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. ha sido 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, se persigue una mejora continua en la calidad del servicio y una 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, 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 nuestro servicio.

- 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 profesional continua 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 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

RESPONSABLE DE SEGURIDAD: FUNCIONES

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, 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.

PROTECCIÓN DE DATOS PERSONALES

Metro de Málaga S.A., trata datos de carácter personal, por lo que mantiene un “registro de las actividades de tratamiento” realizadas bajo su responsabilidad, en los términos establecidos en el RGPD. Todos los sistemas de información de Metro de Málaga S.A. se ajustarán a los niveles de seguridad necesarios para garantizar el tratamiento de datos conforme a los requisitos establecidos en la normativa de aplicación en vigor y proteger los derechos de los interesados.

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.

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 22 de Noviembre de 2023

Firmado digitalmente por
Fernando Lozano Ruiz
22/11/2023 19:42 CET