FORMATO DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Con el fin de evaluar y medir el cumplimiento del proceso, el Instituto FONACOT y las Unidades Administrativas deben llevar a cabo revisiones y auditorías tomando en consideración los siguientes puntos.

1. Con el objeto de impedir que, cualquier tratamiento de datos personales contravenga las disposiciones aplicables a la materia, ¿se establecieron las siguientes medidas de seguridad para la protección de datos personales?	**CUMPLE SI/NO**
Medidas de seguridad de carácter administrativo.	
Medidas de seguridad de carácter físico.	
Medidas de seguridad de carácter técnico.	

2. Para establecer las medidas de seguridad de carácter administrativo, físico y técnico, 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, ¿se han adoptado las siguientes medidas de seguridad?	**CUMPLE SI/NO**
El riesgo inherente a los datos personales tratados.	
La sensibilidad de los datos personales tratados.	
El desarrollo tecnológico.	
Las posibles consecuencias de una vulneración para los titulares.	
Las transferencias de datos personales que se realicen.	
El número de titulares.	
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	
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.	

3. En el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, ¿se incluyó, al menos lo siguiente?	**CUMPLE SI/NO**
Todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en 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.	
Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúan.	
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.	
El proceso general de atención a los derechos ARCO.	

4. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, ¿se realizaron, al menos, las siguientes actividades interrelacionadas?	CUMPLE SI/NO
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.	
Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.	
Elaborar un inventario de datos personales y de los sistemas de tratamiento.	
Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	
Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.	
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimientos cotidiano de las políticas de gestión y tratamiento de los datos personales.	
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.	
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.	

5. En la elaboración del documento de seguridad, ¿se encuentran los siguientes puntos?	CUMPLE SI/NO
El inventario de datos personales y de los sistemas de tratamiento.	
Las funciones y obligaciones de las personas que tratan los datos personales.	
Al análisis de riesgos.	
El análisis de brecha.	
El plan de trabajo.	
Los mecanismos de monitoreo y revisión de las medidas de seguridad.	
El programa general de capacitación.	

6. Respecto a la elaboración del inventario, ¿se consideraron, al menos, los siguientes elementos?	CUMPLE SI/NO
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.	
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 los 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 el responsable.	
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúan, así como las finalidades que justifican éstas.	
El inventario cuenta con información básica de cada uno de los tratamientos de datos personales.	

6.1 En la elaboración del inventario, ¿se consideró el ciclo de vida de los datos personales conforme a lo siguiente?	CUMPLE SI/NO
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 efectúan.	
El bloqueo de los datos personales, en su caso.	
La cancelación, supresión o destrucción de los datos personales.	

6.2 En la elaboración del inventario, ¿se identificaron riesgos inherentes a los siguientes puntos?	CUMPLE SI/NO
Se contempló el ciclo de vida y los activos involucrados en el tratamiento de los datos personales	
Hardware.	
Software.	
Personal.	
Cualquier recurso humano o material que resulte pertinente considerar.	

7. Por lo que respecta a las funciones y obligaciones de las personas que tratan datos personales, ¿se tomaron en cuenta los siguientes elementos?	CUMPLE SI/NO
Establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que tratan datos personales en su organización, conforme al sistema de gestión implementado.	
Establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.	

8. Al realizar el análisis de riesgos de los datos personales tratados, ¿se consideró lo siguiente?	CUMPLE SI/NO
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.	
Los factores previstos en el numeral 2.	

8.1 Con la finalidad de establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información del Instituto, así como disminuir el impacto de eventos adversos, ¿se consideró lo siguiente?	CUMPLE SI/NO
El establecimiento, operación y mantenimiento de un modelo de gobierno de seguridad de la información.	
La identificación de infraestructuras críticas y activos claves del Instituto y la elaboración del catálogo respectivo.	
Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.	
Establecer un Sistema de Gestión de la Seguridad de la Información que proteja los activos de información del Instituto, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.	
Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.	

Vigilar los mecanismos establecidos y el desempeño del Sistema de Gestión de la Seguridad de la Información a fin de prever desviaciones y mantener una mejora continua.	
Fomentar una cultura de seguridad de la información en el Instituto.	

8.2 Con el propósito de identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios del Instituto, ¿se efectuaron las siguientes acciones?	**CUMPLE SI/NO**
La definición de estrategias, metodologías y herramientas que se usarán para administrar los riesgos.	
La integración del marco normativo que resulte aplicable a los riesgos identificados.	
El establecimiento de las reglas para medir la efectividad de los controles en la gestión de los riesgos.	
La definición de la forma y periodicidad con las que se informará sobre los riesgos a los que se encuentran expuestos los procesos y servicios que se utilizan.	
La definición de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas del Instituto.	

9. Para la realización del análisis de brecha, ¿el responsable consideró lo siguiente?	**CUMPLE SI/NO**
Las medidas de seguridad existentes y efectivas.	
Las medidas de seguridad faltantes.	
La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	
Realizar pruebas de penetración.	

10. ¿El responsable elaboró un plan de trabajo, en el que se definieron las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, tomando en consideración lo siguiente?	**CUMPLE SI/NO**
Los recursos designados las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	
El personal interno y externo en su organización.	
Las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	

11. Con la finalidad de verificar el cumplimiento de los objetivos propuestos en materia de seguridad y tratamiento de los datos personales, ¿se monitorea continuamente lo siguiente?	**CUMPLE SI/NO**
Los nuevos activos que se incluyen 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 aquellas 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 ocurridas.	

12. ¿Con el propósito de capacitar a los involucrados internos y externos, se diseñaron e implementaron programas a corto, mediano y largo plazo, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos, tomando en cuenta lo siguiente?	CUMPLE SI/NO
Los requerimientos y actualizaciones del sistema de gestión.	
La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos.	
Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales.	
Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.	

13. ¿Se actualiza el documento de seguridad cuando ocurren los siguientes eventos?	CUMPLE SI/NO
Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.	
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.	
Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.	

14. Adicional a las que señalen las leyes respectivas y la normatividad aplicable, ¿se consideran como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, las siguientes?	CUMPLE SI/NO
La pérdida o destrucción no autorizada.	
El robo, extravío o copia no autorizada.	
El uso, acceso o tratamiento no autorizado.	
El daño, la alteración o modificación no autorizada.	
Alguna otra.	

15. En la bitácora de vulneraciones a la seguridad, ¿se describe la siguiente información?	CUMPLE SI/NO
Fecha en la que ocurrió.	
Motivo de ésta.	
Acciones correctivas implementadas de forma inmediata y definitiva.	

16. En caso de alguna vulneración a los datos personales, ¿se proporciona un informe al titular, señalando lo siguiente?	CUMPLE SI/NO
La naturaleza del incidente.	
Los datos personales comprometidos.	
Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.	
Las acciones correctivas realizadas de forma inmediata.	
Los medios donde puede obtener más información al respecto.