Metro de Málaga S.A. es la sociedad adjudicataria del Contrato de Concesión Administrativa para la construcción y explotación de las líneas 1 y 2 del Metro de Málaga. En virtud del mismo, presta un servicio de transporte público de pasajeros en la ciudad de Málaga.

Desde su constitución, el objetivo primordial de Metro de Málaga S.A. es prestar un servicio a sus clientes cumpliendo los requisitos establecidos, de forma que obtengan la máxima satisfacción con nuestros servicios y se garantice la máxima privacidad y seguridad de la información.

Dicho objetivo de satisfacción de nuestros clientes y confidencialidad de la información es la piedra angular de nuestra política, entendiendo la satisfacción como el cumplimiento de los compromisos contraídos de la forma más eficiente posible, a la vez que se procura cumplir con las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio y relacionadas con el mismo, que el propio cliente nos comunica.

Mediante la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en los requisitos de la norma ISO/IEC 27001:2022, así como el Esquema Nacional de Seguridad conforme al Real Decreto 311/2022, se persigue una mejora continua en la calidad del servicio y continuidad de la actividad que desarrolla nuestra organización, así como un compromiso continuo de mejora técnica de nuestros sistemas, activos y procesos y el de nuestros proveedores, para procurar una continua adaptación a las necesidades tecnológicas de nuestros clientes.

Para ello, Metro de Málaga S.A., considera esta Política como uno de los pilares básicos de la organización para alcanzar la mejora continua de la eficacia de dicho sistema de Gestión y cumplimiento del RD 311/2022, siendo las siguientes directrices las que guíen nuestra actividad:

- Asegurar la satisfacción de sus clientes basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos de actualizaciones y mejoras.

- Cumplir con los requisitos de los clientes y demás grupos de interés, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados.

- Cumplir con los requisitos legales que resulten de aplicación, así como con aquellos requisitos que la organización suscriba evaluando continuamente dicho cumplimiento, en todas sus áreas de actividad.

- Evaluar de forma concienzuda los riesgos de la organización, analizando los posibles riesgos de todos y cada uno de los procesos de la organización y de los activos de información, previendo y evitando de esta manera desviaciones, tomando las oportunas decisiones para minimizar posibles no conformidades.

- Establecer procesos operacionales que salvaguarden a las personas, la propiedad, la información, los datos y las aplicaciones o sistemas de uso para las instancias establecidas por la organización.

- Velar por una continua y permanente actualización de nuestros recursos, tanto tecnológicos como, sobre todo, de nuestro personal, fomentando políticas de información y formación continua profesional que les permitan avanzar en sus conocimientos al ritmo que lo hace nuestro sector, fomentando la conciencia de la seguridad de la información, a fin de incrementar la competencia de las personas trabajadoras.

- Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el compromiso y participación de todo el personal en el desarrollo y consecución de los Objetivos.

- Garantizar la mejora continua, manteniendo el Sistema de forma eficaz y efectivo para constatar el compromiso con los clientes, buscando para ello una mejor organización interna del trabajo y en la forma en que tratamos la información de nuestros clientes

- Lograr que la seguridad de la información y la protección de los datos personales sean una constante:

    - Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.
    - Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro.
    - Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.

- La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad, confidencialidad e integridad de su información y aún más la de sus clientes.

ALCANCE

La organización establece para la norma ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad (RD 311/2022) esta política que se aplica a *"Los sistemas de información que dan soporte al servicio de Transporte Público de pasajeros en metro en Málaga, incluyendo la gestión del mantenimiento del material móvil y las instalaciones"*

MISIÓN

La misión de Metro de Málaga S.A. es ser un sistema de transporte sostenible, con un equipo humano comprometido con el cliente e ilusionado con su desarrollo profesional, apoyado en una tecnología avanzada, moderna, segura y con unas instalaciones de fácil accesibilidad que permiten la conexión con otros transportes púbicos, para hacer de Málaga una ciudad mejor comunicada.

MARCO NORMATIVO

Metro de Málaga S.A. se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general o específico. En particular, en lo que se refiere a seguridad de la información:

- Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
- ISO 9001:2015, Sistemas de Gestión de la Calidad
- ISO 14001:2015, Sistemas de Gestión Ambiental
- ISO 45001:2018, Sistemas de Gestión de Seguridad y Salud en el Trabajo
- ISO 22320:2013, Sistemas de Gestión de emergencias y respuesta ante incidentes
- ISO 27001:2022, Sistemas de Gestión de la Seguridad de la Información
- Reglamento 2016/679/UE, de 27 de abril, que regula la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)
- Real Decreto 1720/2007, de 21 de Diciembre, por el que se desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Ley 9/2014, de 9 de Mayo, General de Telecomunicaciones
- Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)
- Guías de la serie 800 CCN-STIC como guías de estructuración documental

ROLES, FUNCIONES Y RESPONSABILIDADES

OBLIGACIONES DEL PERSONAL

Todas las personas trabajadoras de Metro de Málaga S.A., tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, y deberán cumplir con las siguientes responsabilidades:

- Comunicar las incidencias de seguridad mediante los canales establecidos.
- Aplicar los mecanismos establecidos para el intercambio de información entre el personal, clientes y proveedores.

Se establecerá un programa de concienciación continua, desde su incorporación a la empresa, para todas las personas trabajadoras.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance, recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o, si, por el contrario se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

FUNCIONES Y RESPONSABILIDADES DEL RESPONSABLE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para velar por que la actividad de la Organización se encamine a cumplir con su misión y en particular con los objetivos concretos en que ésta se materialice, a efectos de lo previsto en la ISO 27001:2022, se designa internamente la figura del Responsable de Seguridad de la Información, siendo sus funciones las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga la norma ISO 27001:2022 y el ENS para verificar el cumplimiento de los requisitos de éste.
- Gestionar o promover la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la entidad, con la colaboración de los distintos responsables de sistemas IT/OT.
- Revisar, completar y aprobar, junto al Responsable de Información/Dirección, toda la documentación relacionada con la seguridad del sistema.

- La especificación de requisitos de seguridad corresponde a los responsables de la información y de los servicios, junto con el responsable del registro de actividades de tratamiento de datos de carácter personal. La operación corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad y al técnico de seguridad.

FUNCIONES Y RESPONSABILIDADES DEL COMITÉ DE SEGURIDAD CONFORME A ESQUEMA NACIONAL DE SEGURIDAD

A efectos del Esquema Nacional de Seguridad y de acuerdo con la Guía de Seguridad de las TIC CCN-STIC 801, se ha constituido un Comité de Seguridad que gestiona y coordina la seguridad de la información en la Sociedad. Sus funciones son:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Cualquier asignación de tareas y responsabilidades relacionadas con la seguridad de la información será aprobada por el Comité Interno de Seguridad.

El Comité de Seguridad está formado por los roles y con las funciones y responsabilidades que a continuación se detallan:

1. **Responsable de la Información**
    - Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
    - Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
    - Aprobación de los niveles de seguridad de la información.
    - Proteger los activos.
    - Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos.

2. **Responsable del Servicio**
    - Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
    - Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
    - Aprobación de los niveles de seguridad de los servicios.
    - Proteger los activos.
    - Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos

3. Responsable de Seguridad

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE..).
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa

4. Responsable del Sistema

- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

Puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

DATOS DE CARÁCTER PERSONAL

Metro de Málaga S.A., trata los datos de carácter personal, por lo que mantiene un "registro de actividades de tratamiento", al que tendrán acceso sólo las personas autorizadas, en le que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de Metro Málaga S.A. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro.

OBLIGACIONES DEL PERSONAL

Todos los trabajadores de Metro de Málaga S.A., tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de Metro Málaga S.A., en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o, si, por el contrario, se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

TERCERAS PARTES

Las terceras partes relacionadas con Metro de Málaga S.A., dentro del alcance, formalizarán con la empresa un compromiso de confidencialidad y protección de la información intercambiada.

Cuando Metro de Málaga S.A., utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en esta Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Esta Política será revisada para su continua adecuación, así como los objetivos y metas de la empresa en materia de seguridad de la información, y comunicada a todo el personal de la organización, encontrándose a disposición de cualquier parte interesada en la web oficial de Metro de Málaga, S.A.

En Málaga, a 5 de julio de 2024

Fernando Lozano Ruiz
Director General