COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

CAPUFE
CAMINOS Y PUENTES FEDERALES

DOCUMENTO DE SEGURIDAD
EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES
EN POSESIÓN DE CAMINOS Y PUENTES FEDERALES DE INGRESOS Y SERVICIOS CONEXOS
(CAPUFE)

CONTENIDO

I.- INTRODUCCIÓN

En el año 2009 se reformó el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el cual establece en su segundo párrafo que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición al uso de su información personal en los términos que fija la Ley, esta reforma dio origen a la *Ley Federal de Protección de Datos Personales en Posesión de Particulares* (LFPDP), en el año 2010, no obstante es hasta la reforma del artículo 6to Constitucional del año 2014 cuando se fijan las bases para la emisión de una Ley General respecto de la información en posesión de entes públicos.

En ese contexto, el 26 de enero del año 2017 se publicó la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPPSO) en la cual se establecen las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de entes públicos de los tres órdenes de Gobierno, con la cual se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición mediante procedimientos sencillos y expeditos (derechos ARCO).

Por lo anterior, todas las dependencias y entidades están obligadas a llevar a cabo el tratamiento de datos personales de personas físicas, adquiriendo el carácter de "responsable" debiendo tratar dichos datos conforme a los principios de **licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad**; adoptando medidas de seguridad en atención a los sistemas de datos que traten, establecer en un documento de seguridad dichas medidas, garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición entre otras obligaciones previstas en la normativa en materia de protección de datos personales.

Ahora bien, en atención a que Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE), es un Organismo Público Descentralizado que tiene a su cargo, entre otras funciones, administrar y explotar por sí o a través de terceros, mediante concesión otorgada en términos de las disposiciones legales aplicables, los caminos y puentes federales que ha venido operando, así como en los que en lo futuro se construyan con cargo a su patrimonio o les sean entregados para tal objeto; llevar a cabo por sí o a través de terceros, la conservación, reconstrucción y mejoramiento de dichas vías con cargo a su patrimonio; administrar y explotar por sí o a través de terceros mediante concesión, los servicios conexos y auxiliares a las vías generales de comunicación; construir, administrar y explotar por sí o por terceros, las instalaciones complementarias que requiera para el cumplimiento de su objeto; así como promover y fomentar la participación de particulares bajo el régimen de concesión en la construcción y explotación de caminos y puentes federales, conforme a los lineamientos que emita la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), lo anterior mediante la celebración de Contratos y/o Convenios de Fideicomisos, de servicios de administración, de operación y conservación de tramos carreteros y puentes de cuota con representantes de personas morales. Es un Sujeto Obligado en materia de protección de datos

personales, responsable de los datos personales a los que les brinda un tratamiento durante la realización de sus facultades y atribuciones.

Por lo antes expuesto, se presenta el presente Documento de Seguridad de conformidad con lo establecido en el artículo 35 de la LGPDPPSO.

Este documento fue coordinado por la Unidad de Transparencia de este Organismo, llevándose a cabo las actividades siguientes:

- Se realizaron reuniones con el grupo de trabajo para el seguimiento y atención al Programa Nacional de Datos Personales (PRONADATOS), integrado por el personal designado por cada una de las unidades administrativas, y que permanentemente realizan el tratamiento de datos personales para elaborar el Inventario de los Sistemas de Tratamiento de Datos Personales de CAPUFE.

- Se identificó la estructura con los requisitos mínimos de los Sistemas de Tratamiento de Datos Personales, que deben contener, de conformidad con la normatividad aplicable.

- Se determinaron las medidas de seguridad, así como la propuesta de capacitación para la atención y tratamiento de datos personales.

A partir de estas actividades, se definió la importancia de elaborar el Documento de Seguridad y, de sensibilizar a las personas servidoras públicas adscritas a las diferentes Unidades Administrativas sobre los requisitos normativos para su integración y la metodología para el tratamiento y la entrega de la información sobre los distintos Sistemas de Tratamiento de Datos Personales.

En ese sentido, la Unidad de Transparencia apoyó y asesoró a las Unidades Administrativas, con el objeto de remitir las observaciones pertinentes y brindar cabal cumplimiento a lo establecido en la normatividad de la materia.

Así, las distintas Unidades Administrativas de CAPUFE, que cuentan con Sistemas de Tratamiento de Datos Personales, entregaron conforme a la metodología propuesta para la integración del Documento de Seguridad, la siguiente información:

- Los Sistemas de Tratamiento de Datos Personales con que cuentan, su objetivo y el fundamento normativo para llevar a cabo dicho tratamiento.

- La descripción e identificación de la estructura de dichos Sistemas, en la cual se incluyen los datos personales que contienen y su idoneidad, la manera en que se obtiene, el administrador, los operadores, los usuarios, el tipo de soporte en que se encuentra, las

características del lugar en que se localizan, su portabilidad, la existencia de transferencias y si hay encargados.

- La información de las medidas de seguridad, en donde se incluye la descripción de las existentes de carácter administrativo, físico y técnico, la identificación de riesgos, la determinación de brechas, la elaboración del plan de trabajo, mecanismos de monitoreo y la propuesta de capacitación en medidas de seguridad.

Bajo ese contexto, con la totalidad de la información proporcionada por las distintas unidades administrativas de CAPUFE, se integró el presente Documento de Seguridad.

II.- MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos (CPEUM)
  Artículos 6 y 16.
  D.O.F. del 8 de mayo de 2020 y sus últimas reformas.

- Código Civil Federal
  D.O.F. del 26 de mayo de 1928 y sus últimas reformas.

- Código Fiscal de la Federación
  D.O.F. del 12 de noviembre 2021 y sus últimas reformas.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
  D.O.F. del 26 de enero de 2017.

- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
  D.O.F. 04 de enero de 2000.

- Ley General de Títulos y Operaciones de Crédito
  D.O.F. 27 de agosto de 1932 y sus últimas reformas.

- Ley Orgánica de la Administración Pública Federal (LOAPF)
  D.O.F. del 22 enero de 2020, y sus últimas reformas.

- Ley General de Archivos
  D.O.F. del 15 junio de 2018, y sus últimas reformas.

- Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP).
  D.O.F. del 26 enero de 2018.

- Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales (LPMPPDP)
  D.O.F. del 12 de febrero de 2018.

- Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE).
  D.O.F. del 30 de abril del 2021 (y sus últimas reformas).

- Manual General de Organización de Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE).
  Normateca Interna 29 de 03 de 2000.

- Compendio Operativo para plazas de cobro de CAPUFE
  Normateca Interna 15 de marzo de 2022.

- Compendio de Seguridad y Protección Civil de CAPUFE
  Normateca Interna 31 de 03 de 2011.

- Código de Conducta de CAPUFE
  Normateca Interna 29 de 08 de 2016.

- Directrices de Seguridad de la Información de CAPUFE
  Normateca Interna 13 de 11 de 2020.

- Lineamiento para la atención de las expresiones ciudadanas recibidas en CAPUFE
  Normateca Interna 8 de diciembre de 2021.

- Lineamiento para la operación de la Central de Atención a Usuarios y Centrales de Radio Local
  Normateca Interna 8 de diciembre de 2021.

- Lineamientos para la Prestación de los Servicios de Auxilio Vial
  Normateca Interna 6 de octubre de 2021.

- Lineamiento para la Prestación de los Servicios de Emergencia y Atención Médica Prehospitalaria
  Normateca Interna 3 de marzo de 2022.

III.GLOSARIO DE TÉRMINOS, SIGLAS Y ACRÓNIMOS

Agente de primer nivel: Registra y asigna el ticket de la contingencia responsable de Seguridad de la Subdirección de Tecnologías de Información (STI).
Agente de segundo nivel: Es el encargado de atender la petición.

Agente de tercer nivel: En caso de que, el agente de segundo nivel, turne la petición a un agente de tercer nivel, lo atenderá el supervisor o responsable del área.

APF: Administración Pública Federal.

CAPUFE y/o Organismo y/o Entidad: Caminos y Puentes Federales de Ingresos y Servicios Conexos.

CATT: Centro de Atención Telefónica de Telepeaje.

Central de Atención a Usuarios (CAU): Unidad administrativa y operativa ubicada en Oficinas Centrales de CAPUFE, en donde se atienden y administran el número 074 y la cuenta de Twitter @CAPUFE.

CFDI: Comprobante Fiscal Digital por Internet.

Colector: Dispositivo de Red que recibe y almacena en bitácoras todos los eventos (logs) de los equipos de red y seguridad y los envía al correlacionador para su análisis.

Correlacionador: Analiza los registros de eventos que suceden en la red, su función además de analizar es detectar actividad sospechosa mediante patrones pre establecidos.

CVDSA S.A. DE C.V.: Centro de Validación Digital, S.A. de C.V.

Dato personal: Cualquier información 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

Dato personal sensible: Aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida puedan 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 presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición, todos ellos relacionados con el tratamiento de datos personales.

Directrices de Seguridad de la Información: Base normativa que soporte la implementación del Sistema de Gestión de Seguridad de la Información para contribuir al cumplimiento de leyes y

regulaciones aplicables en materia de seguridad de la información, reducir los riesgos e impactos operativos, financieros, de imagen, de reputación, fortalecer la eficacia y eficiencia de los procesos de CAPUFE.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales

DOF: Diario Oficial de la Federación.

Encargado (a): La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Fideicomitente: Persona física o moral, con capacidad para transmitir la propiedad o la titularidad de los bienes o derechos objeto del fideicomiso, según sea el caso, así como las autoridades judiciales o administrativas competentes para ello.

Fideicomisario: Persona física o moral que tenga la capacidad necesaria para recibir el provecho que el fideicomiso implica.

Fideicomisos: Es el contrato a través del cual una persona transmite la propiedad de uno o más bienes (muebles o inmuebles) o derechos para ser destinados a fines lícitos y determinados.

Fiduciarias: Son las empresas de servicios fiduciarios, Instituciones de crédito, casas de bolsa, Instituciones de seguro, Instituciones de Fianza y a la Financiera rural que lleven a cabo la operación fiduciaria y que tienen autorización de la Secretaría de Hacienda y Crédito Público.

FIREWALL: Dispositivo de Seguridad que bloquea o permite el tráfico que sale y/o entra a la red del cliente desde el servicio de internet.

FONADIN: Fondo Nacional de Infraestructura.

FOVISSSTE: Fondo de la Vivienda del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

GAUTI: Gerencia de Atención a Usuarios de Tecnologías de Información.

IDS: Sistema de detección de intrusos. Es un software de seguridad cuya función es detectar accesos no autorizados en un sistema o una red de ordenadores, y en base a ello, generar algún tipo de alerta o log.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Incidente: Suceso o acontecimiento que genera la ejecución de acciones correctivas dentro de los procedimientos físicos o electrónicos.

IP: Internet Protocol (Protocolo de Internet).

IPS: Intrusion Prevention System (Sistema de Prevención de Intrusos):
Dispositivo de Seguridad de Detección y Prevención de Intrusos en el enlace de internet.

ISSSTE: Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

LFTAIPG: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

LGTAIPG: Ley General de Transparencia y Acceso a la Información Pública Gubernamental.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

MPLS: Multiprotocol Label Switching o MPLS, por su traducción: conmutación de etiquetas multiprotocolo, es un estándar para transmitir datos bajo diferentes etiquetas, creado por la Internet Engineering Task Force, una organización dedicada a mejorar el flujo de trabajo de Internet.

Operador (a): Personas servidoras públicas que operan en el sistema en CAPUFE.

Personas físicas: todo individuo sujeto de derechos y obligaciones.

Personas morales: es toda agrupación de personas individuales, dotada de personalidad jurídica, titular de derechos y obligaciones.

Portal de Control de Operación (PCO): Es la herramienta informática implementada por la Dirección de Operación para el registro en línea de los padrones de residentes y de pago por recorrido, actualizaciones y autorizaciones.

Respaldo: Actividad de copiar archivos, información o bases de datos, de forma que puedan ser preservados en caso de fallas de equipo, sistemas o catástrofes dentro del Organismo, que pudieran causar la pérdida de información.

Responsable del SDP: Persona servidora pública titular de la unidad administrativa, designada por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Representante legal: Persona a la que, por disposición legal, actúa en nombre y representación de otra persona física o moral, produciendo efectos en las relaciones jurídicas de la que es titular el representado.

Ruteador: Dispositivo de red que permite la comunicación entre diferentes redes.

RUSP: Registro de Servidores Públicos del Gobierno Federal.

SAP: Producto de Sistema de Aplicaciones para procesamiento de datos (Systems, Applications, Products in Data Processing). Sistema de información que permite gestionar las diferentes acciones de una empresa, sobre todo las que tienen que ver con la producción, la logística, el inventario, los envíos, la nómina y la contabilidad.

SCHDO: Subdirección de Capital Humano y Desarrollo Organizacional.

SFP: Secretaría de la Función Pública.

SIAC: Sistema Integral para la Administración de CAPUFE.

Identificación Automática Vehicular IAVE: Plataforma mediante la cual la persona usuaria de telepeaje registra sus datos y administra su cuenta.

Sistema Automático Vehicular IAVE: Plataforma mediante la cual la persona usuaria de telepeaje registra sus datos y administra su cuenta.

Sistema de Gestión de Seguridad de la Información: Conjunto de políticas, procedimientos y directrices, que a través del análisis de riesgo y de la definición de procesos y controles define las guías para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

SMTP: Simple Mail Transfer Protocol (Protocolo de Transferencia Simple de Email). Es un protocolo básico que permite que los emails viajen a través de internet.

SSL: Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

STI: Subdirección de Tecnologías de Información.

Remisión datos personales:
Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

Transferencia datos personales:
Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

Transmisión de datos personales: Toda comunicación de datos personales realizada entre el responsable transmisor y el responsable receptor, a partir de la portabilidad de datos personales. Tratándose de servicios de cómputo en la nube, la comunicación de datos personales de un servicio o aplicación de un responsable a otro.

Tratamiento de Datos Personales: Conjunto de acciones de procesamiento de los datos personales (pueden ser: obtención, uso, divulgación o almacenamiento). El uso puede abarcar cualquier acción de acceso, manejo, aprovechamiento, transferencias o disposición de éstos.

Unidad de transparencia: Instancia encargada de vigilar el cumplimiento de la Ley Federal y la Ley General de Transparencia y Acceso a la Información Pública, así como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al interior de CAPUFE.

Unidades de apoyo: Unidades de señalamiento dinámica, unidades de rescate y en ocasiones las unidades de conservación del tramo.

Unidades Regionales: Unidades administrativas en el territorio nacional, coordinadas normativamente por las Unidades Administrativas Centrales y funcionalmente por la Dirección General.

Usuario / Usuaria del SDP: Persona servidora pública facultada por un instrumento jurídico o expresamente autorizado por la persona Responsable del SDP, que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

VPN: Virtual Private Network (Red Privada Virtual). Permite conectarse a través de una conexión segura.

WAF: Web Application Firewall. (Firewall de aplicaciones WEB). Es un Firewall para la protección de todas las aplicaciones y/o páginas WEB que el cliente publica en Internet.

IV.- ÁMBITO DE APLICACIONES Y OBSERVACIONES GENERALES

Las obligaciones que tienen las personas responsables de los tratamientos de los datos personales, se encuentran establecidas en la LGPDPPSO y en *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, y son aplicables para todas las personas servidoras públicas de CAPUFE que en el ejercicio de sus atribuciones y funciones, tengan acceso a los datos personales y que dentro de sus Sistemas de Tratamiento de Datos Personales realicen el manejo, tratamiento, administración, transferencia, divulgación y/o eliminación de los datos personales ya sea completos, o el tramo de información que corresponde.

Aplica para aquellos datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotografía, acústica o en cualquier formato.

Además de las funciones y obligaciones de las personas servidoras públicas involucradas, establecidas de manera específica en el análisis de cada uno de los Sistemas, de manera general deberán observar lo siguiente:

Funciones genéricas:

- Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos.
- Cuando no sean necesarios, suprimir los datos de forma adecuada.

Obligaciones genéricas:

- Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Tratar los datos personales de manera adecuada, pertinente y limitado a lo necesario.
- Contar con capacitación en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales y, en general, que puedan vulnerar la seguridad de los datos personales.

Las personas servidoras públicas responsables del tratamiento de datos personales en todo momento deberán observar los principios generales, así como adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Es importante mencionar que la obligación de confidencialidad debe subsistir aún después de que las personas servidoras públicas hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el Organismo haya concluido.

De manera particular y de conformidad con los cargos, encargos y/o designaciones de las personas servidoras públicas, se definen los siguientes roles en el tratamiento de los datos personales:

Persona responsable del Sistema: será la persona titular de la unidad administrativa que administre el Sistema, el cual deberá:

- ✓ Dar aviso a la Unidad de Transparencia de los Sistemas de Tratamiento de Datos Personales que se encuentren a su cargo.
- ✓ Designar a la persona administradora de cada Sistema de Tratamiento de Datos Personales a su cargo.
- ✓ Validar que la información entregada por las personas titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.
- ✓ Vigilar y coordinar que la información se encuentre actualizada.
- ✓ Dar a conocer las normas de seguridad que deben observarse para el tratamiento de los datos personales.

Persona administradora del Sistema: será la persona servidora pública a quien designe de manera expresa la persona Titular de la Unidad Administrativa. Tiene a su cargo la responsabilidad de la administración del Sistema y de las o los Operadores, deberá:

- ✓ Mantener actualizado el sistema.
- ✓ Determinar a las personas servidoras públicas que tendrán acceso a los datos personales, en función del tratamiento que se les debe aplicar.
- ✓ Autorizar los accesos de las personas servidoras públicas, determinar los privilegios y limitantes y, llevar un registro de los mismos.
- ✓ Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

Persona operadora del Sistema:

- ✓ Sus funciones se determinan de acuerdo al perfil asignado en el tratamiento de los datos personales de cada Sistema.

El incumplimiento a lo establecido en el presente documento, así como a lo establecido por la LGPDPPSO causará la aplicación de medidas de apremio y/o sanciones, que se detallan en dichos instrumentos normativos.

V.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

En el presente documento se estableció un inventario de datos personales de los Sistemas tratados por CAPUFE, los cuales se encuentran en medios de almacenamiento físicos, así como electrónicos.

Los mismos se presentan por las Unidades Administrativas previstas con base a la estructura orgánica y el Estatuto Orgánico de CAPUFE.

Catálogo de Sistemas de Tratamiento o bases de datos personales

Los Sistemas que se enlistan a continuación, corresponden a aquellos cuyos datos personales se encuentran en soporte físico y electrónico:

I. Dirección de Operación (D.O.)

I.1. Sistema Integral de Operación Carretera SIOC.
I.2. Padrón de usuarios residentes a las plazas de cobro.
I.3. Sistema de atención a expresiones ciudadanas.
I.4. Padrón de usuarios exentos de Telepeaje en plazas de cobro.
I.5. Línea Exprés.
I.6. Padrón de usuarios del sistema de Identificación Automática Vehicular IAVE.

II. Dirección Jurídica (D.J.)

II.1. Representantes de Personas Morales que contratan con CAPUFE servicios de administración, operación y conservación de tramos carreteros y puentes de cuota.
II.2. Representantes de las Fiduciarias, de los Fideicomitentes y Fideicomisarios en los Fideicomisos que cuentan con la participación de CAPUFE.

III. Dirección de Administración y Finanzas (D.A.F.)

III.1. Servicio de emisión, envío y resguardo de Comprobantes Fiscales Digitales por Internet (CFDI).
III.2. Sistema de Recursos Humanos.

A continuación, se abordará cada uno de los Sistemas de Tratamiento de Datos Personales referidos, señalando en su descripción los apartados siguientes:

1. Objetivo	Propósito o fin para el cuál fue diseñado, desarrollado, construido o pensado.
2. Fundamento legal	Disposición legal en la que se establezca la obligación de contar con el Sistema, o bien, la atribución o facultad de recabar los datos.

3. Datos personales que se encuentran en el Sistema	Listado de datos personales que contiene el Sistema y su idoneidad.
4. Forma de obtención de los datos personales	Directa: Aquella que se recaba directamente del titular de los datos personales. Indirecta: Aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por la persona Responsable; por el receptor, cuando el titular le hubiera facilitado directamente sus datos y, el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.
5.- Persona servidora pública Responsable del Sistema	Nombre y cargo de la persona servidora pública responsable del Sistema.
6. Persona servidora pública Administradora del Sistema	Nombre y cargo de la persona servidora pública que administra el Sistema.
7. Persona servidora pública Operadora del Sistema	Nombre y cargo de la persona servidora pública que opera el Sistema.
8. Persona servidora pública Usuaria del Sistema	Ciudadano, persona servidora pública u otra persona que hace uso del sistema.
9. Tipos de soportes	Físico, electrónico o combinado.
10. Características del lugar físico donde se Resguardan los sistemas de tratamiento de datos personales	Inmueble, piso, cuadrante, oficina, PC, etc.
11. Portabilidad de datos	Derecho del titular de obtener del responsable una copia de los datos objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita seguir utilizándolos, o bien, cuando el tratamiento se base en el consentimiento o, en su caso, cuando el titular hubiera facilitado directamente sus datos al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.
12. Transferencia de datos	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.
13. Persona Encargada de datos	Persona física o jurídica, pública o privada, ajena a la organización de CAPUFE, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de la Comisión.

A continuación, se describen cada uno de los sistemas de protección de datos personales que tiene CAPUFE:

I. Dirección de Operación

Nombre del Sistema de Datos Personales:
I.1 SISTEMA INTEGRAL DE OPERACIÓN CARRETERA SIOC.

1. Objetivo:
Registro y seguimiento de los servicios carreteros que otorga CAPUFE.

2. Fundamento Legal: (específico)
Artículo 41, fracción I, V y VI del ESTATUTO Orgánico de CAPUFE; Lineamientos para la Prestación de los Servicios de Auxilio Vial; Lineamiento para la Prestación de los Servicios de Emergencia y Atención Médica Prehospitalaria y Lineamiento para la operación de la Central de Atención a Usuarios y Centrales de Radio Local; y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona física	Identificar a la persona física con la que se tendrá comunicación.
Teléfono de casa y/o celular	Mantener contacto con la persona con la que se tendrá comunicación.
Correo electrónico.	Mantener contacto con la persona con la que se tendrá comunicación.
En caso de Servicio médico se puede recabar, además, datos de:	
Dirección	Localizar a familiares
Traumatismos	Que el diagnóstico corresponda al evento ocurrido y no a su condición previa
Antecedentes patológicos	Que el diagnóstico corresponda al evento ocurrido y no a su condición previa
Cinemática del trauma	Para dar a conocer al médico receptor los movimientos a los que estuvo expuesto el usuario
Evaluación primaria pupilas	Forma parte de información que aporta una tabla de diagnóstico que permite evaluar el estado de alerta.
Expectativa de vida	Conocer la gravedad y en consecuencia tomar decisiones para el traslado
Diagnóstico presuntivo	Encausar las primeras atenciones dentro de una unidad hospitalaria
Evaluación secundaria	Revaloración sobre la ambulancia en base a un tratamiento y permitirá la respuesta al mismo
Datos clínicos	Robustecer la información de entrega del paciente al hospital receptor
Tratamiento utilizado	Dejar evidencia del medicamento y tratamientos durante la atención del usuario.

Hospital de destino	Para localización posterior e informar al usuario.
Del vehículo(s) involucrado(s):	
Tipo de vehículo	Para la identificación del vehículo
Marca,	Para la identificación del vehículo
Submarca	Para la identificación del vehículo
Modelo	Para la identificación del vehículo
Color	Para la identificación del vehículo
Placas	Para la identificación del vehículo

4. Forma de obtención de los datos personales

(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico	X	No se presenta esta situación	
Formulario electrónico			
Texto libre físico			
Texto libre electrónico			
Vía telefónica	X		
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lcda. Cynthia Lizeth Cruz Fernández
Cargo	Subdirectora de Servicios al Usuario.
Adscripción	Dirección de Operación
Teléfono y extensión	2073
Correo electrónico institucional	clcruzf@capufe.gob.mx
Funciones	Responsable de los procesos y del sistema Proponer procedimientos para la prestación de servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido; Supervisar la operación de la prestación de servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido; Proponer indicadores para monitorear y evaluar los servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido;
Obligaciones	Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

	Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

6. Persona servidora pública Administradora del Sistema:

Id	Datos de la persona servidora pública administradora	
1	Nombre	Birzayit Lizeth Flores Maldonado
	Cargo	Subgerente de Voz Ciudadana
	Adscripción	Dirección de Operación
	Correo electrónico	bflores@capufe.gob.mx
	Funciones	Gestionar y coordinar las actividades de la Central Telefónica 074, así como de las Centrales de Radio Locales Solicitar funcionalidades y requerimientos del Módulo de CRL/074 Seguimiento y Atención de los folios que correspondan al Módulo de su competencia
	Obligaciones	Deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

Id	Datos de la persona servidora pública administradora	
2	Nombre	Luis Carlos Vicario González
	Cargo	Subgerente de Servicios Médicos
	Adscripción	Dirección de Operación
	Correo electrónico	lcvicariog@capufe.gob.mx
	Funciones	Gestionar y coordinar las actividades de los Servicios Médicos del Organismo Solicitar funcionalidades y requerimientos del Módulo de Servicio Médico Seguimiento y Atención de los folios que correspondan al Módulo de su competencia Coordinación del seguimiento médico-administrativo de los expedientes generados relacionados con los folios SIOC donde se involucre la atención médica prehospitalaria**.**
	Obligaciones	Deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

		El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. • Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. • Todas aquellas que apliquen, estipuladas en la Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados

Id	Datos de la persona servidora pública administradora	
3	Nombre	Julia Dolores Cardona Ramirez
	Cargo	Subgerente de Proyectos
	Adscripción	Dirección de Operación
	Correo electrónico	jcardona@capufe.gob.mx
	Funciones	Gestionar y coordinar las actividades del Servicio de Auxilio Vial. Solicitar funcionalidades y requerimientos del Módulo de Auxilio Vial Seguimiento y Atención de los folios que correspondan al Módulo de su competencia Coordinación del seguimiento administrativo de los expedientes generados relacionados con los folios SIOC donde se involucre el Servicio de Auxilio Vial.
	Obligaciones	Deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública operadora	
1	Nombre	Lista operadores de primer contacto
	Cargo	Lista operadores de primer contacto
	Funciones	Registro Sistematizado de datos iniciales de una incidencia y de las personas usuarias
	Obligaciones	Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

Id	Datos de la persona servidora pública operadora	
2	Nombre	Lista operadores en sitio
	Cargo	Lista operadores en sitio

	Funciones	Registro Sistematizado de datos durante una incidencia y de las personas usuarias Levantamiento de datos e información en los formatos determinados. Acceso y resguardo de expedientes físicos
	Obligaciones	Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

Id	Datos de la persona servidora pública operadora	
3	Nombre	Lista de supervisores
	Cargo	Lista de supervisores
	Funciones	-Revisión y acceso al total de la información con privilegios de modificación y de reemplazar a un operador
	Obligaciones	Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública		Ciudadano (a)		Otro	

Todos los usuarios del sistema SIOC son personas servidoras públicas.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	X

Descripción:

Soporte físico:

- Expedientes que contienen la información asociada a un Folio SIOC, básicamente son generados para los procesos de Auxilio Vial y Atención Médica prehospitalaria, según sea el caso. Cuando existe algún tipo de seguimiento posterior los documentos que se generan son incorporados a dichos expedientes sin que exista ningún tratamiento especial en particular.

Soporte electrónico:

- El Sistema Integral de Operación Carretera SIOC es la herramienta informática implementada para el registro de los servicios otorgados a los usuarios en la red carretera operada por CAPUFE, involucra el seguimiento desde la solicitud a través de una llamada al 074 o servicio generado en el camino, el pulso de la prestación del servicio y hasta su cierre, permitiendo la gestión posterior de los documentos correspondientes a cada servicio.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

-
- El servidor del SIOC se encuentra ubicado en el Centro de Cómputo de Oficinas Centrales, al cual solo tienen acceso las personas autorizadas. Los expedientes físicos se encuentran ubicados en el mismo lugar de trabajo donde se encuentran los operadores responsables que se encuentran en las Bases Operativas, Plazas de Cobro y/o Servicios Médicos en Unidades Regionales.
- Seguridad perimetral exterior:
- Las instalaciones del Organismo cuentan un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:
- Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
- Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
- Todo el acceso peatonal tiene un punto de revisión.
-
- Seguridad perimetral interior
-
- Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
- El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:
-
- Restricción de acceso: El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
- Autorización de acceso: La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
- Registro para el acceso: Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
- Vigilancia: El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:
(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI		NO	X
En caso afirmativo describir:				

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

A) Situaciones previstas en los artículos 22,66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
	No se presenta esta situación		

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	X

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

Nombre del Sistema de Datos Personales:
I.2 PADRÓN DE USUARIOS RESIDENTES A LAS PLAZAS DE COBRO

1. Objetivo:
Registro y administración de los padrones de residentes aledaños a las plazas de cobro.

2. Fundamento Legal: (específico)
Artículo 41, Fracción I, V y VI del Estatuto Orgánico de CAPUFE; y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona usuaria	Identificar a la persona usuaria con la que se tendrá comunicación.
Teléfono de casa y/o celular	Mantener contacto con la persona usuaria.
Correo electrónico.	Mantener contacto con la persona usuaria.
Dirección- domicilio	Contar con la ubicación de la residencia de la persona usuaria

Localidad	Determinar el otorgamiento del beneficio a la persona usuaria
Registro Federal de Contribuyentes (RFC)	Identificar el tipo de contribuyente
Del vehículo(s) involucrado(s):	
Tipo de vehículo	Para la identificación del vehículo
Marca,	Para la identificación del vehículo
Submarca	Para la identificación del vehículo
Modelo	Para la identificación del vehículo
Color	Para la identificación del vehículo
Placas	Para la identificación del vehículo
Número de serie	Para la identificación del vehículo

4. Forma de obtención de los datos personales

(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico	X	No se presenta esta situación	
Formulario electrónico			
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lic. Cynthia Lizeth Cruz Fernández
Cargo	Subdirectora de Servicios al Usuario.
Adscripción	Dirección de Operación
Teléfono y extensión	2073
Correo electrónico institucional	clcruzf@capufe.gob.mx
Funciones	Responsable de los procesos y del sistema • Proponer procedimientos para la prestación de servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido; • Supervisar la operación de la prestación de servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido; • Proponer indicadores para monitorear y evaluar los servicios de auxilio vial, emergencia, asistencia médica prehospitalaria, medios de contacto con las personas usuarias, atención a residentes y pago por recorrido;

Obligaciones	• Deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. • El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. • Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

6. Persona servidora pública Administradora del Sistema:

Datos de la persona servidora pública administradora	
Nombre	Alfredo Fernández Delgado
Cargo	Subgerente de Atención a Residentes
Adscripción	afernandez@capufe.gob.mx
Correo electrónico	Dirección de Operación
Funciones	-Gestionar y coordinar las actividades relacionadas con el Esquema Tarifario de Residentes -Solicitar funcionalidades y requerimientos del Módulo de informático (Portal de Control de Operación). -Seguimiento y Atención de las solicitudes de incorporación, medios de control y nuevas implementaciones, así como del procesamiento de datos
Obligaciones	-Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. -El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. -Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. -Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública operadora	
	Nombre	Lista de Usuarios Operadores del Sistema
	Cargo	Lista de Usuarios Operadores del Sistema
	Funciones	-Recolección de datos a través del formato establecido. -Registro y modificación de datos en el sistema -Acceso y resguardo de expedientes físicos

	Obligaciones	Todas aquellas que apliquen, estipuladas en la LGPDPPSO.

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública	X	Ciudadano (a)		Otro	

Todos los usuarios del sistema informático del padrón de usuarios residentes a las plazas de cobro son personas servidoras públicas.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	X

Descripción:

Soporte físico:

- Expedientes que contienen la información asociada a un usuario residente de una plaza de cobro, se encuentran ubicados en el sitio donde se encuentra el Módulo de Atención a Residentes correspondiente, donde este puede ser en una Plaza de Cobro o en las oficinas de la Unidad Regional correspondiente, el orden puede estar determinado por Clave de Residente o por primer apellido, sin que exista ningún tratamiento especial en particular del expediente.

Soporte electrónico:

- El sistema corresponde actualmente al Portal de Control de Operación (PCO), Sección Residentes, el cual es la herramienta informática implementada para el registro y administración de los padrones de residentes en la red carretera operada por CAPUFE, involucra el registro inicial desde la solicitud, autorizaciones y generación de información para la aplicación operativa, a través de los proveedores, de las listas de tarjetas en carriles.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

El servidor del PCO se encuentra ubicado en el Centro de Cómputo de Oficinas Centrales, al cual solo tienen acceso las personas autorizadas. Los expedientes físicos se encuentran ubicados en los Módulos de Atención a Residentes correspondientes en Unidades Regionales.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

a) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.

b) Para el control de accesos vehiculares, el Organismo cuenta con los "Lineamientos de operación para los estacionamientos de oficinas centrales", en los cuales se establecen las normas y medidas de seguridad a seguirse.
c) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

a) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
b) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

1. **Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
2. **Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
3. **Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
4. **Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:
(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI		NO	X
En caso afirmativo describir:				

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22,66 y 70 de la LGPDPPSO.

Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
No se presenta esta situación		

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	X

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

Nombre del Sistema de Datos Personales:
I.3 SISTEMA DE ATENCIÓN A EXPRESIONES CIUDADANAS (SAEC).

1. Objetivo:
Dar seguimiento a la atención puntual y sistematizada de todas las quejas o cualquier otra expresión ciudadana, asociadas a los servicios que presta el Organismo.

2. Fundamento Legal:
Artículo 41. Fracción X, del ESTATUTO Orgánico de CAPUFE; Lineamiento para la atención de las expresiones ciudadanas recibidas en CAPUFE; y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona física	Identificar a la persona física con la que se tendrá comunicación por correo electrónico.
Teléfono	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
Correo electrónico	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico		No se presenta esta situación	
Formulario electrónico			
Texto libre físico			
Texto libre electrónico	X		

Vía telefónica	X		
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lic. Cynthia Lizeth Cruz Fernández
Cargo	Subdirectora de Servicios al Usuario.
Adscripción	Dirección de Operación
Teléfono y extensión	2073
Correo electrónico institucional	clcruzf@capufe.gob.mx
Funciones	-Fortalecer los medios de contacto con las personas usuarias para mejorar el servicio del Organismo; -Implementar mecanismos para la atención y seguimiento de expresiones ciudadanas
Obligaciones	-Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. -El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera. -Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

6. Persona servidora pública Administradora del Sistema:

Datos de la persona servidora pública administradora	
Nombre	Marisela González Medina
Cargo	Subgerente de Atención del Seguro al Usuario
Adscripción	Dirección de Operación
Correo electrónico	mgonzalezm@capufe.gob.mx
Funciones	-Derivar a los enlaces a través del SAEC las expresiones ciudadanas que interponen las personas usuarias que transitan por los tramos operados por el Organismo. -Seguimiento hasta su conclusión de cada una de las expresiones ciudadanas. -Generación de reportes periódicos acerca de la situación que guardan las expresiones ciudadanas. -Gestionar el mantenimiento del SAEC. -Gestión de nuevas funcionalidades para la mejora continua del sistema y del proceso -Remitir el tiempo y forma las respuestas a las personas usuarias de acuerdo a la Normatividad.
Obligaciones	-Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. -El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

	-Deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. -Todas aquellas que apliquen, estipuladas en la LGPDTPSO.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública operadora	
	Funciones	-Ingresar las expresiones ciudadanas en el Sistema de Atención a Expresiones Ciudadanas, SAEC, captadas por la **Central de Atención a Usuarios (CAU)**, el Órgano Interno de Control y otras áreas. -Revisar diariamente en el SAEC las expresiones ciudadanas que les son derivadas para dar atención en los tiempos establecidos en la normativa. -Emitir las respuestas a las personas usuarias que interpongan algún tipo de expresión ciudadana, a través del SAEC.
	Obligaciones	Todas aquellas que apliquen, estipuladas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública		Ciudadano (a)		Otro	

Todos los usuarios del sistema SAEC son servidores públicos

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	X

Descripción:

Soporte físico:

- Expedientes que contienen la información asociada a la expresión ciudadana atendida por los enlaces designados tanto en las Oficinas Centrales como en las Unidades Regionales, según sea el caso. Cuando existe algún tipo de seguimiento posterior, los documentos que se generan son incorporados a dichos expedientes sin que exista ningún tratamiento especial en particular.

Soporte electrónico:

- El Sistema de Atención a Expresiones Ciudadanas SAEC es la herramienta informática implementada para el registro de la atención a las expresiones ciudadanas de las personas usuarias de las redes carreteras operadas por CAPUFE, involucra el seguimiento desde la captación de dichas expresiones que pueden ser quejas, felicitaciones, comentarios o sugerencias en su caso, relacionadas a la prestación de los servicios que presta el Organismo.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

El servidor del SAEC se encuentra ubicado en el Centro de Cómputo de Oficinas Centrales, al cual sólo tienen acceso las personas autorizadas. Los expedientes físicos se encuentran ubicados en el mismo lugar de trabajo donde se encuentren los enlaces responsables, que puede ser en Oficinas Centrales u oficinas de las Unidades Regionales.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

d) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
e) Para el control de accesos vehiculares, el Organismo cuenta con los "Lineamientos de operación para los estacionamientos de oficinas centrales", en los cuales se establecen las normas y medidas de seguridad a seguirse.
f) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

c) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
d) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

5. **Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
6. **Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
7. **Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
8. **Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:
(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI		NO	X
En caso afirmativo describir:				

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
	No se presenta esta situación		

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	X

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

Nombre del Sistema de Datos Personales:
I.4 PADRÓN DE USUARIOS EXENTOS DE TELEPEAJE EN PLAZAS DE COBRO

1. Objetivo:
Es el control de todos los vehículos con pase exento que utilizan el Sistema de Identificación Automática Vehicular, cruzando por las plazas de cobro autorizadas de pase exento.

2. Fundamento Legal: (específico)
Artículos 91, párrafo I, inciso G, 92, 112 al 131, Compendio Operativo para Plazas de Cobro; Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona funcionaria pública	Para otorgar el pase exento y contar con su registro

Identificación	Para acreditar personalidad
Dirección	Para justificar la necesidad del cruce exento
Centro de trabajo	Para acreditar su pertenencia laboral
Dirección administrativa	Lo identifica en el área en la que labora
Adscripción	Unidad Administrativa a la que pertenece
Correo electrónico	Para intercambio de información
Teléfono y extensión	Para intercambio de información
Vehículo registrado: marca, submarca, modelo, número de serie, color, número de motor	Para el control de los vehículos que cruzan por las plazas de Cobro autorizadas

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico	X	No se presenta esta situación	
Formulario electrónico	X		
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lic. Martha Icsel Prieto Martínez
Cargo	Subdirectora de Sistemas Electrónicos de Peaje
Adscripción	Dirección de Operación
Teléfono y extensión	7773292100 extensión 2117
Correo electrónico institucional	mprietom@capufe.gob.mx
Funciones/perfil	-Supervisar la atención de los servicios a los usuarios de medios electrónicos de pago, así como de usuarios residentes y de exentos, a fin de que la empresa administradora del servicio otorgue un servicio de calidad. -Supervisar la vigilancia de la aplicación de los lineamientos establecidos para vehículos exentos de pago, con el fin de mantener un control de los mismos. -Establecer las disposiciones normativas en materia de operación, otorgamiento de servicios al usuario, seguridad y protección civil, a fin de asegurar el funcionamiento de las plazas de cobro y la seguridad y salvaguarda del Organismo.
Obligaciones	Determinar los mecanismos de capacitación de personal el tratamiento de protección de datos personales.

6. Persona servidora pública Administradores del Sistema:

Datos de la persona servidora pública administradora	
Nombre	Lic. Judith Sosa Limón
Cargo	Gerente de Sistemas Electrónicos de Pago
Adscripción	Dirección de Operación
Correo electrónico institucional	jsosal@capufe.gob.mx
Funciones	• Supervisar la atención de los servicios a los usuarios de medios electrónicos de pago, así como de usuarios residentes y de exentos, a fin de que la empresa administradora del servicio otorgue un servicio de calidad. • Supervisar la vigilancia de la aplicación de los lineamientos establecidos para vehículos exentos de pago, con el fin de mantener un control de los mismos. • Establecer las disposiciones normativas en materia de operación, otorgamiento de servicios al usuario, seguridad y protección civil, a fin de asegurar el funcionamiento de las plazas de cobro y la seguridad y salvaguarda del Organismo.
Obligaciones	Autorizar y remitir consolidado de los cruces firmados mediante un oficio de vehículos exentos.

7. Persona servidora pública Operadora del Sistema:

Datos de la persona servidora pública operadora	
Nombre	María del Pilar Jiménez Carrillo
Cargo	Subgerente de Control de Operaciones y Medios Electrónicos de Pago
Adscripción	Dirección de Operación
Correo electrónico institucional	pjimenez@capufe.gob.mx
Funciones	-Administrar los catálogos de pase exento del personal operativo del sindicato. -Supervisar la validación y conciliación de cruces de los usuarios vehículos, para la operación y conservación y vehículos especiales libres de pago de peaje. -Verificar en el Portal de Control de Operación (PCO) el estado del registro y de la autorización, de toda solicitud de activación / desactivación de tarjeta que reciba por parte de los encargados del Padrón de Usuarios Exentos de Telepeaje en Plazas de Cobro. -Gestionar ante el proveedor, toda activación y desactivación necesaria en atención a las solicitudes recibidas por los encargados del Padrón de Usuarios Exentos de Telepeaje en Plazas de Cobro. -Atender toda solicitud referente al proceso administrativo que requieran los Encargados o Encargadas del Padrón de Usuarios Exentos de Telepeaje en Plazas de Cobro.

	-Obtener del PCO, las actualizaciones a los padrones de Empleados o Empleadas inscritos al Padrón de Usuarios Exentos de Telepeaje en Plazas de Cobro, registradas por los encargados o encargadas a nivel regional para los posteriores procesos de conciliación con el proveedor. -Gestionar periódicamente ante el concesionario las autorizaciones de todas las solicitudes y actualizaciones de registros del padrón, reflejados en el PCO. Entregar al administrador del PCO las listas con los registros de autorizaciones aprobadas por el concesionario, para reflejar dichas autorizaciones en los registros correspondientes del padrón
Obligaciones	Autorizar y remitir consolidado de los cruces firmados mediante un oficio de vehículos exentos.

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública	X	Ciudadano (a)		Otro	

Descripción:

Datos de la persona servidora pública usuaria	
Nombre	Documento correspondiente
Cargo	
Adscripción	
Funciones	Registro y actualización de información de exentos, así como la validación de los cruces registrados
Obligaciones	-Revisar y validar los cruces de vehículos exentos -Autorizar y remitir consolidado de los cruces firmados mediante un oficio.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	X

Descripción:

Descripción del soporte físico:

- Expedientes que contienen: Solicitud para la Obtención de Pase Libre de Pago de Peaje por PC Empleados Sindicalizados, copia de comprobante de domicilio vigente, copia de identificación vigente, copia del último recibo de nómina y copia de factura, carta factura o documento del vehículo que utilizará.
- El expediente físico tiene un número de empleado como control, mismo que es generado cuando es dado de alta administrativamente por el área de Recursos Humanos.

Descripción del soporte electrónico:

- El Portal de Control de Operación (PCO) es la herramienta informática implementada para el registro en línea de los padrones de empleados inscritos al programa Pase Exento y actualizaciones a los mismos.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

Características del lugar donde se resguardan los soportes:

- El servidor del Portal de Control de Operación (PCO) se encuentra ubicado en el Centro de Cómputo de Oficinas Centrales. Los módulos para la atención de empleados inscritos Padrón de Usuarios Exentos de Telepeaje en Plazas de Cobro, se encuentran ubicados en la unidad y/u oficina que determine la Subgerencia de Operación.
- El acceso al Centro de Cómputo, está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
- Los expedientes físicos se encuentran ubicados en las unidades regionales correspondientes, así como en el Archivo de Concentración.

Resguardo de sistemas de datos personales con soportes físicos:

- Las medidas de seguridad implementadas a los soportes físicos evitan la alteración, pérdida y acceso no autorizado a los mismos, de la siguiente manera:

Archivo de trámite

a) Los expedientes se resguardan en estantes que cuentan con cerradura y sólo el personal autorizado cuenta con llaves para accederlos.
b) Los estantes se encuentran identificados en áreas con aire acondicionado para controlar la temperatura, y humedades adecuadas.
c) Las áreas de resguardo cuentan con sistemas de extinción de incendios, los cuales son verificados y en su caso recargados cada 6 meses.
d) Los edificios cuentan con mecanismos para regular y mantener el suministro de energía eléctrica.

- Se cuenta con una lista de las personas que tiene acceso a los soportes físicos.

Bitácoras para accesos y operación cotidiana:

- Existe un documento formal mediante el cual el responsable del sistema lleva un estricto control y registro de las autorizaciones emitidas para facultar el acceso a una persona servidora pública a fin de que ésta, en el ejercicio de sus funciones, pueda interactuar con el SDP. Se mantienen bitácoras en las que se registra:

a) Cuenta de usuario que accede al SDP, la fecha y hora del acceso, así como las transacciones que fueron ejecutadas, así como la fecha y hora de salida.

b) Para los soportes físicos se registra mediante bitácora u oficio y minutario el expediente utilizado, en donde se incluye la fecha del préstamo y el nombre de la persona a quien se realiza el préstamo del expediente. La consulta de expedientes del archivo de concentración e histórico es asistido por un sistema de cómputo que utiliza códigos de barras en los expedientes.
c) Para los soportes electrónicos se mantienen registros sobre las acciones llevadas a cabo por el usuario dentro del Sistema de Datos Personales. El área de informática lleva el control y registro de las bitácoras de eventos ocurridos a nivel sistema operativo en los equipos que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor; accesos de usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.

- Se cuenta con bitácoras físicas para el control de los soportes físicos; y electrónicas para aquellos con soporte electrónico.
- Las bitácoras físicas son almacenadas en los lugares de trabajo de la persona encargada del manejo de bitácoras del SDP. Las bitácoras electrónicas residen en los equipos de cómputo en donde se alojan los SDP. Ambas se almacenan por el tiempo especificado en el Catálogo de Disposición Documental del Organismo.
- Para asegurar la integridad de las bitácoras, las que se mantienen en soportes físicos se resguardan bajo llave por el encargado de las bitácoras del Sistema de Datos Personales, y las electrónicas se respaldan junto con el Sistema de Datos Personales.
- Respecto del análisis de las bitácoras:
  a) Las bitácoras son analizadas frecuentemente por el encargado de bitácoras del SDP.
  b) Las bitácoras en soporte electrónico son analizadas de forma manual con las opciones provistas por el SDP.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

g) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
h) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
i) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

e) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
f) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

9. **Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
10. **Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las

	personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
11.	**Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
12.	**Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:
(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI	X	NO	
En caso afirmativo describir:				

- Eventualmente se realizan transmisiones mediante el traslado sobre redes electrónicas, de la siguiente manera:

a) El envío se realiza a través de la Unidad de Correspondencia.
b) Se utiliza un sobre engrapado, sellado con Diurex y firmado entre el Diurex y el sobre.
c) El sobre se entrega en el área designada por la persona destinataria.
d) En el sobre se incluye una etiqueta con instrucciones para informar si el sobre ha sido violado.
e) En cada transmisión se recaba el acuse de recibo con el sello del área destinataria y la fecha de recibido.
f) El envío de cada transmisión se documenta mediante oficios del área emisora, los cuales se registran en bitácora de tipo minutario.
g) El archivo electrónico que contiene datos personales no es cifrado antes de su envío. Se entrega en el formato y con las medidas de seguridad establecidas por la persona destinataria.

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
No se presenta esta situación		X

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI X		NO	

Se comparte información con Banco Nacional de Obras y Servicios Públicos, S.N.C. (BANOBRAS), de acuerdo a los "Lineamientos para la Identificación de Vehículos que no Pagan Peaje" en el lineamiento Quinto. Vehículos libres de peaje, numeral II inciso f, Artículos 92 y 112 del Compendio Operativo para Plazas de Cobro.

Nombre del Sistema de Datos Personales:
I.5 LÍNEA EXPRÉS

1. Objetivo:
Es la gestión de membresías para cruces Exprés en los puentes internacionales.

El sistema de Línea Exprés permite capturar datos personales de la persona usuaria con la finalidad de que ésta pueda realizar un pago referenciado en el banco. Una vez efectuado el pago, con estos datos se opera el alta, renovación y reposición en el sistema SIAC y a su vez generar la factura correspondiente por el concepto que determinó el usuario en la página web.

2. Fundamento Legal: (específico)
Compendio operativo para las plazas de cobro, Titulo Sexto Línea Exprés; Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona física	Identificar a la persona física con la que se tendrá comunicación por correo electrónico.
Domicilio	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
Teléfono particular	Mantener contacto con la persona con la que se tendrá comunicación vía teléfono.
Teléfono celular particular	Mantener contacto con la persona con la que se tendrá comunicación vía teléfono.
Correo electrónico	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
Firma	Aceptación de los requisitos y condiciones del servicio.
Fotografía	Identificación para la prestación del servicio
RFC	Facturación de la Línea Exprés
Credencial GOES	Tarjeta de identificación por el gobierno de E.U para el uso de la Línea SENTRI (Sentri-card)
Datos Patrimoniales del vehículo	

Datos del Vehículo	Marca, Submarca, Modelo y Placas. Identificar el vehículo.

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico	x	No se presenta esta situación	
Formulario electrónico	x		
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lic. Martha Icsel Prieto Martínez
Cargo	Subdirectora de Sistemas Electrónicos de Peaje
Adscripción	Dirección de Operación
Teléfono y extensión	7773292100 extensión 2117
Correo electrónico institucional	mprietom@capufe.gob.mx
Funciones	-Coordinar y supervisar la captación de ingreso por concepto de peaje, de acuerdo a la tarifa autorizada y el aforo registrado en las plazas de cobro. - Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
Obligaciones	-Coordinar y supervisar que los distintos esquemas tarifarios, en sus distintas modalidades, sean aplicados en las plazas de cobro autorizadas de conformidad con la normatividad establecida. -Determinar los mecanismos de capacitación de personal el tratamiento de protección de datos personales.

6. Persona servidora pública Administradores del Sistema:

Id	Datos de la persona servidora pública administradora	
1	Nombre	Jose Luis Marquez Jaimes
	Cargo	Subgerente de Desarrollo de Proyectos de Interoperabilidad
	Adscripción	Gerencia de Interoperabilidad y Nuevas Tecnologías de Operación
	Funciones	Coordinar y desarrollar la viabilidad de los proyectos de las Línea Exprés y/o Sentri, con el objeto de estandarizar su operación.
	Obligaciones	Elaboración de Documento de Seguridad y Aviso de Privacidad de Línea Exprés

2	Nombre	Eduardo Yamanaka Sámano
	Cargo	Subgerente de Administración de Sistemas de Peaje
	Adscripción	Subdirección de Tecnologías de Información
	Funciones	Administrador de Base de datos (DBA), es el encargado de respaldar la base de datos de acuerdo a los esquemas definidos en su área, así como de brindar apoyo técnico.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
3	Nombre	Carlos Arias Ortiz
	Cargo	Subgerente de Operación del SIAC
	Adscripción	Subdirección de Tecnologías de Información
	Funciones	Coordinar, administrar y dar soporte a la operación del SIAC (SAP), encargado del área de desarrollo y soporte técnico al sistema.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública operadora	
1	Nombre	Guillermo Dionisio Ramos Almanza
	Cargo	Subgerente de Administración (Unidad Regional Reynosa).
	Funciones	Encargado del soporte técnico relacionado a redes y datos de informática y telecomunicaciones en Línea Exprés a fin de garantizar su operación.
	Obligaciones	Administrar de Base de datos (DBA) de Línea Express.
2	Nombre	Ángel Aurelio Figueroa
	Cargo	Subgerente de Ingresos
	Funciones	Es el encargado de las normas, lineamientos y procedimientos de pago Línea Exprés.
	Obligaciones	Administrar de Base de datos (DBA) de Línea Express.

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública	x	Ciudadano (a)		Otro	

Descripción:

Id	Datos de la persona servidora pública usuaria	
1	Nombre	Sofía Mascareñas Ruiz
	Cargo	Cajera Receptor (Unidad Regional Reynosa -PC 37 Línea Exprés Reynosa-Hidalgo)
	Funciones	Coordinar y supervisar que los distintos esquemas tarifarios, en sus distintas modalidades, sean aplicados en las plazas de cobro autorizadas de conformidad con la normatividad establecida.
	Obligaciones	Encargado de atender a los usuarios en oficina para los tres trámites: Contratación, Renovación y Sustitución; capturar las

		altas de los usuarios en el sistema SIAC, así como entrega de la factura respectiva; recepción de documentación del usuario referente a su trámite para la creación de su expediente digital en sistema.
2	Nombre	Jose Luis Lozano Ibarra
	Cargo	Cajero Receptor (Unidad Regional Reynosa -PC 37 Línea Exprés Reynosa-Hidalgo
	Funciones	Coordinar y supervisar que los distintos esquemas tarifarios, en sus distintas modalidades, sean aplicados en las plazas de cobro autorizadas de conformidad con la normatividad establecida.
	Obligaciones	Encargado de atender a los usuarios en oficina para los tres trámites: Contratación, Renovación y Sustitución; capturar las altas de los usuarios en el sistema SIAC, así como entrega de la factura respectiva; recepción de documentación del usuario referente a su trámite para la creación de su expediente digital en sistema.
3	Nombre	Bertha Ivonne González Larumbe
	Cargo	Cajero Receptor (Unidad Regional Reynosa -PC 66 Línea Exprés Juárez-Lincoln)
	Funciones	Coordinar y supervisar que los distintos esquemas tarifarios, en sus distintas modalidades, sean aplicados en las plazas de cobro autorizadas de conformidad con la normatividad establecida.
	Obligaciones	Encargado de atender a los usuarios en oficina para los tres trámites: Contratación, Renovación y Sustitución; capturar las altas de los usuarios en el sistema SIAC, así como entrega de la factura respectiva; recepción de documentación del usuario referente a su trámite para la creación de su expediente digital en sistema.
4	Nombre	Roberto Rubí Frayre
	Cargo	Cajero Receptor (Unidad Regional Reynosa -PC 66 Línea Exprés Juárez-Lincoln)
	Funciones/Perfil	Coordinar y supervisar que los distintos esquemas tarifarios, en sus distintas modalidades, sean aplicados en las plazas de cobro autorizadas de conformidad con la normatividad establecida.
	Obligaciones	Encargado de atender a los usuarios en oficina para los tres trámites: Contratación, Renovación y Sustitución; capturar las altas de los usuarios en el sistema SIAC, así como entrega de la factura respectiva; recepción de documentación del usuario referente a su trámite para la creación de su expediente digital en sistema.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	**X**

Descripción:

Soporte físico:

- Expedientes que contienen: Formato Carta de aceptación del servicio donde vienen los datos personales que otorga la persona usuaria, así como su firma y leyenda de descripción del tratamiento de los datos personales.

Soporte electrónico:

- Se capturan en línea los datos personales con la finalidad de que la persona usuaria pueda realizar un pago referenciado en el banco o pago con tarjeta de crédito en línea y/o TPV (Terminal Punto de Venta). Una vez efectuado el pago, con estos datos se genera su factura por el concepto capturado en la página web.
- Los expedientes digitalizados son entregados por la persona usuaria a través de USB en formato PDF de todos los documentos presentados en ventanilla (copia de credencial de elector, Copia de credencial GOES, Tarjeta de circulación, Comprobante de pago referenciado - en su caso.) se lleva así un control y validación de las personas / vehículos que acreditan ser merecedores a una Línea Exprés.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

- **Características del lugar donde se resguardan los soportes físicos**

a) Los expedientes físicos se encuentran resguardados en archiveros bajo llave de la persona encargada de la Línea Exprés de las plazas de cobro donde se realiza el trámite respectivo: Nuevo Laredo - Laredo (Juárez – Lincoln) y Reynosa – Hidalgo (Puente Reynosa).
b) Los expedientes que estén en el Archivo de trámite se resguardan en estantes de acceso controlado, los cuales cuentan con cerradura y sólo el personal autorizado cuenta con llaves para accederlos.
c) Las áreas de resguardo cuentan con sistemas de extinción de incendios, los cuales son verificados y en su caso recargados cada 6 meses.
d) Los edificios cuentan con mecanismos para regular y mantener el suministro de energía eléctrica.

- **Características del lugar donde se resguardan los soportes electrónicos:**

a) Los archivos electrónicos del sistema de Línea Exprés se encuentran ubicados en el Centro de Cómputo de Oficinas Centrales.
b) Los expedientes digitalizados se encuentran resguardados en un disco duro en las plazas de cobro donde se realiza el trámite respectivo: Nuevo Laredo - Laredo (Juárez – Lincoln) y Reynosa – Hidalgo (Puente Reynosa) y al término de la jornada diaria se resguarda bajo llave por el encargado del Módulo de LINEXP.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

j) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
k) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
l) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

g)	Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
h)	El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:
13.	**Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
14.	**Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
15.	**Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
16.	**Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI	**X**	NO	
En caso afirmativo describir:				

- **Eventualmente se realizan transmisiones mediante el traslado sobre redes electrónicas, de la siguiente manera**:

a) Se envía información mediante correo electrónico a la Subdirección de Finanzas. Los archivos electrónicos que contienen datos personales se compactan antes de su envío mediante una contraseña. Una vez que se transfiere la información por correo electrónico, se intercambia un correo electrónico adicional o bien una llamada telefónica para entregar la contraseña de descompactación.
b) Se utiliza Internet como el canal para las transmisiones, con el protocolo de transmisión "Simple Mail Transfer Protocol (SMTP)".
c) El remitente cuenta con un dispositivo tipo IPS (Intruder Prevention System) para detectar intrusiones en el canal de comunicaciones.
d) El destinatario envía correo electrónico con acuse de recibo de la información transmitida.
e) El envío de cada transmisión se documenta mediante oficios del área emisora, los cuales se registran en bitácoras de tipo minutario.
f) La transmisión de datos vía web se realiza mediante un canal seguro, el sistema utiliza el protocolo de comunicación https contando con un certificado SSL.

g) La transmisión de datos mediante el sistema SIAC se realiza a través de la intranet del Organismo. h) La transmisión de datos personales es de conformidad con el Artículo 35, Fracción VI de la LGPDPPSO.

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO x	

A) Situaciones previstas en los artículos 22,66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22,66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
	No se presenta esta situación		

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO X	

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

Nombre del Sistema de Datos Personales:
I.6 PADRÓN DE USUARIOS DEL SISTEMA DE INDENTIFICACIÓN AUTOMÁTICA VEHICULAR IAVE.

1. Objetivo:
El Padrón de Usuarios del Sistema de Identificación Automática Vehicular IAVE tiene el objetivo de brindar servicio correcto y seguro a las personas usuarias de Telepeaje interoperable a nivel nacional.

2. Fundamento Legal:
Artículo 42 sección XIV y XV del Estatuto Orgánico de CAPUFE, y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona usuaria	Identificar a la persona usuaria con la que se tendrá comunicación por teléfono y correo electrónico.

Nacionalidad de la persona usuaria.	Identificar a la persona usuaria con la que se tendrá comunicación por teléfono y correo electrónico en el idioma adecuado.
Número de identificación oficial.	Validar la legitimidad de identidad de la persona usuaria.
Datos fiscales, solo en caso de requerir factura.	Para estar en facultad de generar la factura del bien y/o servicio.
Teléfono de casa y/o celular.	Mantener contacto con la persona con la que se tendrá comunicación vía telefónica.
Correo electrónico	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
Datos de tarjeta de crédito o débito bancaria en caso de esquema post-pago.	Para poder realizar los cargos por concepto de bien y/o servicio.
Registro de vehículo: tipo de vehículo a registrar (automóvil, motocicleta, autobús y camión con su número de ejes) y placa.	Para definir el cobro correspondiente por cruce de plaza de cobro. La placa es para validar el registro con los datos del vehículo.

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico		No se presenta esta situación	
Formulario electrónico	**X**		
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Lic. Martha Icsel Prieto Martínez
Cargo	Subdirectora de Sistemas Electrónicos de Peaje
Adscripción	Dirección de Operación
Teléfono y extensión	7773292100 extensión 2117
Correo electrónico institucional	mprietom@capufe.gob.mx
Funciones/perfil	- Diseñar y proponer a la Dirección o a la persona servidora púbica titular de la Dirección de Operación las Normas, reglamentos, políticas y Procedimientos para la prestación de los Servicios al Usuario. - Supervisar la operación de los servicios al usuario brindada por el Centro de Atención Telefónica de Telepeaje de CAPUFE.

Obligaciones	--Supervisar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. -Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales. -Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado.

6. Persona servidora pública Administradora del Sistema:

Datos de la persona administradora	
Nombre	Lic. Miguel Hernandez Enríquez
Cargo	Gerente de Comercialización IAVE
Adscripción	Subdirección de Sistemas Electrónicos de Peaje
Funciones/Perfil	-Administrar y gestionar el mantenimiento y mejoras al Sistema de Identificación Automática Vehicular IAVE, única fuente de datos válida para la actualización de padrones de usuarios del Sistema de Identificación Automática Vehicular IAVE. -Recepción y validación de la documentación. -Coordinar con el área de Transparencia diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.
Obligaciones	-Asegurar la integridad del contenido electrónico del Padrón de Usuarios del Sistema de Identificación Automática Vehicular IAVE. -Vigilar que el padrón sea confiable, actualizado y sustentado con la información necesaria.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona operadora	
	Nombre	Judith Robles Iturbe
	Cargo	Superintendente F
	Adscripción	Subdirección de Sistemas Electrónicos de Peaje
	Funciones/Perfil	-Apoyo y seguimiento de los usuarios carreteros para el registro en el del Sistema de Identificación Automática Vehicular IAVE. -Encargada del adecuado funcionamiento del CATT respecto al tratamiento de los datos personales.
	Obligaciones	-Verificar que los servicios que proporciona el CATT a los usuarios de CAPUFE, se otorguen de acuerdo a las normas establecidas y con la máxima calidad. -Adoptar las medidas necesarias para garantizar la seguridad, confidencialidad, integridad, confiabilidad y disponibilidad de los datos personales y evitar su alteración pérdida, transmisión y acceso no autorizado

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública		Ciudadano (a)		Otro	

Id	Datos de la persona usuaria	
	Nombre	Katalina de la Paz Oteo
	Cargo	Supervisor B
	Nombre	Marcos Martínez Castillo
	Cargo	Superintendente D
	Nombre	Ana Laura Montero Escobar
	Cargo	Asistente Ejecutivo
	Nombre	Amelia Sanchez Flores
	Cargo	Técnico Especializado
	Nombre	Federico Reséndiz Cárdenas
	Cargo	Analista Especializado

Descripción:

- Personas encargadas de asesorar a las personas usuarias por medio del CATT, considerando actualización, activación, cancelación, recargas y descarga de facturación, dentro del Sistema de Identificación Automática Vehicular IAVE.
- Soporte para personas usuarias en la adquisición de nuevas Tags IAVE.
- Realizar asesoría con respecto al fondo de garantía.
- Dar información con respecto al Sistema de Identificación Automática Vehicular IAVE.
- Transferir los casos al área correspondiente en la administración de CAPUFE, en casos como cambios de modalidad de pago, validaciones de tarjetas, listas negras, saldos no reconocidos, referencias bancarias, estados de cuenta, actualizaciones de cuenta, cruces duplicados o no reconocidos, Diferencias de tarifa, pagos duplicados, devolución de fondos en garantía, problemas con Tags, residentes, línea exprés y línea Sentri.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico	**X**	Físico		Combinado	

Descripción:

El Sistema de Identificación Automática Vehicular IAVE es la herramienta informática implementada para el registro en línea, tiene un formulario donde se registran los datos personales y las actualizaciones a los mismos, así como para el control de datos. Esta base de datos está en el servidor del Centro de Cómputo de las oficinas centrales del organismo.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

El servidor del Sistema de Identificación Automática Vehicular IAVE se encuentra ubicado en el Centro de cómputo de Oficinas Centrales, el cual cuenta con estrictos sistemas de acceso de seguridad y únicamente accede el personal autorizado.

- **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales**
  a) El SDP mantiene un manejo riguroso de perfiles de usuarios(as) y contraseñas.
  b) Las contraseñas son cifradas por el Sistema de Datos Personales, de tal forma que no es posible descifrarlas aun accediendo a la base de datos.

- **Administración de perfiles de usuario y contraseñas**
  a) El responsable del SDP es quien autoriza la creación de nuevos perfiles en el Sistema de Datos Personales, los cuales son creados con base en las necesidades de los diversos procesos que se manejan en el sistema.
  b) El registro de la creación de nuevos perfiles se mantiene mediante los oficios de solicitud de los usuarios.
  c) Cada usuario(a) será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

- **Acceso remoto al sistema de datos personales**
  a) El acceso remoto se controla a dos niveles: físico, con permisos vía IP en el firewall; y lógico, con usuario y contraseña tanto del sistema operativo como de los componentes de software que lo conforman.
  b) Para evitar el acceso remoto no autorizado se maneja a través de un estricto procedimiento de asignación y autorización de solicitudes de VPN e IP del servidor a donde acceder.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

m) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
n) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
o) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

i) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
j) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

17.	**Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
18.	**Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
19.	**Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
20.	**Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	SI		NO	**X**
En caso afirmativo describir				

Transmisión	SI	**X**	NO	
En caso afirmativo describir:				
Se realizan transmisiones mediante soportes electrónicos cifrados con datos de cuenta Bancaria hacia banco receptor.				

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el sistema, transfiriendo la cuenta bancaria de la persona usuaria del servicio hacia el banco receptor:	SI **X**		NO	

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
	Entidades financieras	Cobro de transacción(es)	Si, mediante la aceptación de términos y condiciones del contrato de adhesión al sistema de telepeaje a través de medios electrónicos.

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO **X**	

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

II. Dirección Jurídica

Nombre del Sistema de Datos Personales:

II.1 REPRESENTANTES DE PERSONAS MORALES QUE CONTRATAN CON CAPUFE SERVICIOS DE ADMINISTRACIÓN, OPERACIÓN Y CONSERVACIÓN DE TRAMOS CARRETEROS Y PUENTES DE CUOTA.

1. Objetivo:
Reunir la documentación legal de los representantes legales de las personas morales que celebren contratos con Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE), para efectos de la elaboración del instrumento contractual correspondiente.

2. Fundamento Legal (específico):
Artículos 27, fracción XII, 35, fracciones IX y X y 47, fracciones III y IV del Estatuto Orgánico de CAPUFE; 45, fracción IV de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 1802 del Código Civil Federal, deberá contar con la acreditación de la personalidad de aquellas personas físicas que como representantes legales de personas morales celebren contratos con la Entidad; y los Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

De las personas físicas (representante legal):

Dato personal	**Idoneidad (informar para que se recaba el dato)**
Nombre completo	Elaboración e integración del instrumento contractual
Identificación oficial	
Dirección electrónica	
Firma	
Teléfono	

De las personas morales:

Dato personal	**Idoneidad (informar para que se recaba el dato)**

Domicilio fiscal	Elaboración e integración del instrumento contractual
Registro Federal de Contribuyentes (RFC)	
Dirección electrónica	
Teléfono	
Nacionalidad	

4. Forma de obtención de los datos personales:

Directa	x	**Indirecta** (Aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por la persona responsable sobre los datos personales proporcionados directamente por el titular en algún otro sistema)	
Formulario físico			
Formulario electrónico			
Texto libre físico	x		
Texto libre electrónico	x		
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Adolfo Amylkar Mateos Medina
Cargo	Subdirector Jurídico Consultivo
Adscripción	Dirección Jurídica
Teléfono y extensión	(777) 329 2100 Ext. 2034
Correo electrónico institucional	aamateosm@capufe.gob.mx
Funciones	Responsable del tratamiento de datos personales de los representantes de personas morales que contratan con CAPUFE servicios de administración, operación y conservación de tramos carreteros y puentes de cuota y de los representantes de las Fiduciarias, de los Fideicomitentes y Fideicomisarios en los Fideicomisos que cuentan con la participación de CAPUFE y demás funciones establecidas en el numeral 1.3.1.- Subdirección Jurídica Consultiva del Manual General de Organización de CAPUFE.
Obligaciones	-Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. -Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos. -Informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. -En caso de que ocurra una vulneración a la seguridad, deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el

	tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

6.- Persona servidora pública Administradora del Sistema:

Nombre	Cielo Eunice Marure Araniegues
Cargo	Subgerente de Fideicomisos y Procedimientos Legales
Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
Teléfono y extensión	(777) 329 2100 Ext. 3128
Correo electrónico institucional	cemarure@capufe.gob.mx
Funciones/perfil	Formular proyectos de convenios y contratos en materia de prestación de servicios de la infraestructura carretera concesionada que administra y opera el Organismo conforme a las disposiciones normativas de CAPUFE, con objeto de que se fijen de manera cierta y conveniente los derechos y obligaciones que adquiere este descentralizado frente a terceros y demás funciones establecidas en el numeral 1.3.0.0.1.- Subgerencia de Fideicomisos y Procedimientos Legales del Manual General de Organización de CAPUFE.
Obligaciones	-Mantener actualizado el sistema. -Determinar a las personas servidoras públicas que deban tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos. -Autorizar los accesos de las personas servidoras públicas, determinar los privilegios y limitantes y llevar un registro de los mismos. -Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

7. Persona servidora pública Operadora del Sistema:

N°	Datos de la persona operadora	
1	Nombre	Jesús León Landa
	Cargo	Asistente de Proyectos
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
	Funciones/perfil	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma.
2	Nombre	Perla Karina Bahena Mendoza
	Cargo	Analista Especializado
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales

	Funciones	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma.
3	Nombre	Brenda Hernández Yañez
	Cargo	Superintendente A
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
	Funciones	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma.

8. Tipos de soportes

(Señalar con una X, según corresponda)

Electrónico		**Físico**		**Combinado**	**X**

Descripción:

Expedientes de contratos que contienen la siguiente documentación: contrato de fideicomisos; convenio (s) modificatorio (s) a los contratos de fideicomisos; escrituras públicas con las que se acredita la representación y facultades de las personas que suscriben los contratos y convenios; oficios y/o comunicados mediante los cuales se notifica del cambio de representantes legales de las fiduciarias, de los fideicomitentes y fideicomisarios, en los fideicomisos que cuentan con la participación de CAPUFE y que también contienen datos personales como el nombre completo, domicilio, teléfono, correo electrónico, firma, RFC, CURP, credencial para votar, etc.

Físico: Los expedientes físicos se encuentran ubicados en las oficinas de la Subdirección Jurídica Consultiva. Específicamente en los archiveros 1, 2, 3, 4, y 5 correspondientes a la Subgerencia de Fideicomisos y Procedimientos Legales.

Electrónico: Archivos de Word, PDF y Excel, que contienen diversos datos personales, los cuales se encuentran resguardados en los equipos de cómputo asignados al personal del área, mismos que se encuentran protegidos mediante una contraseña de acceso, de los cuales únicamente el personal adscrito al área puede acceder a ellos.

9. Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales.

Los expedientes físicos se resguardan en archiveros metálicos ubicados en oficinas centrales (Subdirección Jurídica Consultiva) mismos que cuentan con cerradura y sólo el personal autorizado cuenta con llaves para accederlos.

Los archiveros se encuentran identificados en áreas con aire acondicionado para controlar la temperatura y humedad adecuadas.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

a) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año, (en términos del Compendio de Seguridad y Protección Civil de CAPUFE).
b) Para el control de accesos vehiculares, el Organismo cuenta con los "Lineamientos de operación para los estacionamientos de oficinas centrales", en los cuales se establecen las normas y medidas de seguridad a seguirse.
c) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

a) Acceso controlado.
b) Las oficinas centrales del Organismo cuentan con Cámaras de circuito cerrado.
c) Cuenta con mecanismos para regular y mantener el suministro de energía eléctrica.

- **Acceso a las instalaciones del proveedor:**
  El acceso a las instalaciones del proveedor se realiza de acuerdo a las políticas de seguridad para la protección de la infraestructura del cómputo y comunicaciones del Organismo, a las instalaciones de su centro de datos.

10.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	**SI**		**NO**	**X**
En caso afirmativo, describir				

Transmisión	**SI**		**NO**	**X**
En caso afirmativo, describir				

11.- Transferencia de datos:

(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

12. Persona Encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	X

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

Nombre del Sistema de Datos Personales:

II.2 REPRESENTANTES DE LAS FIDUCIARIAS, DE LOS FIDEICOMITENTES Y FIDEICOMISARIOS EN LOS FIDEICOMISOS QUE CUENTAN CON LA PARTICIPACIÓN DE CAPUFE.

1.-Objetivo:
Reunir la documentación legal de los representantes de las Fiduciarias, de los Fideicomitentes y Fideicomisarios en los Fideicomisos que cuentan con la participación de CAPUFE.

2. Fundamento Legal (específico)
Artículos 27, fracción XII, 35, fracciones IX y X y 47, fracciones III, IV y XII del Estatuto Orgánico de CAPUFE; 381 a 393 de la Ley General de Títulos y Operaciones de Crédito, deberá contar con la acreditación de la personalidad de aquellos representantes de las Fiduciarias, de los Fideicomisos y/o Fideicomitentes en los fideicomisos que cuentan con la participación de la Entidad; y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:
De las personas físicas (representante legal)

Dato personal	**Idoneidad (informar para que se recaba el dato)**
Nombre completo	Elaboración e integración del instrumento contractual
Identificación oficial	
Dirección electrónica	
Firma	
Teléfono	

De las personas morales

Dato personal	**Idoneidad (informar para que se recaba el dato)**
Domicilio fiscal	Elaboración e integración del instrumento contractual
Registro Federal de Contribuyentes (RFC)	
Dirección electrónica	
Teléfono	
Nacionalidad	

4. Forma de obtención de los datos personales:

Directa	x	**Indirecta** (Aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por la persona	

		responsable sobre los datos personales proporcionados directamente por el titular en algún otro sistema)	
Formulario físico			
Formulario electrónico			
Texto libre físico	x		
Texto libre electrónico	x		
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Adolfo Amylkar Mateos Medina
Cargo	Subdirector Jurídico Consultivo
Adscripción	Subdirección Jurídica Consultiva
Teléfono y extensión	(777) 329 2100 Ext. 2034
Correo electrónico institucional	aamateosm@capufe.gob.mx
Funciones/perfil	Responsable del tratamiento de datos personales de los representantes de personas morales que contratan con CAPUFE servicios de administración, operación y conservación de tramos carreteros y puentes de cuota y de los representantes de las Fiduciarias, de los Fideicomitentes y Fideicomisarios en los Fideicomisos que cuentan con la participación de CAPUFE y demás funciones establecidas en el numeral 1.3.1.- Subdirección Jurídica Consultiva del Manual General de Organización de CAPUFE.
Obligaciones	-Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. -Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos. -Informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. -En caso de que ocurra una vulneración a la seguridad, deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

6.- Persona servidora pública Administradora del Sistema:

Nombre	Cielo Eunice Marure Araniegues
Cargo	Subgerente de Fideicomisos y Procedimientos Legales
Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
Teléfono y extensión	(777) 329 2100 Ext. 3128
Correo electrónico institucional	cemarure@capufe.gob.mx

Funciones	Formular proyectos de convenios y contratos en materia de prestación de servicios de la infraestructura carretera concesionada que administra y opera el Organismo conforme a las disposiciones normativas de CAPUFE, con objeto de que se fijen de manera cierta y conveniente los derechos y obligaciones que adquiere este descentralizado frente a terceros y demás funciones establecidas en el numeral 1.3.0.0.1.- Subgerencia de Fideicomisos y Procedimientos Legales del Manual General de Organización de CAPUFE.
Obligaciones	-Mantener actualizado el sistema. -Determinar a las personas servidoras públicas que deban tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos. -Autorizar los accesos de las personas servidoras públicas, determinar los privilegios y limitantes y llevar un registro de los mismos. -Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

7. Persona servidora pública Operadora del Sistema:

N°	Datos de la persona operadora	
1	Nombre	Jesús León Landa
	Cargo	Asistente de Proyectos
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
	Funciones	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma.
2	Nombre	Perla Karina Bahena Mendoza
	Cargo	Analista Especializado
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
	Funciones	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma
3	Nombre	Brenda Hernández Yáñez
	Cargo	Superintendente A
	Adscripción	Subgerencia de Fideicomisos y Procedimientos Legales
	Funciones	Auxiliar en la formulación y atención de proyectos de contratos y convenios de prestación de servicios.
	Obligaciones	Supervisar que la información se encuentre actualizada y que se apliquen medidas de seguridad de acceso a la misma.

8. Tipos de soportes
(Señalar con una X, según corresponda)

Electrónico		**Físico**		**Combinado**	**X**

Descripción:

Expedientes de contratos que contienen la siguiente documentación: contrato de fideicomisos; convenio (s) modificatorio (s) a los contratos de fideicomisos; escrituras públicas con las que se acredita la representación y facultades de las personas que suscriben los contratos y convenios; oficios y/o comunicados mediante los cuales se notifica del cambio de representantes legales de las fiduciarias, de los fideicomitentes y fideicomisarios, en los fideicomisos que cuentan con la participación de CAPUFE y que también contienen datos personales como el nombre completo, domicilio, teléfono, correo electrónico, firma, RFC, CURP, credencial para votar, etc.

Físico: Los expedientes físicos se encuentran ubicados en las oficinas de la Subdirección Jurídica Consultiva. Específicamente en los archiveros 1, 2, 3, 4, y 5 correspondientes a la Subgerencia de Fideicomisos y Procedimientos Legales.

Electrónico: Archivos de Word, PDF y Excel, que contienen diversos datos personales, los cuales se encuentran resguardados en los equipos de cómputo asignados al personal del área, mismos que se encuentran protegidos mediante una contraseña de acceso, de los cuales únicamente el personal adscrito al área puede acceder a ellos.

9. Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales.

Los expedientes físicos se resguardan en archiveros metálicos ubicados en oficinas centrales (Subdirección Jurídica Consultiva), mismos que cuentan con cerradura y sólo el personal autorizado cuenta con llaves para accederlos.

Los archiveros se encuentran identificados en áreas con aire acondicionado para controlar la temperatura y humedad adecuadas.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

a) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año, (en términos del Compendio de Seguridad y Protección Civil de CAPUFE).
b) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
c) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

a) Acceso controlado, (en términos del Compendio de Seguridad y Protección Civil de CAPUFE).
b) Las oficinas centrales del Organismo cuentan con Cámaras de circuito cerrado.
c) Cuenta con mecanismos para regular y mantener el suministro de energía eléctrica.

10.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	**SI**		**NO**	**X**
En caso afirmativo, describir				

Transmisión	**SI**		**NO**	**X**
En caso afirmativo, describir				

11.- Transferencia de datos:

(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI		NO	X

12. Persona Encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	X

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

III. Dirección de Administración y Finanzas

Nombre del Sistema de Datos Personales:

III.1 SERVICIO DE EMISIÓN, ENVÍO Y RESGUARDO DE COMPROBANTES FISCALES DIGITALES POR INTERNET (CFDI) POR CONCEPTO DE PAGO DE PEAJE E INGRESOS DIVERSOS.

1. Objetivo:
Expedir Comprobante Fiscal Digital por Internet (CFDI), para poder acreditar las ventas, servicios que presten o definir el uso temporal u otorgamiento de bienes inmuebles, se realiza la contratación de un proveedor de servicio de emisión de CFDI, envío del CFDI a las personas usuarias que requieran el comprobante y resguardo de comprobantes Fiscales Digitales por Internet (CFDI), por un tiempo de 5 años.

2. Fundamento Legal:
Artículos 29, 29 A, 30 del Código Fiscal de la Federación; Artículos 94 y 28 de la Ley ISR; y Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad (Información para que se recaba el dato)
Particulares	
Nombre completo de la persona física	Identificar a la persona física con la que se tendrá comunicación por correo electrónico.
Razón Social	Identificar a la persona moral con la que se tendrá comunicación vía correo electrónico.
Domicilio Fiscal.	Obligatorio para la emisión de Comprobantes Fiscales Digitales por Internet (Art. 29-A del Código Fiscal del Federación. Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
Régimen Fiscal	Obligatorio para la emisión de Comprobantes Fiscales Digitales por Internet (Art. 29-A del Código Fiscal del Federación.
Correo electrónico	Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.
RFC	Obligatorio para la emisión de Comprobantes Fiscales Digitales por Internet (Art. 29-A del Código Fiscal del Federación.
Código Postal	Obligatorio para la emisión de Comprobantes Fiscales Digitales por Internet (Art. 29-A del Código Fiscal del Federación. Mantener contacto con la persona con la que se tendrá comunicación vía correo electrónico.

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa		Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico		No se presenta esta situación	
Formulario electrónico	X		
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	**Lic. Luis Enrique Oropeza Olguín**
Cargo	Encargado del despacho de la Subdirección de Finanzas
Adscripción	Dirección de Administración y Finanzas
Teléfono y extensión	7773292800 ext. 2153
Correo electrónico institucional	leoropezao@capufe.gob.mx
Funciones	-Atender los requerimientos de las unidades administrativas, que integran el Organismo para llevar a

	cabo el proceso de facturación de los ingresos por cuenta de CAPUFE y del Fideicomiso 1936. -Diseñar y proponer los esquemas, procedimientos y mecanismos de operación para cumplir con el servicio. -Supervisar la emisión, envío y resguardo de CFDI´s expedidos por CAPUFE y el FONADIN.
Obligaciones	-Supervisar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

6. Persona servidora pública administradora del Sistema

Id	Datos de la persona servidora pública administradora del Sistema	
1	Nombre	**L.C. Reyna Calvo Morteo**
	Cargo	Gerente de Tesorería
	Funciones	-Administrar y gestionar procesos de facturación y timbrado.
	Obligaciones	Verificar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
2	Nombre	**L.C. Juan Francisco Corona Cruz**
	Cargo	Gerente de Gestión y Seguimiento de Recursos del Fideicomiso 1936
	Funciones	-Encargado de supervisar la emisión de comprobantes de peaje del FNI.
	Obligaciones	Verificar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública Operadora del Sistema	
1	Nombre	**Ángel Aurelio Figueroa Ramirez**
	Cargo	Subgerente de Ingresos
	Funciones	-Encargado de supervisar la emisión de comprobantes de peaje de la Red Propia de CAPUFE. -Coordinar la atención y seguimiento a solicitudes inherentes a la facturación de CAPUFE.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
2	Nombre	**José de Jesús Villaseca Garcia**
	Cargo	Subgerente de Seguimiento de Ingresos del Fideicomiso 1936
	Funciones	-Encargado de revisar que los CFDI´s que se emitan bajo el presente sistema, se expidan bajo los parámetros establecidos, así como autorizar y controlar al personal de Fondo Nacional de Infraestructura que tenga acceso al sistema bajo características de Administrador.

		-Revisar funcionamiento de web services, atención a usuarios, revisar que los CFDI´s que se emitan bajo el presente sistema, se expidan bajo los parámetros establecidos de la Red FONADIN.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

8.- Persona Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública	X	Ciudadano (a)		Otro	

Descripción:

Id	Datos de la persona servidora pública Usuaria del Sistema	
	Nombre	**Omar Cedillo Escudero**
	Cargo	Superintendente “D”
	Funciones/Perfil	-Revisar funcionamiento de web services, atención a usuarios, revisar que los CFDI´s que se emitan bajo el presente sistema, se expidan bajo los parámetros establecidos de la Red CAPUFE y las reglas fiscales que estén vigentes.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
	Nombre	**Gabriel Aguilar Nuñez**
	Cargo	Supervisor “A”
	Funciones/Perfil	-Facturación del ingreso diario. -Generar la factura global del ingreso diario de las plazas de cobro concesionadas al Fondo Nacional de Infraestructura.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
	Nombre	**Abraham Josué Guzmán Sánchez**
	Cargo	Supervisor “A”
	Funciones/Perfil	-Realizar las facturas de los depósitos realizados a las cuentas bancarias del Fideicomiso 1936 Fondo Nacional de Infraestructura (derecho de vía 1 y 2, otros ingresos, penalizaciones, seguros, venta de tarjetas e intereses) y tramo monetizado México Puebla (seguros o penalizaciones.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
	Nombre	**Cristina Tapia Delgado**
	Cargo	Asistente de Proyectos
	Funciones/Perfil	-Realizar las facturas de pago de peaje en efectivo solicitadas por los usuarios por correo electrónico.

	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
	Nombre	**Navil Castañeda Palomar**
	Cargo	Auxiliar General
	Funciones/Perfil	-Realizar las facturas de pago de peaje en efectivo solicitadas por los usuarios por correo electrónico.
	Obligaciones	Aplicar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico	X	Físico		Combinado	

Descripción:

Gestión de emisión, envío y/o entrega, y resguardo de CFDI´s, así como el registro contable.

El **Servicio de emisión, envío y resguardo de CFDI por concepto de pago de peaje e Ingresos Diversos** permite capturar datos fiscales de la persona usuaria con la finalidad de que ésta pueda obtener un Comprobante Fiscal Digital y que CAPUFE registre contablemente los ingresos.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

El servidor que contiene y resguarda la información de este servicio, se encuentra en el Centro de Cómputo y Telecomunicaciones de las oficinas centrales de este Organismo.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

p) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
q) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
r) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

k) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
l) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

21. **Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.

22.	**Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
23.	**Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
24.	**Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	SI		NO	X
En caso afirmativo describir				

Transmisión	SI	X	NO	
En caso afirmativo describir:				

- Eventualmente se realizan transmisiones mediante el traslado sobre redes electrónicas, de la siguiente manera:

a) Eventualmente se envía información mediante correo electrónico. Los archivos electrónicos que contienen datos personales deben ser encriptados, una vez que se transfieren por correo electrónico, éstos se integran al SIAC.
b) Se utiliza Internet como el canal para las transmisiones, se utiliza el protocolo de transmisión “Simple Mail Transfer Protocolo (SMTP)”.
c) El remitente cuenta con un dispositivo tipo IDS (sistema de detección de intrusos) para detectar intrusiones en el canal de comunicaciones.
d) El destinatario envía correo electrónico con acuse de recibo de la información transmitida.
e) La transmisión de datos vía web se realiza mediante un canal seguro, el sistema utiliza el protocolo de comunicación https contando con un certificado SSL.
f) La transmisión de datos mediante el sistema SIAC se realiza a través de la Intranet del Organismo.
g) La transmisión de datos personales será de conformidad con el artículo 17 de los “Lineamientos de Protección de Datos Personales”, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI	X	NO	

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
A	Autoridades legalmente autorizadas	Investigación y persecución de los delitos, así como la procuración o administración de justicia.	No se requiere

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI	X	NO	

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio: Convenio número 5500010522 CAPUFE y 5500010523 FONADIN vigentes hasta el 12 de febrero de 2023. En proceso de licitación para los nuevos contratos.

Nombre del Sistema de Datos Personales:
III.1 SISTEMA DE RECURSOS HUMANOS

1. Objetivo:
Administración de Estructura Organizativa: Construcción y mantenimiento de un modelo de organización y gestión de personal: Administración de los Procesos básicos requerimientos en la Gestión de Capital Humano- Gestión de Tiempo de Personal Control. - Operación y Mantenimiento de Horario de Trabajo, Planes de horario de Trabajo, Entrada de datos de Tiempo, Calendarios Festivos, Contingentes de Ausentismo y Presencias, Evaluación de Tiempos. - Nómina: Calculo de Percepciones y Descuentos. Pago de Cuotas y Aportaciones ISSSTE, Pago de Ordenes Jurídicas de Pensión Alimenticia, Retención de Impuestos, Prestamos y Descuentos diversos, Contabilidad de Nómina. Generación de archivos a bancos, capacitación y registro de hijos de Trabajadores al Sistema SEP.

Así mismo, hay un dato que se refiere a las evaluaciones psicométricas del personal operativo y que se encuentra en el expediente físico, como en el sistema Psycoweb.

2. Fundamento Legal: (específico)
Artículo 50, fracciones II, IX, X, del Estatuto Orgánico de CAPUFE; Artículos 4, 16 a 18, 20 a 42 y 57 de la LGPDPPSO.

3. Datos personales que se encuentran en el Sistema:

Dato Personal	Idoneidad

	(Información para que se recaba el dato)
Particulares	
Nombre completo de la persona	Datos de identificación del trabajador (a), para su contratación, movimientos de personal, alta en el ISSSTE, otorgamiento de prestaciones, elaboración de credencial de identificación, integración única del expediente personal, cálculo y pago de nómina, cálculos de finiquitos y/o indemnizaciones, información de ingresos, promociones, cambios de adscripción y bajas en el sistema SIAC, pagos a personas beneficiarias por fallecimiento del trabajador (a), elaboración de hojas de Servicio, trámites ante el ISSSTE, integración del RUSP, pago de impuesto sobre nómina, reconocimiento de antigüedad, alta y baja de personal en los lectores de huella digital, recibir y registrar en el SIAC las incidencias.
Domicilio	
Teléfono particular	
Estado civil	
Nombre de familiares, dependientes y beneficiarios	
RFC	
CURP	
Lugar de Nacimiento	
Fecha de Nacimiento	
Nacionalidad	
Edad	
Fotografía	
Datos Laborales	
Actividades extracurriculares	Para la integración única del expediente personal del trabajador (a), pago de nómina y prestaciones. Consulta de personal para concursos escalafonarios.
Trabajos anteriores	
Datos Académicos	
Trayectoria educativa	Consulta de personal para concursos escalafonarios.
Títulos	
Cédula profesional	
Certificados	
Características personales	
Tipo de sangre	Elaboración de credencial del trabajador (a), por cualquier accidente o riesgo de trabajo.
Datos de Salud	
Historial Clínico	Hacer efectivas las incapacidades que el trabajador (a) presente. Verificar que trabajadores (as) son vulnerables, derivado de la contingencia sanitaria SARS-COV-2 (COVID-19). Otorgar la prestación de lentes. Elaboración de las credenciales, a efecto de que contengan datos de identificación, padecimientos y alergias por cualquier accidente o riesgo de trabajo.
Enfermedades	
Discapacidades	
Intervenciones quirúrgicas	
Padecimientos y alergias	

4. Forma de obtención de los datos personales
(Señalar con una X, según corresponda)

Directa	Indirecta (aquella inferida, derivada, creada, generada, obtenida a partir del análisis o el tratamiento efectuado
X	

		por el responsable sobre los datos personales proporcionados directamente por el titular	
Formulario físico		No se presenta esta situación	
Formulario electrónico	X		
Texto libre físico			
Texto libre electrónico			
Vía telefónica			
Otro			

5.-Persona servidora pública responsable del Sistema:

Nombre	Velia Yolanda Bravo Andrade.
Cargo	Subdirectora de Capital Humano y Desarrollo Organizacional.
Adscripción	Dirección de Administración y Finanzas.
Teléfono y extensión	7773292100 Ext. 2152
Correo electrónico institucional	vbravoa@capufe.gob.mx
Funciones	-Dar aviso a la Unidad de Transparencia de los Sistemas de Tratamiento de Datos Personales que se encuentren a su cargo. -Designar a la persona administradora de cada Sistema de Tratamiento de Datos Personales a su cargo. -Validar que la información entregada por las personas titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado. -Vigilar y coordinar que la información se encuentre actualizada.
Obligaciones	--Supervisar el cumplimiento de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. -Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales. -Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado.

6. Persona servidora pública Administradores del Sistema:

Id	Datos de la persona servidora pública administradora	
1	Nombre	Mtra. Elia Luna Morales
	Cargo	Gerente de Administración del Capital Humano
	Adscripción	Subdirección de Capital Humano y Desarrollo Organizacional
	Funciones	-Mantener actualizado el sistema. -Determinar a las personas servidoras públicas que tendrán acceso a los datos personales, en función del tratamiento que se les debe aplicar. -Autorizar los accesos de las personas servidoras públicas, determinar los privilegios y limitantes y, llevar un registro de los mismos.

		-Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.
	Obligaciones	- Verificar que las personas usuarias y resguardarías de la información, lleven a cabo un buen manejo, tratamiento, transferencia, divulgación y uso de la información, a efecto de proteger los datos personales. - Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. - Asegurar que el personal a su cargo y con acceso físico o automatizado a los repositorios de datos personales conozca las normas de seguridad que deben observarse para su tratamiento, sus atribuciones y responsabilidades que tienen. -Capacitación constante en materia de datos personales.
2	Nombre	Lic. David Enrique Martínez Mejía
	Cargo	Gerente de Desarrollo Organizacional y Humano
	Adscripción	Subdirección de Capital Humano y Desarrollo Organizacional
	Funciones	-Mantener actualizado el sistema. -Determinar a las personas servidoras públicas que tendrán acceso a los datos personales, en función del tratamiento que se les debe aplicar. -Autorizar los accesos de las personas servidoras públicas, determinar los privilegios y limitantes y, llevar un registro de los mismos. -Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.
	Obligaciones	- Verificar que las personas usuarias y resguardarías de la información, lleven a cabo un buen manejo, tratamiento, transferencia, divulgación y uso de la información, a efecto de proteger los datos personales. - Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos. - Asegurar que el personal a su cargo y con acceso físico o automatizado a los repositorios de datos personales conozca las normas de seguridad que deben observarse para su tratamiento, sus atribuciones y responsabilidades que tienen. -Capacitación constante en materia de datos personales.

7. Persona servidora pública Operadora del Sistema:

Id	Datos de la persona servidora pública operadora	
1	Nombre	Lic. Gustavo Ontiveros Espinosa
	Cargo	Subgerente de Remuneraciones
	Adscripción	Gerencia de Administración del Capital Humano
	Funciones	Sus funciones se determinan de acuerdo al perfil asignado en el tratamiento de los datos personales de cada Sistema
	Obligaciones	- Implementar medidas de seguridad y control interno, a fin de proteger los datos personales a los que tengan acceso. - Asegurar que la información contenida en el sistema se use y maneje únicamente para la finalidad objeto de su tratamiento.

		- Conocer las normas de seguridad que deben observarse para el tratamiento de datos personales. -Capacitación constante en materia de datos personales. -Resguardar la información y verificar que las transmisiones de datos personales sean acordes a la función que desempeñan y a las instituciones autorizadas para tal efecto. -Utilizar los usuarios y contraseñas del sistema exclusivamente para las funciones asignadas en el trabajo encomendado, a fin de evitar un mal uso de las mismas.
2	Nombre	Lic. Gustavo Rivera Zarate
	Cargo	Subgerente de Admisión y Empleo
	Adscripción	Gerencia de Administración del Capital Humano
	Funciones	Sus funciones se determinan de acuerdo al perfil asignado en el tratamiento de los datos personales de cada Sistema
	Obligaciones	- Implementar medidas de seguridad y control interno, a fin de proteger los datos personales a los que tengan acceso. - Asegurar que la información contenida en el sistema se use y maneje únicamente para la finalidad objeto de su tratamiento. - Conocer las normas de seguridad que deben observarse para el tratamiento de datos personales. -Capacitación constante en materia de datos personales. -Resguardar la información y verificar que las transmisiones de datos personales sean acordes a la función que desempeñan y a las instituciones autorizadas para tal efecto. -Utilizar los usuarios y contraseñas del sistema exclusivamente para las funciones asignadas en el trabajo encomendado, a fin de evitar un mal uso de las mismas.
3	Nombre	Mtra. Karina Angélica Vargas Delgado
	Cargo	Subgerente de Prestaciones y Servicios
	Adscripción	Gerencia de Administración del Capital Humano
	Funciones	Sus funciones se determinan de acuerdo al perfil asignado en el tratamiento de los datos personales de cada Sistema
	Obligaciones	- Implementar medidas de seguridad y control interno, a fin de proteger los datos personales a los que tengan acceso. - Asegurar que la información contenida en el sistema se use y maneje únicamente para la finalidad objeto de su tratamiento. - Conocer las normas de seguridad que deben observarse para el tratamiento de datos personales. -Capacitación constante en materia de datos personales. -Resguardar la información y verificar que las transmisiones de datos personales sean acordes a la función que desempeñan y a las instituciones autorizadas para tal efecto. -Utilizar los usuarios y contraseñas del sistema exclusivamente para las funciones asignadas en el trabajo encomendado, a fin de evitar un mal uso de las mismas.

8.- Persona servidora pública Usuaria del Sistema:
(Señalar con una X, según corresponda)

Persona servidora pública	**X**	Ciudadano (a)		Otro	

Descripción:

Datos de la persona servidora pública usuaria:
Se adjunta la relación de las personas servidoras públicas usuarias del sistema, en la cual consta su nombre, cargo, teléfono y extensión, coreo institucional, adscripción, funciones y obligaciones.

9.- Tipo de soporte:
(Señalar con una X, según corresponda)

Electrónico		Físico		Combinado	**X**

Descripción:

- Electrónico: Base de datos resguardada en servidores informáticos.
- Físico: Expedientes con documentos en papel.

Descripción del soporte físico:

Los Expedientes contienen:

- Solicitud de empleo
- Cédula de evaluación
- Examen psicométrico (caratula)
- Curriculum vitae
- Últimos estudios
- Identificación oficial
- Comprobante de domicilio
- CURP
- Acta de nacimiento y de matrimonio en caso de ser casado
- Reg. Federal de Contribuyentes
- Constancia de Situación Fiscal
- Seguro institucional
- Pliego testamentario
- Compatibilidad de empleo
- Formato de no inhabilitación (CAPUFE)
- Formato de retiro voluntario en otra dependencia
- Formato de sistema de pensión
- Formato de no formar parte de algún juicio
- Constancia de no-inhabilitación (SFP)
  - Formato de obligación para presentar declaración de situación patrimonial y de intereses.
  - Formato de Bajo protesta de decir verdad último domicilio.
  - Formato DAF.
- Altas y bajas del ISSSTE
- Formato de elección del ISSSTE
- Nombramientos
- Movimientos originales con su propuesta (acuerdos y oficios)
- Permisos sindicales para ocupar puestos de confianza, con y sin goce de sueldo.
- Finiquitos
- Renuncia
- Notas buenas

- Notas malas ejemplo: actas administrativas, amonestaciones
- Hojas de servicio de CAPUFE y otras dependencias
- Carta consentimiento para el fondo de ahorro
- Actas nacimiento hijos, cónyuge.
  - CURP hijos, cónyuge.
  - Censo de Recursos Humanos.

Descripción del soporte electrónico:

El Sistema de Recursos Humanos permite la Administración, de Estructura Organizativa: Construcción y Mantenimiento de un modelo de Organización.- Gestión de Personal: Administración de los Procesos básicos, requerimientos en la Gestión de Capital Humano.- Gestión de Tiempo de Personal Control.- Operación y Mantenimiento de Horario de Trabajo, Planes de horario de Trabajo, Entrada de datos de Tiempo, Calendarios Festivos, Contingentes de Ausentismo y Presencias, Evaluación de Tiempos.- Nómina: Cálculo de Percepciones y Descuentos. Pago de Cuotas y Aportaciones ISSSTE, Pago de Ordenes Jurídicas de Pensión Alimenticia, Retención de Impuestos, Prestamos y Descuentos diversos, Contabilidad de Nómina. Generación de archivos a bancos, capacitación y registro de hijos de Trabajadores al Sistema SEP.

No.	Sistema	Descripción del Sistema o Proyecto
1	Psycoweb (PSYCOWEB)	Sistema para el área de personal, utilizado para evaluaciones de aptitudes
2	Hand Keys	Registro de huellas dactilares para control de asistencia del personal. Funcionalidad de importación de las incidencias de RH
3	Alta de becarios	Página de alta de becarios en el área de Recursos Humanos para que sean habilitados y poder revisar las incidencias de sus checadas en el dispositivo lector biométrico de huellas digitales
4	Sistema de Control de Asistencias (Intranet) y recibos	Portal de consulta para empleados (asistencias, vacaciones, justificaciones y recibos de nómina)
5	Sistema Integral de Nomina. (SIN)	Sistema de nómina anterior al SIAC
6	Sala Virtual de Capacitación de CAPUFE	Portal de Capacitación en línea y a distancia
7	Revisiones de Nómina	Herramienta creada en Progress para validar los resultados de la nómina ejecutada en SAP, (percepciones vs deducciones) (validación de ISR)
8	Herramienta para crear archivo de pagos al ISSSSTE (SERICA)	Crea el archivo para pagos al ISSSSTE (SERICA)
9	Generador de código QR (QR)	Desarrolle este sitio para el área de capacitación. Está página genera un código QR con la información del empleado, toma la fecha y el nombre del curso.
10	Sistema Integral para la Administración de CAPUFE (SIAC)	Aplicación que automatiza la mayoría de los procesos administrativos del Organismo e integra las operaciones administrativas de recursos humanos

Nota: La STI brinda el soporte tecnológico a los sistemas No. 1, 4, 5, 7, 9 y 10.

10.-Carácterísticas del lugar físico donde se resguardan los sistemas de tratamiento de datos personales:

Los expedientes se resguardan en estantes dentro de las oficinas que ocupa la Unidad Administrativa y en el archivo de concentración del Organismo, además de contar con cerradura y sólo el personal autorizado cuenta con llaves para accederlos; así como espacio físico de labores cotidianas de los administradores y operadores del Sistema, ubicados en las oficinas que ocupa cada Unidad Administrativa.

El sistema de Sistema de Recursos Humanos se encuentra ubicado principalmente, en el Centro de Cómputo y Telecomunicaciones de Oficinas Centrales.

La arquitectura de seguridad perimetral cuenta con un Firewall perimetral (red perimetral) que protege la Red de CAPUFE de los riesgos existentes en Internet. Asimismo, las oficinas centrales de CAPUFE se encuentran conectadas con cada una de las Unidades Regionales y plazas de cobro, mediante enlaces dedicados.

En el centro de cómputo ubicado en las Oficinas Centrales, se cuenta con una infraestructura de virtualización en alta disponibilidad, la cual está conformada por servidores, equipos de almacenamiento y comunicación, unidades de respaldo de información, software de virtualización y sistemas operativos Windows Server.

- **Seguridad perimetral exterior:**

Las instalaciones del Organismo cuentan con un acceso principal para empleados (as) y visitantes, con las siguientes medidas de seguridad:

s) Los accesos peatonales y vehiculares están custodiados por personal de la policía estatal las 24 horas del día, los 365 días del año.
t) Para el control de accesos vehiculares, el Organismo cuenta con los “Lineamientos de operación para los estacionamientos de oficinas centrales”, en los cuales se establecen las normas y medidas de seguridad a seguirse.
u) Todo el acceso peatonal tiene un punto de revisión.

- **Seguridad perimetral interior**

m) Las oficinas centrales del Organismo cuentan con un sistema de video vigilancia que opera las 24 horas del día, los 365 días del año.
n) El SDP del registro contable en soportes electrónicos se encuentra resguardado en el Centro de Cómputo del Organismo. Entre las políticas de seguridad para la protección de la infraestructura de cómputo y comunicaciones del Organismo, se incluyen:

25. **Restricción de acceso:** El acceso al Centro de Cómputo está restringido y controlado por un sistema de control de acceso con lector de huella digital, el cual opera la apertura de todas las puertas del Centro de Cómputo.
26. **Autorización de acceso:** La persona titular de la Subdirección de Tecnologías de Información y el Gerente de Atención a Usuarios de Tecnologías de Información son las

	personas servidoras públicas facultadas para autorizar el acceso de personal al Centro de Cómputo.
27.	**Registro para el acceso:** Toda persona que le sea autorizado el acceso al Centro de Cómputo, debe registrar sus datos y huella digital en el sistema de control de accesos.
28.	**Vigilancia:** El Centro de Cómputo cuenta con un sistema de video vigilancia, que opera las 24 horas del día, los 365 días del año, y con bitácoras electrónicas en su sistema de control de acceso.

11.- Portabilidad de datos:

Las características del Sistema de tratamiento de datos personales permiten la portabilidad de datos a su titular en:

(Señalar con una X, según corresponda)

Copia	SI	**X**	NO	
En caso afirmativo describir				
Si se permite, no obstante, no es requerido por el titular de los datos personales.				

Transmisión	SI	**X**	NO	
En caso afirmativo describir:				
Si se permite, no obstante, no es requerido por la persona titular de los datos personales.				

12.- Transferencia de datos:
(Señalar con una X, según corresponda)

Se realiza transferencia de los datos contenidos en el Sistema:	SI	**X**	NO	

A) Situaciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.
B) Distintas de las excepciones mencionadas en los artículos 22, 66 y 70 de la LGPDPPSO.

Id	Destinatarios o terceros receptores	Finalidades de la transferencia	Consentimiento de la persona titular
	ISSSTE. SFP. CONSAR. Grupo FAMSA S.A.B. de C.V. BANORTE. INFONACOT. METTLIFE MEXICO S.A. Toka Internacional de S.A.P.I. de C.V.	Altas, Modificaciones, Bajas, Movimientos de personal. RUSP (Registro Único de Servidores Públicos). Ahorro para el retiro. Préstamos a empleados.	No aplica.

		Seguro de vida. Seguro Colectivo de Retiro. Tarjeta vales de despensa.	

13.- Persona encargada de datos:
(Señalar con una X, según corresponda)

Existe un prestador de servicios-persona física o moral, pública o privada ajena al Organismo, que solo o conjuntamente con otros, trate datos personales a nombre y por cuenta de CAPUFE.	SI		NO	**X**

En caso afirmativo mencionar el instrumento jurídico con el que se formaliza la prestación del servicio.

VI. MEDIDAS DE SEGURIDAD.

La LGPDPPSO, establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permitan proteger los datos personales.

De manera particular, en su artículo 31 dispone que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, la persona responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

A su vez, en su artículo 33 prevé que, para establecer y mantener las medidas de seguridad para la protección de datos personales, la persona responsable del SDP deberá realizar las siguientes actividades:

- Crear políticas internas para la gestión y tratamiento de los datos personales que consideren su obtención, uso y posterior supresión.
- Definir funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
- Elaborar un inventario de los datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización de la persona responsable del SDP.

- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas de cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales.
- Monitorear las medidas de seguridad implementadas, así como las amenazas y vulneraciones.
- Diseñar y aplicar distintos niveles de capacitación del personal, dependiendo de sus roles y responsabilidades en el tratamiento de datos personales.

Las medidas de seguridad se abordan en tres modalidades:

I. Administrativas, son las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional y capacitación del personal, en materia de protección de datos personales.

II. Físicas, son el conjunto de acciones y mecanismos para proteger el entorno físico donde se encuentran los datos personales y los recursos involucrados en su tratamiento.

III. Técnicas, son el 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 los recursos involucrados en su tratamiento.

Como medidas de seguridad de manera general CAPUFE cuenta con las siguientes:

I. Administrativas:

Acorde a la LGPDPPSO, las medidas de seguridad administrativas son las 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 y capacitación del personal en materia de datos personales.

Para cumplir la exigencia legal de adoptar estas medidas que garanticen la seguridad de los datos de carácter personal, este Organismo a través de la Dirección de Operación, Dirección de Administración y Finanzas y la Dirección de Planeación, Evaluación y Desarrollo Institucional:

1.- Cuenta con un documento denominado *"Directrices de seguridad de la información"* en el que se establecen las pautas que forman parte de la base para establecer el Sistema de Gestión de Seguridad de la Información en CAPUFE, con el fin de proteger los datos y activos de información que soportan su operación, asegurar el cumplimiento de la LGPDPPPSO, reducir los riesgos por el uso de las tecnologías de la información y comunicaciones.

2.- Se cuenta con un *"Compendio de seguridad y protección civil",* cuyo objetivo es salvaguardar en la medida de lo posible las vidas humanas, y su infraestructura. Establecer criterios técnicos que regulen los servicios de seguridad física prestados por las áreas de seguridad de los niveles de

gobierno y empresas privadas al Organismo, así como organizar medidas que permitan una operación óptima en materia de seguridad y protección civil en todas sus unidades administrativas.

3.- A través de la Subdirección de Transparencia y Control Institucional, se realizó un inventario de los datos personales y sistemas de tratamiento de los mismos en coordinación con las Unidades Administrativas, respecto de la información confidencial que trata este Organismo, el cual estará en constante actualización.

4.- Se promueve la capacitación periódica dirigida al personal adscrito a las Unidades Administrativas de este Organismo sobre el correcto uso y manejo de datos personales.

II. Físicas:

La persona titular o persona responsable de cada centro de trabajo se asegura de que los servicios de seguridad que proporcionan al Organismo las instancias y corporaciones de seguridad incluyan:

Vigilancia, custodia, rondines de supervisión y control de los bienes muebles, inmuebles, equipo, material de información y demás inherentes en la materia que requiera el centro de trabajo o la zona a donde están asignados, a fin de prevenir que los bienes se destruyan, alteren y/o desaparezcan, así como auxiliar a las autoridades en atención de fenómenos naturales o socio organizativos, acciones delictivas, incidentes o accidentes a fin de salvaguardar la integridad de las personas servidoras públicas, de las personas usuarias y los bienes del Organismo.

Criterios para Vigilancia de Perímetros:

a) Interior. - Mantenerse alerta con la presencia del personal que labora o presta un servicio al interior de las instalaciones e infraestructura del Organismo, y cualquier hecho o evento que presuma alguna alteración o irregularidad debidamente fundada y motivada.

b) Exterior. - Mantenerse alerta ante la presencia de personas ajenas al Organismo o cualquier hecho o evento que presuma irregularidad fundada o alteración realizada por el personal asignado al patrullaje de vigilancia.

c) En los centros de trabajo donde se cuenta con circuito cerrado de televisión, se generan grabaciones que pueden ser consultadas ante la ocurrencia de un hecho o un evento extraordinario que se registre.

Criterios para Control de Acceso:

a) Todo el personal adscrito al Organismo porta su gafete oficial, en un lugar visible.

b) El personal que realiza servicio social, prácticas profesionales o actividades temporales o permanentes en el Organismo, porta en un lugar visible gafete proporcionado por el área de recursos humanos correspondiente durante el tiempo que permanezca en el interior del Organismo.

c) Las y los visitantes y proveedores, se registran en la bitácora de Control de Visitas, el registro deberá ser detallado verificando que no se omita ningún dato o información solicitada.

d) Para el personal visitante y proveedores, deberá proporcionarse un gafete, se registra en bitácora, previa autorización de ingreso de la persona a quien visita.

e) El responsable del centro de trabajo en oficinas centrales y foráneas de seguridad según el caso, deberá verificar la existencia de la relación detallada del personal que laborará durante el fin de semana, días festivos o inhábiles.

f) Sin excepción alguna no se permite la entrada a las instalaciones del Organismo, a personal o personas ajenas que ofrezcan productos consumibles y materiales, proveedores y contratistas que ofrecen o prestan algún servicio deberán estar autorizados por el área de servicios materiales.

g) Está prohibido el ingreso o uso de instalaciones e infraestructura del Organismo sea cualquier empleado (a) o personas en notorio estado de ebriedad o intoxicación por drogas o enervantes.

Criterios para Custodia del Personal y Bienes Muebles e Inmuebles del Organismo.

a) El responsable de cada Unidad Administrativa, supervisará la instrumentación de las órdenes de operación que ponga en funciones a los elementos que tengan a su cargo la seguridad física de la instalación, con el fin de que éstas garanticen las condiciones de seguridad para el personal que labora en el Organismo y Plazas de cobro, y cualquier unidad administrativa.

b) Se designará a cada elemento de seguridad un área de custodia, la cual deberá de recibir y entregar, con las consignas particulares que se establezcan.

c) Se les reportará cualquier hecho extraordinario que se presente, como: accidentes, extravíos, incendios, siniestros, reparto de volantes, marchas, mítines, etc., designando a los elementos de seguridad para recabar toda la información posible, comunicándola inmediatamente a Oficinas Centrales a través de un reporte vía correo electrónico o teléfono a la Gerencia de Seguridad en Infraestructura Carretera Operada y ésta a su vez a la Dirección de Operación y Dirección General, según sea el caso.

III. Técnicas

Las medidas de seguridad técnicas, según la definición señalada en la legislación general de la materia, son el 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 los recursos involucrados en su tratamiento.

En ese sentido, y debido a que este Organismo cuenta con equipo compuesto por hardware y software se cuentan con medidas de seguridad aplicables para los sistemas de tratamiento de datos en soporte electrónico que alberga la STI.

a) A fin de evitar los accesos no autorizados a equipos de cómputo, se ha implementado el uso de usuarios y contraseñas para los empleados, mismas que son asignadas a los servidores públicos al ingresar a laborar, por lo que a través de las mismas se otorga un acceso limitado al ordenador
b) Implementar y verificar el uso del software antivirus de los equipos de cómputo de escritorio y portátiles, asignados al personal de las diferentes áreas del Organismo.
c) Asegurar que el acceso a la información está protegido, controlado y autorizado únicamente a personal que por razones de trabajo lo necesite, garantizando así su confidencialidad y calidad.
d) Garantizar la confidencialidad, integridad y disponibilidad de la información en los sistemas que soportan la operación de CAPUFE.
e) Proteger los datos y activos de información que soportan la operación de CAPUFE, cumplir con leyes y regulaciones, así como implementar el Modelo de Gestión de Seguridad de la Información.

VI.A. Análisis de riesgo

Se busca garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente del sistema de recursos humanos, en cuanto al acceso, uso y tratamiento de los datos personales.

A fin de buscar oportunidades de mejora, en el establecimiento de las medidas de seguridad existentes, en la protección de datos personales, se identificaron los riesgos existentes y los controles implementados para mantenerlos en un impacto y probabilidad de ocurrencia bajo.

Riesgos identificados de manera general en el uso del sistema, enfocados a provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.

- Uso no autorizado.
- Acceso ilegítimo a los datos.
- Modificación no autorizada de los datos.
- Eliminación de los datos.

- Pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- Tratamiento de datos distinto al autorizado o a la finalidad con la que se recaban los mismos.
- Transmisión de datos no autorizados por el titular de los mismos.
- Robo, extravío o copia no autorizada.

Controles:

- Resguardo de una copia del contenido completo de la información concentrada en el sistema.
- Revisión continua y actualización cada vez que se produzca un cambio relevante en alguna actividad de tratamiento registrada.
- Creación de usuarios con transacciones delimitadas de acuerdo al perfil y funciones asignadas.
- Resguardo de usuarios y contraseñas, éstas últimas mediante cifrado de documentos.
- Revisión periódica de la información contenida en el sistema.
- Bitácora de las vulneraciones a la seguridad, con la identificación de los datos comprometidos y los controles implementados.

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

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación a la persona 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 la persona 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 toda persona servidora pública 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 las personas servidoras públicas con 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.
- Alteración de la información.

Ante dichos riesgos identificados se hace un análisis de éstos, así como de las amenazas y sus posibles vulneraciones:

Origen de la amenaza **Riesgo o amenaza**	**Causa**	**Posibles consecuencias**

Acceso de personas no autorizadas a los sistemas o plataformas oficiales del Organismo.	Descuidos por parte del sujeto obligado en el manejo de los accesos.	Acceso no autorizado. Divulgación de datos personales. Modificaciones no autorizadas, robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del organismo.	Entrega deliberada de accesos o de la información personal a personas ajenas a la institución	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de las y los ciudadanos. Robo de información.
Personal del Sujeto Obligado con poco conocimiento sobre el tratamiento de datos personales.	Curiosidad. Error involuntario. Por fines económicos.	Ataque a otras personas servidoras públicas. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Robo de información. Extorsión. Modificaciones no autorizadas. Robo de información.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Aquí es muy importante señalar lo poco homogéneo que es la infraestructura tecnológica en este punto. Falta de contraseñas efectivas. Falta de mecanismos para identificar o autenticación de	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales y modificaciones no autorizadas. Robo de información.

	usuarios. Falta de actualización de antivirus.	
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales y modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales y modificaciones no autorizadas. Robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan).	Daño y/o pérdida de los datos personales y modificaciones no autorizadas.

Registro de incidentes:

- Se cuenta con procedimientos para la atención de incidentes en los que se registra:

  Incidentes de soportes electrónicos

  a) Generación del incidente.
  b) Identificación del nodo o aplicación.
  c) Priorización del incidente.
  d) Ejecución de acciones correctivas.
  e) Validación de funcionamiento por parte del usuario final.
  f) En caso de persistencia del incidente se debe solicitar apoyo de un tercero y regresa al inciso d).
  g) Elaboración de acta administrativa, la cual debe contener la relatoría del incidente, las acciones tomadas, las personas que intervinieron, los daños causados y las consecuencias actuales y futuras.
  h) Cierre de incidente, el cual incluye la notificación formal a las áreas afectadas, así como la planeación y ejecución de acciones preventivas.

Procedimientos de respaldo y recuperación de datos:

- Se realizan respaldos completos, basados en un calendario y horario establecidos.

- Los respaldos se almacenan en el Sistema de Respaldos Centralizados de CAPUFE, los cuales son etiquetados acorde a una nomenclatura establecida.
- Personal de Tecnologías de Información es responsable de realizar los respaldos.

Plan de contingencia:

A continuación, se describen las actividades a realizar para la ejecución del plan de contingencia:

1. Comunicar la contingencia a la Mesa de Servicios de CAPUFE la ext. 3999
2. Los agentes de primer nivel registran y asignan el ticket de la contingencia responsable de Seguridad de la Subdirección de Tecnologías de Información (STI).
3. El responsable de la Seguridad de la STI, invoca al personal que sea necesario para solventar la contingencia.
4. Se ejecutan las acciones para solventar los posibles escenarios:

Escenario I: Corrupción en la Base de Datos

Una base de datos puede ser corrompida cómo consecuencias de:

Daño en algún archivo que conforma la base de datos.

Este tipo de desastre requiere la recuperación de la base de datos del sistema y los archivos del sistema operativo (operating file system).

- El tiempo estimado de recuperación es de 8 horas.

Escenario II: Falla en el equipo (Hardware)

Los siguientes tipos de falla en el equipo pueden ocurrir debido a:

- Falla en controlador de discos (RAID Controller).
- Fallas en los componentes del cluster.

- Las fallas en el equipo requieren de:
  - Reemplazar los componentes de hardware dañados.
  - Reinstalación y configuración del servidor (Sistema Operativo).
  - Recuperación de la base de datos y archivos relacionados.

- El tiempo estimado de recuperación es de 24 horas una vez reemplazado el equipo de hardware dañado.

Escenario III: Destrucción parcial o total de las instalaciones del centro de cómputo

- Los componentes que pueden dañarse son los siguientes:
  - Servidores
  - Infraestructura de Soporte (ubs, switches, cableado, etc.)
  - Instalaciones

- La falla o destrucción de los componentes o de la instalación del centro de cómputo puede ser ocasionada por alguno de las siguientes causas:
  - Incendio
  - Temblor
  - Inundación
  - Atentado (Bomba)
  - Robo

- El daño o destrucción de las instalaciones o componentes requiere de:
  - Reemplazo de los componentes de infraestructura de soporte
  - Reemplazo de servidores
  - Reinstalación de los servidores (hardware, sistema operativo, base de datos, etc)
  - Recuperación de la base de datos y archivos relacionados

- El tiempo estimado de recuperación es de 24 horas después de reemplazar todos los componentes de infraestructura de soporte, así como de los servidores. Se recomienda contar con un centro de cómputo alterno para los casos de desastre.

La siguiente tabla muestra las diferentes estrategias de recuperación y los procesos involucrados para la recuperación del sistema.

Estrategia de Recuperación	**Tipo de Incidente**	**Proceso**
Recuperación Parcial	• Corrupción de datos o falla en el equipo	• Obtener el más reciente respaldo. • Restaurar el archivo dañado
Recuperación total de la base de datos	• Corrupción de la base de datos o falla en el equipo	• Obtener el más reciente respaldo. • Restaurar la base de datos. • Restaurar el Sistema
Recuperación total del sistema	• Corrupción del sistema operativo • Corrupción de la Base de Datos • Corrupción en el sistema • Falla de discos	• Para cualquier falla del hardware, se deberá contactar al proveedor para el reemplazo del componente según acuerdos de servicio. • Obtener el último respaldo total del sistema. • Obtener el más reciente respaldo y de archive. • Restaurar el Sistema operativo. • Restaurar la Base de Datos. • Restaurar el Sistema

5. Se notifica al usuario, quien reportó la contingencia, la validación de la disponibilidad de lo reportado, por medio de la mesa de servicios.
6. Una vez obtenida la satisfacción del usuario, se procede al cierre del ticket.

Todas las acciones realizadas por los agentes de primero, segundo y tercer nivel, deben ser documentadas en el ticket asignado a la contingencia.

VI.B. Análisis de brecha

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con diferentes Unidades Administrativas a cargo de los sistemas de datos personales con lo que cuenta este Organismo.

Medidas de seguridad actuales:

El espacio físico o área donde se recaban datos personales, es regularmente dentro de las instalaciones de CAPUFE.

Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial, como @capufe.gob.mx. Aquí cabe señalar que, debido a problemas de infraestructura con la red de intranet en algunas plazas de cobro, en ocasiones ha sido necesario utilizar cuentas de correo de servidores convencionales de correo electrónico como gmail, yahoo y outlook.

En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión de la persona servidora pública, 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 personas servidoras públicas, autorizadas por cada área.

Una vez recabados los datos personales, la persona servidora pública 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 ésta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área personas servidoras públicas 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, la persona responsable del SDP 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, las personas servidoras públicas responsable del SDP, del área tienen acceso a los datos personales.

Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

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 del 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.

Medidas de seguridad faltantes

- Cifrado de bases de datos.
- Actualización periódica de contraseñas en el sistema y en la computadora.
- Revisión de transacciones autorizadas conforme al perfil y funciones asignadas.
- Dar de baja a los usuarios inactivos, dados de baja o con cambio de adscripción.
- Control central de las transacciones autorizadas en las Unidades Regionales.
- Restricción de accesos en el sistema.

VI.C. Mecanismos de Monitoreo

A fin de supervisar y garantizar el cumplimiento y mejora continua de las medidas de seguridad que se encuentran implementadas para la protección de los datos personales, el entorno del espacio físico de trabajo, así como del digital, las Unidades Administrativas responsables de los sistemas de datos personales reportados en el presente Documento de Seguridad, han definido controles de monitoreo que permiten el seguimiento a la implementación de estas medidas de seguridad, reportando lo anterior de manera semestral a la Subdirección de Transparencia y Control Institucional de este Organismo.

VI.D. Plan de Trabajo

De acuerdo al artículo 33, fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, es necesaria la implementación de un Plan de Trabajo, ya que se encuentra descrita como una de las obligaciones que debe contener el documento de seguridad.

VII. PROCEDIMIENTO PARA LA CANCELACIÓN DEL SISTEMA DE DATOS PERSONALES

Cancelación de soportes físicos:

- Para proceder a la baja documental de soportes físicos que contienen datos personales, se observan las disposiciones establecidas en los Lineamientos para la Organización y Conservación de Archivos de CAPUFE, así como en lo establecido en el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (DOF 04/05/2016). Dichos lineamientos prevén el asegurarse de la valoración de la información.

Cancelación de soportes electrónicos:

- El responsable del Sistema de Datos Personales debe solicitar oficialmente a la STI la cancelación del sistema. La solicitud debe incluir: Nombre del Sistema de Datos Personales; Fecha y en su caso hora de aplicación; Motivo de la cancelación e; Indicación sobre si el sistema debe mantenerse para consulta de la información, así como la lista de usuarios y/o roles que pueden tener acceso de consulta.

- La Subdirección de Tecnologías de Información:

  a) En la fecha y hora establecida, bloquea el acceso de todos los usuarios al sistema, mediante el método que la persona administradora del sistema determine más conveniente, por ejemplo: baja de los servicios de la aplicación; inactivación o suspensión de las cuentas de la persona usuaria; bloqueo de la base de datos para uso exclusivo de la persona administradora; entre otros.
  b) Realiza un respaldo completo de la información, acorde a los procedimientos y planes de respaldo aplicables del Sistema de Datos Personales. Además de la base de datos, el respaldo debe incluir, cuando aplique, los programas fuente, archivos ejecutables, archivos de configuración, archivos de datos de la persona usuaria, y en general cualquier componente del sistema. El medio en el que se realice el respaldo debe ser identificado y resguardado conforme a los procedimientos y planes de respaldo aplicables del Sistema de Datos Personales.
  c) Verifica que el respaldo se haya realizado correctamente, para lo cual realiza una prueba de recuperación acorde a los procedimientos y planes establecidos para el Sistema de Datos Personales.

d) Acorde a lo especificado por el responsable del Sistema de Datos Personales, en su caso, se procede a habilitar el esquema de consulta.

- Los Sistemas de Datos Personales permanecerán bloqueados durante el tiempo determinado por la vigencia documental de la información que maneja, acorde a los *Lineamientos para la Organización y Conservación de Archivos de CAPUFE* y a los *Lineamientos Generales para la Organización y Conservación de los Archivos de las Dependencias y Entidades de la Administración Pública Federal* (DOF 20/02/04).

Supresión del sistema:

- La persona responsable del Sistema de Datos Personales debe solicitar oficialmente a la STI la supresión del sistema. La solicitud debe incluir: Nombre del Sistema de Datos Personales; Fecha y en su caso hora de aplicación; y Motivo de la supresión. Asimismo:

- La persona responsable del Sistema de Datos Personales debe notificar oficialmente a las instancias competentes sobre la supresión del sistema, a fin de que se nombren testigos que den fe de los hechos.

- La Subdirección de Tecnologías de Información:

a) Realiza la baja los servicios que forman parte del Sistema de Datos Personales.

b) En presencia de testigos, se hace entrega al responsable del Sistema de Datos Personales del respaldo existente.

c) En presencia de testigos, aplica las técnicas de borrado seguro de todos los soportes electrónicos del sistema a cargo de la STI, con el fin de garantizar la efectiva destrucción de los datos contenidos en soportes electrónicos. Para ello se siguen las siguientes técnicas:

1. Para los discos duros, se sobrescribe con un solo valor (unos o ceros) el 100% de la superficie de los medios de almacenamiento no volátil en los que residen los datos del sistema cancelado.
2. Para las cintas magnéticas, se destruyen físicamente los medios de almacenamiento para lo cual se usan técnicas como la fundición, pulverización o incineración.
3. Cualquier otra técnica que tenga por objeto la destrucción de soportes electrónicos.

d) Se documentan los hechos mediante un Acta Administrativa, la cual contiene la relatoría de los acontecimientos y es firmada por todas las personas participantes y testigos.

Cancelación del Sistema de Datos Personales denominado “Padrón de Usuarios de Telepeaje”:

La Dirección Jurídica mediante oficio 09/J0U/DJ/0279/2023, señaló que llevó a cabo el procedimiento de cancelación y supresión del **Padrón de Usuarios de Telepeaje**, por lo que, solicitó a la Unidad de Transparencia realizar las gestiones necesarias que permitieran suprimir el registro del Programa Nacional de Protección de Datos Personales (PRONADATOS).

VIII. PROGRAMA GENERAL DE CAPACITACIÓN

En CAPUFE se garantizar el derecho humano a la protección de datos personales implica que el tratamiento a los mismos debe ir acorde a los principios, deberes y obligaciones que deberán observar los sujetos obligados conforme a la legislación nacional en materia de archivos y protección de datos personales.

En este sentido con la capacitación en términos de protección de la información, se busca que las personas servidoras públicas, identifiquen el tipo de información que manejan y el nivel de sensibilidad de la misma, además de conocer las mejores prácticas desde el punto de vista de seguridad de la información, propiciando que el tratamiento de datos personales se haga de una manera correcta y se evite el uso, sustracción, divulgación, ocultamiento, alteración, mutilación, destrucción total o parcial de manera indebida de datos personales, que pongan en peligro la confidencialidad, integridad y disponibilidad de la información así como las consecuencias, en caso de incumplimiento de las atribuciones, resguardo o la vulneración de los datos personales.

Para dar cumplimiento a la obligación de capacitación de acuerdo con lo establecido en los artículos 30 fracción III, 33 fracción VIII, 35 fracción VII, 83 y 84 fracción VII de la LGPDPPSO, así como el artículo 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, CAPUFE, a través de su Unidad de Transparencia realizó el Programa de Capacitación Institucional, en el cual se plantea capacitar y actualizar sobre el tratamiento de datos personales a las personas responsables y encargadas según sus roles y responsabilidades y que tienen acceso a datos personales para el desarrollo de sus funciones, con el fin de cumplir con la norma y mejorar los procesos de acceso a la información pública así como la protección de los datos personales, a través de:

- Formar, actualizar y profesionalizar la actividad de manera directa a todas las personas servidoras públicas, en especial a las personas encargadas de implementar las acciones para cumplir con el tratamiento de la información y de los datos personales que tienen bajo su responsabilidad;
- Llevar a cabo el tratamiento de la información y protección de datos personales conforme lo marcan los lineamientos respectivos y cumplir así con las disposiciones legales en la materia;
- Dar confianza a las personas de la protección de su información y datos personales, y
- Satisfacer requerimientos futuros con base a la planeación del manejo de información y de datos personales.

Y conforme a los siguientes ejes:
a) Programas a corto plazo para la difusión en general de la protección de datos personales en la organización y su importancia en el entorno laboral.
b) Programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;
c) Programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de organización de la Institución.

El programa de capacitación se basa en la oferta de cursos que tiene el INAI, los cuales se difundirán al personal de CAPUFE, pero especialmente a las personas servidoras públicas responsables del manejo de datos personales de este Organismo. Siendo algunos de éstos:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables.
- Inventario de Datos Personales.
- Elaboración de Avisos de Privacidad (integral y simplificado).
- Medidas de seguridad orientadas a la protección, seguridad y confidencialidad en el tratamiento de datos personales
- Protección de datos personales y seguridad pública.
- Derecho de portabilidad.
- Seguridad de datos personales y uso responsable de tecnologías en los sectores público y privado.
- Comunicación de datos personales y el flujo transfronterizo de los mismos.

IX. ACTUALIZACIONES

De conformidad con lo establecido en el artículo 36 de la LGPDPPSO, el presente Documento de Seguridad será actualizado cuando ocurra alguno de los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Asimismo, como medida de actualización general, se establece que, cuando se lleve a cabo la creación de un nuevo sistema de tratamiento de datos personales o simplemente la creación de bases de datos personales, independientemente del soporte, la persona titular de la Unidad Administrativa deberá designar al Administrador del sistema y dar aviso a la persona titular de la Unidad de Transparencia, de la creación del nuevo sistema, debiendo mencionar entre otros datos, el nombre, objetivo y fundamento legal del mismo; así como, los nombres, cargos y obligaciones del Responsable del Sistema, de los Administradores y de los Operadores, los datos personales recabados y su finalidad, con el objeto de integrarlos al Inventario de Sistemas de Tratamiento de Datos de CAPUFE.

Otro factor que determinará la actualización, es la emisión por parte del INAI, respecto de las herramientas metodológicas que se encuentra diseñando para orientar a los responsables en el cumplimiento de sus obligaciones en materia de protección de datos personales.

Bajo esa tesitura, la periodicidad para la revisión y en su caso actualización del Documento de Seguridad en el que se actúa, por primera vez se hará de manera anual, y posteriormente de forma bienal.

Finalmente, se informa que cuando exista alguna actualización, el Documento de Seguridad deberá ser sometido nuevamente al análisis, discusión y en su caso aprobación de los Integrantes del Comité de Transparencia de CAPUFE.

X.APROBACIÓN

- **Responsable del desarrollo:**

  Lcda. Martha Icsel Prieto Martínez, Subdirectora de Sistemas Electrónicos de Peaje, con núm. de extensión: **2117** y correo electrónico: fvazquezb@capufe.gob.mx .

  Lcda. Cynthia Lizeth Cruz Fernández, Subdirectora de Servicios al Usuario, con núm. de extensión: **2173** y correo electrónico: clcruzf@capufe.gob.mx .

  Lic. Luis Enrique Oropeza Olguín, Encargado del Despacho de la Subdirección de Finanzas, con núm. de extensión: **2108** y correo electrónico: leoropezao@capufe.gob.mx .

  C. Velia Yolanda Bravo Andrade, Subdirectora de Capital Humano y Desarrollo Organizacional, con núm. de extensión: **2152** y correo electrónico: vbravoa@capufe.gob.mx .

  Lic. Adolfo Amylkar Mateos Medina, Subdirector Jurídico Consultivo, con núm. de extensión: **2134** y correo electrónico: aamateosm@capufe.gob.mx .

- **Revisó:**

  Lcda. Laura Elena Gutiérrez Robledo, Subdirectora de Transparencia y Control Institucional y Titular de la Unidad de Transparencia de CAPUFE, con núm. de extensión: **2132** y correo electrónico: legutierrez@capufe.gob.mx .

  Lic. Christian Vargas Aguilar, Subdirector de Tecnologías de Información, con núm. de extensión: **3165**, correo electrónico: cvargas@capufe.gob.mx .

- **Autorizó:**

  Lcda. Laura Elena Gutiérrez Robledo, Subdirectora de Transparencia y Control Institucional y Titular de la Unidad de Transparencia de CAPUFE, con núm. de extensión: **2132** y correo electrónico: legutierrez@capufe.gob.mx .

- **Fecha de aprobación:**

  Septiembre de 2023.