POLÍTICAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA OFICINA DE LA PRESIDENCIA DE LA REPÚBLICA

TÍTULO PRIMERO
DISPOSICIONES GENERALES
CAPÍTULO ÚNICO

Primera. Las presentes Políticas tienen por objeto, establecer los elementos mínimos que deben tomar en consideración los servidores públicos de la Oficina de la Presidencia de la República, en las actividades de dirección, operación y control de los procesos que, en el ejercicio de las atribuciones que tienen encomendadas, impliquen el tratamiento de datos personales, con la finalidad de garantizar la privacidad y autodeterminación informativa de las personas, así como el debido cumplimiento de las disposiciones contenidas en la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Tratados Internacionales en los que el Estado Mexicano forme parte, así como los Lineamientos que emitan el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, o en su caso, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

El lenguaje empleado en estas Políticas, no pretende generar ningún tipo de discriminación ni marcar diferencias entre hombres y mujeres, por lo que las referencias o alusiones en género masculino, incluyen siempre a hombres y mujeres, abarcando claramente ambos sexos.

Segunda. Además de las definiciones contenidas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para la interpretación de estas políticas, se entenderá por:

I. Activos. A los bienes tangibles o intangibles que posee la Oficina de la Presidencia de la República, donde pueden ser almacenadas las bases de datos.

II. Áreas responsables. A las unidades de apoyo técnico que forman parte integrante de la Oficina de la Presidencia de la República, o en su caso, las unidades administrativas de las que dispongan aquéllas, que en el ejercicio de las atribuciones que tienen encomendadas, involucren el tratamiento de datos personales.

III. Datos biométricos. A la información relacionada con las propiedades físicas, fisiológicas, de comportamiento o rasgos de personalidad, atribuibles a una persona, reconocidos universalmente como únicas, permanentes y medibles.

IV. Comité. Al Comité de Transparencia de la Oficina de la Presidencia de la República.

V. Instituto. Al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

VI. Ley General. A la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

VII. Lineamientos. A los Lineamientos Generales de Protección de Datos Personales para el Sector Público, aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicados en el Diario Oficial de la Federación el veintiséis de enero de dos mil dieciocho.

VIII. Políticas. A estas Políticas de Gestión y Tratamiento de Datos Personales de la Oficina de la Presidencia de la República.

IX. Servidores públicos designados. Los servidores públicos que nombren con tal carácter los titulares de las áreas responsables de la Oficina de la Presidencia de la República, a efecto de atender los requerimientos que, en materia de protección de datos personales, formulen la Unidad de Transparencia y/o el Comité de Transparencia de la Oficina de la Presidencia de la República.

X. Sistema de gestión de seguridad. Al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con las disposiciones contenidas en la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Tratados Internacionales en los que el Estado Mexicano forme parte, así como los Lineamientos que emitan el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, o en su caso, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XI. Solicitante. Toda persona física o jurídica, nacional o extranjera, que formule a la Oficina de la Presidencia de la República, una solicitud relacionada con los derechos ARCO.

XII. Unidad de Transparencia. A la Unidad de Transparencia de la Oficina de la Presidencia de la República.

XIII. Video vigilancia. Al uso de tecnologías de la información y comunicación para la grabación de imágenes fijas o en movimiento, con o sin sonido, de sistemas cerrados de televisión o de cualquier tecnología relativa a la captura de imágenes o video, que involucra la colocación de una o varias cámaras de videograbación en las instalaciones que ocupa la Oficina de la Presidencia de la República, cuyo único fin es la supervisión o monitoreo de las instalaciones y de las personas para su custodia, vigilancia y seguridad.

Tercera. Con independencia de lo establecido en el artículo 9 de la Ley General, respecto de las actuaciones del Comité, la Unidad de Transparencia y las áreas responsables, se aplicarán supletoriamente los Criterios de Integración y Funcionamiento del Comité de Transparencia de la Oficina de la Presidencia de la República.

Cuarta. Todos los servidores públicos de la Oficina de la Presidencia de la República, están obligados a prestar auxilio al Comité en la ejecución, coordinación y supervisión de acciones, que tengan como propósito garantizar el derecho a la protección de los datos personales, para lo cual deberán atender diligentemente los requerimientos que les formule la Unidad de Transparencia, a través de los servidores públicos designados.

Para tal efecto, el Comité tiene la facultad de exhortar a los servidores públicos, a que cumplan con los principios, deberes, bases y procedimientos que rigen en el tratamiento de datos personales, debiendo atender con celeridad y eficiencia los requerimientos específicos que les sean formulados, respetando estrictamente los plazos y términos establecidos en la Ley o disposición legal que resulte aplicable al caso concreto.

Cuando algún servidor público se niegue a atender los requerimientos del Comité o de la Unidad de Transparencia, se dará aviso al titular del área de su adscripción, solicitándole que lo conmine a realizar sin demora las acciones conducentes, con independencia de que pueda darse vista al Órgano Interno de Control, en caso de que se presuma alguna causa de responsabilidad administrativa.

Quinta. Para cumplir con los principios y deberes que rigen en la protección de datos personales, así como respetar el ejercicio de los derechos concedidos a favor de los titulares, prescritos en la legislación de la materia; los servidores públicos designados deberán considerar lo siguiente:

I. Atender oportunamente los requerimientos específicos que les formule la Unidad de Transparencia;

II. Cumplir con celeridad y eficiencia las obligaciones que derivan de la legislación en materia de protección de datos, con el objeto de reducir los tiempos de atención en beneficio de los titulares, considerando:

a) La ampliación del plazo para dar respuesta a las solicitudes relacionadas con el ejercicio de los Derechos ARCO, deberá formularse de manera excepcional y siempre que exista una razón que lo justifique; y

b) Las respuestas a las solicitudes relacionadas con el ejercicio de los Derechos ARCO, deberán ser claras y congruentes con lo requerido, utilizando un lenguaje sencillo y de fácil comprensión para el titular, así como cumplir todos y cada uno de los requisitos legales prescritos en la Ley General y en los Lineamientos.

III. Participar en la capacitación que se imparta en materia de protección de datos personales, conforme al programa aprobado por el Comité.

Sexta. La Unidad de Transparencia deberá llevar el registro de los servidores públicos designados, y mantenerlo permanentemente actualizado.

TÍTULO SEGUNDO

PRINCIPIOS Y DEBERES

CAPÍTULO I

EN RELACIÓN A LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Séptima. Las áreas responsables tratarán datos personales sensibles y/o datos biométricos, siempre y cuando ello resulte adecuado, relevante y estrictamente necesario para la finalidad que justifica su tratamiento, de forma tal que no exista otro medio menos invasivo y no se trate de una intromisión arbitraria en la intimidad de las personas.

Octava. En los casos en que se considere llevar a cabo el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original, las áreas responsables deberán contar con el consentimiento previo del titular, observando para tal efecto las reglas contenidas en la Ley General, los Lineamientos y demás disposiciones en la materia.

Novena. Cuando se determine llevar a cabo el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original, las áreas responsables deberán cumplir con las siguientes acciones:

I. Elaborar un informe justificado, suscrito por el titular del área, en el que se deberán fundar, motivar y razonar debidamente las finalidades concretas, lícitas y legítimas que justifiquen el tratamiento distinto de los datos personales, debiendo mencionar con toda claridad:

a) El mecanismo adoptado para la obtención del consentimiento del titular;

b) La expectativa razonable de privacidad del titular, basada en la relación que tiene con la Oficina de la Presidencia de la República;

c) Los datos personales que serán materia del tratamiento posterior y la naturaleza de éstos;

d) Las consecuencias para el titular, del tratamiento posterior de los datos personales; y

e) Las medidas adoptadas para que el tratamiento posterior cumpla con las disposiciones contenidas en la Ley General y los Lineamientos.

II. Remitir al Comité el informe justificado, a través de la Unidad de Transparencia, con anterioridad al tratamiento distinto de los datos personales.

Décima. Recibido el informe justificado, la Unidad de Transparencia procederá a someterlo a consideración del Comité, conforme al procedimiento previsto en los Criterios de Integración y Funcionamiento del Comité de Transparencia de la Oficina de la Presidencia de la República, a efecto de aprobar, modificar o revocar, en su caso, el tratamiento de los datos personales para finalidades distintas a aquellas que motivaron su tratamiento original.

Décima primera. Una vez que el Comité apruebe el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original, el área responsable deberá poner a disposición del titular, un nuevo aviso de privacidad, en sus dos modalidades.

Décima segunda. Tratándose de las bases de datos relacionadas con la administración de recursos humanos, corresponde a la Dirección General de Recursos Humanos, proveer a los titulares del aviso de privacidad simplificado, desde el momento de la recolección de sus datos personales, circunstancia que deberá ser debidamente documentada.

Por cuanto hace a los registros de acceso a inmuebles y de video vigilancia, la Dirección General de Recursos Materiales y Servicios Generales, deberá adoptar los mecanismos necesarios para que los avisos de privacidad simplificados se encuentren a la vista en los accesos de los inmuebles.

En los casos no previstos en los párrafos anteriores, las áreas responsables deberán adoptar las medidas necesarias para que los titulares conozcan los avisos de privacidad simplificados, desde el momento en que se recolecten sus datos personales, lo que deberá ser debidamente documentado.

Décima tercera. Es facultad exclusiva de las áreas responsables, a través del servidor público designado, solicitar al área técnica que corresponda, la publicación de los avisos de privacidad integrales en la página electrónica de la Oficina de la Presidencia de la República (www.gob.mx/presidencia), en el apartado de "Transparencia", sub apartado "Avisos de Privacidad", así como llevar a cabo el procedimiento de verificación respectivo.

CAPÍTULO II

EN RELACIÓN A LOS DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Décima cuarta. Con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización de las bases de datos, o en su caso, los sistemas de tratamiento que se efectúen, las áreas responsables deberán establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico que garanticen su confidencialidad, integridad y disponibilidad, así como su protección contra daño, pérdida, alteración, destrucción, uso indebido, acceso o tratamiento no autorizados.

Décima quinta. Tratándose de las medidas de seguridad administrativa, las áreas responsables deberán llevar a cabo, de manera enunciativa más no limitativa, las siguientes acciones:

I. No permitir el libre acceso a personal ajeno a la Oficina de la Presidencia de la República, al espacio donde se localizan los sistemas de tratamiento;

II. De existir ventanas o muros divisorios transparentes en el área de resguardo de los sistemas de tratamiento, obstruir la visión mediante películas traslúcidas u otro material análogo;

III. Mantener condiciones ambientales idóneas en el área de resguardo de los sistemas de tratamiento, que permitan preservar en buen estado los soportes físicos durante el tiempo de conservación;

IV. Colocar señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área;

V. En el acceso a las áreas de resguardo, colocar puertas con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura, debiendo mantener cerrado dicho mecanismo en días y horas no hábiles o cuando el personal autorizado que ahí labora se retira del área;

VI. Utilizar mobiliario dentro del área de resguardo, que proteja los soportes físicos en que se contienen los datos personales, de condiciones adversas como la humedad, temperatura, iluminación solar, polvo y presencia de plagas, entre otras;

VII. Utilizar mobiliario para almacenar los datos personales en soportes físicos, que cuente con cerraduras que impidan la libre apertura de sus puertas, cajones o compartimientos;

VIII. Designar a un responsable que mantenga el control y registro de la asignación de llaves, tarjetas, contraseñas de acceso y demás elementos para abrir los mecanismos de apertura de puertas y mobiliario;

IX. Capacitar al personal involucrado en el tratamiento de los datos personales, en materia de protección de los datos personales;

X. Informar al personal involucrado en el tratamiento de los datos personales, de las sanciones por incumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XI. Identificar plenamente los procedimientos en los cuales se lleve a cabo el tratamiento de datos personales;

XII. Llevar a cabo la revisión periódica de los procedimientos en los que se tratan datos personales, para identificar áreas de mejora o actualizar las etapas de los mismos y en su caso, los avisos de privacidad correspondientes; y

XIII. Establecer procedimientos internos para el tratamiento de datos personales, así como los servidores públicos autorizados para llevar a cabo los mismos.

Décima sexta. Respecto de las medidas de seguridad física, la Dirección General de Recursos Materiales y Servicios Generales, en coordinación con las áreas responsables, deberá realizar las siguientes acciones:

I. Desarrollar e implementar los programas de seguridad institucional, intramuros y extramuros, para salvaguardar la integridad del personal de la Oficina de la Presidencia de la República, la información y las instalaciones;

II. Registrar las entradas y salidas de los inmuebles que ocupa la Oficina de la Presidencia de la República, de personas ajenas a la institución, así como de vehículos y cualquier otro bien mueble, incluidos equipos de cómputo, que no sea propiedad de la misma;

III. Establecer áreas delimitadas para el acceso de personas y vehículos a los inmuebles, con presencia permanente de elementos de seguridad, las cuales permanecerán cerradas en días y horas inhábiles;

IV. Mantener en los accesos a los inmuebles, detectores de metales portátiles o de mano (llamados "Garrett"), o en su caso, banda de rayos X, con la finalidad de detectar cualquier metal oculto en bolsas, mochilas y portafolios;

V. Supervisar las cámaras de video vigilancia y demás tecnología de seguridad de la Oficina de la Presidencia de la República, con el único propósito de salvaguardar la seguridad del personal, instalaciones, información y bienes propiedad de ésta.

VI. Gestionar los accesos al Centro de Datos solicitados por la Dirección General de Tecnologías de la Información, con el fin de que solamente personal autorizado pueda llevar a cabo actividades en el mismo.

VII. Elaborar y coordinar los procedimientos y protocolos a seguir en caso de emergencia o contingencia, con el propósito de garantizar la integridad del personal adscrito a la Oficina de la Presidencia de la República, la información y sus instalaciones.

VIII. A través del Programa Interno de Protección Civil, realizar las siguientes acciones:

a) Establecer las acciones preventivas, de auxilio y recuperación o vuelta a la normalidad, destinadas a salvaguardar la integridad física de los empleados y visitantes, así como proteger las instalaciones, bienes e información, ante la ocurrencia de alguna calamidad.

b) Diseñar, instrumentar y operar, medidas para minimizar o evitar los riesgos y/o daños, tanto humanos como materiales, que pudiesen generar por su impacto o presencia de agentes perturbadores (fenómenos de origen natural o aquellos provocados por la acción del hombre).

c) Adoptar medidas para la prevención y combate de incendios como son: la instalación de extinguidores y la revisión de hidrantes, la existencia de una brigada para la prevención y combate de incendios, vigilar el mantenimiento del equipo contra incendio, evitar la sobrecarga de líneas eléctricas y que no exista acumulación de material inflamable, verificar que las instalaciones eléctricas el mantenimiento preventivo y correctivo de manera permanente, para que las mismas

ofrezcan seguridad, conocer el uso de los equipos de extinción de fuego, así como el uso que se le dé, de acuerdo a cada tipo de fuego.

Décima séptima. El desarrollo y administración de las Políticas de Seguridad e Integridad de la Información, así como de los medios de comunicación en materia de tecnología de la información de la Oficina de la Presidencia de la República se regirán de acuerdo a lo dispuesto por el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), o el documento que lo sustituya y que sea publicado en el Diario Oficial de la Federación.

Décima octava. Corresponde a la Unidad de Transparencia, llevar un registro actualizado de las bases de datos con las que cuenta la Oficina de la Presidencia de la República, catalogados por área responsable.

Décima novena. Es responsabilidad exclusiva de las áreas responsables, elaborar y mantener actualizados los sistemas de gestión de seguridad de las bases de datos que administren, debiendo considerar que cada base de datos contará con su propio sistema de gestión de seguridad.

Vigésima. Además de lo dispuesto en el artículo 32 de la Ley General, en la elaboración de los sistemas de gestión de seguridad, las áreas responsables deberán considerar los siguientes aspectos:

I. La **identificación** de los datos personales de acuerdo a su clasificación y tipo, vinculados con la información que permita conocer el tratamiento al que son sometidos y su relación directa con el flujo del sistema;

II. Los **roles y responsabilidades** específicas de los servidores públicos involucrados con los tratamientos de datos personales;

III. El **inventario** de activos; y

IV. El **documento** de seguridad.

Vigésima primera. Con el propósito de adoptar las medidas de seguridad, las áreas responsables deberán atender la siguiente clasificación de datos personales:

I. De identificación. Nombre, domicilio, teléfono y correo electrónico particulares, estado civil, firma autógrafa, Registro Federal de Contribuyentes (RFC), Clave de Elector (INE), Clave Única del Registro de Población (CURP), fecha de nacimiento, edad y nacionalidad, entre otros.

II. Laborales. Información relacionada con el reclutamiento como cargo, incidencias, capacitación, domicilio del trabajo, correo y teléfono institucionales, entre otras.

III. Patrimoniales. Propiedad de bienes muebles e inmuebles, información fiscal, ingresos y egresos, cuentas bancarias, seguros, entre otros.

IV. De procedimientos. Información concerniente a procedimientos laborales, civiles, penales y/o administrativos, en los que el titular sea parte.

V. Académicos. Trayectoria educativa, número de cédula profesional, calificaciones escolares, entre otros.

VI. Ideológicos. Creencias religiosas, afiliación política y sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas.

VII. De salud. Historia clínica, incapacidades médicas, intervenciones quirúrgicas, uso de aparatos oftalmológicos, ortopédicos o auditivos, estado psicológico o psiquiátrico, entre otros.

VIII. Características personales. Tipo de sangre, ácido desoxirribonucleico (ADN), huella digital, iris ocular, entre otros.

IX. Características físicas. Color de piel, color de cabello, señas particulares, estatura, peso y complexión, entre otros.

X. Vida Sexual. Preferencia.

XI. Origen. Étnico o racial.

Vigésima segunda. Para los efectos de la política anterior, los datos personales deberán clasificarse en los siguientes grupos:

Grupo 1. De identificación, laborales y académicos.

Grupo 2. Patrimoniales y de procedimientos.

Grupo 3. Ideológicos, de salud, características personales, características físicas, vida sexual y origen.

Vigésima tercera. En la elaboración del inventario de datos personales, las áreas responsables deberán determinar el ciclo de vida respecto de cada tratamiento que se efectúe, considerando la obtención, almacenamiento, uso, procesamiento, divulgación, bloqueo, cancelación, supresión,

destrucción o cualquier otra operación realizada en función de las finalidades para los que fueron recabados los datos personales.

Vigésima cuarta. Es obligación de las áreas responsables llevar a cabo la supresión de los datos personales, de conformidad con el procedimiento establecido en el sistema de gestión de seguridad de datos personales del sistema de tratamiento que corresponda.

Vigésima quinta. Con independencia de lo dispuesto en la Ley General y los Lineamientos, respecto del plan de trabajo que forma parte del documento de seguridad, las áreas responsables deberán adoptar las siguientes acciones:

I. **Revisión y mantenimiento al análisis de riesgo.** La revisión deberá ejecutarse de acuerdo a lo señalado en el apartado de "Mecanismos de monitoreo y revisión de las medidas de seguridad", bajo la metodología del análisis de riesgo en un proceso de mejora continua.

II. **Actualización del sistema de gestión de seguridad de la información.** Se deberá realizar la actualización a los documentos asociados al análisis de riesgo para documentar algún incidente, en su caso, para determinar el plan de tratamiento y determinación de riesgo de los activos de información. Así mismo, la revisión de los controles de seguridad informática establecidos y en caso de detectarse, la implantación de las medidas de seguridad faltantes.

III. **Evaluación del sistema.** Se deberán revisar, de modo periódico, los documentos y controles para la seguridad tecnológica de los sistemas de gestión de seguridad de las bases de datos y las políticas de gestión y tratamiento de datos personales, así como el cumplimiento de las observaciones de las auditorías correspondientes, en caso que hubiesen.

IV. **Mejora continua.** Deberán evaluarse periódicamente los sistemas de gestión de seguridad de las bases de datos, en las partes en que se demuestre el cumplimiento de las políticas correspondientes y la normativa respectiva.

Vigésima sexta. Como parte de los mecanismos de monitoreo, a efecto de llevar a cabo la verificación de la efectividad de los sistemas de gestión de seguridad de las bases de datos deberán realizarse las siguientes actividades:

I. **Identificación e inventario de datos personales:** Revisión del inventario de datos personales, así como la identificación de nuevos datos personales a los que se les da tratamiento en las áreas responsables, con el fin de agregar los datos personales necesarios, así como eliminar aquellos que no sean o dejen de ser indispensables para las finalidades para las que fueron obtenidos.

II. **Análisis de riesgo:** Su objetivo es la identificación, clasificación y priorización de los riesgos existentes o nuevos, derivados de amenazas o posibles vulnerabilidades, para estar en posibilidades de evaluar el impacto sobre los datos personales.

III. **Análisis de brecha:** Su objetivo es identificar el nivel de resultados y cumplimiento de los controles implementados y en caso de ser necesario implementar medidas físicas, técnicas o administrativas adicionales, posterior a cada análisis de riesgo.

Dichas actividades deberán ser realizadas por el área responsable, preferentemente el servidor público designado, que deberá estar capacitado en materia de protección de datos personales.

La unidad que administra el sistema de tratamiento, deberá realizar las actualizaciones correspondientes, en caso de ser necesarias, e informará al servidor público responsable de los cambios realizados al sistema. Dicha actualización, deberá plasmarse en el documento de seguridad y deberá notificarse al Comité a través de la Unidad de Transparencia de las modificaciones realizadas.

Derivado de los cambios detectados, el área responsable deberá revisar los resultados del análisis de riesgos de los datos personales de la Institución e instruir, en su caso, al área que administra el sistema de tratamiento de datos personales para que se efectúen los trabajos necesarios para su actualización. Los acuerdos establecidos en las reuniones de trabajo para la revisión del análisis de riesgos, deberán formalizarse mediante minutas que deberán ser firmadas por los participantes.

En caso de haber cambios en el sistema de tratamiento, el área responsable deberá revisar, los resultados del análisis de medidas de seguridad de los datos personales implementadas e instruir, en su caso, al área que administra el sistema de tratamiento de datos personales para actualizar los controles de seguridad aplicados y su efectividad. Los acuerdos establecidos en las reuniones de trabajo para la revisión del análisis de brecha, deberán formalizarse mediante minutas que deberán ser firmadas por los participantes.

Vigésima séptima. Durante la fase de monitoreo del sistema, deberá revisarse y registrar al menos los siguientes puntos:

I. Resultados de revisiones periódicas al sistema de gestión.

II. Retroalimentación de usuarios y partes involucradas en el tratamiento de datos personales.

III. Herramientas, técnicas y métodos para la mejora del desempeño y efectividad del sistema.

IV. Estado de las acciones correctivas y preventivas y eventos de seguridad en el área que administra el sistema (incidentes).

V. Vulnerabilidades y/o amenazas no contempladas en el más reciente análisis de riesgo.

VI. Acciones de seguimiento a compromisos de revisiones previas.

VII. Cualquier cambio que pudiera afectar al sistema.

VIII. Recomendaciones para la mejora del sistema.

Vigésima octava. Los resultados de la revisión deberán incluir aspectos relativos a:

I. Mejoras sugeridas.

II. Modificaciones a metodologías o documentos del sistema.

III. Requisitos de seguridad de información.

IV. Requisitos legales.

V. Nuevos riesgos, sus niveles y su asunción o no.

VI. Necesidades de recursos.

Para tales efectos, las áreas responsables deberán mantenerse en constante comunicación con la Dirección General de Tecnologías de la Información, quien administra la plataforma de Tecnologías de la Información y Seguridad de la Información, así como con la Unidad de Transparencia, para la debida actualización de los sistemas de gestión de seguridad de las bases de datos de las áreas responsables, considerando las disposiciones en materias de protección de datos personales, archivos, tecnologías de la información, comunicaciones y de seguridad de la información, así como las recomendaciones emitidas por el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, o en su caso, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Vigésima novena. Corresponde a la Unidad de Transparencia, en conjunto con las áreas responsables, elaborar un programa anual de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales, el cual deberá ser sometido a consideración del Comité, para su aprobación.

Trigésima. Las áreas responsables deberán implementar las medidas de seguridad de nivel alto, medio o bajo, conforme la clasificación de los datos personales que traten, con el objeto de evitar la alteración, pérdida, fuga, acceso o uso no autorizado o fraudulento de los datos personales.

Trigésima primera. Todos los servidores públicos que intervengan en el tratamiento de datos personales, tienen la obligación de guardar confidencialidad respecto de los datos personales que conozcan con motivo del ejercicio de sus atribuciones. Esta obligación subsiste aún después de finalizada la relación que dio origen a la recolección y tratamiento del dato.

Trigésima segunda. Las actualizaciones a los sistemas de tratamiento deberán realizarse siempre que haya cambios en los mismos, por las áreas responsables o a petición de los titulares de las unidades de apoyo técnico o de las unidades adscritas a éstas. Dichas actualizaciones deberán ser notificadas al Comité a través de la Unidad de Transparencia, para que éste a su vez confirme, modifique o revoque dichas actualizaciones.

TÍTULO TERCERO

DE LOS PROCEDIMIENTOS PARA RECIBIR Y RESPONDER DUDAS Y QUEJAS

CAPÍTULO I

DISPOSICIONES COMUNES

Trigésima tercera. Cualquier titular, por sí mismo o a través de su representante, podrá expresar sus dudas o formular quejas, en relación al tratamiento de sus datos personales que lleve a cabo la Oficina de la Presidencia de la República, para lo cual deberá presentar escrito libre ante el área responsable que corresponda o la Unidad de Transparencia, personalmente en su domicilio, vía correo postal o mediante el correo electrónico transparencia@presidencia.gob.mx.

Solo se admitirá la expresión verbal de dudas, cuando las mismas se resuelvan con la orientación a plazos, términos y/o procedimientos establecidos en las disposiciones jurídicas aplicables o a la información publicada en medios de difusión oficiales, debiéndose resolver las mismas de manera inmediata.

Trigésima cuarta. Con exclusión de lo establecido en el último párrafo de la política anterior, cuando la expresión de dudas o la formulación de quejas se realice de manera verbal, los servidores públicos ante quienes se presenten, deberán exhortar al interesado para que las realice por escrito, debiendo informarle los requisitos mínimos que debe contener el mismo, los domicilios del área responsable y de la Unidad de Transparencia, así como los mecanismos para su presentación, lo que se hará constar en un acta circunstanciada.

Trigésima quinta. El escrito de expresión de dudas o de formulación de quejas, deberá cumplir cuando menos los siguientes requisitos:

I. Nombre de quien promueve, así como su domicilio y/o correo electrónico para recibir notificaciones.

II. Tratándose del titular o su representante legal, los documentos que acrediten sus identidades y personalidad, según sea el caso.

III. De ser posible, el área responsable que da tratamiento a sus datos personales, así como la base de datos en que se encuentran registrados los mismos.

IV. Las dudas específicas respecto de las cuales se requiere respuesta o, en su caso, la descripción clara y precisa de los hechos en que se funde la queja.

V. Cualquier otro elemento o medio de convicción en que se sustenten las dudas o quejas formuladas.

Trigésima sexta. Cuando el promovente sea omiso en señalar domicilio o correo electrónico para recibir notificaciones, la Unidad de Transparencia o las áreas responsables, deberán realizar las notificaciones en los estrados que se ubiquen en sus respectivas oficinas.

Trigésima séptima. La presentación mediante correo electrónico de los escritos de expresión de dudas o formulación de quejas, conlleva la aceptación tácita del interesado, para que las notificaciones se efectúen por el mismo medio.

Trigésima octava. Todas las áreas de la Oficina de la Presidencia de la República, tienen la obligación de recibir los escritos de expresión de dudas o de formulación de quejas, aun cuando no sean las responsables del tratamiento de datos personales, caso en que deberán remitir las promociones correspondientes a la Unidad de Transparencia, a más tardar al día siguiente hábil al en que fueron recibidas.

CAPÍTULO II
DE LAS DUDAS

Trigésima novena. Recibido el escrito de expresión de dudas y dentro de un plazo que no exceda de cinco días, improrrogables, las áreas responsables o la Unidad de Transparencia, según corresponda, notificarán al interesado la respuesta respectiva, la cual deberá cumplir con los requisitos de congruencia y exhaustividad que rigen a todo acto administrativo.

Cuadragésima. La Unidad de Transparencia podrá solicitar a las áreas responsables, la información que estime necesaria para dar respuesta a las dudas planteadas por el titular o su representante, ello sin dejar de cumplir con el plazo establecido en la política precedente.

Cuadragésima primera. Si del análisis del escrito de expresión de dudas, se advierte que la pretensión del interesado, consiste en obtener información generada o en posesión de la Oficina de la Presidencia de la República, conforme al ejercicio de las atribuciones que tiene encomendadas o se relaciona con el ejercicio de los Derechos ARCO, el área responsable o la Unidad de Transparencia, procederán acorde con los procedimientos establecidos en la Ley Federal de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como los Lineamientos que en esas materias emita el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, o en su caso, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

CAPÍTULO III
DE LAS QUEJAS

Cuadragésima segunda. Cuando los escritos de queja se presenten ante el área responsable, ésta deberá remitirlos a la Unidad de Transparencia en un plazo de tres días, debiendo adjuntar un informe escrito respecto de los hechos o motivos expresados por el quejoso, así como las pruebas que estime pertinentes para desvirtuarlos.

Cuadragésima tercera. La Unidad de Transparencia podrá prevenir al denunciante, dentro de los tres días posteriores a la recepción de la queja, para que en el plazo de tres días realice lo siguiente:

I. Exhiba los documentos con los que acredite su identidad, o en su caso, la identidad y personalidad, cuando la promoción la realice el titular o su representante.

II. Aclare o precise los motivos de su queja, en relación con los principios o deberes que estime incumplidos.

III. Exhiba las pruebas que se relacionen a los hechos afirmados en su queja, de ser posible.

En el caso de que no se desahogue la prevención en el periodo establecido para tal efecto, deberá desecharse la queja, dejando a salvo los derechos del quejoso para volver a presentar la misma.

Cuadragésima cuarta. Durante el procedimiento a que se refiere el presente capítulo, el Comité y la Unidad de Transparencia, según corresponda, deberá aplicar la suplencia de la deficiencia de la queja, siempre y cuando no se modifiquen los hechos o peticiones expuestas por el quejoso en el escrito correspondiente.

Cuadragésima quinta. Si la queja no versa sobre presuntos incumplimientos a los principios y deberes establecidos en la Ley General, se refiera al ejercicio del derecho de información o de los Derechos ARCO, o corresponda a la promoción de algún medio de impugnación previsto en el citado ordenamiento legal, la Unidad de Transparencia dictará un acuerdo de desechamiento, dejando a salvo los derechos del promovente para que los haga valer por la vía y forma correspondientes.

Cuadragésima sexta. La Unidad de Transparencia deberá notificar al área responsable la queja, dentro de los tres días siguientes a su admisión.

Cuadragésima séptima. El área responsable deberá enviar, a la Unidad de Transparencia, un informe escrito respecto de los hechos o motivos de la queja, dentro de los tres días siguientes a la notificación anterior, aportando los medios de convicción que acrediten el cumplimiento de los principios y deberes en cuestión.

El Comité, a través de la Unidad de Transparencia, podrá realizar las diligencias o verificaciones virtuales que procedan, así como solicitar los informes complementarios al área responsable, para allegarse de los elementos de juicio que considere necesarios para resolver la queja.

En el caso de informes complementarios, el área responsable deberá responder a los mismos en el término de tres días siguientes a la notificación correspondiente.

Cuadragésima octava. Recibido el informe del área responsable, o en su caso los informes complementarios, la Unidad de Transparencia turnará el asunto al Comité, quien deberá resolver la queja dentro de los veinte días siguientes.

La resolución debe ser fundada y motivada e invariablemente debe pronunciarse sobre el cumplimiento de los principios y deberes prescritos en la Ley General.

De existir incumplimiento, se deberá señalar el artículo, fracción, párrafo y/o inciso de la Ley General, que prescribe el principio o deber transgredido, especificando las razones por las cuales se arribó a dicha conclusión, así como las medidas que deberá adoptar el área responsable para garantizar el derecho a la protección de los datos personales del titular, determinando un plazo para su cabal cumplimiento e informe al Comité sobre el mismo.

Cuadragésima novena. La Unidad de Transparencia deberá notificar la resolución al quejoso y al área responsable, dentro de los tres días siguientes a su emisión.

Las resoluciones que emita el Comité son definitivas e inatacables.

El área responsable deberá cumplir con la resolución en un plazo de diez días a partir del día hábil siguiente al en que se le notifique la misma.

Quincuagésima. Transcurrido el plazo señalado en la política anterior, el área responsable deberá informar al Comité, a través de la Unidad de Transparencia, sobre el cumplimento de la resolución.

La Unidad de Transparencia verificará el cumplimiento a la resolución, si considera que se dio cumplimiento a la misma se emitirá un acuerdo de cumplimiento y se ordenará el cierre del expediente.

Cuando la Unidad de Transparencia considere que existe un incumplimiento total o parcial de la resolución, dará vista al Comité, quién analizará el asunto y en caso de corroborar el incumplimiento, ordenará notificar dicha circunstancia al titular del área responsable, para el efecto de que, en un plazo no mayor a cinco días, se dé cumplimiento a la resolución.

En cualquier parte del procedimiento, el Comité podrá dar vista al Órgano Interno de Control, respecto de hechos que pudieran constituir responsabilidad administrativa.

Quincuagésima primera. En caso de que la denuncia verse sobre posibles incumplimientos de la Ley General, distintos a los señalados en el Título Segundo, el Comité determinará la procedencia de la misma y dará vista al Órgano Interno de Control, para que determine lo conducente.

T R A N S I T O R I O S

Primero. Las presentes Políticas entrarán en vigor, al día siguiente de su aprobación por el Comité.

Segundo. Se abrogan las Políticas Generales de Protección de Datos Personales de la Oficina de la Presidencia de la República, aprobadas mediante Acuerdo CT/PR/11SO/2018/VIII, emitido en el Octavo Punto del Orden del Día, correspondiente a la Décima Primera Sesión Ordinaria celebrada el ocho de noviembre de dos mil dieciocho.

Tercero. Se instruye a la Unidad de Transparencia a que realice las gestiones necesarias, a efecto de que las presentes Políticas sean publicadas en el Portal Electrónico de la Oficina de la Presidencia de la República.