ESQUEMA NACIONAL DE SEGURIDAD: COMUNICACIÓN A PROVEEDORES

ACTUALIZACIÓN DEL CLAUSULADO DE HOMOLOGACIÓN CON **METRO LIGERO OESTE**

DECIMA. – PROTECCIÓN DE SERVICIOS EN LA NUBE

Los servicios en la nube consisten en la disposición de software, plataformas o infraestructuras por parte de **EL PROVEEDOR**, accesibles desde Internet, con independencia de donde se encuentren alojados los sistemas de información y de forma transparente para el usuario final de **MLO**.

Estos servicios proporcionados por **EL PROVEEDOR** se pueden categorizar como Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) o Software-as-a-Service (SaaS). Este clausulado aplica a las tres categorías de servicios prestados.

Reconociendo que **MLO** transfiere el control del servicio a **EL PROVEEDOR**, en cumplimiento de lo establecido en el Esquema Nacional de Seguridad (ENS) y más concretamente en su Guía de Seguridad de las TIC, CCNSTIC 823, UTILIZACIÓN DE SERVICIOS EN LA NUBE, con relación a las garantías de seguridad adecuadas, aplicará lo descrito a continuación.

1. **Ubicación de los datos. EL PROVEEDOR** deberá facilitar la identificación de la ubicación de los sistemas de información vinculados con los servicios objeto del contrato, incluyendo todas las ubicaciones asociadas al almacenamiento y prestación del servicio, tanto de sus servicios propios como de aquellos que tenga subcontratados. Se considerarán, a todos los efectos, las limitaciones establecidas en la normativa de protección de datos relativas a transferencias internacionales de datos, siendo condición esencial el cumplimiento de tales previsiones, que se extenderán a las entidades subcontratadas. No podrán realizarse transferencias a un tercer país o una organización internacional fuera de la Unión Europea, salvo en los supuestos específicamente autorizados por el RGPD (Reglamento General de Protección de Datos) y la LOPDGDD (Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales), siendo la única excepción contemplada, la transferencia a países, organizaciones o territorios cuando sea precisa la transferencia en cumplimiento de una obligación legal o requerimiento judicial. Cualquier modificación a lo largo del contrato relativa a las exigencias establecidas en el presente apartado, deberá ser comunicada sin dilación, a **MLO**.

2. **Gestión de la seguridad.** Los sistemas de información que soportan el servicio de **EL PROVEEDOR** deberán ser conformes con el ENS (Esquema Nacional de Seguridad) y/o cumplir con las medidas de seguridad desarrolladas en las guías CCN-STIC o la normativa ISO 27001 que incluirá, entre otros, la garantía de confidencialidad, seguridad e integridad de los datos y requisitos relativos a auditoría de pruebas de penetración (pentesting).

Metro Ligero Oeste, S.A. Inscrita en el Registro Mercantil de Madrid, Tomo 23.111, Libro 0, Folio 200, Sección 8, Hoja M-414182. CIF A84808575.

3. **Gestión de usuarios y privilegios.** La gestión de los usuarios, credenciales de acceso y privilegios corresponde a **MLO**, siendo en caso de imposibilidad técnica transferida esta gestión a **EL PROVEEDOR**, quien seguirá siempre las indicaciones y solicitudes al respecto que le pueda proporcionar **MLO** en cuanto a la creación, modificación y eliminación de usuarios y sus privilegios de acceso.

4. **Recuperación de datos y continuidad del servicio. EL PROVEEDOR** deberá disponer y presentar a **MLO** los mecanismos necesarios para implementar una política de respaldo y de pruebas de recuperación que contemplen como mínimo los requisitos de identificación del alcance de los respaldos, política de copias de seguridad, medidas de cifrado de información en respaldo, procedimiento de solicitud de restauraciones de respaldo y realización de pruebas de restauración. Asimismo, y para garantizar la continuidad de los servicios objeto del contrato, **EL PROVEEDOR** deberá disponer y presentar a **MLO** un plan de recuperación ante cualquier contingencia que impida la disponibilidad total o parcial de los recursos principales, que por cualquier motivo provoque la indisponibilidad de los servicios objeto del contrato. Este plan incluirá la identificación y descripción de los medios alternativos planificados para la provisión de los servicios, personal alternativo, existencia o planificación de instalaciones y medios de comunicación alternativos, pruebas de recuperación, etc. La presentación del plan a **MLO** será necesaria previamente a la contratación de nuevos servicios y en el caso de servicios ya contratados, será necesaria en un periodo máximo de 3 meses desde la aceptación de este clausulado.

5. **Dimensionamiento y capacidad.** Será responsabilidad de **EL PROVEEDOR** la gestión de la capacidad de los medios técnicos que soportan el servicio contratado por **MLO** (capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuarios, etc.) de modo que se asegure la disponibilidad incluida en los acuerdos de nivel de servicio firmado entre **LAS PARTES**.

6. **Finalización del contrato.** Durante la ejecución del contrato, **EL PROVEEDOR** se compromete a facilitar a las personas designadas por **MLO** toda la información y documentación que estas soliciten para disponer del conocimiento suficiente de las circunstancias en las que se desarrollan los servicios, sus actividades y, en general, de todas las operaciones técnicas, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos. Una vez finalizado el contrato, cualquiera que sea la causa de finalización, **EL PROVEEDOR** deberá desarrollar las acciones precisas para la transferencia del conocimiento y de la información, implicados en el servicio. El proceso incluirá, necesariamente y a petición de **MLO**, la devolución de toda la información a la propia **MLO** o a quien esta designe, en un plazo máximo de 1 mes, mediante los medios seguros que sean necesarios y debiendo estar la información en un formato que se acordará ente **EL PROVEEDOR** y **MLO**. A los efectos del cumplimiento de la normativa vigente en materia de protección de datos, se considerarán los periodos de retención legal que pudieran ser obligatorios para **EL PROVEEDOR**, siendo responsabilidad de **EL PROVEEDOR** la eliminación de la información de **MLO** una vez superados estos periodos de retención. Dicha eliminación deberá ser justificada mediante la documentación correspondiente por **EL PROVEEDOR** a **MLO** en un plazo máximo de 3 meses desde su realización.

Metro Ligero Oeste, S.A. Inscrita en el Registro Mercantil de Madrid, Tomo 23.111, Libro 0, Folio 200, Sección 8, Hoja M-414182. CIF A84808575.

Metro Ligero Oeste, S.A.
C/ Edgar Neville, 9
28223 Pozuelo de Alarcón, Madrid
Tel. (+34) 91 503 16 00
metroligero-oeste.es