# Anexo especificaciones técnicos Servicio Respaldo y Recuperación de Información

## Contenido


1. Objeto ..... 3
2. Alcance del Servicio ..... 3
2.1 Realización de copias de seguridad ..... 3
2.2 Ejecución automática y programada ..... 3
2.3 Almacenamiento seguro de respaldos ..... 4
2.4 Restauración de la información ..... 4
2.5 Tipos de Restauraciones ..... 4
2.6 Monitoreo y verificación ..... 4
2.7 Soporte técnico y administración ..... 4
2.8 Cumplimiento normativo y continuidad del servicio ..... 4
3. Diseño de la Solución de Backup ..... 5
3.1 Presentación diseño de la Solución de Backup ..... 6
3.2 Backup cyber resiliente ..... 7
3.2.1 Plan de respuesta a ransomware ..... 7
3.2.2 Sandbox ..... 8
3.2.3 Clean Room ..... 8
3.2.4 PlayRoom, RunBook, Table top ..... 8
4. Infraestructura Tecnológica (Hardware) ..... 8
4.1 Ambiente para pruebas de restauración ..... 8
5. Software de Backup ..... 9
6. Seguridad de la Información ..... 9
7. Implementación del Servicio ..... 9
8. Pruebas de Restauración y Recuperación ante Desastres ..... 10
9. Recuperación de desastres ..... 11
10. Operación y Soporte ..... 11
11. Personal Especializado ..... 11
12. Presentación de hojas de vida del personal asignado al servicio ..... 15
12.1 Fecha presentación ..... 15
12.2 Validación de documentación ..... 15
12.3 Condición para el inicio de la operación ..... 15

13. Entregables ..... 16
13.1 Reportes ..... 16
13.2 Diseño de la arquitectura de backup ..... 16
13.3 Políticas y procedimientos de backup y recuperación ..... 16
13.4 Estrategia de pruebas de recuperación (DR tests) ..... 16
13.5 Controles de ciberseguridad asociados ..... 16
14. Continuidad del Servicio y Contingencias ..... 16
15. Propiedad de la Información y Reversión ..... 17
16. Resultado Técnico Esperado ..... 17
17. Acuerdos de niveles de servicio ..... 17
18. Características de la infraestructura y servicios a respaldar ..... 18
18.1. Infraestructura de TI ..... 19
18.2. Infraestructura de TO ..... 19
19. Periodicidad de las copias y retención ..... 21
20. Resumen de cantidades estimadas ..... 21
20.1. Cantidades estimadas para la infraestructura de TI ..... 22
20.2. Cantidades estimadas para la infraestructura de TO ..... 22
21. Lugar de ejecución de las actividades ..... 22
22. Coordinación del contrato ..... 22

# Anexo especificaciones técnicos Servicio Respaldo y Recuperación de Información

## 1. Objeto

Prestar el servicio de backup en modalidad BAAS

El presente Anexo Técnico define las condiciones técnicas, operativas y funcionales para la prestación del Servicio de Backup como Servicio (BaaS), a cargo del CONTRATISTA, quien deberá garantizar la protección, integridad, confidencialidad, disponibilidad y recuperabilidad de la información institucional durante la vigencia del contrato.

## 2. Alcance del Servicio

El servicio deberá ser prestado de manera integral, administrada y continua, comprendiendo como mínimo: diseño de la solución de backup basado en las buenas prácticas; suministro, administración y operación del hardware requerido; licenciamiento y administración del software de backup; administración, operación y gestión de las librerías de respaldo (BK) con las que cuenta la organización; almacenamiento seguro de la información respaldada de acuerdo a los diferentes escenarios de falla; ejecución de copias de seguridad automáticas y bajo demanda; pruebas periódicas de restauración; atención de solicitudes e incidentes; soporte técnico especializado; monitoreo, reportes y seguimiento del servicio; y garantía de continuidad y disponibilidad de la información.

### 2.1 Realización de copias de seguridad

- Servidores físicos y/o virtuales
- Bases de datos institucionales
- Sistemas de información misionales y administrativos
- Equipos de usuario autorizados
- Repositorios de información corporativa
- Sistema de colaboración Microsoft 365
- Integración a las redes IT como OT
- Respaldo de los sistemas operacionales de las redes Scada, control, dmz, etc

### 2.2 Ejecución automática y programada

- Ejecución de copias programadas (diarias, semanales, mensuales según política)
- Copias completas, incrementales o diferenciales
- Automatización de procesos para minimizar errores humanos
- Automatización de recuperaciones en centro alterno

## 2.3 Almacenamiento seguro de respaldos

- Almacenamiento de los respaldos en medios locales, externos, en la nube o híbridos
- Protección mediante cifrado y control de accesos (RBAC), multifactor de autenticación
- Mecanismos de redundancia y conservación histórica de versiones
- Trampas para aumentar la seguridad de los almacenamientos.

## 2.4 Restauración de la información

- Ante fallos de hardware o software
- Ante eliminación accidental de información
- Ante incidentes de seguridad (virus, ransomware, intrusiones)
- Ante contingencias operativas

## 2.5 Tipos de Restauraciones

- Puntuales (archivos específicos) granulares
- Parciales o completas
- A nivel de sistema, base de datos, máquina física o máquina virtual
- A nivel de Bare Metal Recovery

## 2.6 Monitoreo y verificación

- Monitoreo del estado de las copias de seguridad 7X24X365
- Validación de ejecuciones exitosas
- Alertas ante fallos o inconsistencias
- Reportes de estado del servicio

## 2.7 Soporte técnico y administración

- Administración del sistema de backup
- Soporte técnico ante incidentes
- Ajustes de políticas de respaldo
- Acompañamiento en procesos de restauración
- Acompañamiento en el comité de gestión de cambios

## 2.8 Cumplimiento normativo y continuidad del servicio

- Políticas de seguridad de la información

- Planes de continuidad del negocio para el servicio de Backup (BCP)
- Acompañamiento en los planes de continuidad del negocio para los servicios de Metro de Medellín Ltda.
- Planes de recuperación ante desastres para el servicio de Backup (DRP)
- Acompañamiento en la elaboración de los planes recuperación ante desastres para los servicios de Metro de Medellín Ltda.
- Requisitos de auditoría y control
- Alinear las políticas de copias de seguridad con las políticas de ciber seguridad para definir el protocolo de ciber resiliencia
-

# 3. Diseño de la Solución de Backup

El CONTRATISTA en compañía de personal de METRO DE MEDELLÍN LTDA, deberá realizar el levantamiento de información y el inventario de los activos tecnológicos a respaldar; analizar la criticidad, volumen y tipo de información; definir la estrategia de backup (tipos de respaldo, frecuencias y políticas de retención); definir y cumplir los objetivos RPO y RTO (esta información será suministrada al CONTRATISTA una vez dada la orden de inicio); y presentar la arquitectura técnica de la solución para aprobación del supervisor del contrato.

El diseño de la estrategia de respaldo deberá estar basado mínimo en el modelo 2-2-1-1-0, el cual ha sido definido por METRO DE MEDELLÍN LTDA considerando criterios de optimización de costos, eficiencia operativa y priorización de la información crítica, sin que ello implique disminución en la capacidad de recuperación, integridad y disponibilidad de la información respaldada.

- 2 copias de la información
- 2 medios diferentes de almacenamiento
- 1 copia fuera del sitio (offsite)
- 1 copia inmutable o air-gap
- 0 errores verificados en las copias (mediante pruebas de recuperación)

En consecuencia, el CONTRATISTA deberá estructurar su solución conforme a este modelo, el cual establece el alcance y las condiciones mínimas exigidas por LA ENTIDAD. No obstante, el CONTRATISTA podrá proponer esquemas o modelos alternativos que optimicen la arquitectura, la eficiencia o la operación del servicio, siempre que dichas propuestas no impliquen costos adicionales para LA ENTIDAD ni afecten negativamente los niveles de servicio, y quedan sujetas a la evaluación y aprobación expresa de METRO DE MEDELLÍN LTDA.

El contratista deberá diseñar, implementar y operar la solución de Backup como Servicio (BaaS) incorporando criterios de sostenibilidad que promuevan el uso eficiente de los recursos tecnológicos y energéticos durante la prestación del servicio. Para ello deberá:

a. Implementar mecanismos de optimización del almacenamiento, tales como deduplicación, compresión y gestión eficiente del ciclo de vida de la información respaldada, con el fin de minimizar el consumo de recursos de infraestructura y capacidad de almacenamiento.

b. Priorizar el uso de infraestructuras tecnológicas y centros de datos que cuenten con prácticas orientadas a la eficiencia energética, la reducción de la huella de carbono o certificaciones reconocidas en materia de sostenibilidad, cuando estas estén disponibles.

c. Implementar políticas de retención de información alineadas con los requerimientos del Metro de Medellín, evitando el almacenamiento innecesario de información y promoviendo una gestión eficiente de los recursos tecnológicos.

d. Favorecer el uso de documentación, reportes, procedimientos y evidencias en formato digital, reduciendo el consumo de papel y otros insumos físicos asociados a la operación del servicio.

e. Presentar, durante la ejecución contractual, cuando sea requerido por el supervisor del contrato, información relacionada con las prácticas de sostenibilidad incorporadas en la prestación del servicio y las acciones implementadas para optimizar el uso de recursos tecnológicos.

## 3.1 Presentación diseño de la Solución de Backup

El CONTRATISTA deberá presentar, dentro de los cinco (5) días hábiles siguientes a la adjudicación, el diseño detallado de la solución de backup para la infraestructura de Tecnologías de Información (TI) y para la infraestructura de Tecnología de Operación (TO), según aplique. Dicho diseño deberá cumplir con los requisitos técnicos, funcionales, operativos y de seguridad establecidos en el presente Anexo Técnico.

LA EMPRESA podrá revisar los diseños presentados y, de considerarlo necesario, solicitar ajustes, aclaraciones o información complementaria, así como rechazarlos cuando no cumplan con los requisitos definidos.

La no presentación del diseño dentro del plazo establecido, la presentación incompleta de este o la falta de aprobación por parte de LA EMPRESA constituirán un incumplimiento de las obligaciones contractuales a cargo del CONTRATISTA. En consecuencia, esta situación podrá impedir el inicio de la prestación del servicio, sin que ello genere ampliaciones de plazo, modificaciones contractuales, reconocimientos económicos adicionales o exoneración de las responsabilidades derivadas de dicho incumplimiento.

Cuando el diseño contemple el uso de servicios de computación en la nube, EL CONTRATISTA deberá identificar la ubicación geográfica y el país donde residirá cada copia de respaldo, los proveedores de servicios en la nube involucrados y los subencargados, subcontratistas o terceros que participen en el almacenamiento, procesamiento, administración o tratamiento de la información, especificando el alcance de su participación.

## 3.2 Backup cyber resiliente

La solución de backup deberá estar diseñada bajo un enfoque de ciberresiliencia, garantizando la protección, detección, recuperación y continuidad de la información frente a incidentes de ciberseguridad, fallas operativas, errores humanos y eventos de fuerza mayor, incluyendo ataques de ransomware.

El servicio deberá asegurar que los respaldos sean inmutables, verificables, aislados y plenamente recuperables, incluso en escenarios adversos, protegiéndolos contra borrado malicioso, cifrado no autorizado y cualquier intento de modificación o alteración de la información respaldada.

| **Backup cyber resiliente** | |
|---|---|
| **Capacidades esperadas** | Disco: 70 TB<br>CPU: 128 Cores<br>Memoria: 256GB |

### 3.2.1 Plan de respuesta a ransomware

Definir e implementar un procedimiento integral de respuesta y recuperación ante incidentes cibernéticos que contemple las etapas de aislamiento de los sistemas comprometidos, validación de respaldos limpios y recuperación escalonada de los servicios afectados. Este procedimiento debe garantizar la contención efectiva del incidente, la verificación de la integridad y confiabilidad de los respaldos antes de su restauración, y la priorización ordenada de la recuperación de activos críticos para asegurar la continuidad operativa. Adicionalmente, se deben establecer indicadores de desempeño asociados al proceso, especialmente aquellos relacionados con el tiempo de recuperación ante eventos cibernéticos, con el fin de medir la efectividad de la respuesta y fortalecer las capacidades de resiliencia de la organización.

### 3.2.2 Sandbox

El CONTRATISTA deberá disponer de un entorno aislado para pruebas de restauración, análisis de malware y validación de integridad sin impacto en producción, teniendo en cuenta tanto la infraestructura de TI como la de TO que incluye sistemas legacy.

### 3.2.3 Clean Room

La solución propuesta deberá incluir un entorno seguro para recuperación post-incidente, libre de compromisos, permitiendo restauración confiable de servicios críticos.

### 3.2.4 PlayRoom, RunBook, Table top

El proponente debe incluir y desarrollar cada uno del run book para la ejecución ante un incidente cibernético y hacer simulacros de acuerdo con los tabletop definidos.

## 4. Infraestructura Tecnológica (Hardware)

El CONTRATISTA será responsable de proveer la infraestructura para la administración, el cableado, los gbits y las conexiones, y el almacenamiento necesario (local, nube o híbrida), garantizar alta disponibilidad mediante esquemas de redundancia, asegurar capacidad suficiente para la operación actual y crecimiento proyectado, disponer de controles físicos y lógicos de seguridad y garantizar la separación física o lógica entre ambientes de producción y respaldo. El CONTRATISTA deberá contemplar la inclusión de un switche LAN, tanto para la infraestructura de TI como la infraestructura de TO, de borde que permita la conexión entre la infraestructura de backup y el CORE de Metro de Medellín.

Adicionalmente, el CONTRATISTA será responsable de la gestión integral de la garantía del hardware, incluyendo la atención, coordinación y resolución de incidentes o fallas que se presenten, sin costos adicionales para la entidad, asegurando la continuidad del servicio conforme a los niveles acordados.

### 4.1 Ambiente para pruebas de restauración

En los casos en que así se acuerde expresamente entre las partes, METRO podrá proveer un ambiente de pruebas específico, y el CONTRATISTA será responsable de ejecutar las actividades de configuración, puesta a punto, ejecución y documentación correspondientes, de conformidad con los lineamientos definidos y las necesidades operativas de la empresa. En caso contrario, las pruebas deberán ejecutarse en el ambiente sandbox dispuesto para tal fin.

## 5. Software de Backup

El CONTRATISTA deberá proveer software de backup debidamente licenciado, legal y vigente; garantizar compatibilidad con los sistemas operativos, aplicaciones y bases de datos; configurar automatización de respaldos, encriptación, compresión, deduplicación, monitoreo y alertas; y administrar una consola centralizada de gestión del servicio.

El servicio de Backup as a Service (BaaS) no deberá presentar restricciones por licenciamiento asociadas al sistema operativo de las máquinas protegidas. El CONTRATISTA deberá garantizar la capacidad contratada de respaldo y restauración durante toda la vigencia del contrato, permitiendo la adición, retiro o reemplazo de máquinas, físicas o virtuales, sin costos adicionales ni requerimientos de relicenciamiento, siempre que se mantenga la capacidad total contratada.

## 6. Seguridad de la Información

El servicio deberá cumplir con todas las exigencias y lineamientos establecidos en el anexo de seguridad. Ver **Anexo 1. Anexo de seguridad SaaS, web services y hosting web**

Adicionalmente, la solución deberá contar con entornos de seguridad avanzados que permitan la detección, prevención y respuesta ante incidentes de seguridad de la información.

Durante toda la vigencia del contrato, METRO DE MEDELLÍN LTDA., podrá solicitar al CONTRATISTA, o realizar directamente, pruebas de hacking ético y/o escaneo de vulnerabilidades sobre la plataforma, sus servicios o cualquiera de sus componentes. En estos casos, el CONTRATISTA deberá gestionar, mitigar y cerrar oportunamente las brechas de seguridad identificadas que se encuentren bajo su responsabilidad.

## 7. Implementación del Servicio

El CONTRATISTA deberá presentar un plan de implementación cuya ejecución no supere quince (15) días contados a partir de la fecha de inicio definida por Metro de Medellín. Dentro de dicho

plazo deberá configurar las políticas y rutinas de backup, integrar la solución con la infraestructura existente, documentar la solución implementada, realizar la puesta en producción y validar la ejecución exitosa de los respaldos iniciales. La prestación del servicio objeto del contrato iniciará una vez la implementación haya sido verificada, validada y aceptada por el personal designado por Metro de Medellín. En consecuencia, los cobros y pagos asociados a la prestación del servicio se causarán únicamente a partir de dicha aceptación formal.

## 8. Pruebas de Restauración y Recuperación ante Desastres

El CONTRATISTA deberá ejecutar pruebas periódicas de restauración como parte integral de las pruebas de recuperación ante desastres (Disaster Recovery - DR), las cuales deberán contemplar la restauración parcial y total de los respaldos, así como la validación funcional de los servicios recuperados.

Estas pruebas deberán incluir tanto máquinas de Tecnologías de la Información TI como de Tecnologías de Operación TO que incluyen sistemas SCADA.

Las pruebas de DR deberán basarse en escenarios de riesgo definidos por LA EMPRESA e implicarán la restauración efectiva de los servicios, la validación integral de la operación en condiciones reales o controladas, y la medición de los tiempos de recuperación. Estas pruebas deberán ejecutarse como mínimo dos (2) veces al año.

El CONTRATISTA deberá documentar los resultados, los tiempos de recuperación, las lecciones aprendidas y las desviaciones identificadas, así como implementar los ajustes necesarios para mitigar riesgos y mejorar la capacidad de recuperación.

El CONTRATISTA deberá definir, documentar e implementar un procedimiento integral de respuesta y recuperación ante incidentes de ciberseguridad, incluyendo escenarios de ransomware, que contemple como mínimo: el aislamiento de los sistemas comprometidos, la identificación, verificación y validación de respaldos íntegros y libres de afectación, la restauración progresiva de los servicios afectados y el seguimiento hasta la completa normalización de la operación.

Dicho procedimiento deberá garantizar la contención efectiva del incidente, la verificación de la integridad, disponibilidad y confiabilidad de los respaldos antes de su utilización, y la priorización de la recuperación de los activos críticos, con el fin de asegurar la continuidad del servicio.

Adicionalmente, el CONTRATISTA deberá definir, medir y reportar indicadores de desempeño asociados al proceso de recuperación, incluyendo como mínimo los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO), VS los tiempos y puntos de recuperación actuales (RTA), así como la efectividad de las actividades ejecutadas.

## 9. Recuperación de desastres

Las actividades de recuperación ante desastres (Disaster Recovery - DR) asociadas a los sistemas de información cuyo respaldo esté bajo responsabilidad del CONTRATISTA serán lideradas por METRO DE MEDELLÍN LTDA., quien además proveerá la infraestructura tecnológica sobre la cual se restablecerán los servicios en los escenarios de contingencia o productivos.

El CONTRATISTA deberá acompañar técnica y operativamente la ejecución de dichas actividades, incluyendo el soporte en la activación de los respectivos Planes de Recuperación ante Desastres (DRP), la restauración de los servicios y el apoyo durante la operación en contingencia, así como en el retorno a la normalidad una vez el evento haya sido superado.

Estas actividades corresponden a procesos de restauración real de servicios y datos, ejecutados en escenarios de contingencia o en ambientes productivos, y deberán garantizar la disponibilidad, integridad y consistencia de la información recuperada.

Posterior a la activación de los servidores físicos o virtuales en el entorno de recuperación ante desastres, el CONTRATISTA deberá garantizar la protección de los datos generados durante el período de operación en contingencia, de acuerdo con las políticas de respaldo definidas.

Durante la ejecución de los procesos de recuperación ante desastres, no deberán generarse costos adicionales para LA EMPRESA asociados al tráfico de datos hacia o desde la nube.

## 10. Operación y Soporte

El CONTRATISTA será responsable de la atención de solicitudes de restauración y cambios de configuración, la gestión de incidentes que afecten la disponibilidad o integridad de la información y el cumplimiento de los niveles de servicio acordados.

## 11. Personal Especializado

El CONTRATISTA deberá garantizar la disponibilidad de personal técnico especializado y certificado, con roles claramente definidos y continuidad del servicio ante cambios de personal.

Además, contar con personal que tenga experiencia en infraestructuras críticas y conocimiento específico en entornos TO (Tecnología Operativa), garantizando la adecuada gestión, protección y recuperación de los activos tecnológicos asociados a sistemas de la operación.

# Anexo especificaciones técnicos Servicio Respaldo y Recuperación de Información

El CONTRATISTA deberá cumplir con los siguientes perfiles para la prestación del servicio.

**Rol:** Coordinador del Servicio – mínimo 1

**Actividad donde es requerido:** Transversal al contrato

| Nivel de educación | Experiencia Mínima | Responsabilidades |
|---|---|---|
| Pregrado en Ingeniería de sistemas, de software, electrónica, informática o afines.<br><br>Especialización en proyectos o Certificación e n ITIL foundations Versión 3 o superior o Certificación PMP (Project Managment Profesional) | Dos (2) años de experiencia como líder en implementación de proyectos BAAS. | • Planear, gestionar y controlar los servicios prestados por el CONTRATISTA en los frentes de trabajo relacionados en el alcance.<br>• Coordinar y administrar el personal de tal forma que las actividades que atiende el CONTRATISTA no sean interrumpidos o afectadas por incapacidades, vacaciones o rotación de personal.<br>• Realizar la gestión, clasificación, escalamiento y documentación de todas las solicitudes que el supervisor realice a través de los diferentes canales establecidos para este fin.<br>• Garantizar la calidad en la documentación de todos los incidentes, requerimientos, cambios y problemas atendidos por personal del CONTRATISTA.<br>• Coordinar las actividades programadas que atiende el CONTRATISTA garantizando que se cumplan los cronogramas definidos.<br>• Realizar diagnóstico de fallas repetitivas y presentar planes de acción para mejorar la disponibilidad de los servicios.<br>• Mantener una actitud proactiva frente a las oportunidades de mejora de los servicios, informando el plan a llevar a cabo al supervisor del contrato.<br>• Generar semanal y mensualmente los reportes de gestión del servicio definidos por la Empresa.<br>• Asistir a las reuniones y comités programados por el supervisor del contrato.<br>• Aportar toda la documentación |

| | | |
|---|---|---|
| | | requerida por el supervisor para el pago de facturación.<br>• Documentación de todos los incidentes y solicitudes. Además, garantizar la calidad en la documentación de todos los incidentes, requerimientos, cambios y problemas atendidos. |

**Rol:** Operador del servicio – mínimo 1

**Actividad donde es requerido:** Monitoreo y operación del Backup

| Nivel de educación | Experiencia Mínima | Responsabilidades |
|---|---|---|
| Formación tecnológica o profesional en: sistemas, software, electrónica, telecomunicaciones, informática o afines. | Dos (2) años o superior de experiencia profesional en la operación de la plataforma de Backup que utilizará el CONTRATISTA para la prestación del servicio. | • Garantizar el cumplimiento de los planes de Backup.<br>• Documentar y escalar los incidentes detectados en la operación, en la herramienta que se defina para tal fin.<br>• Ejecutar de manera manual las actividades puntuales de Backup cuando el proceso automático presente fallas. |

**Rol:** Atención de requerimientos e incidentes - mínimo 1

**Actividad donde es requerido:** Mantenimiento de la plataforma, atención de incidentes, Atención solicitudes de respaldo, recuperación y actividades de DRP

| Nivel de educación | Experiencia Mínima | Responsabilidades |
|---|---|---|
| Formación profesional en: sistemas, software, electrónica, telecomunicaciones, informática o afines.<br><br>Certificación por parte del fabricante de la plataforma de Backup a operar, equivalente a: | Dos (2) años o superior de experiencia profesional en administración de plataformas de Backup a operar. | • Implementación de la arquitectura BAAS definida para Metro de Medellín, previa revisión y validación.<br>• Diseño o rediseño y configuración de planes de mantenimiento preventivo y correctivo. |

| | | |
|---|---|---|
| Implementador o<br>Técnico avanzado o<br>Solución de problemas | | • Diseño o rediseño y configuración del esquema de respaldo y recuperación de desastres para los sistemas.<br>• Implementación del esquema de respaldo y recuperación de sistemas. Actualizaciones de las herramientas Backup, previa verificación de la matriz de compatibilidad del software de Backup con los componentes del sistema, a través de upgrade, reinstalación y aplicación de parches. Nuevas instalaciones de la herramienta.<br>• Apoyar las activades<br>• Elaboración de instructivos de procedimientos para el respaldo y recuperación, así como los de continuidad.<br>• Restauración de máquinas físicas y virtuales.<br>• Documentar y escalar al fabricante los incidentes detectados en la operación. |

En el evento de que EL CONTRATISTA requiera realizar un cambio de profesionales, el cambio deberá ser informado a LA EMPRESA con quince (15) días de anticipación, remitiendo la documentación necesaria que acredite calidades y experiencia iguales o superiores a las requeridas. La sustitución solo podrá efectuarse previa evaluación y aval de Metro de Medellín, quien se reserva el derecho de aceptar o rechazar el profesional propuesto cuando este no cumpla con los requisitos técnicos, de experiencia o idoneidad exigidos para la ejecución del contrato.

Durante toda la vigencia del contrato, EL CONTRATISTA deberá garantizar la disponibilidad y permanencia del personal mínimo exigido para la correcta ejecución de las actividades contratadas. En ningún caso los cambios de personal podrán generar una disminución en la capacidad operativa, en la dedicación requerida ni en el cumplimiento de las obligaciones contractuales. La ausencia del personal mínimo exigido o la

sustitución de este sin la aprobación previa de Metro de Medellín constituirá un incumplimiento contractual por parte del CONTRATISTA.

# 12. Presentación de hojas de vida del personal asignado al servicio

## 12.1 Fecha presentación

El Contratista deberá presentar la documentación del personal dentro de los cinco (5) días hábiles siguientes a la adjudicación.

La Empresa podrá validar, solicitar ajustes o rechazar perfiles.

La no presentación o la no acreditación de los perfiles requeridos en los términos establecidos constituirá un incumplimiento de una obligación contractual a cargo del CONTRATISTA. En consecuencia, podrá impedir el inicio de la prestación del servicio, sin que ello genere ampliaciones de plazo, modificaciones contractuales, reconocimientos económicos adicionales o exoneración de las responsabilidades derivadas del incumplimiento.

## 12.2 Validación de documentación

La Empresa se reserva el derecho de:

- Revisar y validar la documentación presentada.
- Solicitar aclaraciones, ajustes o reemplazos.
- Rechazar perfiles que no cumplan con lo definido.

## 12.3 Condición para el inicio de la operación

El incumplimiento de esta obligación podrá afectar el inicio de la operación del servicio, sin que ello genere:

- Ampliación de plazos.
- Reclamaciones contractuales.
- Ni reconocimientos económicos a favor del Contratista.

La validación de la documentación no exime al Contratista de su responsabilidad sobre la idoneidad y permanencia del personal durante toda la vigencia del contrato.

# 13. Entregables

## 13.1 Reportes

El CONTRATISTA deberá entregar reportes mensuales indicando el estado del servicio, informes de ejecución de respaldos y fallos, indicadores de desempeño y capacidad, y acompañamiento en comités de seguimiento contractual.

El nivel de detalle de los reportes será acordado con el coordinador del contrato.

## 13.2 Diseño de la arquitectura de backup

- Tipos de almacenamiento utilizados
- Ubicación de cada copia (on-premise, nube, offsite)
- Mecanismos de inmutabilidad
- Descripción detallada de la estrategia 2-2-1-1-0, explicando cómo se cumple cada componente.

## 13.3 Políticas y procedimientos de backup y recuperación

- Frecuencias de respaldo
- Retención de datos
- Procedimientos de restauración

## 13.4 Estrategia de pruebas de recuperación (DR tests)

- Frecuencia de pruebas
- Evidencia de validación de “0 errores”

## 13.5 Controles de ciberseguridad asociados

- Protección contra ransomware
- Control de accesos
- Monitoreo y alertas

# 14. Continuidad del Servicio y Contingencias

El CONTRATISTA deberá contar con planes de contingencia del servicio de backup y garantizar la recuperación de la información ante eventos críticos, asegurando la continuidad del servicio durante la vigencia contractual.

## 15. Propiedad de la Información y Reversión

La información respaldada será propiedad exclusiva de la entidad contratante. El CONTRATISTA deberá garantizar la portabilidad de los datos, la entrega de respaldos al finalizar el contrato y certificar la eliminación segura de la información bajo su custodia.

## 16. Resultado Técnico Esperado

La entidad contará con un servicio de backup administrado llave en mano, confiable y seguro, que garantice la continuidad de los sistemas de información y minimice el riesgo de pérdida de datos.

## 17. Acuerdos de niveles de servicio

Se espera el cumplimiento de los RTO y RPO por Servicio, tanto si se trata de una recuperación total o granular de un servidor físico o virtual específico.

Si se presenta un fallo o caída que impacte la operatividad de más de un servidor o todos los servidores se espera la recuperación de estos conforme a la criticidad definida, así:

- Todos los servidores de servicios de criticidad Alta: recuperación en 4 horas. Aproximadamente 121
- Todos los servidores de servicios de criticidad Media: recuperación en 8 horas Aproximadamente 73
- Todos los servidores de servicios de criticidad Baja: recuperación en 12 horas. Aproximadamente 49

Nota importante: Las cantidades antes descritas pueden variar durante la ejecución del contrato, ya que se crean nuevas necesidades o algunas migran a la nube como un servicio incluyendo el backup de estas.

En caso de presentarse la caída o fallo que impacte la operatividad de menos de 5 servicios independiente de su criticidad, se espera la recuperación de estos en un tiempo no mayor a 4 horas, si la caída supera los 5 servicios se espera la recuperación conforme al ítem anterior.

Niveles de atención de incidentes y requerimientos del Servicio de Recuperación y Restauración:

| Severidad | Tiempo de Atención (Horario Calendario) | Tiempo Máximo de solución operativa en (Horario Calendario) | Descripción |
|---|---|---|---|
| **Crítico** | Inmediato (máximo 15 minutos) | <= 1 horas | Incidente que interrumpe parcial o completamente la operación normal de todo el servicio de backup.<br><br>Incidente que interrumpe parcial o completamente la operación normal del servicio de backup en uno de sus servicios con criticidad ALTA |
| **Alto** | Inmediato (Máximo 15 minutos) | <= 3 horas | Incidente que interrumpe parcial o completamente la operación normal de un servicio con criticidad MEDIA. |
| **Medio** | 4 horas | <= 12 horas | Incidente que interrumpe parcial o completamente la operación normal de un servicio con criticidad BAJA. |
| **Bajo** | 24 horas | <=120 horas | Incidente que degrada la calidad del servicio de backup o amenaza con la interrupción total del mismo en el corto plazo. |
| **Planificada** | Planificado | Planificado | Incidente que reduce la calidad del servicio de backup y que NO amenaza con la interrupción total del mismo.<br>También aplica para requerimientos de mejoramiento y optimización. |

## 18. Características de la infraestructura y servicios a respaldar

## 18.1. Infraestructura de TI

| Servidores | |
|---|---|
| **Numero de máquinas** | Desarrollo: 18<br>Pruebas: 6<br>Producción: 157 |
| **Sistemas Operativos** | CentOS<br>Windows<br>SUSE<br>Ubuntu<br>Debian<br>Rocky<br>Red Hat |
| **Capacidades totales** | Disco: 202 TB<br>CPU: 200 GHZ – 288 Cores<br>Memoria: 3.4 TB |
| **Infraestructura de office 365** | 2500 cuentas |
| **Equipos personales** | |
| **Numero de equipos** | 12 |
| **Sistema operativo** | Windows |
| **Capacidades por equipo** | Disco 512GB<br>Memoria: 16 GB<br>1 CPU de 10 cores |

Durante la vigencia del contrato, y en caso de que las necesidades del servicio así lo requieran, la Empresa podrá solicitar la inclusión de sistemas operativos adicionales a los inicialmente contemplados en el alcance contractual. La incorporación de dichos sistemas operativos estará sujeta a la validación de viabilidad técnica por parte del contratista y, de ser necesario, a la gestión de las modificaciones contractuales correspondientes, conforme a la normatividad y procedimientos aplicables.

## 18.2. Infraestructura de TO

| Servidores | |
|---|---|
| **Numero de máquinas** | Producción: 52 |
| **Sistemas Operativos** | CentOS<br>Windows<br>Ubuntu |

| | |
|---|---|
| | Debian<br>Red Hat |
| **Capacidades totales** | Disco: 30 TB<br>Memoria: 1.5 TB |
| **Estaciones de trabajo rugerizadas** | 10 maquinas<br>5 TB Total de almacenamiento |
| **Repositorio de información** | 5 TB |

La infraestructura de TO está compuesta por entornos productivos y algunos sistemas legacy, operando sobre redes segmentadas, sin navegación hacia Internet; sin embargo, podrán habilitarse reglas específicas y controladas a través de los dispositivos de seguridad perimetral para permitir únicamente las comunicaciones requeridas para la operación del servicio de backup.

Se debe considerar que todos los activos de TO se encuentran en operación productiva permanente, no se dispone de ambientes independientes de desarrollo o pruebas.

En caso de requerirse la instalación de agentes para la ejecución de copias de seguridad, estos deberán ser livianos, de bajo consumo de recursos y diseñados para minimizar cualquier impacto sobre el desempeño, estabilidad y disponibilidad de los equipos y aplicaciones de TO.

Durante la vigencia del contrato, y en caso de que las necesidades del servicio así lo requieran, la Empresa podrá solicitar la inclusión de sistemas operativos adicionales a los inicialmente contemplados en el alcance contractual. La incorporación de dichos sistemas operativos estará sujeta a la validación de viabilidad técnica por parte del contratista y, de ser necesario, a la gestión de las modificaciones contractuales correspondientes, conforme a la normatividad y procedimientos aplicables.

**Aclaración sobre Infraestructura TI y TO para tener en cuenta en la Arquitectura de Respaldo**

La infraestructura tecnológica correspondiente a Tecnologías de la Información (TI) y Tecnologías de Operación (TO) se encuentra implementada en ubicaciones físicas independientes. No existe ningún tipo de conexión directa, enlace de red, ni integración lógica entre los ambientes de TI y TO. Esta segregación responde a criterios de seguridad, operación y cumplimiento normativo.

Por lo anterior, cualquier definición, diseño o implementación de arquitectura de respaldo debe realizarse de manera completamente independiente para cada entorno,

garantizando que los mecanismos, procedimientos y soluciones de respaldo de TI no dependan ni interactúen con los de TO, y viceversa.

No obstante, para la solución de Backup ciberresiliente establecida en el numeral 3.1, esta condición no aplicará, permitiéndose la implementación de una infraestructura compartida, siempre que se garantice el cumplimiento de los principios de aislamiento lógico, seguridad, control de accesos y protección de la información, evitando riesgos de propagación, dependencia operativa o afectación cruzada entre los entornos de TI y TO.

En este contexto, del total de setenta 70 Teras propuestos, sesenta 60 Teras estarán destinados a la infraestructura de Tecnologías de la Información TI y diez 10 Teras a la infraestructura de Tecnologías de Operación TO.

## 19. Periodicidad de las copias y retención

| **Servidores de TI y TO** | |
|---|---|
| **Ejecución** | 1 full semanal, incremental diario |
| **Retención** | 6 diarios, 5 semanales |
| **Para office 365** | |
| **Ejecución** | 1 full inicial, incremental diario de:<br>Correo<br>OneDrive<br>SharePoint<br>Teams |
| **Retención** | Infinitos desde la primera copia |
| **Computadores personales de TI y TO** | |
| **Ejecución** | 1 full inicial, incremental diario o cada N minutos |
| **Retención** | Infinitos desde la primera copia |

## 20. Resumen de cantidades estimadas

La **cantidad total estimada** objeto del presente contrato corresponde a la suma de una **línea base** de referencia, respecto de la cual existe certeza razonable de consumo o demanda, más una cantidad **variable estimada**, asociada a posibles incrementos derivados de las necesidades operativas que se presenten durante la ejecución contractual, sin que ello constituya una obligación de consumo, sino una proyección

para efectos de planeación y ejecución contractual. A continuación, se detallan dichas cantidades.

## 20.1. Cantidades estimadas para la infraestructura de TI

| Descripción | Unidad de medida | Línea base | Variable estimada | Total cantidad estimada |
|---|---|---|---|---|
| Backup como servicio o BaaS para servidores | Teras | 202 | 28 | 230 |
| Backup como servicio o BaaS para office 365 | Cuentas | 2500 | 200 | 2700 |
| Backup como servicio o BaaS para equipos personales | Equipos | 12 | 3 | 15 |
| Backup cyber resiliente | Teras | 60 | 5 | 65 |

## 20.2. Cantidades estimadas para la infraestructura de TO

| Descripción | Unidad de medida | Línea base | Variable estimada | Total cantidad estimada |
|---|---|---|---|---|
| Backup como servicio o BaaS para servidores | Teras | 35 | 5 | 40 |
| Backup como servicio o BaaS para equipos personales | Equipos | 10 | 2 | 12 |
| Backup cyber resiliente | Teras | 10 | 2 | 12 |

# 21. Lugar de ejecución de las actividades

Las actividades se desarrollan en las instalaciones del CONTRATISTA y acceden a la infraestructura de Metro de Medellín Ltda. a través de conexión remota.

# 22. Coordinación del contrato

Para efectos contractuales, el funcionario designado por el área de Sistema Operativo de Metro de Medellín para coordinar los aspectos del contrato relacionados con la infraestructura TO se denominará en adelante “Coordinador del Contrato”. Este será el responsable de la coordinación, seguimiento, validación y control de las actividades que involucren la

infraestructura de TO y actuará como interlocutor entre LA EMPRESA y EL CONTRATISTA para los asuntos asociados a dicha tecnología.

Así mismo, para efectos contractuales, el funcionario designado por el área de Gestión de Tecnologías de Información de Metro de Medellín para coordinar los aspectos del contrato relacionados con la infraestructura de T) se denominará en adelante "Coordinador del Contrato". Este será el responsable de la coordinación, seguimiento, validación y control de las actividades que involucren la infraestructura de TI y actuará como interlocutor entre LA EMPRESA y EL CONTRATISTA para los asuntos asociados a dicha tecnología.

Cuando la ejecución del contrato involucre actividades que impacten de manera conjunta la infraestructura de TI y TO, ambos coordinadores deberán articular las acciones requeridas dentro de sus respectivos ámbitos de responsabilidad para garantizar la correcta ejecución, seguimiento y control de las actividades contratadas.