

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

CONTENIDO

- I. GLOSARIO
- II. INTRODUCCIÓN
- III. OBJETIVOS DEL PROGRAMA.
- IV. RESPONSABILIDADES DENTRO DEL PROGRAMA.
- V. ALCANCE DEL PROGRAMA.
- VI. POLÍTICA DE GESTIÓN DE LOS DATOS PERSONALES.
- VII. MEJORA CONTINUA DEL PROGRAMA.
- VIII. SANCIONES.



I. GLOSARIO

Para efectos del Programa de Protección de Datos Personales de la Secretaría de Marina, se entenderá por:

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por la Secretaria de Marina, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificada cuando se acredita su identidad a través de cualquier información relacionada ella, por ejemplo, su nombre, teléfono, domicilio, fotografía, huellas dactilares o cualquier otro dato personal.

Asimismo, será una persona identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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

Acceso: Derecho del titular para acceder a sus datos personales que obren en posesión de la Secretaría de Marina, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Rectificación: Derecho del titular para solicitar a la Secretaría de Marina la corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

Cancelación: Derecho del titular para solicitar a la Secretaría de Marina que sus datos

personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.

Oposición: Derecho del titular para solicitar a la SEMAR, cuando ésta pretenda realizar el tratamiento de datos personales, que se abstenga de hacerlo en determinadas situaciones o para que cese el tratamiento.

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

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

como Organismo Garante en materia de protección de datos personales en posesión de los sujetos obligados.

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

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

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

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

Medidas de seguridad administrativas: Políticas y/o procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro, así como la

sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

De manera enunciativa más no limitativa, se consideran las actividades siguientes:

- Prevenir el acceso no autorizado al perímetro de la SEMAR, sus instalaciones físicas, áreas críticas, recursos e información; Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la SEMAR, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la SEMAR; y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

- Reglamento Interior de la ASF: Reglamento Interior de la Auditoría Superior de la Federación.

Responsable: La SEMAR en tanto que decide sobre el tratamiento de datos personales, de conformidad con lo dispuesto en el artículo 3º, en correlación con el 1º de la Ley General de Datos de Personales.

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

Instancia encargada de coordinar y evaluar las acciones relativas a la política transversal de protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia.

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

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, utilización, comunicación,

difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia.



II. INTRODUCCIÓN

Este Programa se elabora en cumplimiento a lo dispuesto por los artículos 30 fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como 47 de los Lineamientos para la Protección de Datos Personales para el Sector Público que establecen que entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, está la elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la Secretaria Marina.

El Programa está construido con base en el documento de seguridad de la Secretaria de Marina que materializa y da cuenta del Sistema de Gestión para la Protección de los Datos Personales, de conformidad con el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual tiene como objetivo establecer políticas internas de gestión y

tratamiento de datos personales, así como proveer los mínimos exigibles en medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales.

III. OBJETIVOS DEL PROGRAMA

El presente Programa tiene como objetivos los siguientes:

- A. Proveer el marco de trabajo para la protección de los datos personales en posesión de las Áreas Administrativas de la Secretaría Marina.
- B. Avanzar en el cumplimiento de las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, y
- C. Promover la adopción de mejores prácticas en la protección de datos personales, una vez que el Programa haya alcanzado un nivel de madurez adecuado, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.
- D. Verificar el cumplimiento de los principios y deberes que establece la Ley General de

Protección de Datos Personales en Posesión de
Sujetos Obligados y los Lineamientos para la
Protección de Datos Personales para el Sector
Público.

IV. RESPONSABILIDADES DENTRO DEL PROGRAMA

Con fundamento en los artículos 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que señala que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este Programa.

- A. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
- B. Dar a conocer el Programa al interior del sujeto obligado;
- C. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;

- D. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de las áreas técnicas que estime pertinente;
- E. Supervisar la correcta implementación del Programa;
- F. Establecer, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar,
- G. Las demás que de manera expresa señale el propio Programa.

Dado que el Programa es para la observancia de todos los integrantes de la Secretaría que en el ejercicio de sus funciones traten datos personales, resulta fundamental que el Programa se conozca al interior de las áreas Administrativas, por lo que el Comité de Transparencia se encargará de su difusión.

- H. Se tendrá como finalidad única el impulsar la debida implementación del Programa al interior de esta entidad, pero no podrá suplir ni afectar las funciones que otorgan los artículos 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.
- J. Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la Ley General de Datos Personales y los Lineamientos Generales, el Programa será de observancia obligatoria para todos los servidores públicos de la Secretaria de Marina que en el ejercicio de sus funciones traten datos personales.

V. ALCANCE DEL PROGRAMA

El presente Programa aplicará a todas las áreas Administrativas y a todos los tratamientos de datos personales que éstas realicen en ejercicio de sus atribuciones.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este Programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.

VI. POLÍTICA DE GESTIÓN DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las áreas administrativas deberán cumplir con los principios, deberes y obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para lo cual procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de desarrollo que exista, de acuerdo con el Sistema de Gestión para la Protección de los Datos Personales y documento de seguridad que desarrollen las áreas considerando las fases: planificar, hacer, verificar y actuar. Para el cumplimiento de las obligaciones que establecen los artículos 3, fracción XIV, 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

A este tenor, las áreas administrativas deberán identificar los Principios generales de protección de datos personales que cumplen y garantizan los deberes y

obligaciones que establece el artículo 7 de los Lineamientos para la Protección de Datos Personales para el Sector Público, en la etapa de obtención de los datos personales:

- a. Licitud.
- b. Finalidad.
- c. Lealtad.
- d. Consentimiento.
- e. Calidad.
- f. Proporcionalidad.
- g. Información.
- h. Responsabilidad.



VII. MEJORA CONTINUA DEL PROGRAMA

En esta fase del Programa, se adoptarán las medidas preventivas y correctivas que hayan resultado de las auditorías y revisiones realizadas, o bien que se hayan obtenido de otras fuentes de información relevantes.

Los puntos de mejora de la implementación del Programa pueden ser de dos tipos:

- a. Acciones preventivas: son aquéllas encaminadas a eliminar las posibles causas de "no conformidades" con relación a lo establecido en este Programa.

Entre ellas se encuentran las siguientes acciones:

1. El análisis y revisión de las posibles causas de no conformidad.
2. Determinar las no conformidades que podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales.

3. Evaluar las acciones necesarias para evitar que la no conformidad ocurra.
4. Determinar e implementar estas acciones.
5. Documentar los resultados de las acciones tomadas.
6. Revisar la eficacia de las acciones preventivas tomadas.
 - b. Acciones correctivas: son aquéllas encaminadas a eliminar las causas de la no conformidad con el cumplimiento de las obligaciones, entre tales acciones correctivas se deben llevar a cabo:
 - a). Analizar y revisar la no conformidad.
 - b). Determinar las causas que dieron origen a la no conformidad.
 - c). Evaluar las acciones necesarias para evitar que la no conformidad vuelva a ocurrir.
 - d). Implementar estas acciones.



- e). Documentar los resultados de las acciones tomadas.
- f). Revisar la eficacia de las acciones correctivas tomadas.

El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia.

El Comité de Transparencia deberá establecer un plazo límite para que se corrijan las no conformidades detectadas, así como documentar las medidas preventivas o correctivas realizadas para la mejora continua.

IX. SANCIONES

La Unidad de Transparencia informará al Comité cualquier incumplimiento de alguna obligación prevista en este Programa, quien realizará un exhorto a la unidad administrativa correspondiente para que lleve a cabo las acciones que resulten pertinentes, con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De conformidad con el artículo 163 de la Ley de Datos, serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

- 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 previstos en la Ley de Datos 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 Ley de Datos;
- 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 Ley de Datos, 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. La sanción sólo procederá

- cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
- VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley de Datos;
 - VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley de Datos;
 - IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley de Datos;
 - X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley de Datos;
 - 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 Ley de Datos,
y
 - XIII. No acatar las resoluciones emitidas por el INAI.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, y XII, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves. Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia, a través de la Unidad de Transparencia, tomará las medidas necesarias para dar a conocer esta información a los servidores públicos, prestadores de servicio, y quienes intervengan en cualquier tipo de tratamiento de los datos personales al interior del Instituto.