Controles para Asegurar la Confidencialidad de las Personas que Intervienen en Cualquier Fase del Tratamiento de Datos Personales.

CONTENIDO

I. MARCO JURÍDICO

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su capítulo II “DE LOS DEBERES”, dispone las medidas de seguridad adoptadas por el responsable en el tratamiento de datos personales que realicen los sujetos obligados.

Los artículos 31, 32, 33, 34, 35 y 36 de citada Ley establecen de forma particular las medidas de seguridad que deberá implementar el sujeto obligado a efecto de proteger los datos personales en su posesión.

En particular, el artículo 31 de dicha ley señala que el responsable del tratamiento deberá establecer y mantener medidas de seguridad para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Demás leyes aplicables en materia de protección de datos personales.

II. OBJETIVO

Describir y dar cuenta de forma genérica y dinámica los controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales en este Instituto Armado, mediante la implementación de medidas para garantizar la integridad de los datos personales en su posesión atendiendo a la protección de todo dato personal.

III. ALCANCE

Promover e impulsar una cultura de Protección de Datos Personales en los servidores públicos pertenecientes a este Instituto Armado, con la finalidad de garantizar la Confidencialidad y Protección de Datos Personales de los titulares, a través de la observancia de las obligaciones y atribuciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados..

IV. CONTROLES PARA ASEGURAR LA CONFIDENCIALIDAD.

Como parte de los procedimientos internos para mejores prácticas en materia de protección de datos personales de esta Dependencia se lleva a cabo lo siguiente:

Los Mandos Navales están obligados a garantizar la integridad y conservación de los expedientes y documentos, facilitar y controlar su uso y destino final, así como permitir la adecuada conformación de la memoria institucional de la Unidades y Establecimientos Navales de la Secretaría de Marina-Armada de México.

El acceso restringido a la información confidencial requiere asegurar su conservación y custodia, por lo que los archivos se convierten en el instrumento fundamental para evitar que se usen, oculten, destruyan, divulguen o alteren indebidamente los expedientes y documentos.

En las Unidades y Establecimientos Navales de la Secretaría de Marina-Armada de México, existirá un archivo de trámite y se nombrará un responsable que estará bajo la responsabilidad del Jefe de Detall o del Coordinador Administrativo u otros responsables de oficinas, adoptarán medidas y procedimientos técnicos que garanticen la conservación de la información y la seguridad de sus soportes, contar con espacios diseñados y destinados exclusivamente a la recepción, organización y resguardo temporal o definitivo de los documentos y contar con sistemas de control ambiental y de seguridad para conservar los documentos. Asimismo, las áreas de archivo contarán con personal de apoyo que se consideren necesarios.

La Secretaría de Marina-Armada de México, cuenta con un archivo de Concentración y un Archivo Histórico,

bajo la responsabilidad de la Dirección del Archivo General.

Los Mandos y Directores Navales, deberán asegurarse del adecuado funcionamiento de los archivos de trámite de las Unidades y Establecimientos de la Secretaría de Marina-Armada de México. Asimismo, deberán elaborar los instrumentos de consulta y control que propicien la organización, conservación y localización expedita de sus archivos administrativos, por lo que deberán contar al menos con lo siguiente:

A. El cuadro general de clasificación archivística.
B. El catálogo de disposición documental.
C. Los inventarios documentales:
    a) General.
    b) De transferencia.
    c) De baja.
    d) La guía simple.

e) Para la elaboración de los instrumentos de control señalados en los puntos anteriores, deberán coordinar con el Archivo General de la Secretaría de Marina-Armada de México.

El expediente de personal se integra en el archivo de concentración bajo la responsabilidad del Archivo General de la Secretaría de Marina-Armada de México, con diversos documentos.

Asimismo, el expediente de cuerpo se integra en las Unidades y Establecimientos Navales al causar alta, con diversos documentos:
Normatividad aplicable para los expedientes de Cuerpo, Personal, Clínico y Afiliación.

a.- Los expedientes de cuerpo de los Almirantes, Capitanes y Oficiales, al causar baja de la Unidad, se remiten al Archivo de Concentración bajo la

responsabilidad de la Dirección de Patrimonio Documental, foliados cronológicamente verificando que, el primer documento debe ser el oficio de alta y el último, el de movimiento por cambio de adscripción o situación.

b.- Los expedientes de cuerpo del personal de clases y marinería, al causar baja de la escuela o Unidad, se remiten a la Unidad de destino, foliados cronológicamente verificado, el primer documento debe ser el oficial de alta o movimiento y el último su oficio de movimiento por cambio de adscripción o situación.

c.- A los 30 días posteriores de causar baja del Servicio Activo de la Armada de México o ascenso a Oficial, los expedientes de cuerpo se remiten al Archivo de Concentración bajo la responsabilidad del Archivo General, foliados cronológicamente verificado que el primer documento debe ser el

oficio de alta y el último su oficio de movimiento por cambio de adscripción o situación.

d.- El personal que reingrese al Servicio Activo de la Armada de México, se le integrara un nuevo expediente con la documentación que genere.

e.- Para los expedientes de personal, cuerpo, clínico y de afiliación, se clasificarán mediante la utilización de la Clave Única de Registro de Población(CURP), haciendo la anotación en la carátula del expediente. En el caso de los expedientes clínico para los derechohabientes aperturarlos en relación con la Clave Única de Registro de Población (CURP del militar).

f.- La apertura de los expedientes clínicos deberán sujetarse a lo que establece la NOM-0168, su organización será conforme al Cuadro General de Clasificación Archivística y Manual de Administración Archivística Tomo I.

g.- A seis meses posteriores al cambio de adscripción del militar las unidades médicas deberán remitir el expediente clínico del personal a su nueva adscripción y en caso de que los familiares radiquen en un lugar distinto al de la adscripción del militar, el expediente que éstos utilicen será conforme a la Clave Única de Registro de Población (CURP) del mismo.

Normatividad aplicable para los expedientes de materiales.

a.- Los expedientes de materiales se clasificarán conforme al Cuadro General de Clasificación Archivística.

b.- En el catálogo de disposición documental se establecerán los periodos de vigencia de las series documentales, sus plazos de conservación, así como su carácter de reserva o confidencialidad. Para efecto de los periodos de reserva de los

expedientes, el catálogo deberá vincularse al índice de expedientes reservados que establece la legislación en la materia. Las Unidades y Establecimientos Navales de la Secretaría de Marina-Armada de México, enviarán a la Dirección del Archivo General, para su validación y registro, una copia de su catálogo de disposición documental actualizado en soporte electrónico.

Sin olvidar que se tiene un procedimiento de baja documental de dicha información, misma que debe cumplir con los lineamientos establecidos en la legislación para su correcta destrucción.

De la misma forma el personal que labora en las áreas de resguardo de datos personales se encuentra sujeto a las siguientes disposiciones:

1. En la aplicación de una política de escritorios limpios para proteger documentos en papel y

dispositivos de almacenamiento removibles que puedan tener datos personales, durante el horario normal de trabajo como fuera del mismo.

2. Se emitió la directiva para el uso seguro de dispositivos electrónicos portátiles, en la que cada área debe contar con un usb oficial para su uso y transmisión de datos, el cual se encuentra encriptado y codificado para su utilización, este dispositivo debe estar autorizado por el jefe de la unidad y no se permite el acceso de otros dispositivos de almacenamiento, para evitar las vulneraciones de seguridad especialmente en las áreas que manejan bases de datos personales.

3. Deberán adquirir el compromiso de protección y no divulgación de la misma mediante la firma del “ACUERDO DE NO REVELACIÓN DE INFORMACIÓN”.

Así mismo, es necesario mencionar que el Comité de Transparencia de la Secretaría de Marina se ha preocupado por proponer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, todo ello a través del Jefe de la Unidad de Transparencia de la Secretaría de Marina, de tal forma que se sensibilice al personal que maneja los datos confidenciales dentro de la institución y los proteja, particularmente los datos confidenciales sensibles.

Por su parte la Unidad de Transparencia de la Secretaría de Marina ha venido asesorando a las áreas administrativas de la Dependencia, en materia de protección de datos personales, se ha implementado exitosamente el aviso de privacidad, para que el personal naval tenga conocimiento .de que hace cada área con sus datos personales, para que son requeridos y como pueden ejercer sus derechos ARCO.

Específicamente por lo que hace al tratamiento de datos personales, el personal naval se encuentra monitoreado por un oficial de seguridad de la información (OSI), nombrado por cada una de las áreas administrativas y sensibles con las que cuenta la Dependencia, encargado de velar por la protección de datos personales entre otro tipo de información, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Es pertinente resaltar que a pesar de que en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se menciona la posibilidad de nombrar un **Oficial de protección de datos personales**, perteneciente a la Unidad de Transparencia de la Dependencia de que se trate, esta Institución ha tenido a bien nombrar un **Oficial de Seguridad de la Información**

en todas y cada una de sus áreas administrativas con las que cuenta la Secretaría de Marina, lo que conlleva a una mejor práctica de tratamiento de la información, en particular de los datos personales, pues como se sugiere en la legislación en la materia, limita el actuar del oficial a conocer de las medidas de seguridad en toda la Dependencia, lo cual es una carga de trabajo que no podría ser llevada a cabo, con la exactitud y buen funcionamiento que exige el Derecho a la protección de datos personales, sin embargo, el contar con un oficial de seguridad de la información en todas y cada una de las áreas administrativas garantiza la supervisión y cumplimiento de la protección de datos personales.

Así mismo al oficial de seguridad de la información, le corresponde la aplicación directa de las políticas, guías, procedimientos, directivas y ordenamientos relacionada con la custodia y el control de la información clasificada. El

cual cuenta con las siguientes funciones y responsabilidades:

1. Análisis de riesgo y administración de las vulnerabilidades y fortalezas de los sistemas de información.
2. Elaboración de un croquis de la Unidad Administrativa, con base al análisis de riesgo, implementándolas en las denominadas, áreas de seguridad; las cuales funcionan para la protección y resguardo de la información de esta Dependencia, así como la de datos personales, teniendo como función primordial lograr la división de los espacios físicos para el resguardo de la misma, como se indica a continuación:

   A. **Área blanca:** Máxima seguridad. Es el área que cuenta con un mayor control, ya que son los lugares de acceso restringido y controlados a través de

sistemas electrónicos y/o con autorización permanente del personal que labora en citada área.

B. **Área gris:** Acceso restringido. Es el área que cuenta con un control moderado y con ciertas medidas de seguridad, son las áreas comunes donde se presta algún servicio al público en general, por ejemplo: pasillos generales, departamento de reclutamiento, departamento de seguridad y bienestar social, etc.

C. **Área negra:** Área de mínimo control. Es el área con un mínimo de control sobre el transito del personal, como son las áreas periféricas de los establecimientos.

3. Definirá el espacio físico para resguardar la información de datos personales, con base a los parámetros siguientes:

A. Identifica el área que alojará la información resguardada, debiendo ser discreta, con un señalamiento mínimo, que cuente con un perímetro de seguridad claramente definido y con las medidas de protección físicas debidamente documentadas.

B. Supervisa la implantación de un área de recepción para controlar la entrada y salida del personal y documentos, atendida por personal confiable.

C. Supervisa la inspección y el registro de cada ingreso y egreso del personal así como el ingreso y egreso de la información (datos personales) al área protegida.

D. Supervisa que el personal que labora en áreas protegidas cuenten con un tipo de identificación

(gafete), quienes tienen la instrucción de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

E. Revisa y actualiza en un periodo semestral, los permisos de acceso a las áreas protegidas.

4. Ejecuta el plan de concientización para promover una doctrina en materia de seguridad de la información y protección de datos personales.

5. Supervisa y evalúa continuamente, las buenas prácticas del personal de la Institución.

6. Atiende y responde en forma inmediata a las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.