



## **ANEXO CIBERSEGURIDAD**

### **SERVICIO DE ADMINISTRACIÓN Y OPERACIÓN DE CIBERSEGURIDAD PARA METRO S.A.**

- 1) El Contratista del servicio que deba ejercer funciones dentro de las instalaciones de Metro, deberá conocer y aplicar las políticas y procedimientos y control de acceso físico y lógico que hubiere establecido Metro.
- 2) El Contratista de servicio deberá restringir los privilegios de acceso de los usuarios únicamente a los necesarios aplicando a los sistemas la regla del menor privilegio a asignar.
- 3) El Contratista del servicio deberá gestionar oportunamente con Metro la remoción de accesos lógicos y físicos a los activos de información en caso de desvinculación, renuncia o cambio de funciones de los dependientes destinados a desempeñar funciones para Metro
- 4) El Contratista del servicio deberá gestionar activamente el ciclo de vida de las cuentas de acceso de los usuarios a los distintos sistemas y redes, considerando controles efectivos para la autorización, creación, uso, actividad, bloqueo y eliminación de las mismas.
- 5) El Contratista, deberá someter cualquier cambio a las soluciones, servicios, y/o procesos ya aprobados, a la autorización de Metro.
- 6) El Contratista de Servicios deberá proporcionar a Metro toda la documentación (manuales, procedimientos e instructivos) utilizados como parte de la prestación del servicio, estos deberán estar actualizados, y deberán contar con la validación de Metro quien será el responsable del almacenamiento y resguardo. Esta documentación deberá ser entregada a la puesta en marcha del servicio.
- 7) El Contratista deberá entregar a la Gerencia de Seguridad de Información de Metro de Santiago, evidencia de cada una de las pruebas de ciberseguridad realizadas para corroborar la seguridad de la solución o servicio, en el momento en que esta gerencia lo solicite después que estas hayan sido ejecutadas.
- 8) El Contratista del servicio deberá realizar respaldos regulares de la data y configuraciones. Los respaldos deberán realizarse con una periodicidad acorde a las necesidades del proceso que se está respaldando. La regularidad de los respaldos y reportes respectivos los definirá Metro al inicio de la prestación del servicio.



- 9) El Contratista deberá controlar la obsolescencia del equipamiento y sistemas, generando planes de capacidad que permitan administrar este proceso. Del punto de vista de los sistemas operativos se deberán mantener actualizados en paralelo a las aplicaciones y sistemas de información, de manera que no podrá quedar obsoleta una aplicación por la actualización de un sistema operativo, ambos, aplicaciones y sistemas base, se deberán mantener al día y sin caer en obsolescencia. Las actualizaciones tanto de sistemas como equipamiento se deberán efectuar en coordinación y de acuerdo a los procedimientos que Metro defina.
- El plan de capacidad deberá contar al menos con lo siguiente:
  - Monitorización del rendimiento y la carga de los servidores.
  - Ajustes de rendimiento para asegurar el uso más eficiente de la infraestructura.
  - Comprensión de las demandas del servicio y planes futuros de aumento o disminución de carga.
  - Administración de la obsolescencia de sistemas e infraestructura.
- 10) Controles Antimalware: El Contratista del servicio deberá contar con controles eficaces para detectar, prevenir y reducir la presencia de malware o código malicioso, especialmente controlando la descarga y uso de software no autorizado.
- 11) El Contratista del servicio deberá mantener registros de los eventos (logs) de la actividad realizada sobre los sistemas por un periodo de retención mínimo de tres meses, salvo que se acuerde un periodo diferente en las bases de licitación o especificaciones técnicas del servicio. Estos registros de eventos deberán estar protegidos contra escritura y acceso no autorizado.
- 12) El Contratista del servicio deberá entregar reportes regulares del estado de la plataforma, de acuerdo a los establecido en las Especificaciones Técnicas.
- 13) El Contratista deberá proporcionar y mantener al día, un inventario de activos del equipamiento o sistemas según corresponda, debiendo al menos contemplar los siguientes aspectos:
- Deberán ser clasificados de acuerdo a su criticidad e impacto en el negocio.
  - Informar la ubicación física del activo.
  - Indicar el responsable a cargo de su resguardo.
  - El activo deberá ir rotulado para su fácil identificación.
- Adicionalmente el activo deberá contar con un proceso de eliminación o destrucción aprobado por Metro.
- 14) El Contratista del servicio tiene la obligación de reportar de manera inmediata todo evento o incidente de seguridad o ciberseguridad que ponga en riesgo o impacte la confidencialidad, integridad o disponibilidad de la información, activos de información o la disponibilidad de los servicios de Metro de Santiago.
- 15) El Contratista del servicio deberá reportar a la Gerencia de Seguridad de la Información de Metro de manera urgente, cualquier incidente de pérdida, extravío,



robo o hurto de cualquier medio de almacenamiento que contenga información de Metro.

- 16) En relación al manejo de contraseñas, el Contratista deberá:
  - Establecer contraseñas seguras que cumplan con la norma de contraseñas vigentes en Metro.
  - Resguardar por todos los medios la no divulgación ni exposición de las contraseñas.
- 17) Difusión: El Contratista será responsable de dar a conocer a sus dependientes las cláusulas contractuales, especificaciones técnicas, procedimientos y directrices relativas a seguridad de información y ciberseguridad que se relacionen con este servicio o producto, quienes deberán aplicarlas, en lo que corresponda, al desempeño de las funciones y roles que se ejecuten como parte del servicio contratado a Metro S.A.
- 18) Para el otorgamiento del servicio o desarrollo de una solución el proveedor deberá asignar a dependientes que cumplan con un perfil (habilidades y capacidades) acorde a las exigencias y requisitos estipulados en las especificaciones técnicas.
- 19) El Contratista del servicio deberá establecer controles para la verificación de los conocimientos técnicos de todos sus trabajadores que desempeñen funciones para Metro.
- 20) El Contratista tiene la obligación de informar a Metro sobre cualquier cambio de roles o funciones de sus trabajadores dependientes, así como de las desvinculaciones, con el objetivo de que se eliminen o ajusten de forma inmediata, según sea el caso los derechos de acceso de la persona respectiva, además de devolver los activos que eventualmente Metro pudiera haberle asignado.
- 21) Disponibilidad y Cumplimiento SLAs: El Contratista, deberá cumplir todos los alcances, requerimientos y acuerdos de nivel de servicio (SLA) expresados en las EE.TT. y Bases Administrativas del presente servicio.
- 22) El Contratista deberá contar con redundancia del servicio de ser requerido por Metro, de lo contrario deberá contar con un plan de recuperación ante desastres que considere la recuperación total del servicio en el menor tiempo posible.
- 23) El Contratista del servicio deberá otorgar las facilidades a Metro S.A. para la realización de evaluaciones de vulnerabilidad y actividades de revisión de aseguramiento de calidad en ciberseguridad (QA de Ciberseguridad) para corroborar la eficacia de los controles de seguridad de información y ciberseguridad. Estas revisiones deberán realizarse, por lo general, de manera programada, salvo en caso de materializarse un incidente de seguridad de información, algún incidente operativo grave con impacto en la disponibilidad del servicio o cambio significativo en las condiciones del servicio prestado. El Contratista deberá gestionar los



hallazgos, implementando acciones correctivas para mitigar el riesgo al más breve plazo.

- 24) Auditoría: El Contratista del servicio deberá otorgar las facilidades para la realización de revisiones o auditorías por parte de las unidades de la Contraloría de Metro S.A. o su Gerencia de Seguridad de Información, o bien, sus organismos fiscalizadores o auditores externos. Estas auditorías o revisiones deberán realizarse, por lo general, de manera programada, salvo en caso de materializarse un incidente de seguridad de información, o algún incidente operativo grave con impacto en la disponibilidad del servicio o cambio significativo en las condiciones del servicio prestado. El Contratista deberá gestionar los hallazgos, implementando acciones correctivas para mitigar el riesgo al más breve plazo.
- 25) Los Sistemas de Información (Aplicaciones y sistemas operativos) deben estar debidamente licenciados y a nombre de Metro. Para el caso de ser licencias tipo OEM el Contratista será responsable del reemplazo físico del equipo como también de la restauración de la licencia.
- 26) El Contratista deberá proporcionar acceso seguro a la nube, usando protocolos de encriptación robustos, evitando la interceptación de la conexión, siendo necesario filtrar el acceso únicamente desde Chile si Metro lo requiere.
- 27) Mientras se encuentre vigente el presente contrato, Metro tendrá derecho a solicitar acceso o la entrega de cualquiera respaldo de información realizado como parte de la ejecución del servicio, en forma legible. Los tiempos de entrega o acceso a estos respaldos deberán ser acordados entre las partes dependiendo de su volumen y tiempo de retención, pero nunca superar el plazo de 15 días hábiles.