Subgerencia de Sistemas
División de negocios

ESPECIFICACIONES TECNICAS

LICITACIÓN PÚBLICA
SWITCH TRANSACCIONAL

Enero 2024

CONTENIDO

1 ANTECEDENTES

Metro S.A. forma parte del Sistema de Transporte de Santiago, en conjunto con buses y trenes, y como tal, debe operar los medios de pago que el Ministerio de Transporte y Telecomunicaciones (MTT) establezca. Es así como desde el año 2007 Metro opera con la tarjeta bip!, como el medio de pago integrado del sistema de transporte. Por otro lado, a partir del año 2012 Metro se encuentra a cargo de los servicios de emisión y comercialización; administración de la Red de Carga subterráneo y superficie y post venta del Medio de Acceso al Sistema de Transporte Público de pasajeros de Santiago, mediante un contrato suscrito con el MTT.

Como consecuencia, Metro cuenta con distintos servicios que permiten integrar, administrar y dar continuidad operacional a la Red de Carga y sistemas anexos al Medio de Acceso. Estos servicios se resumen en:

1. Gestión de #RA
2. Integración de pagos con autorizador bancario

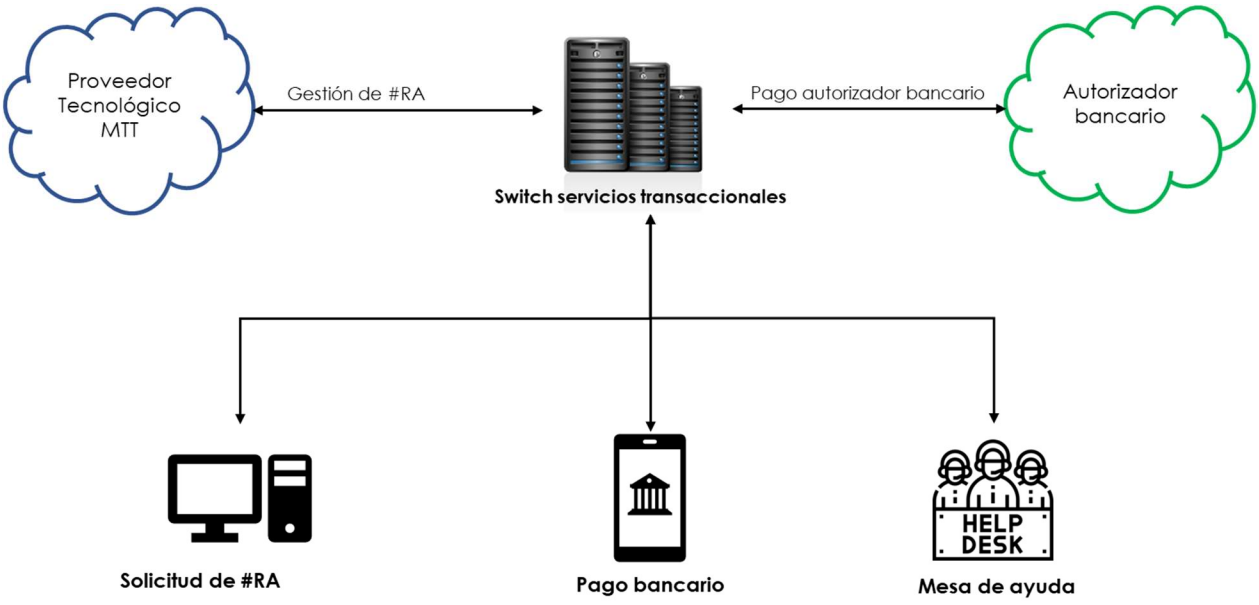

Imagen 001: Diagrama general del servicio

2 OBJETIVO

El objetivo de la presente licitación es dar continuidad operacional a los distintos servicios integrados en un switch transaccional. Todos estos relacionados en un punto en común, que es la necesidad de generación de #RA, para variados servicios y gestionar los pagos a través de Transbank en nuestras maquinas autoservicio.

MATRIZ DE REQUERIMIENTOS

En el siguiente capitulo se enumeran y describen los requerimientos sobre los servicios que se requieren contratar.

2.1 Gestión de #RA

Dentro de los procesos internos de Metro, existe la generación de cargas remotas para Tarjetas bip! (#RA), lo cual se solicita al proveedor tecnológico del MTT, mediante protocolos de comunicación e intercambio de información ya definidos.

La información necesaria para la integración de este tipo de servicios será entregada al Proveedor adjudicado.

El proceso de solicitud de generación de #RA pueden venir desde distintas fuentes. Estas son:

1. #RA Masivos: Solicitudes ingresadas manualmente para su generación masiva.
2. #RA Retail: Solicitudes ingresadas mediante plataformas de autoatención de retail ubicadas en la Región Metropolitana.
3. #RA Ticket de viaje: Solicitudes masivas que se generan a través de una plataforma de canje de tickets.

2.1.1 #RA Masivos

REQ - 01.
El proceso de generación de #RA Masivos se ejecuta mediante archivos que consolidan la información necesaria para las solicitudes y son enviados al Proveedor Tecnológico del MTT. El archivo para la solicitud de #RA masivos se crea en formato CSV y debe ser gestionado a través del Switch transaccional con el proveedor tecnológico del MTT.

Dentro del proceso de generación de #RA, existen aquellos provenientes de tótem de autoatención ubicados en cadenas de retail. El flujo dentro del Retail es el siguiente:

Imagen 002: Flujo generación #RA en Retail

REQ - 02.

Todo el proceso es gestionado mediante un tótem de autoatención desarrollado por la cadena de Retail. Para este caso, una vez finalizado el flujo descrito en la Imagen 002, el Switch deberá capturar el archivo generado por el software de Retail y procesarlo contra el sistema del Proveedor Tecnológico del MTT.

REQ - 03.

Las comunicaciones entre el Switch y los sistemas de Retail será mediante enlace de comunicaciones. Se deben considerar un enlace principal y un respaldo.

2.1.2 #RA Ticket de viaje

El sistema de Ticket de Viaje es un software de propiedad de Metro que tiene por objeto disponibilizar una plataforma web que permite a los usuarios el canje de ticket de evacuación por un #RA del mismo valor del servicio al momento de ser evacuados ante contingencias en la operación de Metro, que provoque una interrupción en el viaje de los usuarios.
Cada vez que un usuario genere el canje de un ticket, el software registra la solicitud el switch de Metro y genera un proceso de compra de #RA en el Proveedor Tecnológico del MTT

REQ - 04.

El Switch deberá tomar los archivos generados y depositados por el Software de Ticket de Viaje y procesar las solicitudes de generación de #RA contra los sistemas del Proveedor Tecnológico del MTT, pero antes de gestionar la generación deberá realizar la validación del estado de la tarjeta contra el switch del MTT.
El archivo debe registrar periodo del incidente y tarifa asociada.

REQ - 05.

Considerando que es una plataforma que opera ante contingencias, el Switch deberá cada cierto tiempo validar si existe o no un archivo generado pendiente de gestionar. El tiempo debe ser configurado por Metro mediante el Módulo de parámetros generales de la Interfaz de administración del sistema.

REQ - 06.
El Switch deberá tener un mecanismo de autocontrol que no permita crear solicitudes de generación de #RA duplicados.

2.2 Gestión de Pagos con autorizador bancario

El Switch deberá prestar servicios de gestión de autorización bancaria de los canales de pago electrónico que Metro mantiene disponible. Estos son:

1. Equipos Red de Carga de Metro

Botón de pago con servicio webpay

2.2.1 Equipos Red de Carga

Actualmente el equipamiento de la Red de Carga de Metro cuenta con dispositivos de pago bancarios provistos por la empresa Transbank. Los dispositivos actualmente que operan son:

- UX 100 botonera
- UX 400 sin contacto
- UX 300 Lector de Tarjeta

Imagen 003: Comunicación Host to Host entre máquinas y el autorizador bancario

REQ - 07.
Se requiere de la implementación del modelo de comunicación Host to Host entre las Máquinas de Autoservicio de Metro y el autorizador bancario de Transbank.

REQ - 08.
Adicionalmente, para que la comunicación del proceso de autorización bancario se ejecute, es necesario el desarrollo de una DLL para ser instalada en las Máquinas de Autoservicio y que interactúe con el aplicativo del equipo.

REQ - 09.

Los protocolos de comunicación e integración de la DLL en las máquinas de autoservicio deberán ser entregados a Metro con la finalidad de que esto pueda ser integrado en equipamiento de autoservicio futuro.

2.2.2 Botón de pago en línea

Dentro de los servicios actuales de Metro, existe la página web https://adultomayor.tarjetabip.cl/adultomayor/. Esta plataforma cuenta con un botón de pago bancario WebPay.

REQ - 010.
Se requiere de la Implementación de un desarrollo que permita gestionar el pago de la tarjeta adulto mayor a través de la plataforma WebPay de Transbank.

REQ - 011.
El proveedor deberá contar con certificación PCI y cumplir con protocolos de seguridad del proveedor y las políticas de Metro.

REQ - 012.
El proveedor será responsable de la habilitación, implementación, operación, mantenimiento, soporte y monitoreo del sistema transaccional Webpay de Metro S.A, considerando WebService SOAP. Adicional a lo anterior la nueva integración será capaz de manejar el tipo del medio de pago CREDITO/DEBITO lo cual quedará registrado e individualizado para cada operación realizada.

2.3 Requerimientos generales

2.3.1 Software switch

REQ - 013.

El switch está en el punto central entre las distintas redes de POS, el switch del administrador tecnológico del transporte público y los autorizadores de los medios de pago, por tanto, el diálogo con cada una de las partes debe disponer de los elementos que garanticen la confidencialidad, integridad y disponibilidad de todas las transacciones generadas en el origen.

El esquema de seguridad a adoptar para el Switch Transaccional debe garantizar para las distintas transacciones que transiten por los atributos de:

Transparencia y Confidencialidad: La circulación de datos por el Switch en muchas ocasiones será con información confidencial, abierta o encriptada, debiendo garantizarse que ella no sea registrada o descifrada.

Integridad (no modificación): Las transacciones que circulan por el Switch, no podrán ser modificadas en sus campos críticos por parte del servicio, garantizándose siempre su integridad.

No Repudiación: Para aquellas transacciones que se resuelven en el Switch Transaccional, deberán tomarse las medidas para que el ejecutor de la transacción no pueda repudiarlas.

Confirmación: Se deberá garantizar que toda transacción que implique la asignación de cuotas de transporte a una tarjeta Bip/Multivía sea debidamente almacenada y reportada a Metro y/o los operadores que corresponda.

Variación: Se utiliza una "working key" en el diálogo entre los POS y el Switch Transaccional, la que es generada por un ente externo al Switch y debe ser utilizada por éste.

Log Básico: Corresponde a un registro de todas las operaciones efectuadas por el Switch, sean estas técnicas o financieras, que permitan determinar el origen, destino, fecha y hora de ejecución, etc., y que a su vez se pueda recurrir a él para estadísticas y el seguimiento ante problemas

REQ - 014.
Debe existir una plataforma web que permita las siguientes funcionalidades:

- **Ingreso de generación de #RA masivos**: que permita cargar a través de un archivo csv u otro la solicitud de generación.
- **Ingreso unitario de generación de #RA**: que permita generar unitariamente la solicitud de #RA.
- **Módulo de reportería**: que permita generar reportes de todas las transacciones registradas por el software.
- **Módulo de monitoreo**: monitoreo del estado de los servicios (retail, webpay, switch MTT, etc).
- **Módulo de gestión de usuarios**: mantenedor de usuarios del sistema.
- **Módulo de parámetros generales**: parametrización del sistema (mantenedores de comercio, servicios, líneas, equipos, etc).
- **Módulo de auditoría**: que permita la obtención de la trazabilidad del uso del sistema.

REQ - 015.

La plataforma debe contar con un servicio de reporte para proceso de conciliación, cuadraturas de Transacciones de carga y baja de #RA. Esta deberá ejecutar de manera automatizada las siguientes tareas:

- Transporte seguro de archivos planos de operaciones, diferencias y ajustes.
- Rendición de operaciones en formatos paramétricos de archivos.
- Cuadre local de operaciones, generación y transporte de diferencias y aplicación local de ajustes.
- Cuadre externo de operaciones, transporte de diferencias y generación y transporte de ajustes.
- Consulta de operaciones y diferencias por emisor y/o autorizador.

REQ - 016.

La solución a implementar, deberá proporcionar una plataforma de monitoreo con información en tiempo real y/o franjas horarias, integrando todos los servicios monitoreados en una sola consola y considerando transacciones, procesos en servidores, hosts autorizadores, servicios del switch transaccional, equipamiento en punta, aplicativos, sistemas, plataformas Web y móviles que sean conectado a los sistemas licitados, considerando el envío de alarmas vía correo o mensajería instantánea y otro medio para eventos a definir con área operacionales de Metro.

Funciones centrales del monitoreo que se esperan como un mínimo de la solución:

- Registrar actividad del monitoreo en BD.
- Monitoreo no asistido y abstraído de la lógica de negocio del Switch, orientado al tiempo real y con despliegue gráfico asociado.
- Registrar información de los procesos servidores, estados, máximo, transacciones (TRX) encoladas, tiempos de TRX, cantidad de $ recaudados, fallo de servicios, fallos de componentes, etc.
- Registrar paramétricamente los mensajes que fluyen entre servidores, aceptados, rechazados por diversos motivos desde los autorizadores, Time Out, etc.
- Detectar y alarmar de los Host de autorizadores que presentan algún problema, para su rápida atención.

REQ - 017.
Se podrá acceder a la plataforma web mediante la identificación de un usuario y contraseña. Los usuarios se deberán identificar mediante el número de RUT y la contraseña deberá contener al menos:

- 6 caracteres
- Letras, al menos 1 número y al menos 1 carácter especial.
- No se podrán utilizar las últimas 3 contraseñas anteriores.
- Deberá contar con un sistema de bloqueo y cambio de contraseña ante intentos reiterados y fallidos.
- Deberá contar con un sistema de recuperación de contraseñas.

REQ - 018.
Configuración del Sistema. La plataforma debe contemplar un módulo que permita la configuración de los parámetros de explotación del Sistema, permitiendo configurar el valor de la compra de #RA a asignar a los contratos validados y, la creación de líneas y nuevas estaciones.

REQ - 019.
Configuración de Tipos de tarjeta. La plataforma debe contemplar un módulo para la configuración de los distintos tipos de tarjetas y la actualización del valor asociado a la compra de la tarjeta se realizará solicitando los siguientes campos:

- **Código de Contrato**: Ingreso del código de contrato, se validará que el ingreso corresponda a un valor numérico al momento de solicitar guardar el nuevo ingreso realizado.
- **Descripción**: Detalle del contrato ingresado.
- **Valor Tarifa**: Tarifa a asignar para la compra de #RA cuando se determine el contrato valido en el ingreso de la tarjeta, se validará que el ingreso corresponda a un valor numérico al momento de solicitar guardar el nuevo ingreso realizado.

La pantalla de configuración de Tipos de Tarjeta deberá desplegar los contratos previamente ingresados, permitiendo su edición en caso de requerirlo.
Las opciones establecidas corresponden a:

- **Limpiar**: Borra el contenido de las líneas de edición.
- **Guardar**: Guarda el ingreso del nuevo Tipo de Tarjeta Ingresado o su Actualización.
- **Eliminar**: Elimina el código de Contrato seleccionado, además de generar una pregunta con la opción de asegurar la eliminación deseada.
- **Salir**: Retorna al menú principal, cerrando la página de ingreso de Tipos de Tarjetas.

REQ - 020.
Todos los desarrollos y servicios deberán contar con medidas de seguridad tales como:

- Hardening de servidores de aplicación
- Sitio HTTPS
- Aplicación de Proxy reverso
- Redirección HTTP a HTTPS
- Aplicación de certificado SSL
- Firewall y seguridad perimetral
- Seguridad en inyección de transacciones, perdida de autenticación, gestión de sesiones, exposición de datos sensibles, falsificación de peticiones en sitios cruzados, uso de componentes con vulnerabilidades, redirecciones y reenvíos no validados
- Antivirus
- Acceso a datos controlados
- Protocolos de comunicaciones seguros (SFTP- SSH).

2.3.2 Infraestructura

REQ - 021.
El Proponente debe considerar el suministro de los servicios IAAS para el sistema antes descrito, para lo cual deberá implementar 3 ambientes (Producción, QA y Desarrollo).

El servicio considera la habilitación de equipamiento, conectividad, configuración, puesta en marcha del hardware y software necesario (sistema operativo, motores de base de datos y servicios de respaldo necesario para la correcta operación del sistema antes descrito.

REQ - 022.
El Datacenter donde el oferente proveerá el servicio IAAS deberá estar al menos homologado a un estándar TIER III, lo anterior, será un requisito excluyente para avanzar con la revisión de la propuesta técnica.

REQ - 023.
El Proponente deberá garantizar alta disponibilidad de los servicios, de modo que asegure el cumplimiento de los indicadores de calidad de servicios establecidos en el **Anexo 001** de las especificaciones técnicas de la presente licitación.

2.3.3 Ambientes

Actualmente, para los desarrollos y servicios transaccionales contamos con 2 ambientes. Uno dedicado exclusivamente a Producción y otro destinado a QA (pruebas) exclusivas del Laboratorio de Metro.

REQ - 024.
Es requerido que todos los servicios, plataformas, desarrollos y/o todo lo que entregue el proveedor adjudicado sea en 3 ambientes "Desarrollo, Producción y QA".

REQ - 025.
La solución deberá considerar la creación de tantos ambientes QA como servicio sean licitado e implementaciones asociadas a nuevos negocios que se incorporen durante la vigencia del contrato asociado a la licitación. Además deberá considerar acceso a estos ambientes para cada cliente de metro.

REQ - 026.
Deberá considerar la implementación y configuración de nuevos negocios para compra de cuotas de transporte, #RA,C2D (QR), considerando canales de compra y autorizador de pago con Tarjetas de Crédito y Débito. Además de compras masivas de #RA para certificaciones en laboratorio.

REQ - 027.
Deberá considerar un servicio de monitoreo centralizado que permita monitorear los procesos de ambiente de producción como los de ambiente de certificación y QA, que contenga mensajería por indisponibilidad y errores de proceso a definir por Metro.

2.3.4 Capacitación

El proveedor adjudicado deberá entregar y ejecutar un plan de capacitación y entregamiento al personal de Metro.

El contenido de la capacitación y plan de capacitación deberá ser entregado a Metro con una anticipación de treinta días (30) a la fecha estipulada para la actividad. Esto, con la finalidad de que METRO realice la revisión completa de la documentación entregada.

El plan de capacitación deberá contar al menos con los siguientes puntos:

- Objetivos generales y específicos del curso.
- Responsable de la capacitación.
- Agenda de la actividad (ubicación, horarios, duración, sesiones o módulos, entre otros.)
- Descripción de los conocimientos que el personal asistente en la actividad va a adquirir.
- Materiales para dictar la capacitación

La duración de la actividad no debe superar las horas indicadas en el plan. No obstante lo anterior el Proveedor adjudicado podrá proponer a Metro una capacitación con menor cantidad de horas justificándolo a través de los contenidos, cumpliendo satisfactoriamente y a cabalidad el traspaso de conocimientos de todos los temas planteados.

Todos los gastos asociados a la ejecución de esta actividad serán de costo del Proveedor adjudicado.

Respecto de la disponibilidad de horario del personal a capacitar, esta es limitada, razón por la cual es necesario que el Proveedor adjudicado confirme a Metro el inicio de la actividad con al menos 10 días hábiles de anticipación.

2.3.5 Listado de entregables

10 días posterior a la firma del contrato, el Proveedor adjudicado deberá entregar y acordar con Metro el listado de entregables de la solución a implementar. Este listado deberá contar con al menos:

- Documento de diseño desarrollo solución
- Documento diseño integración autorizador bancario (DLL y botón de pago WebPay)
- Documento de diseño infraestructura de la solución
- Cuadernos de pruebas unitarias e integradas
- Protocolo y políticas de housekeeping de la infraestructura de la solución
- Protocolos de comunicación mesa de ayuda (escalamiento)
- Manuales de usuario

2.3.6 Experiencia del proponente

Las empresas postulantes al proceso de licitación deben ser empresas con al menos 10 años de experiencia en proyectos/servicios similares, detallando lo siguiente:

- Nombre del proyecto

- Breve descripción
- Empresa en la que se ejecutó el proyecto
- Cantidad de personas del equipo de trabajo que ejecuto el proyecto.
- Tiempo de duración del proyecto
- Referencia de la empresa en la cual se ejecutó el proyecto

En caso de que se externalice algún servicio, este deberá ser declarado en su Oferta Técnica y deberá presentar la experiencia de la empresa a la cual se esta externalizando, la cual deberá cumplir con lo señalado anteriormente.

2.3.7 Implementación

La implementación deberá realizarse a más tardar en 4 meses desde la firma del contrato y el proveedor deberá presentar una planificación que al menos debe considerar lo siguiente:

- Diseño
- Desarrollo (especificado por cada uno de los módulos requeridos)
- Pruebas Unitarias (especificado por cada uno de los módulos requeridos)
- Pruebas Integradas
- Prototipo con usuarios clave
- Capacitaciones (especificado por cada uno de los módulos requeridos)
- Migración

La planificación será consensuada entre Metro y el contratista, abarcando tanto los hitos como los plazos. El cumplimiento del proyecto será evaluado conforme a esta definición.

El proveedor deberá considerar y detallar un plan de migración, el cual deberá ser definido en la etapa de diseño y aprobado previamente por Metro.

2.3.8 Periodo de garantía de la implementación

El proponente debe considerar y detallar en su oferta técnica, la garantía mínima de 6 *meses* desde el paso a producción del proyecto.

NOTA: La garantía debe considerar cualquier falla o problema con el *producto*.

Durante el periodo de garantía del proyecto de software, no menor a 6 meses, METRO podrá solicitar cuando estime conveniente la última versión de los programas fuentes y la ejecución de la compilación o despliegue de la solución. Dicha operación deberá ser realizada en dependencias METRO, en los ambientes que se definan para este fin.

CRITERIO DE ACEPTACIÓN DEL SOFTWARE

Los criterios de aceptación del proyecto de software corresponderán a la recepción satisfactoria de METRO de los siguientes aspectos técnicos:

- Término del plan de pruebas de la aplicación.
- Recepción de la documentación completa.
- Compilación o despliegue de la solución desde los programas fuentes y generación exitosa de versiones ejecutables del software.

3 ANEXO Nº 001: Indicadores de Desempeño y Calidad de Servicio

Se describen los indicadores en base a los cuales se medirá el desempeño y calidad en la prestación de los servicios contratados. Estos indicadores o criterios son aplicables a los servicios contratados en relación con los siguientes aspectos:

a) Servicio de explotación de aplicaciones

b) Mantención de aplicaciones

c) Cumplimiento de horario de servicio mesa de ayuda y soporte usuarios

Para cada uno de estos servicios se define un conjunto de criterios de desempeño y calidad y el nivel mínimo que se considera satisfactorio.

3.1.1 Servicio de explotación de aplicaciones.

Criterio/Indicador	Período de medición	Nivel de servicio	Manejo de multas
Disponibilidad del Servicio	Diaria (00:00 a 23:59)	99,99%	Ver artículo 9 de bases título segundo
Máximo tiempo de respuesta promedio	Diaria (00:00 a 23:59)	0,3 segundos	Ver artículo 9 de bases título segundo
Tiempo de recuperación ante un Servicio Degradado (Servicio en funcionamiento, pero con deterioro).	Ocurrencia específica	2 [Hrs.]	Ver artículo 9 de bases título segundo

Tiempo de recuperación ante un Sistema Bloqueado (Servicio inoperable).	Ocurrencia específica	1 [Hrs.]	Ver artículo 9 de bases título segundo

3.1.2 Mantención De Aplicaciones

Estos indicadores se miden por días calendario corridos.

Criterio/Indicador	Período de medición	Nivel de Servicio	Manejo de Multas
Corrección de errores no críticos.	Ocurrencia específica	3 [días]	Ver artículo 9 de bases título segundo
Corrección de errores críticos.	Ocurrencia específica	1 [día]	Ver artículo 9 de bases título segundo
Tiempo máximo de habilitación de un nuevo autorizador	Ocurrencia específica	20 [días]	Ver artículo 9 de bases título segundo
Tiempo máximo de habilitación de una nueva red de POS	Ocurrencia específica	20 [días]	Ver artículo 9 de bases título segundo

Los niveles de criticidad de los errores de la aplicación serán definidos por METRO S.A., a su juicio exclusivo, en cada oportunidad y en función del impacto que el error genere de cara a los clientes.

3.1.3 Cumplimiento De Servicio De Mesa De Ayuda Operacional

Estos indicadores se miden en horario definido para el servicio día calendario

Criterio / indicador	Período de medición	Nivel de Servicio	Manejo de Multas
Tiempo de atención de una llamada telefónica.	Ocurrencia específica	6 [Rings telefónicos]	Ver artículo 9 de bases título segundo
Tiempo máximo de resolución de una Orden de Trabajo (OT) para el ambiente de producción	Ocurrencia específica	1 [Hrs.]	Ver artículo 9 de bases título segundo
Tiempo máximo de resolución de una Orden de Trabajo (OT) para el ambiente de testing.	Ocurrencia específica	2 [Hrs.]	Ver artículo 9 de bases título segundo
Tiempo máximo de retraso en entrega de archivos de cierre, cuadratura o reportes.	Ocurrencia específica	2 [Hrs.]	Ver artículo 9 de bases título segundo

3.1.4 Reportes de desempeño

Criterio / indicador	Período de medición	Nivel de Servicio	Manejo de Multas
Generación de informe de ejecución de mantenimiento preventivo	Por cada Evento	2 días hábiles posterior a la ejecución del Mantenimiento	Ver artículo 9 de bases título segundo
Generación de reporte mensual de cumplimiento de indicadores para la	Mensual	Al día 5 del mes siguiente	Ver artículo 9 de bases título segundo

generación del estado de pago			

4 ANEXO Nº 002: Ciberseguridad

DOMINIO	REQUERIMIENTO
Dominio 1 CONTROL DE ACCESO	Contar con procesos y herramientas para identificar, prevenir y corregir el incorrecto uso y configuración de privilegios de acceso a los equipos, redes y aplicaciones.
Dominio 1 CONTROL DE ACCESO	El acceso a los activos de información críticos ya sea remoto o local, debe realizarse de acuerdo a una definición formal, con procesos de validación y registro. los accesos deberán pasar por procesos de autenticación, restringiendo los privilegios únicamente a los necesarios. Se debe emplear la lógica de "el mínimo privilegio es el primero que se asigna".
Dominio 1 CONTROL DE ACCESO	Gestionar activamente el ciclo de vida de las cuentas de acceso a sistemas (creación, uso, inactividad, bloqueo y eliminación) para reducir su utilización por parte de un
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Los proveedores deberán establecer controles para prevenir, detectar y corregir vulnerabilidades técnicas de ciberseguridad tanto en la construcción como en el mantenimiento de soluciones.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Los proveedores deben establecer mecanismos de autenticación con una robustez acorde a la información que se necesite proteger, ejemplo doble factor de autenticación cuando se trate de información sensible.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Asegurar la confidencialidad e integridad de las transacciones electrónicas que contengan información sensible, ejemplo, pagos, datos personales o estratégica de Metro de Santiago (trazado de nuevas líneas, actas de directorio u otras). Para el flujo de transacciones con información confidencial o crítica, utilizar comunicaciones encriptadas con

	algoritmos robustos y protocolos de comunicación seguros.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Establecer controles de hardware y/o software para: -. Evitar la pérdida, duplicación o alteración no autorizada de transacciones. -. Identificar y alertar cualquier transacción fraudulenta o no autorizada.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Generar y almacenar de manera segura detalles y registros de las transacciones de acceso público, respetando los requerimientos legales que existan para tal efecto, ejemplo, respecto a su retención.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	El proveedor debe contar con entornos de desarrollo seguro, donde se realicen los proyectos de construcción e integración de soluciones sin poner en riesgo las soluciones y entornos productivos.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	El acceso al código fuente debe estar restringido para prevenir su extravío, la introducción de funcionalidades no autorizadas, la propiedad intelectual . Asimismo, se debe mantener un log de los accesos al código fuente.
Dominio 2 IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS	Los sistemas operativos de los servidores que soportan el servicio deberán ser actualizados y parchados según recomendaciones del fabricante, evitando que estos queden expuestos a vulnerabilidades de seguridad, fallas o sin soporte de fábrica.
Dominio 3 ENTORNOS DE PRUEBA	Las pruebas deben realizarse en un ambiente controlado, para asegurar que no se introduzcan vulnerabilidades y se asegure la confiabilidad de las mismas.
Dominio 4 PRUEBAS DE CIBERSEGURIDAD	La implantación o mantenimiento de soluciones debe considerar la preparación de un plan detallado de pruebas de ciberseguridad que aborde todos los riesgos y amenazas relacionadas con la solución y el establecimiento de los resultados esperados en cada caso. La extensión de las pruebas debe ser proporcional a la importancia y la naturaleza de la solución.
Dominio 5 OPERACIONES INFORMÁTICAS	El o los data center utilizados por el proveedor para proporcionar el servicio contratado, deberán contar con una

	certificación TIER acorde a la criticidad del servicio y la disponibilidad garantizada mínima requerida por Metro para el mismo. Para determinar el valor TIER requerido, referirse a la siguiente tabla: Características Disponibilidad Garantizada Tier 1: Sin capacidad redundante (ejemplo 1 sola UPS o 1 solo proveedor de datos) 99.671%, Tier 2: Tier 1 + Dispositivos con componentes redundantes 99.741%, Tier 3: Tier 1 + Tier 2 + Equipos de alimentación eléctrica dual y varios enlaces de salida 99.982%, Tier 4: Tier 1 + Tier 2 + Tier 3 + todos los componentes tolerantes a falla incluyendo enlaces de datos, almacenamiento, aire acondicionado, energía eléctrica, etc. 99.995%
Dominio 5 OPERACIONES INFORMÁTICAS	El proveedor deberá realizar respaldos regulares de la data y configuraciones. Los respaldos deberán realizarse con una periodicidad acorde a las necesidades del proceso o servicio. La regularidad de los respaldos y reportes respectivos los definirá Metro al inicio de la prestación del servicio. El servicio debe contemplar copias de seguridad incrementales con a lo menos una frecuencia semanal de la información.
Dominio 5 OPERACIONES INFORMÁTICAS	Los medios de respaldo se deben almacenar en un lugar seguro distante al lugar de procesamiento de la información
Dominio 5 OPERACIONES INFORMÁTICAS	El proveedor deberá asegurar que la información y las instalaciones o centros donde se procese información de Metro de Santiago estén protegidos contra malware o código malicioso. Por lo tanto, el proveedor deberá establecer una política que prohíba el uso de software no autorizado e implementar controles para detectar y prevenir el uso de software no autorizado.
Dominio 5 OPERACIONES INFORMÁTICAS	Contar con planes de continuidad para recuperar sistemas en el caso que ataques de malware, que incluya respaldos y todo lo necesario para que el sistema pueda volver a operar con normalidad.
Dominio 5 OPERACIONES INFORMÁTICAS	El proveedor tiene la responsabilidad de garantizar a su costo la vigencia del equipamiento, sistemas operativos y

	aplicativos de las máquinas del sistema, poniendo especial énfasis en mantener actualizados y vigentes los sistemas operativos base en conjunto con las aplicaciones que son ejecutadas, de manera que se evite caer en obsolescencia. Lo anterior deberá ser aplicado los años que dure el servicio, salvo que por contrato se acuerde lo contrario. Las actualizaciones tanto de sistemas como de equipamiento se deberán efectuar en coordinación y de acuerdo a los procedimientos que Metro defina.
Dominio 5 OPERACIONES INFORMÁTICAS	El proveedor deberá asegurar la aplicación oportuna de los parches de seguridad, en particular, los parches para subsanar vulnerabilidades de seguridad catalogadas como críticas, altas o medias tanto del del software base (sistema operativo) como del software o herramientas instaladas en los servidores y computadores cuya administración sea de su responsabilidad precaviendo que estas acciones no afecten la eficacia y rendimiento de los sistemas y se realicen las pruebas para evitar poner en riesgo la disponibilidad del servicio.
Dominio 5 OPERACIONES INFORMÁTICAS	Los ambientes productivos sólo deben contener códigos ejecutables, evitándose almacenar en ellos, código fuente o compilados.
Dominio 5 OPERACIONES INFORMÁTICAS	El proveedor debe estar al día y consciente de las vulnerabilidades técnicas a que puede estar expuesta la infraestructura y los sistemas de información que se utilizan, con el objeto de no comprometer a Metro de Santiago o algún proceso critico de negocio y contar con procedimientos de respuesta frente a la detección de vulnerabilidades técnicas.
Dominio 6 REDES Y COMUNICACIONES	Establecer controles y herramientas adecuadas para prevenir la fuga de información y mitigar los efectos de este tipo de incidentes, asegurando la confidencialidad e integridad de la información digital.
Dominio 6 REDES Y COMUNICACIONES	Establecer el uso de controles criptográficos para proteger la confidencialidad de la

	información y asegurar la autenticidad y no repudiación de los mensajes.
Dominio 7 SEGURIDAD FÍSICA Y AMBIENTAL	El perímetro de seguridad de las instalaciones debe estar claramente definido y ser concordante con la sensibilidad de la información, requisitos de seguridad y criticidad de riesgo de los activos que se alberguen en ellas.
Dominio 7 SEGURIDAD FÍSICA Y AMBIENTAL	Se deben proteger adecuadamente los recintos de procesamiento, almacenamiento y transmisión de información confidencial. El acceso a áreas seguras debe contar con registros. Todos los visitantes deben ser controlados independiente que hayan visitado antes el lugar. El registro de acceso de personas debe ser almacenado y mantenido en forma segura, con el propósito de responder a auditorías y/o revisiones, pudiendo ser dicho registro, físico o lógico. En los lugares físicos que utilice el proveedor para procesar o almacenar información de Metro deberá disponer de los mecanismos de seguridad, tanto físicos como lógicos, que permitan proteger y prevenir fugas de información o eventos que puedan afectar la confidencialidad e integridad de los datos.
Dominio 7 SEGURIDAD FÍSICA Y AMBIENTAL	El acceso de personal externo a áreas de procesamiento de información confidencial debe estar restringido, debidamente autorizado y las actividades a realizar deben ser monitoreadas.
Dominio 8 GESTIÓN DE INCIDENTES	El proveedor deberá mantener información de evidencia para análisis forense y proporcionársela a Metro de Santiago cuando le sea requerida para la investigación de algún incidente.
Dominio 8 GESTIÓN DE INCIDENTES	El proveedor deberá contar con un proceso, procedimientos y un equipo de respuesta a incidentes, que le permita detectar eventos, incidentes y ataques, monitorearlos, analizarlos, escalar a Metro, contener el daño de forma efectiva, neutralizar al atacante o vector y restaurar la integridad y disponibilidad de los sistemas y la red de manera oportuna y efectiva.

Dominio 9 GESTIÓN DE PROYECTOS	La etapa inicial de los proyectos (etapa de diseño) debe considerar, una evaluación de riesgos relacionados con seguridad de la información y ciberseguridad y una propuesta de los controles mitigantes a ser aplicados.
Dominio 12 MANEJO DE CONTRASEÑAS	Usuarios, proveedores y contratistas deberán cambiar la contraseña inicial que se le asigne cuando utilicen una cuenta de Metro por primera vez. Asimismo, proveedores y contratistas deberán cambiar las contraseñas por defecto de las soluciones que se implementen para Metro.
Dominio 12 MANEJO DE CONTRASEÑAS	Toda plataforma o sistema deberá contar con su propio sistema de autenticación, en el cual las credenciales deberán cumplir con lo siguiente: • Deberá ser compatible con sistemas SSO estandarizados • Deberá ser compatible Azure Active Directory
Dominio 12 MANEJO DE CONTRASEÑAS	El proveedor está obligado a resguardar por todos los medios la no divulgación ni exposición de las contraseñas.
Dominio 12 MANEJO DE CONTRASEÑAS	Las contraseñas no deberán contener espacios en blanco.
Dominio 12 MANEJO DE CONTRASEÑAS	Las contraseñas de Metro de Santiago deben caracterizarse por ser "contraseñas seguras", lo que implica que debe restringirse sistémicamente el uso de los siguientes elementos al construir contraseñas: • Fechas en los formatos más usuales, ejemplo: mesyy, ddmmayy, mm/yy, dd/mm/yy, mm-yy, dd-mm-yy, yymm, yymmadd, yy/mm, yy/mm/dd, yy-mm, yy-mm-dd • El patrón de teclado (QWERTY) • Números en secuencia o repetidos (1234, 11111, 22222 o similares). • La palabra "Metro", • La palabra "Soporte", • Las palabras "Admin", "Administrador", "Superusuario" o similares • Año actual o próximos al año actual ejemplo: 2020, 2021, 2022 etc. • Nombre de meses: enero, marzo, abril, mayo.... etc.
Dominio 12 MANEJO DE CONTRASEÑAS	Las contraseñas nunca deberán estar incluidas o informarse a través de programas de mensajería, correo electrónico o similares, ejemplo, Outlook, WhatsApp etc. salvo excepciones debidamente fundamentadas y

	autorizadas por la Gerencia de Seguridad de Información, en cuyo caso deberán viajar de manera cifrada.
Dominio 12 MANEJO DE CONTRASEÑAS	Queda prohibida la utilización de contraseñas de acceso como parte del código fuente de los programas, procedimientos o scripts de bases de datos.
Dominio 13 CONTROLES CRIPTOGRAFICOS	Establecer controles criptográficos para proteger información confidencial, resguardar la integridad y autenticidad de la información, velar por el no repudio y autenticación.
Dominio 13 CONTROLES CRIPTOGRAFICOS	Utilizar algoritmos criptográficos seguros, con una clave robusta acorde a las mejores prácticas (largo mínimo 12 caracteres, con mayúsculas, minúsculas, caracteres especiales y sin blancos entremedio).
Dominio 14 CUMPLIMIENTO NORMATIVO	Deben establecerse controles para prevenir el extravío del código fuente y asegurar el resguardo de las versiones, especialmente aquellas que correspondas con la últimas versiones ejecutables puestas en producción.
Dominio 16 CONFIDENCIALIDAD DE INFORMACION	La información "Confidencial" de Metro, deberá estar debidamente protegida frente a robos, mal uso y/o exposición sin autorización de Metro. La información "Confidencial" debe estar protegida de manera que solo las personas autorizadas puedan accederla, las cuales deben estar definidas explícitamente por el propietario de la información. No se debe divulgar esta información a menos que tenga la autorización correspondiente del propietario. Ejemplos de información "Confidencial" es, pero no limitada a: Informes de auditoría, Informes financieros y de contabilidad, Registros de Incidentes y evidencias, Actas y minutas de Directorio y junta de accionistas, Bases de licitación privada, Cláusulas o acuerdos de confidencialidad, Documentos legales, contratos y anexos, Notificación juzgado civil, Información de nuevos proyectos, planes estratégicos, Metodologías propietarias (desarrolladas por Metro o adquiridas para un grupo específico de trabajadores), Antecedentes personales,

	documentos de postulación e ingreso como trabajador, Antecedentes laborales, Antecedentes, licencias y Exámenes médicos, Certificados, Contraseñas, Contratos de trabajo, Cotización previsional, Evaluaciones de trabajadores, Información de sueldos, Proceso disciplinario, Información de clientes, Documentación disponible en web de Auto consulta, Documentación disponible en web de Openagora, Documentación disponible en web de Exámenes preventivos.
Dominio 16 CONFIDENCIALIDAD DE INFORMACION	La información "De uso Interno" de Metro, deberá estar debidamente protegida frente a robos, mal uso y/o exposición sin autorización de Metro. La información "De Uso Interno" solo debe ser accedida por personal de Metro de Santiago. Si otra persona requiere acceso, éste deberá ser autorizado explícitamente por el Propietario de la Información respectivo. No se debe divulgar a menos que sea autorizado por su dueño. Ejemplos de información "De Uso interno" es, pero no limitada a: Información de clientes que hayan solicitado en forma explícita su tratamiento como tal, Información cuyo propietario requiera un nivel moderado de protección, Información de incidentes y riesgos, Matrices de riesgo, Correos masivos a través de Andén en Línea, Información Web2Push, Políticas, Normas, Reglamentos, Manuales, Procedimientos internos, Instructivos, Programas, Procesos y Protocolos de las distintas divisiones y gerencias, Documentación operacional interna, Informes y documentación técnica, criterios de diseño, especificaciones, diagramas, esquemas, instrucciones de ingeniería, inspecciones, memorias de cálculo, modelos 3D, cubicación y presentaciones, Informes en general, Planos y cartografía, Convenio colectivo, Derecho a saber, Obligación a informar, Organigramas, Presupuestos, autorizaciones, propuestas, tasaciones, ofertas y evaluaciones técnicas/

	económicas, garantías y pólizas, Hoja de Entrega de Servicios (HES), órdenes de compra/pago/trabajo/cambio, notas de crédito, guías, facturas/boletas, requerimientos, registros, actas, formularios, informativos, circulares, Contratos de servicio, Cuenta anual fondo de Bienestar, Minutas de reunión, Memorándum, Términos de referencia, diccionarios y glosario, Términos y condiciones, Documentación disponible en intranet Metro (anden.metro.cl), Documentación disponible en web de beneficios (misbeneficios.metro.cl), Documentación disponible en los distintos sitios web de operaciones.
Dominio 19 CONTINUIDAD DE SERVICIOS	Debe contar con planes de continuidad de negocio (BCP) y recuperación ante desastres (DRP), los cuales deben estar debidamente documentados. Estos planes deberán ser presentados a los miembros del equipo Metro que lideran la adquisición del servicio y a los miembros del área de Seguridad de la Información de Metro, cuando sea requerido para su revisión y aprobación.
Dominio 19 CONTINUIDAD DE SERVICIOS	Los proveedores deberán probar a lo menos una vez al año su plan de continuidad y/o recuperación y entregar a Metro de Santiago un reporte de las pruebas realizadas.
Dominio 19 CONTINUIDAD DE SERVICIOS	Anualmente los proveedores deberán revisar y eventualmente mejorar y actualizar el plan de continuidad que cubre los servicios prestados a Metro de Santiago.
Dominio 19 CONTINUIDAD DE SERVICIOS	Los proveedores que presten servicios de almacenamiento y/o procesamiento de información y que soporten procesos críticos para Metro de Santiago, sería ideal que contaran con sitios de contingencias físicamente aislados de su sitio principal. Asimismo, los proveedores que entreguen estos servicios dentro de las instalaciones de Metro de Santiago, idealmente deberían considerar la habilitación de sitios alternativos al principal en el diseño de las soluciones que propongan a Metro.

Dominio 19 CONTINUIDAD DE SERVICIOS	En aquellos casos particulares donde sea imperativo asegurar la disponibilidad de un servicio y su información, el proveedor deberá contar con una estrategia y herramientas anti-denegación de servicios (DDoS / DoS). En este sentido, la criticidad del servicio y su información deberán ser analizadas caso a caso entre el dueño del servicio en Metro y la Gerencia de Seguridad de Información" y en conjunto decidir si amerita o no la aplicación de esta exigencia.
Dominio 22 SERVICIOS CLOUD COMPUTING	Cuando se contraten servicios en la nube en las modalidades SaaS, PaaS o IaaS, el proveedor a cargo deberá proporcionar como parte de su propuesta, un estudio de vulnerabilidades basado en OWASP Top 10 o Ethical Hacking o considerar como parte de las pruebas un "Test de Penetración", a cargo de especialistas aprobados por la Gerencia de Seguridad de Información de Metro de Santiago. Las vulnerabilidades detectadas en estas pruebas se deberán revisar y mitigar adecuadamente, en plazos consensuados con la Gerencia de Seguridad de Información de Metro de Santiago de acuerdo a la complejidad y severidad de riesgo de las mismas.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Cuando se implementen soluciones WEB el proveedor a cargo deberá proporcionar como parte de su propuesta, un estudio de vulnerabilidades basado en OWASP Top 10 o Ethical Hacking o considerar como parte de las pruebas un "Test de Penetración", a cargo de especialistas aprobados por la Gerencia de Seguridad de Información de Metro de Santiago. Las vulnerabilidades detectadas en estas pruebas se deberán revisar y mitigar adecuadamente, en plazos consensuados con la Gerencia de Seguridad de Información de Metro de Santiago de acuerdo a la complejidad y severidad de riesgo de las mismas.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	No pasar parámetros entre páginas WEB a través de los links.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Incorporar protección SSL (obligatoriamente certificados TLS1.3 y suite de algoritmos de al menos 256 bits) en

	todas las operaciones de transferencia de información, código de sesión (identificador de sesión) y tiempo de sesión.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Utilizar UserID distinto a Username u otros parámetros de acceso a sistema o Base de datos.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Evitar y controlar la inyección de código a través de los parámetros en las URL's, los campos de un formulario u otro método que permita este tipo de interacciones. Verificar los tipos de archivo, en caso de presentar la funcionalidad de carga de archivos. Evitar la carga y descarga de archivos ejecutables y scripting (exe, bat, sh, rb, etc.).
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Incorporar configuración necesaria para evitar ataques de tipo cross-site-scripting, clickjacking y listadas en Owasp top10.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Si se utilizan Cookies, estas deben estar encriptadas y configuradas con flags secure y httponly
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	La URL, no puede mostrar el contenido de los directorios.
Dominio 23 CREACIÓN Y MODIFICACIÓN DE SOLUCIONES WEB	Mantener un log o registro de las acciones realizadas por los usuarios conectados al sistema, idealmente en una base de datos con acceso restringido. Estos registros podrán ser auditados por Metro.