

ANEXO 6

1.T. MEDIDAS DE SEGURIDAD (DEBER DE SEGURIDAD)

2.T. DOCUMENTO DE SEGURIDAD

6.1 Generales:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> Establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad e impedir que cualquier tratamiento contravenga las disposiciones del marco normativo en la materia. 	<p>1. Establecer y mantener medidas de seguridad administrativas, técnicas y físicas para la protección de los datos personales, a partir de las acciones que se describen en esta sección.</p>	<p>La Gerencia de Tecnologías de la Información, la Gerencia de Recursos Materiales, con la participación de las unidades administrativas.</p>	<ul style="list-style-type: none"> Programa de Protección de Datos Personales. Documento de seguridad. Evidencia generada en la implementación de los controles de seguridad.
<ul style="list-style-type: none"> Tomar en cuenta otras disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando éstas contemplen una mayor protección para el titular o complementen lo dispuesto por la 	<p>2. Revisar el marco normativo que regula el tratamiento específico de los datos personales, a fin de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación.</p>	<p>Unidad administrativa responsable del tratamiento con el apoyo de la Gerencia de Tecnologías de la Información.</p>	<ul style="list-style-type: none"> Marco normativo que regula en lo particular el tratamiento en cuestión.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
LGPDPPSO y los Lineamientos Generales.			

6.2 Políticas internas:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> • Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión, y en las que se incluya lo siguiente: <ol style="list-style-type: none"> I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y los presentes Lineamientos generales; II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen; III. Las sanciones en caso de incumplimiento; 	<p>3. Incluir en el Programa de Protección de Datos Personales los elementos señalados en la columna anterior.</p>	<p>Comité de Transparencia.</p>	<ul style="list-style-type: none"> • Programa de Protección de Datos Personales. • Documentación que se genere con motivo de la implementación y evaluación del Programa.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>IV. 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;</p> <p>V. 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, y</p> <p>VI. El proceso general de atención de los derechos ARCO.</p>			

6.3 Funciones de los servidores públicos que tratan datos personales:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> • Establecer y documentar las funciones, obligaciones y cadena de rendición de cuentas del personal involucrado en el tratamiento de datos personales. • Establecer mecanismos para asegurar que los servidores públicos involucrados en el tratamiento conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento. 	<p>4. Definir las funciones, obligaciones y cadena de mando de cada servidor público que trate datos personales, por unidad administrativa.</p> <p>5. Comunicar a cada uno de los servidores públicos la información antes señalada, así como capacitarlos en la materia.</p>	<p>Unidad administrativa responsable del tratamiento.</p>	<ul style="list-style-type: none"> • Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada servidor público, por unidad administrativa, que trate datos personales. • Documento mediante el cual se haya comunicado la información antes señalada. • Constancias de capacitación al personal.

6.4 Inventario:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> • Elaborar un inventario de datos personales y de los sistemas de tratamiento, en el que se incluyan los siguientes elementos: <ol style="list-style-type: none"> I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; II. Las finalidades de cada tratamiento de datos personales; III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; 	<p>6. Elaborar el inventario de datos personales y de los sistemas de tratamiento con los elementos señalados en la columna anterior.</p>	<p>Comité de Transparencia en conjunto con las unidades administrativas encargadas del tratamiento.</p>	<ul style="list-style-type: none"> • Inventario de tratamiento de datos personales según el apartado 6.1 de este Programa.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y</p> <p>VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.</p> <ul style="list-style-type: none"> • Considerar en el inventario el ciclo de vida de los datos personales, conforme a lo siguiente: <ol style="list-style-type: none"> 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; 			

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;</p> <p>V. El bloqueo de los datos personales, en su caso, y</p> <p>VI. La cancelación, supresión o destrucción de los datos personales.</p>			

6.5 Análisis de riesgo, de brecha y plan de trabajo:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> ● Realizar un análisis de riesgo de los datos personales, considerando lo siguiente: <ol style="list-style-type: none"> I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales; IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; V. El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos 	<p>7. Elaborar el análisis de riesgo tomando en cuenta los elementos señalados en la columna anterior.</p>	<p>Gerencia de Tecnologías de la Información con la participación de las unidades administrativas.</p>	<ul style="list-style-type: none"> ● Análisis de riesgo documentado. ● Documento de seguridad.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;</p> <p>VI. La sensibilidad de los datos personales tratados;</p> <p>VII. El desarrollo tecnológico;</p> <p>VIII. Las transferencias de datos personales que se realicen;</p> <p>IX. El número de titulares;</p> <p>X. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y</p> <p>XI. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.</p>			
<ul style="list-style-type: none"> Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del 	<p>8. Realizar el análisis de brecha con los elementos señalados en la columna anterior.</p>	<p>Gerencia de Tecnología de la Información con la participación de las unidades administrativas.</p>	<ul style="list-style-type: none"> Análisis de brecha documentado. Documento de seguridad.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>responsable, considerando lo siguiente:</p> <ol style="list-style-type: none"> I. Las medidas de seguridad existentes y efectivas; II. Las medidas de seguridad faltantes, y III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente. 			
<ul style="list-style-type: none"> • Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales. <p>Este plan de trabajo deberá elaborarse de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.</p>	<p>9. Elaborar el plan de trabajo después de contar con el análisis de riesgo y de brecha, priorizando las medidas de seguridad más relevantes y urgentes, considerando los recursos designados; el personal interno y externo en su organización, y estableciendo fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.</p>	<p>Gerencia de Tecnologías de la Información con la participación de las unidades administrativas.</p>	<ul style="list-style-type: none"> • Plan de trabajo elaborado. • Documentos de análisis de riesgo y de brecha.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.			

6.6 Revisión y vigilancia:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> • Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: <ol style="list-style-type: none"> I. Los nuevos activos que se incluyan en la gestión de riesgos; II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; V. Las vulnerabilidades identificadas para determinar aquellas expuestas a 	<p>10. Elaborar un plan de monitoreo periódico de las medidas de seguridad implementadas, las amenazas y las vulnerabilidades a las que estén sujetos los datos personales, tomando en cuenta los elementos señalado en la columna anterior.</p> <p>11. Implementar el plan de monitoreo periódico.</p>	<p>Gerencia de Tecnologías de la Información, con la participación de las unidades administrativas.</p>	<ul style="list-style-type: none"> • Plan de monitoreo periódico. • Documentación que se genere a partir de la implementación del plan.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>amenazas nuevas o pasadas que vuelvan a surgir;</p> <p>VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y</p> <p>VII. Los incidentes y vulneraciones de seguridad ocurridas.</p>			

6.7 Capacitación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, seguridad de los datos personales y el perfil de los puestos. 	<p>12. Realizar las acciones previstas en el apartado de “Capacitación” de la sección 6.2.5 “Otras obligaciones” de la Guía.</p>	<p>Comité de Transparencia.</p>	<ul style="list-style-type: none"> Programa de capacitación según el apartado 6.2.5 de este Programa. Documentación que se genere a partir de la aplicación de la capacitación.

6.8 Sistema de gestión:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> Implementar un sistema de gestión para la seguridad de los datos personales, que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad. 	<p>13. Implementar el presente Programa de Protección de Datos Personales que se basa en un sistema de gestión integral, que no sólo abarca medidas de seguridad sino la totalidad de obligaciones previstas en la LGPDPSO y los Lineamientos Generales.</p>	<p>Comité de Transparencia, Gerencia de Tecnologías de la Información y las unidades administrativas.</p>	<ul style="list-style-type: none"> Programa de Protección de Datos Personales. Documentación que se genere a partir de la implementación del Programa.

6.9 Documento de seguridad:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> • Elaborar un documento de seguridad con la siguiente información: <ul style="list-style-type: none"> • El inventario de datos personales y de los sistemas de tratamiento; • Las funciones y obligaciones de las personas que traten datos personales; • El análisis de riesgos; • El análisis de brecha; • El plan de trabajo; • Los mecanismos de monitoreo y revisión de las medidas de seguridad, y • El programa general de capacitación. 	14. Elaborar el documento de seguridad con la información antes señalada.	Gerencia de Tecnologías de la Información.	<ul style="list-style-type: none"> • Documento de seguridad.
<ul style="list-style-type: none"> • Actualizar el documento de seguridad cuando ocurran los siguientes eventos: <ul style="list-style-type: none"> ○ Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; 	15. Actualizar el documento de seguridad cuando ocurra alguno de los supuestos antes señalados.	Gerencia de Tecnología de la Información.	<ul style="list-style-type: none"> • Documento de seguridad.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> ○ Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; ○ Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e ○ Implementación de acciones correctivas y preventivas ante una vulneración de seguridad. 			

7. Lista de comprobación

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	<input type="checkbox"/>	<input type="checkbox"/>
2. 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 específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	<input type="checkbox"/>	<input type="checkbox"/>
3. El Programa de Protección de Datos Personales de la organización toma en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, e incluye lo siguiente: <ul style="list-style-type: none"> • El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y los presentes Lineamientos generales; • Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen; • Las sanciones en caso de incumplimiento; • 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; • 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, y El proceso general de atención de los derechos ARCO. 	<input type="checkbox"/>	<input type="checkbox"/>
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	<input type="checkbox"/>	<input type="checkbox"/>
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	<input type="checkbox"/>	<input type="checkbox"/>
5. Se ha elaborado el inventario de datos personales con los siguientes elementos: <ul style="list-style-type: none"> • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; 	<input type="checkbox"/>	<input type="checkbox"/>

<ul style="list-style-type: none"> • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican. 		
<p>6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente:</p> <ul style="list-style-type: none"> • La obtención de los datos personales; • El almacenamiento de los datos personales; • 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; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales. 	<input type="checkbox"/>	<input type="checkbox"/>
<p>7. Se ha realizado el análisis de riesgo, considerando lo siguiente:</p> <ul style="list-style-type: none"> • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; • El valor y exposición de los activos involucrados en el tratamiento de los datos personales; • Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y 	<input type="checkbox"/>	<input type="checkbox"/>

<ul style="list-style-type: none"> El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. 		
<p>8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente:</p> <ul style="list-style-type: none"> Las medidas de seguridad existentes y efectivas; Las medidas de seguridad faltantes, y La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente. 	<input type="checkbox"/>	<input type="checkbox"/>
<p>9. Se ha elaborado el plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales, a partir del análisis de riesgo y brecha realizado, y priorizando las medidas de seguridad más relevantes e inmediatas a establecer.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>10. Se monitorea y revisa de manera periódica s medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente:</p> <ul style="list-style-type: none"> 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 de su organización 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, y Los incidentes y vulneraciones de seguridad ocurridas. 	<input type="checkbox"/>	<input type="checkbox"/>
<p>11. Se cuenta con un programa de capacitación para los servidores públicos y externos involucrados en el tratamiento de datos personales, y se implementa.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>12. Se implementa un sistema de gestión para la seguridad de los datos personales.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>13. Se cuenta con el documento de seguridad con la información que establece el artículo 35 de la LGPDPPSO.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>14. En el documento de seguridad se establece un procedimiento para su actualización, en caso de que ocurra alguno de los supuestos del artículo 36 de la LGPDPPSO.</p>	<input type="checkbox"/>	<input type="checkbox"/>