CONTENIDO

1. OBJETIVO

Con la finalidad de dar cumplimiento con los principios, deberes y obligaciones en la normativa aplicable en de Protección de Datos Personales, se establecen los siguientes lineamientos a fin de garantizar una adecuada gestión de la seguridad de los datos personales que son tratados dentro de la organización.

2. ALCANCE

El presente documento tiene como alcance el tratamiento de los datos personales en el diseño, administración y operación de productos para medios de pago y servicios de atención telefónica a cliente, con base en el inventario de datos personales de TOKA, en cumplimiento con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, además de los deberes de seguridad, confidencialidad y las obligaciones establecidas en la Ley.

3. REFERENCIAS

Recomendaciones para la designación de la persona o departamento de Datos Personales.
Parámetros de Autorregulación en materia de Protección de Datos Personales.
Resolución Miscelánea Fiscal en su versión vigente
Sistemas de Gestión de la Calidad - Requisitos norma ISO 9001
Sistemas de Gestión de Seguridad de la Información – Requisitos norma ISO 27001
Sistemas de Gestión de la Continuidad del Negocio – Requisitos norma ISO 22301
Sistemas de Gestión Antisoborno – Requisitos norma ISO 37001
Sistemas de Gestión de Seguridad de Datos Personales – Conforme a la LFPDPPP, su Reglamento y Lineamientos.

4. DEFINICIONES

Activo: Cualquier bien que tiene valor para la organización (sistemas, equipos, soportes, edificios, personas, documentos, etc.).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Aviso de privacidad: Documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaban sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos, de conformidad con el artículo 14 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Confidencialidad: Acceso a la información por parte únicamente de quienes están autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datos personales: Información que corresponde a una persona física identificada o identificable. Una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Disociación: Procedimiento por el cual los datos personales no pueden asociarse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación del mismo.

Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Incidente: Acontecimiento repentino o inesperado que representa un peligro potencial y que podría terminar en daño físico, material, interrupción del proceso productivo y/o

compromiso de la integridad, confidencialidad y disponibilidad de la información de la empresa.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Parte interesada: Persona o grupo de personas con intereses específicos sobre una organización. Por ejemplo: inversionistas, clientes, proveedores, autoridades de protección de datos y titulares.

Persona Encargada o Encargado: Persona física o jurídica que sola o juntamente con otras trate datos personales por cuenta del responsable.

Política de gestión de datos personales: Documento controlado que estable los lineamientos a los cuales se deben de someter los procesos y tratamientos relacionados con la gestión de datos personales, determinando los principios, así como los roles y responsabilidades que tienen las partes involucradas.

Remisión: Comunicación de datos personales entre el responsable y el encargado, que se realiza dentro o fuera del territorio mexicano.

Responsable o Sujeto Regulado: Personas físicas o morales de carácter privado que llevan a cabo el tratamiento de los datos personales.

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

SGSDP: Sistema de Gestión de Seguridad de Datos Personales.

Titular o Persona Titular: Persona física a quien corresponde los datos personales.

Transferencia: Es el acto de comunicar o enviar datos personales a otra persona o entidad que no sea el titular (la persona dueña de los datos), el responsable (la entidad que decide

sobre el tratamiento de los datos) o el encargado (la persona o entidad que realiza el tratamiento de los datos personales por cuenta del responsable).

Tratamiento: Cualquier operación o conjunto de operaciones (acciones) realizadas sobre datos personales ya sea mediante procedimientos manuales o automatizados, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. ROLES Y RESPONSABILIDADES

Es responsabilidad del Director General:

- Determinar y asignar los recursos materiales, financieros y humanos necesarios para establecer, implementar, operar, mantener y mejorar el sistema de seguridad de protección de datos personales.
- Aplicar el proceso disciplinario ante los incidentes de seguridad de datos personales originado por los colaboradores.

Es responsabilidad del departamento de Datos Personales:

- Participar en la elaboración del SGSDP y en la presente política.
- Vigilar la implementación del SGSDP y la presente política de manera cotidiana.
- Comunicar las presentes políticas.
- Brindar asesoría técnica en materia de protección de datos personales y en la realización de proyectos.
- Elaborar y actualizar los avisos de privacidad.
- Dar trámite a las solicitudes de los titulares de datos personales, para el ejercicio de los derechos ARCO.
- Fomentar la protección de datos personales al interior de la organización.
- Realizar y administrar las notificaciones requeridas a la Secretaría y a otras autoridades, de conformidad con lo previsto en la Ley, su Reglamento y demás normativa aplicable.

- Realizar y administrar las comunicaciones requeridas a los interesados en relación con el SGSDP, la presente política y los esquemas.
- Atender los requerimientos realizados por la Secretaría y las autoridades sectoriales competentes.

Es responsabilidad del todos los Colaboradores:

- Cumplir con lo establecido en las presentes políticas.
- Informar al departamento de datos personales cualquier información adicional que será tratada.

6. POLÍTICAS DE SEGURIDAD DE DATOS PERSONALES

Toka, sus Colaboradores y Directores, se comprometen a cumplir con la legislación en protección de datos personales enlistadas dentro de los distintos procesos, acorde a las finalidades convenidas con los titulares, por lo que se emiten las siguientes políticas que serán de carácter obligatorio:

- El cumplimiento de todos los principios que establece el artículo 5 de la Ley: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, conforme a lo que señala la propia Ley, su Reglamento y demás normativa aplicable;

- Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud);

- Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento);

- Todo el personal de TOKA, deberá recabar los datos personales necesarios para relación jurídica a través de medios lícitos y previo consentimiento del titular (principio de licitud);

- El departamento de Desarrollo Organizacional deberá informar a los titulares los datos durante proceso de reclutamiento, selección y contratación, la información que se

recabará de ellos y con qué fines, a través FO-E-GE-02-01-01 Aviso de privacidad candidatos y FO-E-GE-02-01-02 Aviso de privacidad para trabajadores respectivamente (principio de información);

- Todos los colaboradores de TOKA, deberán asegurar que los datos personales tratados sean correctos y actualizados (principio de calidad);
- Queda estrictamente prohibido la utilización de datos personales para fines que no se encuentren establecidos en los avisos de privacidad (principio de finalidad);
- Todo el personal de TOKA, velará por que se respete la expectativa razonable de privacidad de los titulares (principio de lealtad);
- TOKA deberá tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en los avisos de privacidad (principio de proporcionalidad);
- Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad);
- Establecer y mantener medidas de seguridad (deber de seguridad);
- Guardar la confidencialidad de los datos personales (deber de confidencialidad);
- Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen;
- Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la organización;
- Respetar los derechos de los titulares en relación con sus datos personales;
- Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;

- Desarrollar e implementar un SGSDP de acuerdo a la política de gestión de datos personales, y;

- Definir las partes interesadas y miembros de la organización con responsabilidades específicas y a cargo de la rendición de cuentas para el SGSDP.

7. CUMPLIMIENTO A LOS PRINCIPIOS, DEBERES Y OBLIGACIONES EN PROTECCIÓN DE DATOS PERSONALES

Las presentes políticas pretenden instituir y afianzar la cultura de protección de datos personales entre los colaboradores de TOKA, personal externo y proveedores. Por lo que, cualquier violación a las mismas será penalizada de acuerdo con el RI-S-TH-03-09-01 Reglamento Interior de Trabajo o de manera penal, de acuerdo con las circunstancias, si así lo ameritan (en cumplimiento a los principios de licitud y lealtad).

Toka, cuenta con el aviso de privacidad integral vigente, publicado en la página de internet www.toka.com.mx, además del aviso de privacidad simplificado en el IVR, lo anterior con el objeto de informar a los usuarios los datos que son recabados y su finalidad, poniéndose a su disposición previo consentimiento del titular (en cumplimiento a los principios de licitud, lealtad, consentimiento, información, finalidad, calidad, responsabilidad).

Toka en cumplimiento a los principios de consentimiento, proporcionalidad, finalidad, calidad, responsabilidad, deberá prever en su relación con terceros, la inclusión de cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la organización. Asimismo, se deberá revisar el contrato generado entre la organización y el prestador respecto al nivel de servicio, incluyendo cualquier actualización de los términos y condiciones. Esto es importante en el caso de la designación de encargados por parte de un responsable de datos personales.

En temas de contratos de seguridad de servicios de almacenamiento de información y computo en la nube con un prestador de servicios en dicha rama, además de revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos

personales, de manera particular se deberá verificar: el nivel de acceso que tiene el prestador y limitar el tratamiento a lo estrictamente necesario para el cumplimiento de las condiciones del servicio; verificar el ciclo de vida de la información (por ejemplo, donde se almacena, como se replica, como se elimina en un ambiente distribuido, como se garantiza la eliminación de la información) y la ubicación física de la infraestructura del prestador.

Todos los colaboradores que recaben datos personales se encuentran obligados a notificar y consultar al departamento de datos personales cualquier información adicional que será tratada para que esta sea integrada al RE-E-GE-02-04-01 Inventario de datos personales, así como en el aviso de privacidad correspondiente (en cumplimiento a los principios de información, proporcionalidad y finalidad).

Toka tiene a su cargo elaborar una capacitación anual para la actualización y concientización del personal con acceso a datos personales, sobre las obligaciones en materia de protección de datos personales en el desarrollo de sus funciones. (en cumplimiento a los principios de información y responsabilidad).

Velar por la protección de los datos personales, poniendo a disposición de todos los colaboradores de Toka, la clasificación de los datos personales, así como el riego equivalente contenida en el RE-E-GE-02-04-01 Inventario de datos personales, así como en el MA-E-GE-02-01 Manual del sistema de gestión de datos personales, para efectos de concientizar sobre las implicaciones que trae consigo todo tratamiento de datos personales y la importancia de su privacidad. (en cumplimiento a los principios de información y responsabilidad).

Toka cuenta con el PO-S-TI-07-01 Políticas de Seguridad de la Información para evitar fuga de información o el acceso indebido a los datos personales, misma a la que deberán apegarse todos los colaboradores de Toka. (en cumplimiento a los principios de calidad y confidencialidad).

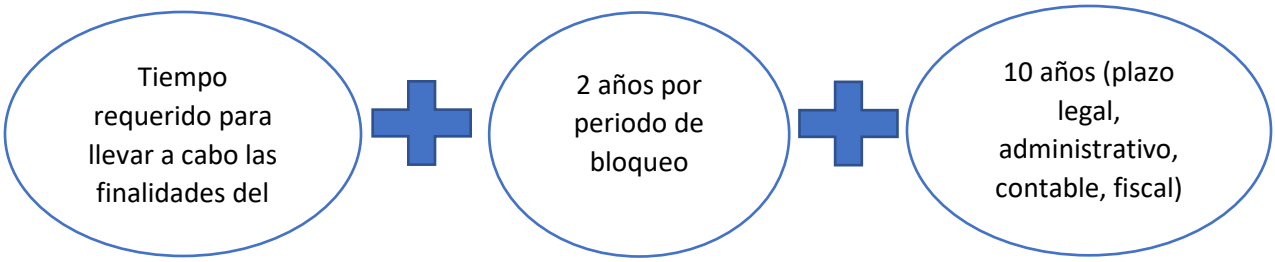
Se firma el FO-E-GE-02-01 Convenio de confidencialidad con terceros que tengan acceso a los datos personales en posesión Toka para que cumplan con la obligación de confidencialidad y realicen el tratamiento de los datos de conformidad con los términos

señalados en el aviso de privacidad de Toka. (en cumplimiento a los principios de consentimiento, proporcionalidad, finalidad, calidad, responsabilidad y confidencialidad).

Toka cuenta con un PG-E-GC-02-04 Programa anual de auditoría, mismo que le que permite supervisar, vigilar y verificar el grado de cumplimiento de la organización en materia de protección de datos personales. (en cumplimiento al principio de responsabilidad).

Los datos personales serán almacenados una vez cumplida su finalidad por el tiempo previsto en el RE-E-GE-02-04-01 Inventario de datos personales (10 años) (en cumplimiento al principio de proporcionalidad y calidad).

Los datos personales serán eliminados, de las bases de datos cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previo periodo de bloqueo y bajo la siguiente fórmula (en cumplimiento al principio de calidad).



De ser necesario y aplicable la eliminación de datos personales se deberá notificar al departamento de protección de datos personales para el apego de las disposiciones aplicables acorde al giro de la organización (en cumplimiento al principio de calidad).

TOKA se compromete a velar por los derechos de los titulares en relación con sus datos personales, a través de las buenas prácticas de sus colaboradores, así mismo, velará por el cumplimiento de estos principios, debiendo adoptar las medidas necesarias para su correcta aplicación, así como estableciendo y manteniendo medidas de seguridad (en cumplimiento a los principios de calidad y confidencialidad).

Mantener un sistema de gestión de seguridad de datos personales actualizado acorde a la normatividad aplicable, a través un encargado, que en este caso es el titular de la Dirección

de Normatividad, tal como se designa en el **MA-E-GE-02-01 Manual del sistema de gestión de datos personales** (en cumplimiento a los principios de licitud y lealtad).

8. COMUNICACIÓN Y REVISIÓN

- Las presentes políticas se encuentran disponibles y son comunicadas dentro de la organización por medio de intranet, fondos de pantalla y capacitaciones; la revisión de estas será en un periodo no mayor a un año o en caso de presentarse algún cambio relevante que impacte el sistema seguridad de datos personales.

9. CONTROL DE CAMBIOS

Revisión	Fecha	Cambio	Motivo	Responsable	Aprobó
00	24/04/23	Recodificación derivada de la estructura del Sistema de Gestión de Calidad.	Mejora	Normatividad	Dirección General
01	25/04/24	Se realiza la revisión acorde con el mantenimiento, sin sufrir cambios.	Mantenimiento	Normatividad	Dirección General
02	09/07/25	Actualización de los apartados **3. Referencias** y **4. Definiciones.**	Mejora	Normatividad	Dirección General