POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA COMISIÓN NACIONAL FORESTAL

UNIDAD DE TRANSPARENCIA.

Enero 2024

INTRODUCCIÓN

De conformidad con el artículo 33, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en el 56 de los Lineamientos Generales de Protección de Datos Personales para el sector público, en los cuales se prevén la realización de políticas que tomen en cuenta el contexto en el que se realiza el tratamiento de los datos personales de acuerdo a lo siguiente:

1. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y en Lineamientos generales.
2. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de la organización, relacionados con los tratamientos de datos personales que se efectúen.
3. Las sanciones en caso de incumplimiento.
4. La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.
5. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.
6. El proceso general de atención de los derechos ARCO

Con la instrumentación de estas políticas se posibilita a las Unidades Administrativas que integran esta Entidad, realizar un tratamiento de datos personales, en estricto apego a los principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones legales aplicables, lo cual permite garantizar su adecuada protección y el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición por parte de sus titulares.

El objetivo general será implementar y asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales y, el presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la Comisión Nacional Forestal que conforme a sus atribuciones realicen tratamiento de datos personales.

GLOSARIO

Acuerdo de Confidencialidad: documento que tiene por objeto que terceros distintos al personal de la Comisión Nacional Forestal que conozcan sobre datos personales.

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Área: áreas administrativas a las que se confieren atribuciones Según el Estatuto Orgánico de la Comisión Nacional Forestal.

CONAFOR: Comisión Nacional Forestal.

Comité de Transparencia: instancia a la que hacen referencia los artículos 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Criterio: pauta que obliga a tomar en cuenta todos los elementos disponibles de un caso para elegir de entre las posibles alternativas la mejor, con la finalidad de establecer los principios para la resolución de casos subsecuentes.

Derechos ARCO: son los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Documento: los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro sin importar su fuente o fecha de elaboración.

Encargado: 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 de la Comisión Nacional Forestal.

Enlace en materia de datos personales: persona o personas designadas por las personas titulares de cada área competente ante la Unidad de Transparencia, con la finalidad de mantener un vínculo de

comunicación permanente para las gestiones derivadas de las normas aplicables en la materia.

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

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Políticas: Políticas internas para la gestión y el tratamiento de los datos personales en posesión de la Comisión Nacional Forestal.

Remisión: toda comunicación de datos personales realizada entre las áreas competentes de la Comisión Nacional Forestal y el encargado del tratamiento de datos personales, dentro o fuera del territorio mexicano.

Sistema o sistemas de datos personales: archivo físico, electrónico o mixto que contenga datos personales recabados en el ejercicio de las funciones, facultades y atribuciones de las áreas competentes.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Terceros: cualquier individuo diverso al personal que, por motivos académicos, proyectos, prestación de servicios o alguna otra causa, conozca los datos personales en posesión de la Comisión Nacional Forestal.

Transferencia: toda comunicación de datos personales nacional o internacional realizada a persona distinta del titular, las áreas competentes de la Comisión Nacional Forestal o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Titular: la persona física a quien corresponden los datos personales.

DISPOSICIONES GENERALES

1. Se debe realizar el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas de la CONAFOR dentro del marco legal en la materia y del consentimiento de la persona titular.

2. Las áreas deberán identificar los avisos de privacidad que se requieren, según los tratamientos que realicen.

3. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado; el aviso de privacidad debe encontrarse en un lugar visible o publicado en la página oficial de la CONAFOR.

4. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.

5. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de sus atribuciones y funciones.

6. Es obligación de todas las personas servidoras públicas de la CONAFOR que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

7. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos.

8. Los avisos de privacidad deberán contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.

9. Las áreas deberán verificar que sus avisos de privacidad se difundan en la página oficial de la CONAFOR.

PRINCIPIOS, DEBERES Y DEMÁS OBLIGACIONES.

Principio de licitud: Los datos personales tienen que ser tratados de manera lícita, esto es, se debe definir claramente para qué se tratan los datos personales de manera concreta, licita, explicita y legitima.

Asimismo, deberán estar relacionados con las atribuciones que la normatividad aplicable confiera.

Actividades vinculadas al principio de licitud:

1. Revisar que los datos se traten conforme a la LGPDPPSO, Lineamientos Generales de Protección de Datos Personales para el Sector Públicos y demás normativa aplicable.
2. Las áreas deben identificar el marco normativo que en el ámbito de sus funciones se encuentra relacionado con el tratamiento de datos personales, el tipo de datos objeto de tratamiento y las finalidades para ello.

Principio de Finalidad: Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, se deben definir claramente para qué se tratan los datos personales, las cuales deben ser:

- Concretas
- Lícitas
- Explícitas y
- Legítimas

Actividades vinculadas al principio de finalidad:

1. Establecer detalladamente en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales, las cuales deben ser acordes a las atribuciones o facultades que tienen encomendadas.
2. Tratar los datos personales, conforme a las finalidades concretas, lícitas, explícitas y legítimas, expresadas en el aviso de privacidad.
3. No pedir datos que no son necesarios (“por si acaso después hace falta”). Sólo pueden ser tratados los datos que resulten adecuados, pertinentes y no excesivos en relación con la finalidad para la que se obtuvieron.

Principio de Lealtad: El Responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos,

privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en el Responsable, respecto de que los datos personales proporcionados serán tratados conforme a los términos establecidos por esta Ley.

Actividades vinculadas al principio de lealtad:

1. Obtener y tratar los datos personales sin que medie dolo, mala fe o negligencia.
2. Tratar los datos conforme lo acordado e informado a la persona titular de los datos personales.
3. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.
4. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta.

Principio de Consentimiento: las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Es necesario para el tratamiento de sus datos que el consentimiento sea:

-Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

-Específico: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e

-Informado: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

El consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario en términos de lo señalado en el artículo 21, segundo párrafo de la Ley General.

Actividades vinculadas al principio de consentimiento:

1. Obtener el consentimiento del/de la titular, previo al tratamiento de los datos, salvo que se actualice alguno de los supuestos de excepción descritos en el artículo 22 de la Ley General.
2. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.
3. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que este se requiera.

Principio de calidad: El Responsable 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.

Se entiende que los datos personales son:

I. Exactos y correctos: Cuando los datos personales no presentan errores que pudieran afectar su veracidad, es decir, son verdaderos o fieles.
II. Completos: Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y las atribuciones del responsable.
III. Actualizados: Cuando los datos personales responden fielmente a la situación actual del/de la titular.
IV. Se presume que se cumple con la calidad en los datos personales cuando estos son proporcionados directamente por el/la titular y hasta que no manifieste y acredite lo contrario.

Actividades vinculadas al principio de calidad:

1. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos.
2. Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística.
3. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

Principio de proporcionalidad: Las áreas que realicen tratamiento de datos personales deberán recabar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

En términos del artículo 25 de la Ley General y los presentes Lineamientos generales, se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable.

Actividades vinculadas al principio de proporcionalidad:

1. Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
2. Limitar al mínimo posible el periodo de tratamiento de datos personales.
3. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.

Principio de información: Las áreas que realicen tratamiento de datos personales deben informar a los/las titulares a través de los avisos de privacidad, las características principales del tratamiento al que serán sometidos sus datos personales.

Actividades vinculadas al principio de información:

1. Poner gratuitamente a disposición de los/las titulares el aviso de privacidad en los términos que fije la Ley General y los Lineamientos Generales, aunque no se requiera su consentimiento para el tratamiento de los datos personales.
2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular.
3. Promover que los avisos de privacidad sean redactados de conformidad con lo establecido por la Ley General y los Lineamientos Generales, de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento.
4. Comunicar el aviso de privacidad a quienes se transfieran datos personales.

Principio de responsabilidad. Conforme al principio de responsabilidad, las áreas deben velar por el cumplimiento del resto de los principios, promover la adopción de medidas necesarias para su aplicación y, demostrar ante los/las titulares y la autoridad, que se cumplen con las obligaciones en torno a la protección de los datos personales.

Actividades vinculadas al principio de responsabilidad:

1. Incentivar la capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
2. Revisar periódicamente el programa de protección de datos personales y el Documento de Seguridad para determinar las modificaciones que se requieran.
3. Establecer procedimientos para recibir y responder dudas y quejas de los/las titulares.

Deber de confidencialidad. Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Actividades vinculadas al deber de confidencialidad:

1. Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados.
2. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con el responsable o con la persona titular.
3. Implementar campañas de sensibilización y capacitación para el personal, sobre la importancia de la confidencialidad de los datos personales y para que conozcan sus obligaciones con relación al tratamiento de datos personales.

Deber de seguridad. Las áreas deberán establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales a fin de evitar cualquier afectación a estos y a su titular, como daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Actividades vinculadas al deber de confidencialidad:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.
2. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en el cual se desarrolle dicho tratamiento.
3. Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales

CICLO DE VIDA DE LOS DATOS PERSONALES

El ciclo de vida de los datos personales, es una secuencia de etapas por las que pasan los datos a lo largo de toda su vida útil, el ciclo de vida proporciona una visión general de alto nivel de las etapas que intervienen en su generación, uso y reutilización.

Tener una visión clara de las etapas en las que se encuentran los datos permite a las organizaciones manejarlos con mayor eficiencia y seguridad.

Por lo anterior y en relación al artículo 59 de los Lineamientos Generales, el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;

II. El almacenamiento de los datos personales;

III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;

IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

V. El bloqueo de los datos personales, en su caso, y

VI. La cancelación, supresión o destrucción de los datos personales. El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

Por lo que el personal que labora dentro de la Comisión Nacional Forestal y se ve involucrado en el tratamiento de datos personales deberá de tomar en cuenta las 5 fases del ciclo de vida de los datos personales.

1. Generación. En esta fase, los datos llegan a la institución, normalmente a través de la adquisición desde una fuente externa. Por lo que una vez se haya acreditado el consentimiento, los datos se deberán de identificar, etiquetar y registrar dentro del inventario de datos personales.
2. Mantenimiento. En esta etapa, los datos se deberán organizar y procesar y luego se cuidarán continuamente para mantenerlos accesibles y optimizados para los usuarios. Asimismo, se podrán someter a procesos como la integración, la depuración y la extracción-transformación-carga.
3. Uso de datos: Una vez que los datos se han procesado adecuadamente, llegan a la fase de su utilización. En esta fase es fundamental que los datos sean fácilmente accesibles y seguros. Asimismo, los datos se utilizan para apoyar los objetivos de la CONAFOR.
4. Archivo de datos: En esta etapa, se tendrá que realizar una copia de los datos en un software donde se podrán almacenar por si se vuelven a necesitar en un entorno activo. Después de cierto tiempo, los datos dejan de ser útiles para las operaciones diarias. Sin embargo, es importante mantener copias de los datos a los

que no se accede con frecuencia para posibles necesidades de investigación. Finalmente, ésta es la etapa en que los datos se eliminan de todos los entornos activos, y se deberán archivar por si se vuelven a necesitar en el futuro.

5. Destrucción de datos. En esta etapa final del ciclo de vida de los datos, se depuran de los registros y se destruyen de forma segura. Los datos se eliminan de los archivos cuando superan el periodo de retención requerido o ya no tienen un propósito significativo para la Comisión Nacional Forestal.

ROLES Y RESPONSABILIDADES

Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, la áreas deberán establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales, conforme al sistema de gestión implementado.

SANCIONES

Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 163 de la Ley General:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
VII. Incumplir el deber de confidencialidad;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;
XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes; y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y A Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

En relación y en cumplimiento al artículo 33 de la Ley General, el responsable deberá realizar una serie de actividades con la finalidad de establecer y actualizar los mecanismos y medidas de seguridad.

Del mismo modo, el artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece que el responsable deberá evaluar y medir los resultados de las políticas, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua de acuerdo a lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos.
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

- Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.

- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

- Los incidentes y vulneraciones de seguridad ocurridos.

Por lo anterior, la CONAFOR generó los siguientes mecanismos:

A) Etapa de Monitoreo. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

- Si se han definido y se mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.
- Si se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad a las previstas en la Ley General y los Lineamientos Generales.
- Si se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.
- Si se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.
- Si se ha elaborado el inventario de Tratamiento de datos personales.
- Si se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales

B) Etapa de Supervisión. La Unidad de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un oficio en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas administrativas las atiendan y remitan las evidencias de su cumplimiento.

Para medir los resultados en las medidas de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas, cuando se presenta alguna de las situaciones antes descritas, será obligatorio analizar las causas por las cuales se presentó dicha vulneración y así poder efectuar las acciones preventivas y correctivas para evitar que la vulneración afecte a más titulares o se vuelvan a repetir. Además, si la vulneración tiene el riesgo de repercutir significativamente en los derechos patrimoniales o morales de sus titulares, se deberá informar sobre ésta, sin demora alguna, a los titulares afectados.

El anterior aviso, previene a los titulares para que puedan tomar las medidas correspondientes en la defensa de sus derechos, por lo que será necesario que cada área de la Comisión Nacional Forestal cuente con su propio registro de vulneraciones.

C) Etapa de actuación ante vulneraciones a la seguridad de los datos personales.

Cualquier persona que conozca sobre alguna vulneración de datos personales dentro de los sistemas de la Comisión Nacional Forestal, deberá informar inmediatamente a la persona responsable de la seguridad de datos personales que haya sido designada en el área de su adscripción.

A su vez, la persona responsable deberá informar inmediatamente sobre la violación a la persona titular del área de su adscripción y entablar contacto con la Unidad de Transparencia, a través de su titular, para informar el hecho y que ésta disponga lo conducente para orientar y acompañar en las gestiones que deban documentarse, las cuales deberán realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.

La Unidad de Transparencia junto con la persona responsable, coordinarán las acciones preventivas que se estimen convenientes al interior del área de su adscripción para asegurar el cese inmediato de la vulneración, registrando los siguientes datos:

- El nombre del Inventario de Tratamientos de Datos Personales.
- El tratamiento de datos personales que fueran afectados.
- La persona que tuvo conocimiento de la vulneración del tratamiento de los datos personales.
- La fecha, hora y lugar en que tuvo conocimiento del hecho.
- Tipo de vulneración, pérdida o destrucción; robo, extravío o copia; uso, acceso o tratamiento indebido; daño, alteración o modificación.
- Fecha y hora que tuvo conocimiento la Unidad de Transparencia respecto a la vulneración.

Una vez que fuera registrada esta información, se deberán formular las acciones correctivas de corto plazo, entre la Unidad de Transparencia y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes, asimismo, en cualquier caso se deberá informar a los titulares y/o al organismo garante sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales.

Finalmente, se deberán establecer las acciones correctivas implementadas y/o planeadas por las áreas competentes, así como las áreas involucradas en su consecución.

EJERCICIO DE LOS DERECHOS ARCO

Para efectos de este procedimiento, se considera que los derechos ARCO comprenden:

I. Acceso: Derecho del/de la titular para acceder a sus datos personales en posesión de la CONAFOR, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.
II. Rectificación: Derecho del/de la titular para solicitar a la CONAFOR la corrección de sus datos personales, cuando estos resulten incorrectos, inexactos, imprecisos, incompletos o no se encuentren actualizados.

III. Cancelación: Derecho del/de la titular para solicitar a la CONAFOR que sus datos personales sean bloqueados y eliminados de los archivos, registros, expedientes y sistemas institucionales, a fin de que los mismos no se encuentren más en su posesión y, por lo tanto, dejen de ser tratados.
IV. Oposición: Derecho del/de la titular para solicitar a la CONAFOR que se abstenga de utilizar información personal para ciertos fines o de requerir que se concluya su uso, a fin de evitar un daño o afectación a su persona.

Para realizar las solicitudes, será a través de la Plataforma Nacional de Transparencia (PNT), por el correo electrónico unidadtransparencia@conafor.gob.mx, o por escrito libre ante la Unidad de Transparencia de la CONAFOR con domicilio en Periférico Poniente No. 5360, edificio B, cuarto piso, ala poniente, Colonia San Juan de Ocotán, Zapopan, Jalisco con la siguiente información:

1. Nombre del titular de los datos personales, su domicilio o cualquier otro medio para recibir notificaciones.
2. Documentos que acrediten la identidad de la o el titular, en su caso, nombre del representante de la o el titular y documentos para acreditar su identidad y personalidad.
3. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.
4. Descripción clara y precisa de los datos personales y del derecho que se quiere ejercer o de lo que se solicita.
5. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular. (Acceso, Rectificación, Cancelación y/u Oposición).
6. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

La Unidad de Transparencia es la responsable de turnar las solicitudes de ejercicio de derechos ARCO que sean presentadas a la CONAFOR a aquellas áreas que conforme a sus funciones y atribuciones, puedan o deban poseer los datos personales, a fin de atenderlas en los plazos y términos establecidos en la Ley General, los Lineamientos Generales y demás disposiciones aplicables en la materia.

Las áreas deben llevar a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los Derechos ARCO de los/las titulares, acorde con los principios, deberes y obligaciones en materia de protección de datos personales y, trabajar en conjunto con la Unidad de Transparencia para atender las solicitudes, así como, cuando resulte necesario formular los alegatos derivados de los recursos de revisión interpuestos en términos de la Ley General, con motivo de las respuestas otorgadas.

La resolución que emita el Instituto es vinculante para la CONAFOR y, una vez recibida, la Unidad de Transparencia lleva a cabo las gestiones que resulten necesarias ante las áreas competentes para su cumplimiento.