMPRESA los datos almacenados, se debe destruir la información que sea propiedad o se encuentre bajo responsabilidad de LA EMPRESA y que se encuentre almacenada en las bases de datos y equipos de EL CONTRATISTA o ALIADO DE NEGOCIO, con procedimientos que garanticen la no recuperación de esta.

EL CONTRATISTA o ALIADO DE NEGOCIO una vez realizado el borrado seguro de la información y en un plazo máximo de quince (15) días calendario posterior a este, debe suministrar una certificación firmada por el representante legal en la que brinde información sobre el procedimiento aplicado, así como las herramientas de hardware y software, técnicas o algoritmos utilizados para la eliminación de la información.

Análisis de vulnerabilidad sobre la plataforma o servicio: Antes de la puesta en productivo del software y cuando se realicen cambios grandes sobre este o su infraestructura base, EL CONTRATISTA o ALIADO DE NEGOCIO con sus propias herramientas o través de un tercero autorizado, debe realizar auditoría técnica de seguridad sobre el aplicativo o servicio web y la infraestructura que lo soporta con el fin de identificar posibles vulnerabilidades que pongan en riesgo la información de LA EMPRESA o la disponibilidad del servicio. El informe de las auditorías de seguridad realizadas y las remediaciones aplicadas deben ser entregados a LA EMPRESA.

En caso de que LA EMPRESA lo requiera podrá realizar sus propias auditorías técnicas sobre el aplicativo o servicio web y la infraestructura que lo soporta, con la previa aprobación de EL CONTRATISTA O ALIADO DE NEGOCIO y con la coordinación y planificación de ambas partes, sin que esto implique sobre costos, ni afectación del servicio. El resultado del análisis de vulnerabilidades será compartido con EL CONTRATISTA O ALIADO DE NEGOCIO para que realice la remediación de los hallazgos en un plazo acordado entre las partes.

Acuerdo de transmisión de datos personales: En caso de tratamiento de datos personales por parte de EL CONTRATISTA o ALIADO DE NEGOCIO se deberá firmar entre este y LA EMPRESA un acuerdo de transmisión de datos personales.

Transferencia o transmisión de datos personales: En caso de Transferencia y Transmisión de Datos Personales se debe cumplir con lo establecido en el numeral 3.2 de la circular externa 002 del 23 de marzo de 2018 emitida por la Superintendencia de Industria y Comercio, sobre los países que cuentan con un nivel adecuado de protección de datos personales:

Alemania, Australia, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia y los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea.

Ver circular: https://www.sic.gov.co/sites/default/files/normatividad/032018/CIRCULAR-EXTERNA-002.pdf

Seguridad de los datos en tránsito: La información debe viajar cifrada cuando es transmitida entre los dispositivos del usuario final y las bases de datos de EL CONTRATISTA o ALIADO DE NEGOCIO. Asimismo, cuando para cumplir con el alcance del contrato se requiera intercambiar información sensible o datos personales con terceros que no tienen acceso directo a las bases de datos, se deberá realizar mediante canales seguros de comunicación que permitan mantener la confidencialidad e integridad de esta. Algunos métodos admitidos son:

- Servidor SFTP - Secure File Transfer Protocol (Protocolo de transferencia segura de archivos)
- Cifrar la información antes de transmitirla por correo electrónico corporativo o herramientas corporativas para el almacenamiento e intercambio de información.

EL CONTRATISTA o ALIADO DE NEGOCIO podrá sugerir otros métodos para el intercambio seguro de información los cuales deben ser evaluados y contar con el visto bueno de los profesionales responsables del proceso de ciberseguridad de LA EMPRESA.

Seguridad de los datos en reposo: La información o datos personales que por objeto del contrato o alianza sea almacenada en las bases de datos de EL CONTRATISTA o ALIADO DE NEGOCIO, deberá contar con mecanismos que garanticen la confidencialidad e integridad de esta y el acceso únicamente a personal autorizado, para el mantenimiento y soporte de los sistemas y para llevar a cabo las actividades establecidas en el alcance del contrato.

Seguridad de la infraestructura del servicio: La infraestructura interna que soporta el funcionamiento de las bases de datos y el software, servicio o aplicación web proporcionados por EL CONTRATISTA o ALIADO DE NEGOCIO debe estar protegida por equipos de seguridad informática debidamente configurados que controlen el acceso y comunicaciones desde y hacia internet y que permitan mitigar riesgos de ataque cibernético y fuga de información, entre otros.

Respaldo y recuperación de la información: EL CONTRATISTA o ALIADO DE NEGOCIO debe demostrar que cuenta con mecanismos y rutinas periódicas para el respaldo de la información y su recuperación en caso de incidentes o desastres, asimismo, debe informar a LA EMPRESA el tiempo promedio de recuperación que tiene establecido en sus planes de recuperación ante desastres (DRP).

Monitoreo de sistemas de información: EL CONTRATISTA o ALIADO DE NEGOCIO debe realizar el monitoreo permanente de las bases de datos, sistemas de información y la infraestructura tecnológica que los soporta, así como las actividades que realizan los usuarios autorizados y no autorizados con el fin de evitar afectaciones a la integridad, confidencialidad y disponibilidad de la información y actuar oportunamente en caso de cualquier evento o incidente de seguridad.

Acuerdos de Nivel de Servicio (ANS) y Métricas del servicio: EL CONTRATISTA o ALIADO DE NEGOCIO debe informar cual será disponibilidad comprometida sobre el servicio o aplicación, la cual no podrá ser inferior al 99,9%. La disponibilidad de infraestructura no incluye las paradas planificadas o trabajos programados los cuales serán acordados con LA EMPRESA.

EL CONTRATISTA o ALIADO DE NEGOCIO debe contar con las herramientas que permitan medir el cumplimiento de estas métricas.

Integración con otros sistemas de información: el software debe soportar la integración con otras plataformas tecnológicas de LA EMPRESA, por lo menos una de las siguientes:

- **Integración con directorio activo Microsoft on premise mediante VPN site to site:** modelo de integración a través del cual la base de datos de usuarios que tendrán acceso al software se encuentra alojada en un directorio activo Microsoft on premise y para lograrlo se implementa una VPN site-to-site entre los servidores que alojan el software, servicio o aplicación web y el firewall de la Empresa. EL CONTRATISTA o ALIADO DE NEGOCIO es responsable de adquirir, implementar y mantener disponible dicha integración.

- **Single Sign On Office365:** modelo de integración a través del cual la base de datos de usuarios que tendrán acceso al software se encuentra alojada en un directorio activo Microsoft y sincronizada con Office365, así, los usuarios utilizan sus credenciales de Office 365 para acceder al software. EL CONTRATISTA o ALIADO DE NEGOCIO es responsable de implementar la conexión y registrar la aplicación con Microsoft para que aparezca disponible para los usuarios con suscripción.

EL CONTRATISTA o ALIADO DE NEGOCIO debe especificar cuál de los anteriores mecanismos de integración soporta actualmente o estaría en capacidad de soportar, de modo que, si LA EMPRESA lo solicita, se realice la integración.

Para cumplir con lo anterior, EL CONTRATISTA o ALIADO DE NEGOCIO debe aportar a LA EMPRESA un documento firmado por el representante legal o su delegado, en el que acepte los requisitos de seguridad generales y específicos e indique como cumple con cada uno de ellos.

Durante la ejecución del contrato, LA EMPRESA podrá realizar inspecciones y auditorías previamente acordadas con EL CONTRATISTA o ALIADO DE NEGOCIO para verificar el cumplimiento de los requisitos de seguridad de la información establecidos. El resultado de estas auditorías será compartido con EL ENCARGADO para que este realice la remediación de las vulnerabilidades encontradas en un plazo acordado entre las partes.