



CITYBUS
SISTEMA DE TRANSPORTE
COLECTIVO METROPOLITANO
CITYBUS OAXACA.

"2025, BICENTENARIO DE LA PRIMERA CONSTITUCIÓN POLÍTICA DEL
ESTADO LIBRE Y SOBERANO DE OAXACA"

Documento de Seguridad para la Protección de Datos Personales en Posesión del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca.



Carretera Internacional Cristóbal Colón # 3909, Col Eucaliptos, Agencia de Pueblo Nuevo, Oaxaca de Juárez. C.P. 68274

citybus@oaxaca.gob.mx

Handwritten signature

Handwritten signature

Handwritten signature



Índice.

- I. Presentación.
- II. Glosario de Términos.
- III. Inventario y Catálogo de Datos Personales.
- IV. Las Funciones y Obligaciones de las Personas que Traten Datos Personales.
- V. Análisis de Riesgo.
- VI. Análisis de Brecha.
- VII. Plan de Trabajo.
- VIII. Los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad.
- IX. Medidas de Seguridad para Garantizar la Protección de Datos Personales.
- X. Sistemas de Gestión de Seguridad de la Información dentro del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca.
- XI. Programa General de Capacitación y Actualización.
- XII. Modalidad de Capacitación.
- XIII. Técnicas Utilizadas para la Supresión y Borrado Seguro de los Datos Personales.





I. PRESENTACION.

El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos consagra el derecho a la protección de datos personales, su importancia radica en garantizar su seguridad, debido a que su protección es un derecho humano. En consecuencia, se deben establecer medidas de seguridad que prevengan y mitiguen los efectos de un mal uso de ellos, evitando daños a la imagen o integridad de una persona titular de datos personales y sanciones a las y los servidores públicos.

Este SISTEMA DE TRANSPORTE COLECTIVO METROPOLITANO CITYBUS OAXACA, como Organismo Público Descentralizado del Poder Ejecutivo del Estado de Oaxaca, ha llevado a cabo un análisis en los datos personales que obran en su poder, con la finalidad de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas titulares de los datos personales, y dar cumplimiento con los principios de lealtad, licitud, finalidad, consentimiento, calidad, proporcionalidad, información y responsabilidad, establecidos en el artículo 9 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.

Se dicta el presente DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES, en cumplimiento al artículo 28 y 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículo 27 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; con el objetivo de asegurar: la integridad, confidencialidad y disponibilidad de la información personal en posesión. La homogeneidad en la organización, procesos y sistemas. Que el Comité de Transparencia de este Sistema y los responsables de los sistemas de datos personales, han definido las medidas de seguridad administrativas, físicas y técnicas con las que se contará para garantizar la debida protección de los datos personales. Así mismo, controlar internamente el universo de sistemas de datos personales que se poseen; el tipo de datos personales que contiene cada uno, y los sistemas de tratamiento; el análisis de riesgos, análisis de brecha, plan de trabajo y las medidas de seguridad que se enfocan en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso; acceso o tratamiento no autorizado; los responsables; encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas; así como, evitar las vulneraciones.





II. GLOSARIO DE TÉRMINOS.

- **Bases de Datos:** Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
- **Catálogo de Bases de Datos Personales:** Lista detallada del conjunto ordenado de bases datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
- **Clasificación:** Acto por el cual se determina que la información que posee La Junta de Arbitraje para los Empleados al Servicio de los Poderes del Estado de Oaxaca es reservada o confidencial.
- **Confidencialidad:** Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos no autorizados.
- **Comité de Transparencia:** Comité de Transparencia de cada sujeto obligado en los términos de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca, y el artículo 73 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, y demás normatividad aplicable;
- **Datos Personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
- **Datos Personales Sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
- **Destinatario:** Cualquier persona física o moral pública o privada que recibe datos personales.





- **Documentos:** Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;
- **Encargado:** El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.
- **Inventario de Datos Personales:** Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable;
- **Ley General:** Ley General de Transparencia y Acceso a la Información Pública;
- **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca;
- **Ley de Transparencia:** Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca;
- **Medidas de Seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales
- **Medidas de Seguridad Administrativas:** Políticas, acciones y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;
- **Medidas de Seguridad Físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
- **Medidas de Seguridad Técnicas:** Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
- **Titular:** La persona física a quien corresponden los datos personales;
- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro,





organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales

III. INVENTARIO Y CATÁLOGO DE DATOS PERSONALES.

La Ley General y la Ley definen dos tipos, datos personales que es cualquier información concerniente a una persona física identificada o identificable, para lo que se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información. El otro tipo, son los datos personales sensibles, que son aquellos que se refieren a la esfera más íntima, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste, para enunciar algunos se consideran sensibles los datos que revelan aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas o morales, así como, las opiniones políticas o preferencias sexuales, etc.

Esté Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, tiene acceso a diferentes inventarios de datos personales, que los distribuye en los respectivos sistemas de tratamientos. A continuación, se describen de forma generalizada, con base en las atribuciones descritas en el Reglamento Interno del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca:

- **Datos de identificación y contacto:** nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- **Datos biométricos:** huella dactilar
- **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos:** trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros:** ingresos, egresos y cuentas bancarias.
- **Datos sobre pasatiempos, entretenimiento y diversión:** pasatiempos, aficiones, deportes que practica y juegos de interés.
- **Datos legales:** situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)





- **Datos de salud:** estado de salud físico presente, pasado o futuro y estado de salud mental presente, pasado, o futuro.
- **Datos personales de naturaleza pública:** Datos que por mandato legal son de acceso público.

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales, quienes pueden ser:

- Personas que laboran en el Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca;
- Personas externas que prestan algún servicio para el Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca;
- Personas externas que ejercen su derecho de petición ante el Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca; y
- Personas externas que participan en actividades que llevan a cabo el Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca (capacitaciones y concursos).

IV. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Dentro de cada uno de los sistemas de tratamiento, incluidos en este documento, se especifican las funciones y obligaciones para aquellos servidores públicos que se encuentran en contacto, resguardo y en la transferencia de datos personales. En términos generales, dentro de las obligaciones, es el de hacer responsable a cualquier servidor público que tiene bajo su resguardo información que contiene datos personales, archivos físicos y electrónicos con fundamento en las atribuciones existentes en el Reglamento Interno del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca.

Los Titulares de las áreas administrativas que integran el Sistema de Transporte Colectivo de Transporte Colectivo Metropolitano Citybus Oaxaca, (Dirección General, Departamento Administrativo, Departamento Jurídico, Unidad de Planeación, Unidad de Supervisión y Asistencia, Unidad de Estadística y Seguimiento, Departamento de Estudios y Proyectos, Departamento de Licitación y Supervisión, Departamento de Mantenimiento, Departamento de Supervisión de Rutas, Departamento de Operatividad, Departamento de Estadística y Departamento de Infraestructura Especializada y Tecnológica)





deben asegurarse que el personal a su cargo y con acceso físico y automatizado a los repositorios de los datos personales, conozcan:

- A.** Las normas de seguridad que deben observarse para su tratamiento;
- B.** Sus atribuciones respecto a los sistemas de tratamiento;
- C.** Las responsabilidades que tienen, junto con la firma de la carta responsiva y confidencialidad; y
- D.** Las consecuencias en caso de incumplimiento de las atribuciones, resguardo o la vulneración de los datos personales.

Dentro de los Lineamientos Generales de Protección de Datos Personales, se habla de la obligación que tienen las personas que desempeñan los puestos anteriormente mencionados, en el manejo, tratamiento, transferencia, divulgación y uso datos personales. Como obligaciones las siguientes:

A) De los Servidores Públicos que recaban datos personales directamente de sus titulares:

- 1) Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos, cerciorándose de que el titular de los datos personales conozca íntegramente el contenido de dicho aviso;
- 2) Resolver las dudas que los titulares de los datos personales tengan en relación al aviso de confidencialidad;
- 3) Orientar a los titulares de los datos personales sobre las formas en las que pueden ejercer sus derechos ARCOP, a través del procedimiento de protección de datos personales y remitirlos al Comité de Transparencia para cualquier duda o inicio de dicho procedimiento.
- 4) Al obtener los datos personales, cerciorarse de que la información esté completa, actualizada, veraz, y comprensible;
- 5) Comunicar cuando se dé cuenta, al encargado del tratamiento de los datos personales, la existencia de una discrepancia entre los datos personales que están siendo tratados y los que recabó originalmente;
- 6) Conservar los datos personales siguiendo medidas de seguridad que minimicen los riesgos de uso para finalidades distintas para los que fueron recabados, de su divulgación, pérdida, transferencia y/o alteración; y
- 7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones, quedando prohibida su transmisión a terceros sin autorización expresa.

B) De los Servidores Públicos encargados de su tratamiento:





"2025, BICENTENARIO DE LA PRIMERA CONSTITUCIÓN POLÍTICA DEL
ESTADO LIBRE Y SOBERANO DE OAXACA"

- 1) Utilizar los datos personales estrictamente para los fines para los cuales fueron recabados;
- 2) En caso de que sea necesario utilizar los datos personales para finalidades distintas a las especificadas en el aviso de confidencialidad, se deberá modificar el aviso de privacidad y notificarse a los titulares de los datos personales;
- 3) Autorizar el uso de los datos personales, únicamente a aquellos servidores públicos que formen parte del procedimiento que inicie, de seguimiento o concluya un trámite o servicio en concreto;
- 4) En caso de que exista una resolución del Comité de Transparencia por medio del cual se ordene el acceso, corrección, rectificación o se autorice la oposición de los datos personales, deberá de acatar las medidas que resuelva dicho Comité para dichos efectos;
- 5) Resguardar los datos personales siguiendo las medidas de seguridad que minimicen los riesgos de uso distinto para el que fueron recabados, de su divulgación, pérdida, transferencia y/o alteración; y
- 6) Mantener estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

C) De los Servidores Públicos autorizados para ser parte del tratamiento:

- 1) Mantener estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones, quedando prohibida su transmisión a terceros no autorizados expresamente

V. ANÁLISIS DE RIESGO.

Esté Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, utiliza y custodia datos personales en sus áreas administrativas (Dirección General, Departamento Administrativo, Departamento Jurídico, Unidad de Planeación, Unidad de Supervisión y Asistencia, Unidad de Estadística y Seguimiento, Departamento de Estudios y Proyectos, Departamento de Licitación y Supervisión, Departamento de Mantenimiento, Departamento de Supervisión de Rutas, Departamento de Operatividad, Departamento de Estadística y el Departamento de Infraestructura Especializada y Tecnológica). Y para mayor garantía de seguridad de los datos personales, en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, se implementa las medidas de seguridad que corresponden a UN NIVEL DE RIESGO INHERENTE





MEDIO, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales se ha logrado identificar los siguientes riesgos posibles, ante los que se pudiera enfrentar esté Sujeto Obligado:

- Obtención de datos incompletos o incorrectos;
- Omitir la notificación al titular de los datos personales del aviso de privacidad;
- No difundir el aviso de privacidad;
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad;
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico;
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales;
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios;
- Daño de la base de datos que contenga información confidencial;
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos,
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones;
- Pérdida, robo o extravío de expedientes; y
- Alteración de la información.

Ante dichos riesgos identificados, es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

VI. ANÁLISIS DE BRECHA.

Una vez identificados los posibles riesgos a los que esté Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los reportes de las áreas administrativas, respecto a las medidas de seguridad existentes:





**"2025, BICENTENARIO DE LA PRIMERA CONSTITUCIÓN POLÍTICA DEL
ESTADO LIBRE Y SOBERANO DE OAXACA"**

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite;
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones del Sistema;
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial;
- En la mayoría de las áreas (donde se recibe a los ciudadanos y se recaban datos personales) el acceso se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir, si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos;
- Cada oficina cuenta con puertas que separa el área al momento de terminar labores;
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área,
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico;
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada está en archiveros o puesta en resguardo electrónico, tienen acceso los servidores públicos del área;
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área;
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma;
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, solo los servidores públicos del área tienen acceso;
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen; y
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas este sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes





se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas. Al implementar:

- **Términos y condiciones de empleo:** como parte de las funciones de las y los servidores públicos, se deberán acordar o establecer términos o condiciones de confidencialidad, de acuerdo al tratamiento y responsabilidad de los datos personales que obran en su poder.
- **Sensibilidad y capacitación:** las y los servidores públicos deberán recibir capacitación de manera periódica de acuerdo con el tratamiento que realicen de los datos personales.
- **Seguridad en la transferencia o remisión:** en caso de contar con la figura de encargado, contar con el documento que avale la transferencia y que contenga una cláusula de confidencialidad de la información.
- **Eliminación de los derechos de acceso:** los derechos de acceso de las y los servidores públicos o encargados, a las instalaciones o al tratamiento de la información, deben ser removidos en cuanto termine la relación laboral o de servicios, o en caso de realizar ajustes a las funciones del servidor público o encargado.

VII. PLAN DE TRABAJO.

La existencia del Documento de Seguridad, busca enmarcar los deberes de este Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, para la máxima protección de datos personales de acuerdo al artículo 30, fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 26 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.

Debido a la importancia y el contexto actual en materia de datos personales, es necesaria la implementación de un Plan de Trabajo, ya que se encuentra descrita como una de las obligaciones que al menos debe contener el documento de seguridad, el cual permita alcanzar los objetivos.

ACTIVIDADES	TEMPORALIDAD	ÁREAS INVOLUCRADAS	ACTUALIZACIÓN
Creación de políticas internas para el tratamiento de datos personales	Anual	Delimitación del personal que maneja datos personales en las áreas	En acontecimientos que se susciten y los lineamientos que se publiquen





Revisión de los inventarios de datos personales	Anual	Todas las áreas administrativas	Mensual
Establecer comunicación directa con la Unidad de Transparencia en relación a cuestionamientos relativos a la protección de datos personales.	Siempre que sea necesaria	Titular de área, habilitado de transparencia, o cualquier persona que maneje datos personales	Siempre que sea necesaria
Seguimiento al plan de capacitación en relación a la protección de datos personales	Según la temporalidad de las sesiones establecidas	Personal que maneje datos personales	Mensual
Revisión periódica de las medidas de seguridad señaladas en el documento de seguridad.	Mensual	Personal que maneje datos personales	Mensual
Implementar cartas responsivas para las personas servidoras públicas.	Anual	Personal que maneje datos personales	Anual
Verificación de las finalidades establecidas	Anual	Personal que maneje datos personales	Anual

VIII. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Las medidas de seguridad propuestas a implementar en cada una de las áreas del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, se evaluarán para determinar su eficacia o vulnerabilidad de manera trimestral, con base en la Ley General y la Ley en la materia. Y se considerará:





**"2025, BICENTENARIO DE LA PRIMERA CONSTITUCIÓN POLÍTICA DEL
ESTADO LIBRE Y SOBERANO DE OAXACA"**

- a) El riesgo inherente a los datos personales tratados;
- b) La sensibilidad de los datos personales tratados;
- c) El desarrollo tecnológico;
- d) Las posibles consecuencias de una vulneración para los titulares;
- e) Las transferencias de datos personales que se realicen;
- f) El número de titulares;
- g) Las vulneraciones previas ocurridas en los sistemas de tratamiento;
y
- h) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Por esta razón, se generarán acciones que establezcan el mantenimiento de las medidas de seguridad, en las cuales de manera general se destaca que el objeto de las mismas es la protección de los datos personales. Y para ello, al menos se consolidarán las siguientes acciones interrelacionadas:

1. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
2. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
3. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
4. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal responsable, entre otros;
5. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
6. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
7. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y





8. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Acciones que en buena medida se encuentran desarrolladas en este Documento de Seguridad, realizando su análisis y seguimiento de las mismas, a fin de poderlas incluir en la siguiente actualización de las políticas de Seguridad de la Información, existentes. Y se deberán atender los siguientes elementos:

- Que existan controles en donde se garantice la validación, confidencialidad, integridad y disponibilidad de los datos personales en posesión de este Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca;
- Que se cuente con las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;
- Mantenerse atentos para implementar las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;
- Contar con un proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;
- Tener la seguridad adecuada para que los controles garanticen que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento, y
- Implementar las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas.

Las áreas administrativas que integran el Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, deberá analizar todas las causales de ocurrencia de una vulneración, a fin de implementar dentro del plan de trabajo las acciones preventivas y correctivas que se ajusten con las medidas de seguridad correspondiente para dar el tratamiento de los datos personales adecuados, y evitar que el riesgo de vulnerabilidad persista.

También, se establecerán controles y mecanismos que tengan el objetivo de que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad, respecto de éstos. Obligación que subsistirá aún después de finalizar sus relaciones con el mismo, a través de cartas





de responsabilidad que serán firmadas por cada uno de los servidores públicos o personas externas; sin menoscabo de lo establecido en las disposiciones aplicables en materia de acceso a la información pública.

IX. MEDIDAS DE SEGURIDAD PARA GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES.

Las Medidas de Seguridad, son conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales. Las cuales se pueden definir y agrupar de la siguiente manera:

- A. **Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como, la sensibilización, formación y capacitación del personal, en materia de protección de datos personales;
- B. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:
- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
 - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
 - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
 - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
- C. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:





- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En relación al monitoreo de la seguridad, es de observarse lo dispuesto en el artículo 26 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, el cual refiere que se deberá elaborar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar acciones de mejoras de manera continua. Siendo las siguientes:

- Los nuevos activos que se incluyen en la gestión de riesgos;
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras;
- Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo; y
- Los incidentes y vulneraciones de seguridad ocurridas.

**X. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
DENTRO DEL SISTEMA DE TRANSPORTE COLECTIVO
METROPOLITANO CITYBUS OAXACA.**

El Sistema de Gestión de Seguridad de la Información (SGSI), es un sistema que identifica los diversos activos (personas, hardware, software, documentos, etc.), para llevar a cabo un análisis de los riesgos a los que pueden estar expuestos





y realizar acciones que permitan minimizar el impacto en caso de presentarse. Todo esto para garantizar la confidencialidad, la integridad y la disponibilidad de dichos activos.

Como Sistema de Gestión se han documentado políticas, procesos, procedimientos, protocolos, formatos y demás actividades a fin de poder ser auditados y llevar acciones correctivas, con la finalidad de tener un proceso de mejora continua. Que pueden ser:

- Gestionar las amenazas de la institución que puedan afectar el cumplimiento de los objetivos: esto implica la identificación, el análisis y el tratamiento de los riesgos;
- Permitir a la organización un enfoque al riesgo: esto implica conocer cuántos y cuáles pueden ser los riesgos y verificar su impacto en la operación de cada elemento operativo;
- Contar con criterios y políticas específicas que permitan minimizar las amenazas que pudieran presentarse e impactar a los objetivos, institucionales, tácticos y operativos; y
- Garantizar que nuestra información mantenga su confidencialidad, su integridad y su disponibilidad, para su adecuada utilización.

XI. PROGRAMA GENERAL DE CAPACITACIÓN Y ACTUALIZACIÓN.

Una de las partes fundamentales para la permeabilidad y factibilidad de la transparencia, el acceso a la información y la protección de datos personales, se encuentra en la capacitación, formación y profesionalización de los servidores públicos en general, debido a que existe un gran desconocimiento de la materia y además una cultura muy pobre como sociedad en estos temas. En ese sentido y de conformidad con la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca en sus artículos 10 fracción V, 14 fracción I y 73 fracción VI, así como los artículos 27 fracción VII y 74 fracción VIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; que establece la obligación de capacitar en temas de transparencia y acceso a la información pública y de realizar un programa de capacitación en el tema de la protección de los datos personales.

Se estima necesaria la implementación de un programa de capacitación en materia de transparencia y protección de datos personales para el personal del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, buscando la especialización de la misma.





Siendo su propósito general:

- El de cumplir con la norma y mejorar los procesos de acceso a la información pública, así como la protección de los datos personales;
- Elevar el nivel de conocimiento de los servidores públicos, para mejorar la calidad del servicio y esto se traduce en un bienestar social;
- Mejorar la relación entre sujeto obligado y sociedad;
- Satisfacer requerimientos futuros en base a la planeación del manejo de información y de datos personales;
- Generar conductas positivas y mejoras en la calidad del tratamiento de información y protección de datos personales;
- Cumplir con las disposiciones legales en la materia; y
- Dar confianza a las personas de la protección de su información y datos personales.

XII. MODALIDAD DE CAPACITACIÓN.

Con la finalidad de garantizar que las y los servidores públicos del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, cuenten con conocimientos que permitan contribuir a un adecuado tratamiento de los documentos que contienen datos personales, se ha programado realizar capacitaciones en los siguientes rubros:

1. **Formación:** Su propósito es impartir conocimientos básicos orientados a proporcionar una visión general y amplia con relación al contexto de desenvolvimiento.
2. **Actualización:** Se orienta a proporcionar conocimientos y experiencias derivados de recientes avances científico-tecnológicos en una determinada actividad.
3. **Especialización:** Se orienta a la profundización y dominio de conocimientos y experiencias o al desarrollo de habilidades, respecto a un área determinada de actividad.
4. **Perfeccionamiento:** Se propone completar, ampliar o desarrollar el nivel de conocimientos y experiencias, a fin de potenciar el desempeño de funciones técnicas, profesionales, directivas o de gestión.
5. **Complementación:** Su propósito es reforzar la formación de un colaborador que maneja solo parte de los conocimientos o habilidades demandados por su puesto y requiere alcanzar el nivel que este exige.



Amelia B

[Handwritten signature and initials]



XIII. TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

Los datos personales una vez que su ciclo de vida transcurriera según corresponda, a la finalidad por la cual fueron recabados, procederá a la supresión y borrado, durante dicho periodo no se podrán realizar acciones relativas al tratamiento de los mismos, procediendo de esta manera a la supresión de la base de datos, archivo o registro respectivo, se aplicara la normatividad archivística aplicable para la legal aplicación de esta técnica.

Se establece la documentación de los procedimientos que se utilizaran para la supresión y borrado de los datos personales que el responsable tiene en su poder, en el cual se incluirá los plazos de conservación si en su caso se requiriera, así como la realización de una revisión periódica sobre la necesidad de su conservación.



Handwritten signatures and initials in blue ink, including a large signature at the top and several circular stamps or initials below it.



Este Documento de Seguridad para la Protección de Datos Personales en Posesión del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca, en coordinación con las áreas que recaban datos personales; fue aprobado por el Comité de Transparencia del Sistema de Transporte Colectivo Metropolitano Citybus Oaxaca en la Quinta Sesión Extraordinaria, de fecha 09 de septiembre de 2025.

Handwritten signature in blue ink.

Handwritten signature in blue ink.

Handwritten signature in blue ink.

Handwritten signature in blue ink.

