Contenido

1. Objeto ... 3
2. Alcance del Servicio ... 3
2.1 Realización de copias de seguridad ... 4
2.2 Ejecución automática y programada ... 5
2.3 Almacenamiento seguro de respaldos ... 5
2.4 Restauración de la información ... 6
2.5 Tipos de Restauraciones ... 7
2.6 Monitoreo y verificación ... 7
2.7 Soporte técnico y administración ... 8
2.8 Cumplimiento normativo y continuidad del servicio ... 8
3. Diseño de la Solución de Backup ... 9
3.1 Presentación diseño de la Solución de Backup ... 14
3.2 Backup cyber resiliente ... 16
3.2.1 Plan de respuesta a ransomware ... 17
3.2.2 Sandbox ... 19
3.2.3 Clean Room ... 20
3.2.4 PlayRoom, RunBook, Table top ... 21
4. Infraestructura Tecnológica (Hardware) ... 21
4.1 Ambiente para pruebas de restauración ... 22
5. Software de Backup ... 22
6. Seguridad de la Información ... 23
7. Implementación del Servicio ... 25
8. Pruebas de Restauración y Recuperación ante Desastres ... 25
9. Recuperación de desastres ... 29
10. Operación y Soporte ... 31
11. Personal Especializado ... 32
12. Presentación de hojas de vida del personal asignado al servicio ... 36
12.1 Fecha presentación ... 36
12.2 Validación de documentación ... 36
12.3 Condición para el inicio de la operación ... 37

13. Entregables 37
13.1 Reportes 37
13.2 Diseño de la arquitectura de backup 37
13.3 Políticas y procedimientos de backup y recuperación 38
13.4 Estrategia de pruebas de recuperación (DR tests) 39
13.5 Controles de ciberseguridad asociados 39
14. Continuidad del Servicio y Contingencias 39
15. Propiedad de la Información y Reversión 40
16. Resultado Técnico Esperado 41
17. Acuerdos de niveles de servicio 41
18. Características de la infraestructura y servicios a respaldar 43
18.1. Infraestructura de TI 43
18.2. Infraestructura de TO 44
19. Periodicidad de las copias y retención 46
20. Resumen de cantidades estimadas 47
20.1. Cantidades estimadas para la infraestructura de TI 47
20.2. Cantidades estimadas para la infraestructura de TO 48
21. Lugar de ejecución de las actividades 48
22. Coordinación del contrato 48

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.

Entendemos, aceptamos y cumplimos. SVAIT prestará a Metro de Medellín el servicio de Backup como Servicio (BaaS) bajo un modelo integral y administrado, conforme a las condiciones técnicas, operativas y funcionales del Anexo Técnico.

Nuestro enfoque de ciberresiliencia comprende la protección de la información durante todo su ciclo de respaldo y recuperación. Para ello, gestionaremos controles de integridad, confidencialidad y disponibilidad, y verificaremos la **recuperabilidad mediante pruebas de restauración y evidencias documentadas**. El servicio se orientará a que Metro pueda recuperar su información y restablecer los servicios incluidos en el alcance frente a fallas, errores humanos o incidentes de ciberseguridad, de acuerdo con los objetivos y procedimientos aprobados.

Valor diferencial: SVAIT asume la recuperación verificable como resultado del servicio. No basta con reportar que una copia terminó correctamente: debemos demostrar que la información respaldada puede restaurarse y utilizarse.

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.

Entendemos, aceptamos y cumplimos. SVAIT prestará un servicio BaaS integral, administrado y continuo. Asumiremos el diseño de la arquitectura; el suministro, administración y operación del hardware requerido; el licenciamiento y administración del software; y la gestión de las librerías de respaldo existentes de Metro de Medellín, conforme a su inventario y condiciones técnicas.

Nuestro diseño partirá de la **identificación de los activos digitales**, en línea con la función *Identificar* y la categoría de gestión de activos del NIST CSF 2.0. Para cada activo incluido en el servicio relacionaremos su responsable, criticidad, dependencias, política de respaldo y procedimiento de recuperación. Con esa información definiremos las copias automáticas y bajo demanda, su almacenamiento seguro y los escenarios de falla que debe cubrir la solución.

La operación incluirá monitoreo, atención de solicitudes e incidentes, soporte especializado, reportes de seguimiento y pruebas periódicas de restauración. **SVAIT aportará evidencia de que las copias pueden recuperarse**, junto con la gestión de las fallas y acciones de mejora necesarias para sostener la continuidad del servicio durante el contrato.

Valor que destacamos: el alcance une inventario, tecnología y operación con pruebas reales de recuperación. Así, Metro puede seguir la protección de cada activo desde su identificación hasta la validación de la información restaurada.

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

Entendemos, aceptamos y cumplimos. SVAIT protegerá los activos de TI y TO incluidos en el alcance aprobado por Metro de Medellín: servidores físicos y virtuales, bases de datos, sistemas misionales y administrativos, equipos de usuario autorizados, repositorios corporativos y servicios de colaboración Microsoft 365.

Para cada activo identificaremos al responsable, la criticidad, las dependencias, el método de respaldo, la frecuencia, la retención y el procedimiento de recuperación. En bases de datos y aplicaciones definiremos respaldos consistentes con su operación, de modo que sea posible validar la información después de restaurarla.

Los sistemas de **SCADA, control, DMZ y demás componentes de TO** se tratarán conforme a sus restricciones operativas y de seguridad. Diseñaremos los respaldos de TI y TO de manera independiente, sin establecer una conexión directa entre ambas redes. Cualquier agente,

comunicación o intervención en TO quedará sujeto a validación técnica y autorización de Metro para evitar impactos en producción.

Valor aportado por SVAIT: cada carga tendrá una ruta de recuperación definida y comprobable, con especial atención a la continuidad de los sistemas operacionales.

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

Entendemos, aceptamos y cumplimos. SVAIT configurará copias diarias, semanales o mensuales según la política aprobada para cada activo y el punto de recuperación objetivo (RPO) definido por Metro de Medellín. Utilizaremos copias completas, incrementales o diferenciales según las características de cada carga, sus ventanas operativas y las necesidades de restauración.

Automatizaremos la ejecución, supervisión, generación de alertas y registro de resultados. Las copias fallidas se gestionarán hasta su corrección, dejando evidencia de la causa, la acción aplicada y el resultado de la nueva ejecución. Esto reducirá la dependencia de tareas manuales y permitirá detectar oportunamente períodos sin protección.

Para el centro alterno, definiremos y probaremos **secuencias de recuperación automatizables** que respeten las dependencias entre infraestructura, bases de datos y aplicaciones. Su activación se realizará mediante el procedimiento y las autorizaciones acordadas con Metro, verificando al final que los servicios recuperados funcionen correctamente.

Valor aportado por SVAIT: la automatización cubrirá tanto la generación de copias como la preparación de la recuperación; cada falla y cada prueba quedarán documentadas.

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.

Entendemos, aceptamos y cumplimos. SVAIT diseñará una arquitectura de almacenamiento local, externo, en nube o híbrido, según los escenarios de falla que deban cubrirse y las políticas de Metro de Medellín. Identificaremos la ubicación, función y período de retención de cada copia, e incorporaremos redundancia, conservación de versiones y mecanismos de inmutabilidad o aislamiento conforme a la estrategia aprobada.

Protegeremos los respaldos mediante cifrado, control de acceso basado en roles (RBAC) y autenticación multifactor. Separaremos los permisos de operación, administración y eliminación, con registros que permitan auditar los accesos y cambios sobre los repositorios. Los respaldos de TI y TO conservarán el aislamiento exigido en el anexo.

Para atender el requisito de **«trampas»**, definiremos con Metro mecanismos señuelo o *canary* en los repositorios donde sean técnicamente viables. Estos permitirán generar alertas tempranas ante accesos, modificaciones o intentos de borrado sospechosos, y activar el procedimiento de investigación y respuesta. Su configuración se documentará y probará sin afectar las copias legítimas.

Valor aportado por SVAIT: combinamos protección de las copias con detección temprana de intentos de alterarlas. La alerta servirá para actuar antes de que se comprometa la capacidad de recuperación.

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

Entendemos, aceptamos y cumplimos. SVAIT atenderá las solicitudes de restauración originadas por fallas de hardware o software, eliminación accidental, incidentes de seguridad y contingencias operativas. Para cada caso identificaremos el activo afectado, el impacto sobre el servicio, el punto de recuperación requerido y la secuencia de restauración aplicable.

Ante una eliminación accidental o una falla técnica, seleccionaremos la copia adecuada y verificaremos la integridad y funcionalidad de la información restaurada con el responsable designado por Metro de Medellín.

Ante virus, ransomware o intrusiones, la restauración se coordinará con el procedimiento de respuesta a incidentes de Metro. Antes de recuperar, verificaremos el estado de las copias y seleccionaremos un punto de recuperación confiable; después, validaremos el servicio en un entorno controlado cuando el escenario lo requiera. La reconexión a producción se realizará con la autorización correspondiente, para reducir el riesgo de reinfección.

En contingencias operativas, ejecutaremos la recuperación conforme a la criticidad y las dependencias de los servicios, documentando el punto recuperado, los tiempos alcanzados y la validación funcional.

Valor aportado por SVAIT: cada restauración concluirá con evidencia de que la información es utilizable y de que el servicio afectado puede volver a operar; en un incidente cibernético, incluiremos la comprobación de que el punto restaurado sea confiable.

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

Entendemos, aceptamos y cumplimos. SVAIT realizará restauraciones granulares de archivos y elementos específicos, así como recuperaciones parciales o completas de los activos incluidos en el servicio. Según la necesidad, la recuperación podrá ejecutarse a nivel de sistema operativo, base de datos, máquina virtual o servidor físico, incluido **Bare Metal Recovery** cuando aplique.

Antes de cada intervención confirmaremos con Metro el alcance solicitado, el punto de recuperación y el destino de la restauración, para evitar sobrescribir información vigente. En bases de datos y sistemas con dependencias, verificaremos además la consistencia de la información y la secuencia necesaria para restablecer la aplicación.

Documentaremos la ejecución y solicitaremos al responsable del servicio la **validación funcional** del resultado. Esta validación permitirá establecer si se recuperó únicamente el dato solicitado o si el sistema completo volvió a operar.

Valor aportado por SVAIT: Metro podrá solicitar desde un archivo puntual hasta la reconstrucción de un servidor, con un procedimiento y una comprobación acordes con el impacto de cada escenario.

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

Entendemos, aceptamos y cumplimos. SVAIT monitoreará el estado de las copias de seguridad **7 × 24 × 365**, incluyendo su ejecución, duración, fallos, alertas e integridad reportada por la plataforma.

Verificaremos diariamente los resultados de los respaldos. Una tarea marcada como «exitosa» se contrastará con la política esperada para identificar activos sin copia reciente, ejecuciones incompletas o desviaciones en la ventana de respaldo. Los fallos e inconsistencias generarán alertas, registro del incidente, escalamiento según su impacto y seguimiento hasta su resolución.

Entregaremos reportes de estado del servicio con los respaldos ejecutados, excepciones, acciones correctivas, capacidad utilizada y resultados de las pruebas de restauración. Estos reportes permitirán a Metro identificar qué información está protegida y dónde persiste un riesgo de recuperación.

Valor aportado por SVAIT: el monitoreo identifica fallas; la verificación y el seguimiento permiten corregirlas y dejar evidencia de la protección efectiva.

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

Entendemos, aceptamos y cumplimos. SVAIT administrará la plataforma de backup, sus políticas, repositorios, alertas y componentes incluidos en el servicio. Atenderemos los incidentes técnicos mediante diagnóstico, escalamiento, seguimiento y documentación hasta su resolución, conforme a los niveles de servicio acordados.

Ajustaremos las políticas de respaldo cuando cambien los activos, la criticidad, la capacidad o las necesidades de recuperación de Metro de Medellín, previa evaluación del impacto y aprobación correspondiente. Acompañaremos las restauraciones desde la selección de la copia hasta la validación del resultado por el responsable del servicio.

Participaremos en el **comité de gestión de cambios** para evaluar las intervenciones que puedan afectar la protección o recuperabilidad de la información. Cada cambio tendrá un análisis de impacto, una ventana de ejecución, un plan de reversa cuando aplique y una verificación posterior de que los respaldos continúan operando.

Valor aportado por SVAIT: conectamos la administración diaria con la gestión de incidentes y cambios, para que una modificación de la infraestructura no deje activos críticos sin respaldo ni comprometa su recuperación.

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

Entendemos, aceptamos y cumplimos. SVAIT operará el servicio de backup conforme a las políticas de seguridad de la información de Metro de Medellín y a los requisitos contractuales aplicables. Documentaremos los controles, procedimientos y evidencias necesarios para su seguimiento y auditoría.

Mantendremos un **plan de continuidad del propio servicio de backup (BCP)** para sostener su operación ante fallas de personal, plataforma, conectividad o instalaciones, y un **plan de recuperación ante desastres del servicio (DRP)** para restablecer sus componentes cuando una contingencia afecte su funcionamiento.

Acompañaremos a Metro en la elaboración y ejecución de los BCP y DRP de los servicios que protegemos, aportando el inventario de copias, las dependencias, los procedimientos de restauración y los resultados de las pruebas. Metro conservará la dirección y las decisiones de activación de sus planes institucionales.

Alinearemos las políticas de respaldo con las políticas de ciberseguridad para definir conjuntamente un **protocolo de ciberresiliencia**: detección y escalamiento de un posible compromiso, protección de las copias, selección y validación de un punto de recuperación confiable, restauración priorizada y autorización del retorno a producción. Registraremos las decisiones, los tiempos alcanzados, las desviaciones y las acciones de mejora.

Valor aportado por SVAIT: entregamos a Metro una relación comprobable entre sus políticas, los planes de continuidad, la respuesta ante un incidente cibernético y la recuperación efectiva de los servicios.

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)

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:

Entendemos, aceptamos y cumplimos. SVAIT realizará, junto con los responsables de TI y TO de Metro de Medellín, el levantamiento e inventario de los activos tecnológicos incluidos en el servicio. Para cada activo identificaremos su responsable, criticidad, volumen y tipo de información, dependencias y necesidades de recuperación. A partir de este análisis definiremos los tipos y frecuencias de respaldo, las políticas de retención y la arquitectura técnica que presentaremos para aprobación del supervisor del contrato.

Una vez Metro suministre los objetivos **RPO y RTO** después de la orden de inicio, los incorporaremos al diseño y verificaremos mediante dimensionamiento y pruebas que la solución permita cumplirlos para los servicios incluidos en el alcance. La arquitectura documentará por separado los componentes y flujos de TI y TO, conforme a los requisitos de segregación del anexo.

Como **valor agregado**, SVAIT propone aplicar la estrategia **3-2-1-1-0**: tres copias de la información —el dato en producción y dos copias de respaldo—, almacenadas mediante al menos dos medios o plataformas diferentes; una copia fuera del sitio; una copia inmutable o aislada; y pruebas de recuperación satisfactorias, sin errores pendientes. Cada componente quedará identificado en el diseño y respaldado por evidencias de configuración y restauración.

Esta estrategia se incluirá **dentro del precio ofertado, sin costos adicionales para Metro**, sin afectar negativamente los niveles de servicio. Por tratarse de un esquema propuesto por el contratista, lo someteremos a la **evaluación y aprobación expresa de Metro de Medellín**, tal como dispone el anexo. Si Metro solicita ajustes, mantendremos como mínimo las condiciones exigidas para la protección y recuperación de la información.

Diseñaremos, implementaremos y operaremos la solución con criterios de **uso eficiente del almacenamiento y de los recursos tecnológicos y energéticos**. El dimensionamiento tendrá en cuenta la criticidad y las políticas de retención aprobadas, evitando consumo innecesario de capacidad sin comprometer la integridad, disponibilidad o recuperabilidad de las copias.

Precisión para la oferta: conviene mostrar en el diagrama cuáles son las dos copias de respaldo del modelo 3-2-1-1-0. Así Metro podrá comprobar exactamente qué aporta SVAIT frente al mínimo del pliego, sin dejar la comparación sujeta a distintas formas de contar el dato en producción.

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.

Entendemos, aceptamos y cumplimos. SVAIT implementará mecanismos de **deduplicación y compresión**, de acuerdo con las capacidades de la plataforma y las características de cada carga protegida. Además, configurará el ciclo de vida de las copias conforme a las frecuencias y períodos de retención aprobados por Metro de Medellín.

Monitorearemos el crecimiento de los repositorios, la capacidad disponible y la efectividad de estos mecanismos. Con esa información propondremos ajustes para utilizar eficientemente la infraestructura y anticipar necesidades de capacidad, **sin modificar unilateralmente las retenciones ni comprometer la integridad o recuperabilidad de la información**.

Valor aportado por SVAIT: la optimización será medible y estará ligada a las políticas de protección de Metro; una reducción de almacenamiento nunca se dará por válida si perjudica la recuperación.

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.

Entendemos, aceptamos y cumplimos. Al seleccionar la infraestructura y los centros de datos que soportarán el servicio, SVAIT dará prioridad a opciones que acrediten prácticas de eficiencia energética, medición y reducción de la huella de carbono o certificaciones reconocidas en

sostenibilidad, **cuando estén disponibles y sean compatibles con los requisitos técnicos, de seguridad y de ubicación de los datos establecidos por Metro de Medellín**.

Documentaremos los criterios utilizados en la selección y las evidencias aportadas por los proveedores. Durante la operación, revisaremos el uso de capacidad y las oportunidades de optimización de recursos, sin afectar la protección ni la recuperación de la información.

Valor aportado por SVAIT: la sostenibilidad será un criterio verificable de selección y operación, subordinado a la seguridad y continuidad que exige el servicio.

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.

Entendido, aceptamos y cumplimos La solución propuesta permitirá configurar y administrar políticas de retención diferenciadas de acuerdo con el tipo de información, criticidad de los servicios, frecuencia de respaldo, requerimientos operativos y tiempos de conservación establecidos por la entidad.

Estas políticas contemplarán, entre otros aspectos:

- Definición de esquemas de retención diaria, semanal, mensual y anual, conforme a los requerimientos del Metro de Medellín.
- Configuración de ciclos de vida de la información que permitan conservar únicamente las copias requeridas durante los períodos establecidos.
- Eliminación controlada y automatizada de copias que hayan cumplido su período de retención, evitando el crecimiento innecesario del almacenamiento.
- Optimización del consumo de los recursos tecnológicos mediante mecanismos propios de la solución, tales como deduplicación, compresión y gestión eficiente de la capacidad, cuando aplique.
- Aplicación de políticas específicas por plataforma, carga de trabajo, servicio o nivel de criticidad.
- Monitoreo periódico del consumo y crecimiento del almacenamiento para anticipar necesidades de capacidad.
- Generación de reportes sobre utilización, retención, capacidad disponible y cumplimiento de las políticas configuradas.
- Revisión y ajuste de las políticas durante la operación del servicio cuando se presenten cambios en los requerimientos del Metro de Medellín.
- Conservación de la información de acuerdo con los criterios de disponibilidad, recuperación, seguridad e inmutabilidad definidos para la estrategia de respaldo y ciberresiliencia.

Durante la fase de implementación se realizará conjuntamente con el Metro de Medellín el levantamiento y validación de las políticas de retención requeridas. Posteriormente, estas serán configuradas, documentadas y verificadas mediante pruebas que permitan evidenciar su correcta aplicación.

De esta manera, se garantiza una gestión eficiente del ciclo de vida de los respaldos, reduciendo el almacenamiento innecesario de información y optimizando la utilización de la infraestructura tecnológica, sin comprometer los requerimientos de recuperación, continuidad y protección de la información establecidos por el Metro de Medellín.

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.

Entendido, aceptamos y cumplimos, Durante la ejecución, operación y seguimiento del servicio, se priorizará el uso de medios digitales para la generación, almacenamiento, consulta, actualización y entrega de la documentación asociada, incluyendo informes técnicos, reportes de gestión, procedimientos operativos, evidencias de respaldo y recuperación, actas, registros de pruebas, indicadores, matrices y demás entregables definidos por el Metro de Medellín.

La gestión documental se realizará mediante mecanismos electrónicos que permitan mantener la información organizada, disponible, trazable y actualizada, facilitando su consulta y conservación durante la vigencia del servicio.

Asimismo, se minimizará la generación de documentos impresos, utilizando formatos digitales como mecanismo principal de entrega y gestión de evidencias, salvo en aquellos casos en los que el Metro de Medellín solicite expresamente documentación física o exista un requerimiento normativo que así lo establezca.

Con esta práctica se contribuye a reducir el consumo de papel, tinta y demás insumos físicos asociados a la operación, al tiempo que se fortalece la trazabilidad, eficiencia operativa, disponibilidad de la información y sostenibilidad ambiental 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.

Entendido, aceptamos y cumplimos, Durante la operación del servicio se mantendrá trazabilidad sobre las principales acciones orientadas a la sostenibilidad y eficiencia tecnológica, incluyendo, entre otras:

- Uso prioritario de documentación, reportes, procedimientos y evidencias en formato digital.
- Optimización del consumo de almacenamiento mediante políticas de retención, deduplicación, compresión y gestión eficiente de capacidad, cuando estas funcionalidades apliquen a la solución implementada.
- Monitoreo del crecimiento y utilización de los recursos tecnológicos asociados a la plataforma.
- Revisión periódica de la capacidad utilizada y disponible, con el fin de identificar oportunidades de optimización.
- Administración eficiente de los ciclos de vida de la información, evitando la conservación innecesaria de datos fuera de los períodos definidos.
- Aprovechamiento eficiente de la infraestructura tecnológica disponible, procurando reducir consumos innecesarios de recursos de cómputo, almacenamiento y comunicaciones.

Cuando el supervisor del contrato lo requiera, se entregará la información disponible en formato digital, incluyendo reportes, registros, evidencias e indicadores relacionados con estas prácticas, de acuerdo con el alcance contractual y los mecanismos de seguimiento establecidos por el Metro de Medellín.

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.

Entendido, aceptamos y cumplimos, El diseño será elaborado con base en los requerimientos establecidos en el Anexo Técnico y contemplará, como mínimo, la arquitectura lógica y física de la solución, sus componentes, integraciones, flujos de respaldo y recuperación, capacidades, políticas de protección, esquemas de retención, mecanismos de inmutabilidad, seguridad, monitoreo y operación.

Asimismo, el documento de diseño incluirá la diferenciación y tratamiento de los ambientes TI y TO, considerando las particularidades de cada entorno, especialmente en aspectos de segmentación de red, disponibilidad, criticidad de los activos, ventanas de respaldo, recuperación, compatibilidad tecnológica y protección frente a amenazas de ciberseguridad.

El diseño deberá contemplar, según corresponda:

- Arquitectura detallada de la solución de backup y recuperación.
- Componentes de software, hardware, almacenamiento y comunicaciones.

- Integración con la infraestructura existente del Metro de Medellín.
- Definición de flujos de respaldo, réplica y recuperación.
- Políticas de backup, retención, versionamiento e inmutabilidad.
- Definición de RPO y RTO conforme a los requerimientos establecidos.
- Controles de acceso, roles, autenticación y mecanismos de seguridad.
- Cifrado de la información en tránsito y en reposo, cuando aplique.
- Segmentación y consideraciones específicas para los ambientes TI y TO.
- Estrategia de monitoreo, alertamiento, reportería y trazabilidad.
- Procedimientos generales de recuperación y validación de respaldos.
- Dimensionamiento de capacidad y proyección de crecimiento.
- Identificación de dependencias, prerrequisitos y consideraciones técnicas para la implementación.

El diseño será entregado para revisión y validación por parte del Metro de Medellín y servirá como documento base para la posterior implementación, configuración, pruebas y puesta en operación de la solución.

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.

Entendido, aceptamos y cumplimos, se entregaran los diseños elaborados para la revisión conforme a la solicitud, sin embargo estaremos prestos para ajustar cualquier requerimiento en el diseño.

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.

Entendido, aceptamos y cumplimos, Nos comprometemos a presentar el diseño completo dentro del plazo contractual establecido, incorporando todos los elementos técnicos, funcionales, operativos y de seguridad exigidos.

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 CPU: 128 Cores Memoria: 256GB

Entendido, aceptamos y cumplimos, con el requerimiento de diseñar e implementar la solución de backup bajo un enfoque integral de **ciberresiliencia**, orientado a proteger la información y garantizar su disponibilidad y capacidad de recuperación ante incidentes de ciberseguridad, fallas operativas, errores humanos, indisponibilidad de componentes y eventos de fuerza mayor, incluyendo escenarios de ransomware.

SVAIT estructurará la solución considerando controles preventivos, de detección, protección, recuperación y continuidad, de manera que las copias de seguridad constituyan una última línea confiable de recuperación ante eventos adversos.

La arquitectura propuesta contemplará, de acuerdo con los componentes finalmente seleccionados y aprobados por LA EMPRESA, los siguientes principios:

- **Inmutabilidad de los respaldos**, evitando su modificación, sobrescritura o eliminación durante el período de retención definido.
- **Aislamiento lógico y/o físico de las copias de seguridad**, reduciendo la exposición directa de los repositorios frente a compromisos de la infraestructura productiva.
- **Protección contra ransomware y borrado malicioso**, mediante controles de acceso, segregación de privilegios y mecanismos de protección propios de la plataforma.
- **Verificación de integridad y recuperabilidad**, mediante validaciones periódicas que permitan comprobar que los respaldos se encuentran íntegros, disponibles y aptos para recuperación.
- **Cifrado de la información**, tanto en tránsito como en reposo, cuando aplique a la arquitectura implementada.
- **Control de acceso basado en roles**, principio de mínimo privilegio y mecanismos reforzados de autenticación para las funciones administrativas.
- **Separación de credenciales y privilegios administrativos**, buscando reducir el impacto de una eventual afectación de cuentas del ambiente productivo.

- **Monitoreo, alertamiento y trazabilidad** sobre eventos relacionados con respaldos, fallos, modificaciones de configuración y operaciones administrativas.
- **Pruebas periódicas de restauración**, orientadas a validar la recuperación efectiva de archivos, aplicaciones, máquinas virtuales, bases de datos o sistemas protegidos, según corresponda.
- **Estrategias de recuperación ante incidentes**, definiendo procedimientos para restauración controlada de la información en escenarios de indisponibilidad, corrupción o compromiso de los sistemas productivos.
- **Documentación y evidencias de recuperación**, permitiendo demostrar el estado de las copias, los resultados de las pruebas y las acciones correctivas implementadas.

SVAIT buscará además que la arquitectura se alinee con principios reconocidos de protección de respaldos, tales como esquemas tipo **3-2-1-1-0 o equivalentes**, cuando sean compatibles con el alcance contratado, combinando múltiples copias, diferentes medios o ubicaciones, al menos una copia aislada o inmutable y mecanismos de verificación que minimicen errores de recuperación.

Durante la fase de diseño detallado se documentarán los mecanismos específicos mediante los cuales se garantizarán la **inmutabilidad, aislamiento, integridad, verificación y recuperación** de las copias de seguridad. Estos controles serán posteriormente implementados, probados y evidenciados durante la puesta en operación del servicio.

De esta manera, SVAIT garantizará que la solución de backup no se limite a la generación de copias de seguridad, sino que forme parte de una estrategia de **ciberresiliencia y continuidad tecnológica**, orientada a mantener disponibles copias confiables, protegidas y recuperables incluso ante escenarios severos de compromiso de la infraestructura.

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.

Entendido, aceptamos y cumplimos, SVAIT establecerá y documentará un procedimiento de **Cyber Recovery** integrado con la estrategia de backup y ciberresiliencia, contemplando como mínimo las siguientes etapas:

- **Identificación y activación del procedimiento:** detección del incidente, clasificación inicial, identificación de los activos afectados y activación de los responsables definidos para la atención y recuperación.
- **Contención y aislamiento:** aislamiento de sistemas, servidores, redes, cuentas o componentes comprometidos, evitando que la amenaza pueda propagarse hacia otros activos o hacia los repositorios de respaldo.
- **Protección de las copias de seguridad:** preservación de los respaldos inmutables y/o aislados, restringiendo operaciones administrativas que puedan afectar las copias requeridas para la recuperación.
- **Identificación del punto seguro de recuperación:** análisis de los respaldos disponibles para determinar una versión anterior al incidente que pueda ser utilizada como punto confiable de restauración.
- **Validación de respaldos limpios:** verificación de integridad, consistencia y recuperabilidad de las copias seleccionadas antes de incorporarlas nuevamente al ambiente productivo.
- **Validación de seguridad previa a la restauración:** cuando la arquitectura y las herramientas implementadas lo permitan, los respaldos podrán ser sometidos a verificaciones adicionales en ambientes segregados, sandbox, clean room o mecanismos equivalentes antes de su recuperación definitiva.
- **Priorización de activos y servicios:** establecimiento de un orden de recuperación de acuerdo con la criticidad definida por LA EMPRESA, las dependencias tecnológicas, los RTO/RPO establecidos y las necesidades de continuidad operativa.
- **Recuperación escalonada:** restauración progresiva de infraestructura, servicios base, aplicaciones, bases de datos y demás componentes, evitando la incorporación masiva de sistemas sin validaciones previas.
- **Validación posterior a la recuperación:** comprobación de integridad, disponibilidad, funcionalidad y conectividad de los servicios restaurados antes de autorizar su retorno a operación.
- **Retorno controlado a producción:** reincorporación de los activos recuperados de acuerdo con los procedimientos de LA EMPRESA y con las autorizaciones correspondientes.
- **Documentación y cierre:** generación de evidencias de las actividades realizadas, tiempos de recuperación, resultados obtenidos, desviaciones, acciones correctivas y oportunidades de mejora.

SVAIT establecerá adicionalmente mecanismos de **trazabilidad y medición del proceso de recuperación**, mediante indicadores que permitan evaluar su desempeño. Entre los indicadores a considerar, de acuerdo con el alcance contractual y los datos disponibles, se podrán incluir:

- Tiempo transcurrido desde la declaración del incidente hasta el inicio de las actividades de recuperación.
- Tiempo efectivo de recuperación de cada servicio o activo.
- Cumplimiento del **RTO** establecido.
- Cumplimiento del **RPO** definido para las cargas protegidas.
- Tiempo requerido para identificar y validar un punto de recuperación confiable.
- Porcentaje de restauraciones ejecutadas satisfactoriamente.

- Porcentaje de respaldos verificados como recuperables.
- Número de intentos requeridos para completar una recuperación.
- Tiempo total requerido para restablecer los servicios priorizados.
- Desviaciones frente a los tiempos objetivos de recuperación y acciones de mejora derivadas.

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.

Entendido, aceptamos y cumplimos

SVAIT contemplará dentro de la arquitectura de la solución un entorno aislado, tipo **Sandbox, Clean Room**, destinado específicamente a actividades de recuperación y validación segura. Este entorno permitirá ejecutar procesos de restauración controlada antes de reincorporar información, servidores o servicios a producción.

El entorno aislado deberá considerar, como mínimo:

- **Segmentación y aislamiento de red**, evitando conectividad directa no controlada con los ambientes productivos.
- **Restauración segura de máquinas virtuales, servidores, aplicaciones y datos** para validación previa.
- **Análisis de malware y amenazas**, utilizando las capacidades disponibles en las herramientas implementadas y los controles de seguridad definidos por LA EMPRESA.
- **Validación de integridad, consistencia y recuperabilidad** de los respaldos antes de su retorno a operación.
- **Pruebas periódicas de recuperación**, con generación de evidencias y trazabilidad de resultados.
- **Controles de acceso y segregación de privilegios**, restringiendo el acceso al entorno únicamente al personal autorizado.
- **Protección del ambiente productivo**, garantizando que las actividades de prueba no generen afectación sobre sistemas en operación.
- **Registro de eventos y actividades**, permitiendo auditar los procesos de restauración y validación realizados.

Para los ambientes de **Tecnologías de Información (TI)**, el entorno permitirá validar la recuperación de las cargas de trabajo protegidas conforme a los procedimientos definidos y a los RTO/RPO establecidos.

Para los ambientes de **Tecnología de Operación (TO)**, SVAIT tendrá en cuenta las particularidades propias de estos sistemas, incluyendo segmentación, restricciones de

conectividad, compatibilidad tecnológica y condiciones operativas que limiten la interacción directa con los sistemas productivos.

En el caso de **sistemas legacy**, se realizará previamente una validación de compatibilidad técnica considerando sistema operativo, hipervisor, controladores, aplicaciones, dependencias y mecanismos de restauración disponibles. Cuando una carga legacy no permita una restauración automatizada en el entorno aislado, SVAIT documentará y aplicará un procedimiento alternativo de recuperación y validación, acorde con las restricciones técnicas identificadas y aprobado por LA EMPRESA.

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.

Entendido, aceptamos y cumplimos, SVAIT contemplará dentro de la arquitectura de la solución un entorno aislado, tipo **Sandbox, Clean Room**, destinado específicamente a actividades de recuperación y validación segura. Este entorno permitirá ejecutar procesos de restauración controlada antes de reincorporar información, servidores o servicios a producción.

El entorno aislado deberá considerar, como mínimo:

- **Segmentación y aislamiento de red**, evitando conectividad directa no controlada con los ambientes productivos.
- **Restauración segura de máquinas virtuales, servidores, aplicaciones y datos** para validación previa.
- **Análisis de malware y amenazas**, utilizando las capacidades disponibles en las herramientas implementadas y los controles de seguridad definidos por LA EMPRESA.
- **Validación de integridad, consistencia y recuperabilidad** de los respaldos antes de su retorno a operación.
- **Pruebas periódicas de recuperación**, con generación de evidencias y trazabilidad de resultados.
- **Controles de acceso y segregación de privilegios**, restringiendo el acceso al entorno únicamente al personal autorizado.
- **Protección del ambiente productivo**, garantizando que las actividades de prueba no generen afectación sobre sistemas en operación.
- **Registro de eventos y actividades**, permitiendo auditar los procesos de restauración y validación realizados.

Para los ambientes de **Tecnologías de Información (TI)**, el entorno permitirá validar la recuperación de las cargas de trabajo protegidas conforme a los procedimientos definidos y a los RTO/RPO establecidos.

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.

Entendido, aceptamos y cumplimos, SVAIT desarrollará los Runbooks operativos necesarios para soportar la ejecución ordenada, controlada y trazable de las actividades requeridas durante un incidente cibernético. Estos documentos servirán como guía práctica para los equipos técnicos, operativos y de gestión involucrados en la respuesta y recuperación.

Los Runbooks contemplarán, según aplique, como mínimo:

- Criterios de activación y escalamiento del incidente.
- Roles y responsabilidades de los equipos participantes.
- Procedimientos de aislamiento y contención.
- Protección de repositorios y copias de seguridad.
- Identificación y validación del punto de recuperación seguro.
- Verificación de integridad y confiabilidad de los respaldos.
- Procedimientos para recuperación en entornos aislados, Sandbox o Clean Room.
- Secuencia de recuperación de servicios de acuerdo con criticidad y dependencias.
- Procedimientos específicos para ambientes TI, TO y sistemas legacy.
- Validaciones técnicas y funcionales posteriores a la restauración.
- Procedimientos para retorno controlado a producción.
- Canales de comunicación, escalamiento y toma de decisiones.
- Evidencias requeridas durante cada fase del proceso.
- Criterios de cierre del incidente y actividades posteriores de mejora.

SVAIT desarrollará Runbooks específicos para los diferentes escenarios de recuperación definidos conjuntamente con LA EMPRESA, incluyendo, cuando aplique, eventos de **ransomware, corrupción de información, eliminación accidental o maliciosa, compromiso de credenciales administrativas, indisponibilidad de infraestructura, afectación de sistemas críticos y pérdida parcial o total de servicios**.

Adicionalmente, SVAIT participará en la planificación y ejecución de ejercicios **Tabletop**, en los cuales se simularán escenarios de incidentes cibernéticos con el propósito de validar los procedimientos, responsabilidades, dependencias, tiempos de respuesta y capacidad efectiva de recuperación.

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.

Entendido, aceptamos y cumplimos

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.

Entendido, aceptamos y cumplimos, con el requerimiento de asumir la gestión integral de la garantía del hardware suministrado dentro del alcance contractual.

SVAIT será responsable de gestionar de manera directa la atención, coordinación, seguimiento y resolución de los incidentes o fallas asociados al hardware cubierto por garantía, actuando como punto de contacto frente a los fabricantes, mayoristas o centros de soporte autorizados que intervengan en el proceso; SVAIT realizará el seguimiento necesario hasta el restablecimiento del componente o servicio afectado, procurando mantener la continuidad operativa y el cumplimiento de los niveles de servicio 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.

Entendido, aceptamos y cumplimos, Cuando METRO disponga y acuerde expresamente el uso de un ambiente de pruebas específico, SVAIT será responsable de realizar las actividades necesarias de **configuración, puesta a punto, ejecución, validación y documentación** de las pruebas, de acuerdo con los lineamientos técnicos, de seguridad y operativos definidos por la entidad. En los casos en que METRO no suministre un ambiente de pruebas específico, SVAIT ejecutará estas actividades en el **ambiente Sandbox o entorno aislado dispuesto dentro de la solución**, garantizando la segregación respecto de los ambientes productivos y evitando cualquier afectación sobre la operación.

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.

Entendido, aceptamos y cumplimos, Para el servicio de **Backup as a Service (BaaS)**, SVAIT estructurará el esquema de licenciamiento y prestación del servicio de forma que no se generen restricciones por el sistema operativo de las máquinas protegidas, siempre dentro de las condiciones técnicas y comerciales de la solución finalmente ofertada y contratada.

La capacidad del servicio será administrada con base en la **capacidad total contratada**, permitiendo durante la vigencia del contrato:

- Adicionar nuevas máquinas físicas o virtuales.
- Retirar máquinas existentes.
- Reemplazar cargas de trabajo.
- Modificar la distribución de las cargas protegidas.
- Incorporar cambios derivados de procesos de renovación tecnológica o virtualización.

Estas modificaciones podrán realizarse **sin costos adicionales ni requerimientos de relicenciamiento**, siempre que la capacidad total utilizada se mantenga dentro de los límites contratados y que las nuevas cargas se encuentren soportadas por la tecnología seleccionada.

SVAIT realizará el seguimiento permanente del consumo de capacidad, crecimiento, utilización y disponibilidad de recursos, con el fin de asegurar que la plataforma mantenga durante toda la vigencia contractual la capacidad requerida tanto para los procesos de **backup como de restauración**.

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.

Entendido, aceptamos y cumplimos, SVAIT implementará la solución bajo un enfoque de **protección por capas y ciberresiliencia**, incorporando controles técnicos y operativos que permitan reducir la superficie de ataque, detectar comportamientos anómalos y responder oportunamente ante eventos que puedan comprometer la integridad, disponibilidad o confidencialidad de la información respaldada.

La solución contemplará, según las capacidades de la tecnología seleccionada, como mínimo:

- **Detección de amenazas y comportamientos anómalos** sobre los respaldos, repositorios y componentes de la plataforma.
- **Protección contra ransomware**, borrado malicioso, cifrado no autorizado y alteración de copias de seguridad.
- **Inmutabilidad y aislamiento de respaldos**, reduciendo la posibilidad de afectación ante compromisos del ambiente productivo.
- **Control de acceso basado en roles (RBAC)** y aplicación del principio de mínimo privilegio.
- **Autenticación reforzada**, incluyendo mecanismos de MFA cuando sean soportados por la solución.
- **Cifrado de información en tránsito y en reposo**, conforme a las capacidades de la plataforma y lineamientos de METRO.
- **Monitoreo y generación de alertas** ante eventos relevantes de seguridad, cambios administrativos y fallos de protección.
- **Registro y trazabilidad de eventos**, permitiendo auditoría y análisis posterior de las acciones realizadas sobre la plataforma.
- **Validación de integridad y recuperabilidad** de las copias de seguridad.
- **Entornos aislados tipo Sandbox o Clean Room** para restauración controlada, análisis y validación de respaldos antes de su retorno a producción.
- **Integración con los procedimientos de respuesta a incidentes y Runbooks** definidos para la estrategia de ciberresiliencia.

SVAIT administrará estos mecanismos como parte integral del servicio, manteniendo la plataforma configurada de acuerdo con los lineamientos de seguridad aprobados por METRO y generando las evidencias requeridas sobre eventos, alertas, validaciones y acciones ejecutadas.

- 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.

Entendido, aceptamos y cumplimos, SVAIT brindará el acompañamiento técnico requerido para la ejecución controlada de estas pruebas, procurando que se desarrollen bajo condiciones previamente coordinadas que minimicen riesgos sobre la disponibilidad y operación de los servicios.

Cuando como resultado de dichas evaluaciones se identifiquen vulnerabilidades o brechas de seguridad cuya gestión se encuentre bajo responsabilidad de SVAIT, se realizará el correspondiente proceso de análisis, priorización, mitigación, remediación y cierre.

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.

Entendido, aceptamos y cumplimos, SVAIT estructurará el plan de implementación con actividades, responsables, dependencias, hitos y entregables claramente definidos, orientados a garantizar la puesta en operación de la solución dentro del plazo establecido. SVAIT realizará seguimiento al avance del plan durante toda la etapa de implementación, gestionando oportunamente las dependencias, riesgos y posibles desviaciones que puedan afectar el cumplimiento del plazo contractual.

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.

Entendido, aceptamos y cumplimos, SVAIT incorporará estas pruebas dentro del modelo operativo del servicio, incluyendo cargas de **Tecnologías de la Información (TI)** y **Tecnologías de Operación (TO)**, considerando las particularidades de los sistemas industriales y **SCADA**, sus dependencias, restricciones de conectividad, criticidad operativa y requerimientos de seguridad.

Las pruebas de DR contemplarán, como mínimo:

- Restauración parcial de archivos, bases de datos, aplicaciones, máquinas virtuales o componentes específicos.
- Restauración total de máquinas, servidores o servicios seleccionados dentro del escenario de prueba.
- Recuperación de cargas TI y TO incluidas dentro del alcance contractual.
- Pruebas específicas sobre sistemas SCADA, cuando correspondan al escenario definido por LA EMPRESA.
- Ejecución de las restauraciones en ambientes controlados, Sandbox, Clean Room o ambientes de prueba autorizados por METRO, evitando afectaciones sobre la operación productiva.
- Validación de la integridad y consistencia de la información recuperada.
- Validación funcional de aplicaciones y servicios restaurados.
- Verificación de dependencias entre infraestructura, sistemas operativos, bases de datos, aplicaciones y servicios asociados.
- Validación de los puntos de recuperación utilizados.
- Medición del tiempo efectivo de restauración y recuperación.
- Comparación de los resultados obtenidos frente a los objetivos de **RTO y RPO** definidos para los servicios evaluados.
- Registro de incidentes, desviaciones, hallazgos y oportunidades de mejora.
- Generación de evidencias técnicas y documentación de los resultados.

Las pruebas serán estructuradas con base en los **escenarios de riesgo definidos por LA EMPRESA**, pudiendo contemplar, entre otros, indisponibilidad de infraestructura, corrupción de información, pérdida de máquinas, errores operativos, fallas de almacenamiento, incidentes de ransomware o afectaciones sobre servicios críticos.

Para cada ejercicio, SVAIT elaborará previamente un plan de prueba que establecerá el alcance, sistemas involucrados, escenario de riesgo, responsables, prerrequisitos, secuencia de recuperación, criterios de aceptación y mecanismos de medición. La ejecución será soportada por los **Runbooks de recuperación** definidos para cada tipo de servicio.

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.

Entendido, aceptamos y cumplimos, VAIT generará para cada prueba, simulacro o ejercicio de recuperación un informe técnico de resultados que incluirá, como mínimo:

- Alcance y escenario de riesgo evaluado.
- Sistemas, servicios y cargas involucradas.
- Fecha y condiciones de ejecución.
- Punto de recuperación utilizado.
- Tiempo de restauración y tiempo total de recuperación.
- Comparación de los resultados frente a los RTO y RPO definidos, cuando apliquen.
- Resultado técnico y funcional de los servicios recuperados.
- Incidentes, fallas o desviaciones presentadas durante la ejecución.
- Dependencias técnicas y operativas identificadas.
- Lecciones aprendidas.
- Riesgos identificados durante el ejercicio.
- Recomendaciones y acciones correctivas.
- Evidencias de las actividades ejecutadas.
- Responsables y fechas objetivo para la implementación de las acciones de mejora.

Las desviaciones identificadas serán analizadas y clasificadas de acuerdo con su criticidad e impacto sobre la capacidad de recuperación. Con base en este análisis, SVAIT definirá e implementará los ajustes técnicos, operativos y documentales que correspondan dentro del alcance contractual.

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.

Entendido, aceptamos y cumplimos, SVAIT desarrollará este procedimiento como parte integral de la estrategia de **ciberresiliencia, Backup y Disaster Recovery**, contemplando como mínimo las siguientes etapas:

- **Activación y clasificación del incidente:** identificación del evento, determinación preliminar de su alcance y activación de los responsables y procedimientos correspondientes.
- **Aislamiento y contención:** segregación de los sistemas, servidores, redes, cuentas o componentes comprometidos con el propósito de limitar la propagación del incidente y proteger los repositorios de respaldo.
- **Protección de las copias de seguridad:** preservación de los respaldos inmutables, aislados y disponibles para recuperación, evitando su eliminación, modificación o cifrado no autorizado.
- **Identificación del punto seguro de recuperación:** determinación del respaldo o versión adecuada previa al incidente, considerando la línea de tiempo del evento y los puntos de recuperación disponibles.
- **Verificación y validación de respaldos:** comprobación de integridad, consistencia y recuperabilidad de las copias antes de iniciar el proceso de restauración.

- **Validación de seguridad:** cuando las capacidades de la solución lo permitan, ejecución de análisis de malware y verificaciones adicionales en ambientes aislados tipo Sandbox, Clean Room o equivalentes, evitando reincorporar información comprometida a producción.
- **Restauración progresiva:** recuperación escalonada de infraestructura, servicios base, sistemas operativos, bases de datos, aplicaciones y demás componentes, de acuerdo con su criticidad y dependencias.
- **Validación técnica y funcional:** comprobación del correcto funcionamiento de los servicios restaurados antes de autorizar su reincorporación al ambiente productivo.
- **Retorno controlado a operación:** habilitación progresiva de los servicios una vez se hayan completado las validaciones técnicas, funcionales y de seguridad correspondientes.
- **Seguimiento hasta normalización:** monitoreo de los servicios recuperados y atención de cualquier desviación hasta alcanzar la completa estabilización de la operación.
- **Documentación y cierre:** consolidación de evidencias, tiempos de recuperación, hallazgos, desviaciones, acciones ejecutadas y lecciones aprendidas.

En escenarios de **ransomware**, SVAIT dará especial atención a la separación entre los ambientes comprometidos y los repositorios de backup, a la identificación de un punto de recuperación confiable y a la validación de las copias antes de su restauración, reduciendo el riesgo de reintroducir código malicioso o información cifrada al ambiente recuperado.

El procedimiento incluirá adicionalmente la definición de **roles, responsabilidades, criterios de escalamiento, dependencias, Runbooks, puntos de control y mecanismos de comunicación** necesarios durante la atención del incidente.

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.

Entendido, aceptamos y cumplimos, con el requerimiento de garantizar, mediante el procedimiento de respuesta y recuperación ante incidentes, la contención efectiva del evento, la validación previa de los respaldos y la recuperación priorizada de los activos críticos para 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.

Entendido, aceptamos y cumplimos, SVAIT establecerá un conjunto de indicadores técnicos y operativos que permitan comparar los objetivos definidos por METRO frente a los resultados reales obtenidos durante pruebas, simulacros o eventos de recuperación.

Como mínimo, se contemplarán los siguientes indicadores:

- **RTO – Recovery Time Objective:** tiempo objetivo máximo definido para restablecer un servicio o activo después de una interrupción.
- **RPO – Recovery Point Objective:** máxima pérdida de información aceptable, expresada en tiempo, con respecto al último punto de recuperación disponible.
- **RTA – Recovery Time Actual:** tiempo real empleado para recuperar y restablecer el servicio durante una prueba o evento de recuperación.
- **Punto de recuperación real obtenido:** punto efectivo desde el cual fue posible restaurar la información, permitiendo compararlo frente al RPO establecido.
- **Cumplimiento de RTO:** validación de si el tiempo real de recuperación se encuentra dentro del objetivo definido.
- **Cumplimiento de RPO:** validación de si el punto de recuperación alcanzado se encuentra dentro del nivel de pérdida de información permitido.
- **Porcentaje de restauraciones exitosas.**
- **Porcentaje de servicios recuperados satisfactoriamente.**
- **Tiempo de validación de respaldos antes de la restauración.**
- **Tiempo total hasta la normalización del servicio.**
- **Número de desviaciones presentadas durante el proceso de recuperación.**
- **Efectividad de las actividades ejecutadas**, considerando el cumplimiento de las tareas definidas en los procedimientos y Runbooks de recuperación.

Para cada prueba o ejercicio de recuperación, SVAIT documentará la comparación entre los valores objetivo y los resultados reales obtenidos. Este análisis permitirá identificar desviaciones relacionadas con tiempos de restauración, capacidad de recuperación, dependencias, desempeño de la infraestructura o efectividad de los procedimientos establecidos.

Cuando se identifiquen desviaciones frente a los RTO, RPO u otros indicadores definidos, SVAIT realizará el correspondiente análisis de causa y establecerá las acciones correctivas o de mejora que se encuentren dentro de su alcance contractual.

Los indicadores serán consolidados en los reportes de gestión del servicio y presentados a METRO con la periodicidad acordada, manteniendo trazabilidad histórica que permita evaluar tendencias, identificar oportunidades de optimización y evidenciar la evolución de la capacidad de recuperación

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.

Entendido, aceptamos y cumplimos, SVAIT reconoce que **METRO DE MEDELLÍN LTDA. liderará las actividades de DR** y será responsable de proveer la infraestructura tecnológica requerida para el restablecimiento de los servicios, tanto en escenarios de contingencia como en ambientes productivos.

Dentro de este esquema, SVAIT será responsable de ejecutar y soportar las actividades relacionadas con la recuperación de la información respaldada, incluyendo como mínimo:

- Identificación y validación del punto de recuperación requerido.
- Verificación de integridad, disponibilidad y confiabilidad de los respaldos.
- Ejecución de las restauraciones conforme a los procedimientos y Runbooks definidos.
- Recuperación de archivos, máquinas virtuales, servidores, bases de datos, aplicaciones o componentes incluidos dentro del alcance contratado.
- Coordinación técnica con los equipos designados por METRO durante la ejecución del DR.
- Validación técnica de la información restaurada.
- Medición y registro de los tiempos efectivos de recuperación.
- Generación de evidencias y documentación de las actividades ejecutadas.
- Reporte de desviaciones, hallazgos y acciones de mejora identificadas durante el proceso.

SVAIT realizará las actividades de restauración sobre la infraestructura suministrada y habilitada por METRO, previa validación de los prerrequisitos técnicos necesarios para garantizar la correcta recuperación de los servicios. La recuperación se ejecutará de acuerdo con la priorización, secuencia, ventanas de trabajo y criterios de activación definidos y liderados por METRO, manteniendo coordinación permanente entre las partes durante todas las fases del ejercicio o evento real.

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.
Entendido, aceptamos y cumplimos

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.
Entendido, aceptamos y cumplimos

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.

Entendido, aceptamos y cumplimos, siempre en cuando este dentro del alcance contratado como backup como servicio.

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.

Entendido, aceptamos y cumplimos, SVAIT gestionará estas actividades mediante procedimientos operativos definidos, asegurando trazabilidad, priorización, escalamiento y seguimiento hasta su cierre.

Dentro del alcance se contemplará, como mínimo:

- Atención de solicitudes de restauración de archivos, máquinas virtuales, servidores, bases de datos, aplicaciones y demás cargas protegidas dentro del alcance contractual.
- Validación previa del punto de recuperación solicitado y de la disponibilidad del respaldo requerido.
- Ejecución controlada de restauraciones y validación posterior de la información recuperada.
- Gestión de solicitudes de cambio relacionadas con políticas de backup, retención, ventanas de ejecución, programación, configuración, alertas y demás parámetros de la solución.
- Análisis de impacto previo a la ejecución de cambios que puedan afectar la operación del servicio.
- Gestión de incidentes relacionados con fallas de respaldo, errores de restauración, indisponibilidad de componentes, corrupción de información, alertas de capacidad o eventos que comprometan la integridad de las copias.
- Escalamiento técnico a fabricantes o terceros cuando sea necesario.
- Seguimiento continuo de los casos hasta su resolución y cierre.
- Documentación de actividades, tiempos de atención, acciones ejecutadas y evidencias correspondientes.
- Identificación de causas recurrentes y definición de acciones correctivas o preventivas cuando aplique.

SVAIT realizará la atención de estos requerimientos conforme a los **niveles de servicio definidos contractualmente**, aplicando los tiempos de respuesta, atención y solución acordados de acuerdo con la criticidad y prioridad de cada solicitud o incidente.

Asimismo, se mantendrán registros de gestión que permitan medir el cumplimiento de los SLA, identificar desviaciones y generar los reportes requeridos por METRO DE MEDELLÍN LTDA.

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

Entendido, aceptamos y cumplimos, con el requerimiento de disponer durante toda la vigencia contractual de personal técnico especializado, certificado y con roles claramente definidos para la prestación del servicio.

SVAIT garantizará la continuidad operativa ante cambios de personal mediante esquemas de respaldo, transferencia de conocimiento, documentación y asignación de recursos con competencias equivalentes.

Asimismo, se dispondrá de personal con experiencia en **infraestructuras críticas de IT y entornos TO (Tecnología Operativa)**, incluyendo conocimiento en protección, respaldo, recuperación y gestión de activos tecnológicos asociados a sistemas de operación.

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. 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. 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. • 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.

		• Garantizar la calidad en la documentación de todos los incidentes, requerimientos, cambios y problemas atendidos por personal del CONTRATISTA. • Coordinar las actividades programadas que atiende el CONTRATISTA garantizando que se cumplan los cronogramas definidos. • Realizar diagnóstico de fallas repetitivas y presentar planes de acción para mejorar la disponibilidad de los servicios. • Mantener una actitud proactiva frente a las oportunidades de mejora de los servicios, informando el plan a llevar a cabo al supervisor del contrato. • Generar semanal y mensualmente los reportes de gestión del servicio definidos por la Empresa. • Asistir a las reuniones y comités programados por el supervisor del contrato. • Aportar toda la documentación
		requerida por el supervisor para el pago de facturación. • Documentación de todos los incidentes y solicitudes. Además, garantizar la calidad en la documentación de todos los incidentes, requerimientos, cambios y problemas atendidos.

Entendido, aceptamos y cumplimos, se anexará la información correspondiente de acuerdo con la solicitud.

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. • Documentar y escalar los incidentes detectados en la operación, en la herramienta que se defina para tal fin. • Ejecutar de manera manual las actividades puntuales de Backup cuando el proceso automático presente fallas.

Entendido, aceptamos y cumplimos se anexará la información correspondiente de acuerdo con la solicitud.

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. 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. • Diseño o rediseño y configuración de planes de mantenimiento preventivo y correctivo.
Implementador o Técnico avanzado o Solución de problemas		• Diseño o rediseño y configuración del esquema de respaldo y recuperación de desastres para los sistemas.

		• 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. • Apoyar las activades • Elaboración de instructivos de procedimientos para el respaldo y recuperación, así como los de continuidad. • Restauración de máquinas físicas y virtuales. • Documentar y escalar al fabricante los incidentes detectados en la operación.

Entendido, aceptamos y cumplimos se anexará la información correspondiente de acuerdo con la solicitud.

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.

Entendido, aceptamos y cumplimos, se informará y anexara la documentación necesaria para dar cumplimiento del cambio del personal.

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.

Entendido, aceptamos y cumplimos, SVAIT presentará, dentro de los cinco (5) días hábiles siguientes a la adjudicación, la documentación correspondiente a los perfiles requeridos para la prestación del servicio, acreditando experiencia, formación, certificaciones y demás condiciones exigidas por METRO DE MEDELLÍN LTDA.

Asimismo, SVAIT acepta que LA EMPRESA podrá revisar y validar la documentación presentada, solicitar aclaraciones, ajustes o reemplazos, y rechazar aquellos perfiles que no cumplan con los requisitos definidos.

En caso de presentarse observaciones, SVAIT realizará oportunamente los ajustes o sustituciones requeridas, garantizando que los perfiles asignados cumplan con las condiciones contractuales establecidas.

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.

Entendido, aceptamos y cumplimos, SVAIT reconoce que el incumplimiento de esta obligación podrá afectar el inicio de la operación, sin que ello genere ampliación de plazos, reclamaciones contractuales ni reconocimientos económicos adicionales a favor del CONTRATISTA.

Asimismo, SVAIT mantendrá durante toda la vigencia contractual la responsabilidad sobre la **idoneidad, disponibilidad y permanencia del personal asignado**, garantizando que los recursos dispuestos cumplan con los perfiles, experiencia y competencias requeridas por METRO DE MEDELLÍN LTDA.

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.

Entendido, aceptamos y cumplimos, SVAIT presentará informes periódicos que incluirán, como mínimo:

- Estado general del servicio.
- Ejecución de respaldos exitosos, fallidos y con advertencias.
- Incidentes y acciones correctivas ejecutadas.
- Indicadores de desempeño del servicio.
- Indicadores de capacidad y crecimiento.
- Estado de restauraciones y pruebas de recuperación.
- Cumplimiento de niveles de servicio.
- Riesgos, desviaciones y recomendaciones.
- Seguimiento de compromisos y acciones de mejora.

El nivel de detalle, formato y estructura de los reportes será acordado con el coordinador del contrato.

Respecto al **diseño de la arquitectura de backup**, SVAIT documentará de manera detallada:

- Los tipos de almacenamiento utilizados.
- La ubicación de cada copia de respaldo, incluyendo ambientes on-premise, nube y/o offsite, según aplique.
- Los mecanismos de inmutabilidad implementados.
- Los mecanismos de aislamiento y protección de las copias.
- Los flujos de respaldo, réplica y recuperación.
- La relación entre los diferentes repositorios y componentes de la solución.

Asimismo, SVAIT documentará de forma explícita el cumplimiento de la estrategia **2-2-1-1-0**, identificando cómo la arquitectura implementada satisface cada uno de sus componentes:

- **2 copias** de la información protegida.
- **2 medios o repositorios diferenciados**, de acuerdo con la arquitectura definida.
- **1 copia fuera del ambiente principal (offsite)**.
- **1 copia aislada, offline o inmutable**, protegida frente a modificación o eliminación no autorizada.
- **0 errores**, mediante mecanismos de verificación, validación de integridad y pruebas de recuperación.

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

Entendido, aceptamos y cumplimos, con el requerimiento de definir, documentar e implementar las políticas y procedimientos de backup y recuperación, la estrategia de pruebas de recuperación y los controles de ciberseguridad asociados al servicio.

SVAIT documentará como mínimo los siguientes componentes:

1. Políticas y procedimientos de backup y recuperación

- Definición de las frecuencias de respaldo de acuerdo con la criticidad de los servicios, ventanas operativas y RPO establecidos por METRO.
- Configuración de políticas de retención conforme con los requerimientos técnicos y operativos definidos.
- Procedimientos documentados para restauraciones parciales y totales.
- Validación de integridad y disponibilidad de los respaldos antes de su utilización.
- Definición de responsables, flujos de escalamiento y evidencias requeridas para cada proceso de recuperación.

2. Estrategia de pruebas de recuperación – DR Tests

SVAIT establecerá una estrategia periódica de pruebas de recuperación que permita verificar la recuperabilidad real de la información y de los servicios protegidos.

Las pruebas contemplarán:

- Frecuencia de ejecución conforme a lo definido contractualmente por METRO.
- Restauraciones controladas en ambientes de prueba, Sandbox o entornos autorizados.
- Validación funcional de los servicios recuperados.
- Medición de tiempos reales de recuperación.
- Comparación frente a RTO y RPO definidos.
- Documentación de resultados, hallazgos y acciones correctivas.

- Evidencias de validación orientadas al principio de **"0 errores"**, demostrando que los respaldos seleccionados son íntegros, consistentes y recuperables antes de considerarlos satisfactorios.

3. Controles de ciberseguridad asociados

La solución contará con controles orientados a proteger la plataforma de backup y los repositorios frente a amenazas de seguridad, incluyendo:

- Protección contra ransomware, borrado malicioso y modificación no autorizada.
- Inmutabilidad y aislamiento de respaldos, cuando aplique.
- Control de accesos basado en roles y principio de mínimo privilegio.
- Mecanismos de autenticación reforzada, incluyendo MFA cuando sea soportado.
- Monitoreo continuo de la plataforma y de la ejecución de respaldos.
- Generación de alertas ante fallos, eventos anómalos, cambios de configuración o condiciones de riesgo.
- Registro y trazabilidad de las actividades administrativas y operativas.

De esta manera, SVAIT garantizará que las políticas de backup, las pruebas de recuperación y los controles de ciberseguridad operen de forma integrada dentro de la estrategia de **ciberresiliencia y continuidad tecnológica** definida para METRO DE MEDELLÍN LTDA.

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.

Entendido, aceptamos y cumplimos, con el requerimiento de contar con planes de contingencia para el servicio de backup y garantizar la recuperación de la información ante eventos críticos durante toda la vigencia contractual.

SVAIT definirá, documentará y mantendrá procedimientos de contingencia orientados a asegurar la continuidad operativa de la plataforma de respaldo y recuperación frente a fallas de infraestructura, indisponibilidad de componentes, incidentes de ciberseguridad, errores operativos o eventos que puedan afectar la prestación del servicio.

14. 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.

Entendido, aceptamos y cumplimos

15. 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.

Entendido, aceptamos y cumplimos de acuerdo con el alcance del presente proceso.

16. 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.

Entendido, aceptamos y cumplimos, SVAIT realizará la planificación, configuración y operación de la solución de backup con el propósito de soportar estos tiempos de recuperación. No obstante, el cumplimiento efectivo de los RTO y RPO dependerá también de las condiciones y capacidades de la infraestructura tecnológica suministrada o administrada por METRO, entre ellas:

- Capacidad de cómputo disponible para la recuperación.
- Rendimiento y disponibilidad del almacenamiento origen y destino.
- Capacidad, disponibilidad y latencia de las redes y canales de comunicación.
- Ancho de banda disponible entre los repositorios de respaldo y los ambientes de recuperación.
- Disponibilidad de hipervisores, servidores físicos y plataformas destino.
- Dependencias de aplicaciones, bases de datos y servicios de infraestructura.
- Cantidad de servicios que deban ser recuperados simultáneamente.
- Volumen de información a restaurar y punto de recuperación requerido.
- Disponibilidad de la infraestructura de contingencia proporcionada por METRO.

Por lo anterior, SVAIT realizará durante la fase de diseño y puesta en operación una **validación de capacidad y desempeño de la infraestructura**, con el fin de determinar que los recursos tecnológicos, redes, canales y plataformas de recuperación sean suficientes para soportar los RTO y RPO solicitados.

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. 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. También aplica para requerimientos de mejoramiento y optimización.

Entendido, aceptamos y cumplimos, los niveles de atención de incidentes y requerimientos

17. Características de la infraestructura y servicios a respaldar

17.1 Infraestructura de TI

Servidores	
Numero de máquinas	Desarrollo: 18 Pruebas: 6 Producción: 157
Sistemas Operativos	CentOS Windows SUSE Ubuntu Debian Rocky Red Hat
Capacidades totales	Disco: 202 TB CPU: 200 GHZ – 288 Cores Memoria: 3.4 TB

Infraestructura de office 365	2500 cuentas
Equipos personales	
Numero de equipos	12
Sistema operativo	Windows
Capacidades por equipo	Disco 512GB Memoria: 16 GB 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.

Entendemos el ambiente de infraestructura de IT del metro de Medellín como base para la copia de seguridad como servicio, en base a las capacidades, compatibilidades de sistemas operativos.

17.2 Infraestructura de TO

Servidores	
Numero de máquinas	Producción: 52
Sistemas Operativos	CentOS Windows Ubuntu
	Debian Red Hat
Capacidades totales	Disco: 30 TB Memoria: 1.5 TB
Estaciones de trabajo rugerizadas	10 maquinas 5 TB Total de almacenamiento
Repositorio de información	5 TB

Entendido, Entendemos el ambiente de infraestructura de OT del metro de Medellín como base para la copia de seguridad como servicio, en base a las capacidades, compatibilidades de sistemas operativos.

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.

Entendido, aceptamos y cumplimos, con las condiciones establecidas para la operación de la solución de backup sobre la infraestructura de Tecnología Operativa (TO).

SVAIT tendrá en cuenta que los entornos TO se encuentran en operación productiva permanente, operan sobre redes segmentadas y no cuentan con navegación directa hacia Internet. Por lo tanto, cualquier comunicación requerida por la solución de backup será previamente identificada, documentada y coordinada con METRO DE MEDELLÍN LTDA., utilizando únicamente reglas específicas y controladas a través de los dispositivos de seguridad perimetral.

La implementación en TO se realizará bajo criterios de mínimo impacto operativo, considerando especialmente:

- Segmentación y aislamiento de las redes TO.
- Uso exclusivo de puertos, protocolos y comunicaciones estrictamente requeridas.
- Validación previa de conectividad y dependencias.
- No habilitación de navegación general hacia Internet.
- Coordinación de ventanas de instalación, configuración o mantenimiento cuando sean necesarias.

- Protección de la estabilidad y disponibilidad de los sistemas productivos.

En los casos en que sea requerida la instalación de agentes de backup, SVAIT utilizará componentes soportados por la solución seleccionada, procurando que sean **livianos y de bajo consumo de CPU, memoria, almacenamiento y comunicaciones**, y configurándolos para minimizar cualquier afectación sobre el desempeño de los equipos y aplicaciones TO.

Para los **sistemas legacy**, SVAIT realizará una validación previa de compatibilidad considerando sistema operativo, versión, arquitectura, aplicaciones instaladas, controladores, mecanismos de comunicación y demás restricciones técnicas. Cuando una plataforma legacy no permita la instalación de agentes o no se encuentre soportada por la solución, SVAIT documentará la condición y propondrá, cuando sea técnicamente viable, un mecanismo alternativo de protección o recuperación para validación por parte de METRO.

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.

Entendido, aceptamos y cumplimos

18. 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: Correo OneDrive SharePoint 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

Entendido, aceptamos y cumplimos con las retenciones y las políticas de copia de seguridad definas por el Metro de Medellín, además de garantizar el histórico de backup de 3 años de Microsoft 365

19. 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.

19.1 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

Entendido, aceptamos y cumplimos con el dimensionamiento en base a las cantidades estimadas para la infraestructura de IT, para el servicio de Baas para servidores, Office365, equipos personales y la estrategia de cyber resiliente (Sandbox y clean Room)

19.2 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

Entendido, aceptamos y cumplimos con el dimensionamiento en base a las cantidades estimadas para la infraestructura de OT, para el servicio de Baas para servidores, equipos personales y la estrategia de cyber resiliente (Sandbox y clean Room)

20. 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.

Entendido, aceptamos y cumplimos

21. 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

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

Entendido, aceptamos y cumplimos

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.

Entendido, aceptamos y cumplimos