**MECANISMOS DE MONITOREO Y REVISIÓN**

**DE LAS MEDIDAS DE SEGURIDAD**

**Mecanismo de monitoreo y supervisión**

Con fundamento en el artículo 30, fracción V y 84, fracción V de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, que establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales; por lo que el Comité de Transparencia será el encargado de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

1. **Etapa de Monitoreo**. El AIFA, a través del Comité de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales la elaboración de un reporte, en el que deberán precisar:

|  |  |  |
| --- | --- | --- |
|  | **Sí** | **No** |
| 1. Se han definido, se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales. |  |  |
| 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 específica o adicional a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación. |  |  |
| 3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa. |  |  |
| 4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa. |  |  |
| 5. Se ha elaborado el inventario de datos personales con los siguientes elementos:   * 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 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. |  |  |
| 6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente:   * 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; * La cancelación, supresión o destrucción de los datos personales. |  |  |
| 7. Se ha realizado el análisis de riesgo, considerando lo siguiente:   * La sensibilidad de los datos personales tratados; * El desarrollo tecnológico; * Las transferencias de datos personales que se realicen; * El número de titulares; y * 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. |  |  |
| 8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente:   * 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. |  |  |

1. **Etapa de Supervisión.** El Comité de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado “No” como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.