SISTEMAS DE SUPERVISIÓN Y VIGILANCIA PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA SECRETARÍA DE SALUD

Av. Marina Nacional 60 piso 15, Col. Tacuba, Miguel Hidalgo, C.P. 11410, CDMX. Tel: 5062 1600, Ext.53366#, www.gob.mx/salud

I. Mecanismos de supervisión, vigilancia, monitoreo, revisión, alertas, vulneraciones y auditoría en materia de datos personales.

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), 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. En ese sentido, el artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad. Al respecto, el numeral 33, fracción VII, de dicha legislación, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.
2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales. Respecto del monitoreo y supervisión periódica de las medidas de seguridad, el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) dispone que el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo anterior, dicho numeral estipula que se deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos (activo es todo elemento de valor involucrado en el tratamiento de datos personales, como pueden ser una base de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel).
2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

Av. Marina Nacional 60 piso 15, Col. Tacuba, Miguel Hidalgo, C.P. 11410, CDMX. Tel: 5062 1600, Ext.53366#, www.gob.mx/salud

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y
riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

7. Los incidentes y vulneraciones de seguridad ocurridos. Además de lo expuesto, el artículo referido estipula que el responsable deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Así, bajo un esquema de mejora continua, a efecto de mantener el monitoreo y revisión de los aspectos en cita, se presentan los mecanismos siguientes:

A. Mecanismo de monitoreo y supervisión en la protección de datos personales.
B. Mecanismo de actuación ante alertas y vulneraciones a la seguridad de los datos personales.
C. Mecanismo de Auditoría en Materia de Datos Personales.

II. Mecanismo de monitoreo y supervisión en la protección de datos personales

Para establecer y mantener la seguridad de los datos personales, el artículo 33, fracción VII, de la Ley General, establece que se deberán 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. Al respecto, la Unidad de Transparencia a través de su Oficial de Protección de Datos Personales, será el área encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, el cual se integrará por las etapas de monitoreo y supervisión.

Av. Marina Nacional 60 piso 15, Col. Tacuba, Miguel Hidalgo, C.P. 11410, CDMX. Tel: 5062 1600, Ext.53366#, www.gob.mx/salud

La etapa de monitoreo consistirá en el requerimiento por parte del Oficial de Protección de Datos Personales de la Secretaría de Salud, del Reporte de Seguridad de Datos Personales, el cual deberá ser desahogado por las instancias que, en el ámbito de sus atribuciones, sean las encargadas de los sistemas de tratamiento de datos personales.
La etapa de supervisión consistirá en el análisis por parte del Oficial de Protección de Datos Personales del Reporte de Seguridad de Datos Personales, al cual corresponderá un Dictamen de Seguridad de Datos Personales en el que se plasmen las recomendaciones o requerimientos que se consideren pertinentes.
El proceso anterior, se describe de la forma siguiente:

A continuación, se describe cada una de las etapas citadas.

· Etapa de Monitoreo

Se realizará tomando como punto de partida lo informado por cada instancia ante la Unidad de Transparencia en la integración del Documento de Seguridad, lo cual abarcó, entre otros aspectos, lo siguiente:

1. Datos personales que se obtienen o reciben en cada tratamiento.
2. Motivos y fundamento legal por los cuales se recaban o reciben los datos personales.
3. Tecnologías empleadas para el tratamiento.
4. Medidas de control implementadas, incluyendo su objetivo, la forma en que se instrumentan y el responsable de su ejecución.
5. Identificación de controles preventivos.
6. Identificación de controles correctivos.

En vista de lo anterior, la Unidad de Transparencia requerirá a cada instancia, por cada uno de los tratamientos que realiza, la elaboración del Reporte de Seguridad de Datos Personales, en el que deberán precisarse los elementos siguientes:

1. Acciones desarrolladas para la ejecución de las medidas de control existentes.
2. Manifestación de si existe alguna actualización o modificación respecto de las medidas de seguridad y controles implementados en el

tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación.

3. Indicar de manera clara la actualización de los aspectos siguientes:

· La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.

· El surgimiento de nuevas amenazas en el tratamiento de los datos.

· La posibilidad de que las nuevas amenazas actualicen una vulnerabilidad en el tratamiento de datos respectivo (Vulnerabilidad: debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta).

· Casos en los que una amenaza haya sufrido alguna modificación que derive en el incremento del impacto que tendría su materialización en la seguridad de los datos personales.

El requerimiento a cada instancia del Reporte de Seguridad de Datos Personales se realizará de acuerdo con el calendario respectivo, mismo que será elaborado por la Unidad de Transparencia y sometido a consideración del Comité de Transparencia para su aprobación.

· Etapa de Supervisión

La Unidad de Transparencia analizará los reportes de seguridad de datos personales remitidos por las instancias, verificando especialmente lo siguiente:

1. La idoneidad y efectividad de las medidas de seguridad y control respecto del tratamiento.
2. La suficiencia de controles preventivos y correctivos.
3. La gestión interna de nuevas amenazas, vulnerabilidades e incrementos en el impacto de probables daños.
4. Avances generados conforme a lo establecido en el Plan de Trabajo.
5. El cumplimiento de políticas, planes, procesos y procedimientos en materia de seguridad de datos personales.

Posterior a su examinación, se elaborará un Dictamen de Seguridad en el que se plasmaran las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad. Lo que será notificado a las instancias, puntualizando las cuestiones que se estimen de atención prioritaria, señalando la forma en que las recomendaciones y/o requerimientos habrán de ser desahogados, destacando el plazo en que deberán remitirse las evidencias de su cumplimiento a la Unidad de Transparencia. Si de las recomendaciones concluidas puede derivarse una estrategia que maximice la seguridad de los datos personales, la Unidad de Transparencia la integrará en el Plan de Trabajo de la Secretaría de Salud, con el objeto de que sean atendibles por aquellas instancias que les pueda resultar aplicable. Asimismo, de advertir una modificación sustancial a determinado tratamiento que derive en un cambio en su nivel de riesgo o una estrategia que maximice la seguridad de los datos personales que pueda ser aplicable a diversas instancias, la Unidad de Transparencia deberá analizar la necesidad de actualizar el Documento de Seguridad, en términos de lo establecido para esos efectos.

III. Mecanismos de actuación ante alertas y vulneraciones a la seguridad de los datos personales

El artículo 33, fracción VII, de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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. En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas. El artículo 14, fracción VI, del Acuerdo General, establece que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, la Unidad de Transparencia deberá monitorear y revisar de manera periódica dichas medidas, así como las amenazas y

vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar de la Dirección General de Tecnologías de la Información.
Bajo ese panorama, en este documento se definen los mecanismos que las áreas administrativas de la Secretaría de Salud, a través de la Unidad de Transparencia, deberán operar ante el surgimiento de una alerta o vulneración en las medidas de seguridad de los datos personales. Para la comprensión de los mecanismos referidos, resulta elemental distinguir entre una alerta y una vulneración de seguridad.
La diferencia entre ambos conceptos, se exponen de la forma siguiente:

Dichos mecanismos, deberán desarrollarse, como se representa a continuación:

Sentado lo anterior, se procede a exponer el mecanismo que las áreas administrativas de la Secretaría de Salud deberán efectuar cuando:
1. Se materialice una alerta de seguridad en cualquier fase del tratamiento de datos personales.
2. Se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales.
Lo anterior, se desarrollará en la forma que se describe a continuación. 1. Alertas seguridad de los datos personales
El mecanismo que aquí se describe, resulta obligatorio para las instancias que en ejercicio de sus funciones realicen el tratamiento de datos personales. El artículo 31 de la Ley General, estipula que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, se deberán establecer y mantener 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.
El párrafo segundo del artículo 55 de los Lineamientos Generales, dispone que dichas medidas constituyen mínimos exigibles, por lo que podrán adoptarse las medidas adicionales que se estimen necesarias para brindar

mayores garantías en la protección de los datos personales. En ese sentido, afecto de maximizar la protección de los datos personales en posesión de la Secretaría de Salud, el presente mecanismo persigue los objetivos siguientes:

· Registrar las amenazas que configuren alertas de seguridad.

· Analizar las alertas de seguridad registradas con la finalidad de definir estrategias para la prevención de una vulneración de seguridad.

· Integrar las estrategias de prevención en el Plan de Trabajo a efecto de que, en los casos conducentes, se implementen como medidas adicionales de seguridad.

Es importante destacar, que resultará indispensable identificar que efectivamente los hechos acaecidos constituyan una alerta a la seguridad de los datos personales, para lo cual, las instancias deberán verificar la materialización de los supuestos siguientes:

1 Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.

1 Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para la instancia. En mérito de lo anterior, en caso de advertir una alerta de seguridad se deberá proceder conforme al mecanismo siguiente:

A. Al segundo día hábil siguiente a la fecha en que se detecte la amenaza, la instancia respectiva deberá elaborar un Reporte de Alerta de Seguridad, en los términos que más adelante se abordarán.

B. Al tercer día hábil siguiente a la fecha en que se detecte la anomalía, el reporte deberá ser remitido a la Unidad de Transparencia quien efectuará el análisis correspondiente. Si del análisis de la alerta de seguridad, la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención, procederá a su integración en el Plan de Trabajo. Lo que precede, se representa de la forma siguiente:

Reporte de Alerta de Seguridad

Una vez que la instancia advirtió un incidente en el tratamiento de los datos personales, deberá definir si este constituye una alerta de seguridad. Se reitera que, para considerar la configuración de una alerta de seguridad, se deberán actualizar los supuestos siguientes:

C. Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para la instancia.

Verificada la existencia de una alerta de seguridad, la instancia deberá emitir un Reporte de Alerta de Seguridad, en el cual se deberá considerar, como mínimo, el desarrollo de los aspectos siguientes:

· Detección. Nombre, cargo y adscripción del servidor público que detectó la amenaza. Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta. Tratamiento o sistema en que ocurrió. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema. Datos personales involucrados en la amenaza.

· Proyección de una posible vulneración. Elementos que permitieron el desarrollo o persistencia de la amenaza. Elementos que contuvieron el desarrollo o persistencia de la amenaza. Actuaciones que pueden evitar la reincidencia de la amenaza. Descripción de los efectos que hubiera causado la anomalía si hubiere persistido hasta materializar una vulneración.

· Medidas de seguridad involucradas. Descripción clara de los controles físicos o electrónicos involucrados en la amenaza. Circunstancias que, individual o conjuntamente, permitieron la existencia de la amenaza. Justificar si la amenaza pudo ser prevenida, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención. Ante la materialización de la amenaza, justificar si en el futuro puede evitarse su reincidencia, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente puedan impedirlo. Si la forma de prevenir o evitar la reincidencia de la amenaza, involucran una nueva medida de seguridad, deberá ser claramente descrita.

Av. Marina Nacional 60 piso 15, Col. Tacuba, Miguel Hidalgo, C.P. 11410, CDMX. Tel: 5062 1600, Ext.53366#, www.gob.mx/salud

Concluido lo anterior, al tercer día hábil siguiente a la detección de la alerta, el reporte deberá ser remitido a la Unidad de Transparencia.

Registro y análisis de la alerta de seguridad

Recibido el Reporte de Alerta de Seguridad, la Unidad de Transparencia procederá a su registro y realizará un análisis que deberá dilucidar los aspectos siguientes:

a) El impacto que tiene la alerta en la seguridad de los datos personales.

b) Observaciones en materia de seguridad que la instancia debe observar en el futuro desarrollo del tratamiento.

c) Medidas de seguridad adicionales que se estime conducente implementar.

d) Si resulta posible determinar una estrategia de prevención con instancias en las que la alerta de seguridad pueda desencadenarse. Si del análisis de la alerta de seguridad la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención, procederá a su integración en el Plan de Trabajo del Documento de Seguridad del área responsable.

IV. Vulneraciones de seguridad de los datos personales

El mecanismo que aquí se describe, resulta obligatorio para las áreas administrativas que en ejercicio de sus funciones realicen el tratamiento de datos personales. En primer término, de conformidad con lo establecido en el artículo 38 de la Ley General, resulta indispensable que la instancia identifique que efectivamente los hechos acaecidos constituyan una vulneración a la seguridad de los datos personales, para lo cual, deberán verificar la materialización de los supuestos siguientes:

1 Que exista una afectación concreta en el tratamiento de los datos personales que haya generado conjunta o separadamente los supuestos siguientes:

1. La pérdida o destrucción no autorizada.
2. El robo, extravío o copia no autorizada.
3. El uso, acceso o tratamiento no autorizado.
4. El daño, la alteración o modificación no autorizada.

1 Que la afectación implique un daño a las bases de datos, al personal, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para las instancias de la Secretaría de Salud.

Si alguno de los puntos anteriores no se actualiza, no se considerará una vulneración de los tratamientos o sistemas de datos personales, razón por la cual no será necesario la ejecución del proceso descrito en este apartado, y deberá procederse, en su caso, en los términos previstos para una alerta de seguridad. Ante una vulneración en la seguridad de los datos personales, los artículos 37 a 41 de la Ley General, establecen las obligaciones siguientes:

1. Analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar que la vulneración se repita.
2. Inscribir la vulneración en la bitácora de las vulneraciones.
3. Informar sin dilación alguna al titular y al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), las vulneraciones que afecten de forma significativa derechos patrimoniales o morales, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Se procede a describir la forma y tiempo en que se acreditará el cumplimiento de cada uno de los puntos anteriores. Lo anterior, de conformidad con el esquema siguiente:

· Elaboración del Informe de Causas y Acciones en una Vulneración por la instancia: día hábil siguiente a partir de la detección de la vulneración.
· Remisión a la Unidad de Transparencia: segundo día hábil siguiente a partir de la detección de la vulneración.

Análisis de las causas de la vulneración

· La Unidad de Transparencia tendrá 24 horas a partir de que se le haya notificado la vulneración por parte de la instancia respectiva.

Inscripción en la Bitácora de Vulneraciones

· La Unidad de Transparencia tendrá 72 horas a partir de que se detecte de la vulneración. Notificación al INAI
· La Unidad de Transparencia tendrá 72 horas a partir de que se detecte la vulneración. Notificación al particular afectado
· La Unidad de Transparencia tendrá 72 horas a partir de que se detecte la vulneración.

Análisis de las causas por las cuales se presentó la vulneración y de las acciones preventivas y correctivas correspondientes

Una vez verificada la existencia de la vulneración, procederá realizar lo siguiente:

Dentro del día hábil siguiente a la fecha en que se detecte, la instancia respectiva deberá elaborar un Informe de Causas y Acciones de una Vulneración, en los términos que más adelante se abordarán. Al segundo día hábil siguiente a la fecha en que se detecte, la instancia deberá remitir el informe a la Unidad de Transparencia, quien efectuará el registro y análisis correspondiente. Lo que precede, se representa de la forma siguiente:

Informe de Causas y Acciones de una Vulneración

Para la emisión del informe en mención, necesariamente habrá que considerar, como mínimo, el desarrollo de los aspectos siguientes:

1. Información general de la vulneración

§ Detección: Nombre, cargo y adscripción del servidor público que detectó la vulneración. Fecha, hora y lugar en que se detectó la vulneración. Tratamiento o sistema que fue

vulnerado. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema. Datos personales involucrados en la vulneración. Descripción detallada de la forma en que se detectó la vulneración.

§ Investigación: Fecha y hora en que se inició la investigación de la vulneración. Nombre y cargo del servidor público designado para la investigación de la vulneración. Naturaleza de la vulneración. Fecha y hora

de la vulneración. Descripción detallada de la forma en que se desarrolló la vulneración. Descripción detallada de las afectaciones que fueron materializadas. Tipo y número aproximado de titulares afectados. Posibles consecuencias de la vulneración.

§ Medidas de seguridad vulneradas e impacto causado: Descripción clara de cada uno de los controles físicos o electrónicos que operan en el tratamiento o sistema, incluyendo el servidor público responsable de su implementación. Identificación de la totalidad de las personas que cuentan con acceso a cualquiera de las fases del tratamiento, incluyendo servidores públicos o personas ajenas a la Secretaría de Salud. Identificación y descripción de la vulneración materializada. Determinación del nivel de impacto causado por la vulneración en relación con el tratamiento o sistema (alto, medio, bajo), considerando el número de titulares afectados, así como el tipo y naturaleza de los datos personales involucrados en la vulneración. Determinación relativa a si la vulneración generó una afectación significativa a los derechos patrimoniales y/o morales de los titulares de los datos personales. De conformidad con lo previsto en los párrafos tercero y cuarto del artículo 66 de los Lineamientos Generales, para determinar la existencia de una afectación significativa patrimonial o moral, se deberán atender los criterios siguientes:

2. Acciones preventivas y correctivas

· Justificar si la vulneración pudo ser prevenida, es decir, si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.

· Si la vulneración no puso ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.

· Analizar las medidas que, de acuerdo con la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.

· Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración.
· Recomendaciones para el titular afectado.
· Medio puesto a través del cual pueda obtenerse mayor información respecto de la vulneración.
· Datos de contacto de los servidores públicos designados para la gestión de la vulneración.
· Cualquier información y/o documentación que se considere conveniente.

Hecho lo anterior, al segundo día hábil siguiente a la fecha en que se detectó la vulneración, la instancia deberá remitir el informe a la Unidad de Transparencia, quien efectuará el registro y análisis correspondiente.

3. Análisis de la vulneración de seguridad

Recibido el Informe de Causas y Acciones de una Vulneración, la Unidad de Transparencia procederá a su registro y realizará un análisis que deberá dilucidar los aspectos siguientes:

· El impacto que tiene la vulneración de seguridad en la protección de los datos personales.
· Observaciones en materia de seguridad que la instancia debe observar en el futuro desarrollo del tratamiento.
· Medidas de seguridad adicionales que se estime conducente implementar.
· Si resulta posible determinar una estrategia de prevención en diversos tratamientos en los que la vulneración de seguridad pueda desencadenarse. Si del análisis de la vulneración, la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención procederá a su integración en el Plan de Trabajo del Área responsable.

4. Inscripción en la bitácora de vulneraciones

De conformidad con el artículo 39 de la Ley General, se deberá llevar una bitácora de las vulneraciones a la seguridad en la que se realice una descripción de ésta, la fecha en la que ocurrió, su motivo y las acciones correctivas implementadas de forma inmediata y definitiva. En ese sentido, la Unidad de Transparencia integrará la Bitácora de Vulneraciones a la Seguridad de los Datos Personales, en la que se concentrarán las

vulneraciones acaecidas en la totalidad de las Unidades Responsables de la Secretaría de Salud. Por lo que, dentro del plazo de 24 horas siguientes al en que la instancia notifique la vulneración, se deberá proceder a su registro. La inscripción realizada, deberá ser informada por la Unidad de Transparencia al Comité de Transparencia, para su conocimiento y efectos conducentes. Posterior a la inscripción deberá remitirse una copia de dicho registro a la instancia respectiva, a efecto de que sea integrada a su bitácora interna de incidentes y vulneraciones a la seguridad, en términos del artículo 18, fracción I, del Acuerdo General.

5. Informe de la vulneración al INAI y al titular de los datos personales

El artículo 40 de la Ley General dispone que, ante una vulneración que afecte de forma significativa derechos patrimoniales o morales, se deberá informar sin dilación alguna al titular y al INAI. Dicho informe, deberá realizarse en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos. Al respecto, el artículo 66 de los Lineamientos Generales estipula que la notificación del informe al titular y al Instituto referido deberá realizarse dentro en un plazo máximo de 72 horas, a partir de que se confirme la ocurrencia de la vulneración y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. Bajo ese panorama, ocurrida una vulneración, la Unidad de Transparencia deberá realizar lo siguiente:

A. Notificar la vulneración al INAI.

B. Verificar que la instancia respectiva notifique al particular o particulares afectados por la vulneración identificada. Lo anterior, en los términos que se explican a continuación.

6. Notificación de la vulneración al INAI

La Unidad de Transparencia analizará de forma exhaustiva las particularidades de la vulneración y, de conformidad con el artículo 66 de los Lineamientos Generales, realizará lo siguiente:

Av. Marina Nacional 60 piso 15, Col. Tacuba, Miguel Hidalgo, C.P. 11410, CDMX. Tel: 5062 1600, Ext.53366#, www.gob.mx/salud

a) Identificará si en el Informe de Causas y Acciones de una Vulneración, la instancia respectiva consideró que la afectación sufrida causaba un daño significativo patrimonial o moral en detrimento de los titulares de los datos personales afectados.
b) Supervisará las acciones implementadas por la instancia para restituir la seguridad del tratamiento de los datos personales. Por ello, en términos de lo establecido en los artículos 40 y 41 de la Ley General, en caso de que la instancia haya considerado que la afectación al patrimonio o la moral causada es significativa, dentro de las 72 horas siguientes a la confirmación de la ocurrencia de la vulneración, la Unidad de Transparencia realizará un informe dirigido al INAI que, de conformidad con el artículo 67 de los Lineamientos Generales, considere los aspectos siguientes: La hora y fecha de la identificación de la vulneración. La hora y fecha del inicio de la investigación sobre la vulneración. La naturaleza de la vulneración ocurrida. La descripción detallada de las circunstancias en torno a la vulneración ocurrida. Las categorías y número aproximado de titulares afectados. Los sistemas de tratamiento y datos personales comprometidos. Las acciones correctivas realizadas de forma inmediata. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida. Las recomendaciones dirigidas al titular. El medio puesto a disposición del titular para que pueda obtener más información al respecto. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al INAI. Cualquier otra información y documentación que se considere conveniente hacer del conocimiento del INAI.

7. Notificación de la vulneración a los particulares

De haberse considerado la actualización de una afectación significativa al patrimonio o a la moral del titular o titulares de los datos personales, la instancia respectiva deberá realizar un informe que considere los aspectos siguientes:

- La naturaleza de la vulneración.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que este pueda adoptar para proteger sus intereses.

· Las acciones correctivas realizadas de forma inmediata.
· Los medios donde puede obtener más información al respecto.
· La descripción de las circunstancias generales en torno a la vulneración ocurrida, que le ayuden a entender el impacto de la vulneración.
· Cualquier otra información y documentación que se considere conveniente para apoyar a los titulares de los datos personales afectados.

La Unidad de Transparencia podrá auxiliar al Área Administrativa en la elaboración del informe, el cual deberá notificarse por la instancia respectiva al particular o los particulares afectados dentro de las 72 horas siguientes a la detección de la vulneración. Dicha notificación, deberá efectuarse a través del medio que resulte idóneo y de fácil acceso, considerando la forma en que se obtuvieron los datos personales, el perfil que guarda el titular y la forma en que se mantiene contacto con él y en ninguno de los casos, deberá generarle costo alguno; lo anterior, en los términos establecidos en el artículo 68 de los Lineamientos Generales. Hecho lo anterior, la instancia respectiva deberá remitir a la Unidad Administrativa el acuse de recibo respectivo.

V. Mecanismo de auditoría en materia de datos personales

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados (Ley General), establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión. Por tanto, con la finalidad de comprobar el cumplimiento de las políticas de protección de datos personales, así como para monitorear y revisar la eficacia y eficiencia del sistema de gestión, se elaboró el presente Mecanismo de Auditoría en Materia de Datos Personales.

· Finalidades y objetivos

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

1 Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable.

1 Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión y el Documento de Seguridad.

1 Verificar la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas. 1 Validar el avance de los objetivos planteados en el Plan de Trabajo.

1 Prevenir la materialización de vulneraciones a la seguridad de los datos personales.

1 Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.

En ese sentido, el Mecanismo de Auditoría en Materia de Datos Personales tiene como objetivos principales los siguientes:

1. Determinar la forma en que se desarrollarán las etapas de las auditorías en materia de datos personales.
2. Establecer los aspectos a examinar.
3. Puntualizar los documentos a través de los cuales se asentará el desarrollo de las etapas respectivas, las observaciones advertidas y las aclaraciones conducentes.
4. Precisar el proceso a través del cual se seleccionarán las Áreas Administrativas auditables.

Es importante referir que el alcance que tendrán las auditorías practicadas se concentrará exclusivamente en el análisis de la forma en que cada instancia, en el ámbito de su competencia, implementa las políticas que les resulten aplicables en materia de datos personales, así como la evaluación del estado de seguridad en que se encuentran los datos personales bajo su tratamiento; lo anterior, con la finalidad de implementar mejoras que de manera progresiva permitan a la Secretaría de Salud perfeccionar el manejo y protección de los datos personales.

· Instancia ejecutora del programa y ámbito de aplicación

La Secretaría de Salud a través de la Unidad de Transparencia y por conducto del Oficial de Protección de Datos Personales, debe establecer

un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.

Consecuentemente, el Programa de Auditoría en materia de Datos Personales será ejecutado por la Unidad de Transparencia. Por lo que se refiere al ámbito de aplicación, se indica que las instancias que en ejercicio de sus funciones realicen el tratamiento de datos personales, serán los sujetos auditables materia del programa, de modo que se encuentran obligadas a coadyuvar activamente con la Unidad de Transparencia para el desarrollo de las auditorías respectivas.

· Etapas de las auditorías en materia de datos personales

Las auditorías en materia de protección de datos personales estarán conformadas por las etapas de apertura, revisión y conclusiones.

1. La etapa de apertura: tendrá la finalidad de definir el personal de la instancia auditada ante el cual la Unidad de Transparencia substanciará la auditoría, así como los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial o virtual), y los requerimientos específicos necesarios para su realización.
2. En la etapa de revisión: se realizará el escrutinio de la forma en que la instancia acredita el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad, de conformidad con lo previsto en la normativa aplicable, así como en el Programa de Protección de Datos Personales y el Documento de Seguridad.
3. En la etapa conclusiva: la Unidad de Transparencia puntualizará a la instancia auditada las consideraciones efectuadas, abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y señalará la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que las Unidades Responsables deberán remitir las evidencias correspondientes.

Etapa de apertura- Notificación de auditoría

De conformidad con el calendario de auditorías en materia de datos personales, la Unidad de Transparencia por conducto del Oficial de Protección de Datos Personales, comunicará por oficio a el área administrativa correspondiente, lo siguiente:

· La fecha en que dará inicio la auditoría, la cual deberá realizarse con un mínimo de 5 días hábiles entre la notificación del oficio y su celebración.
· La necesidad de que la instancia auditada designe al personal con el que la Unidad de Transparencia substanciará la auditoría.
· La convocatoria a una reunión previa al inicio de la auditoría, entre el personal de la Unidad de Transparencia y el personal designado por la instancia auditada. Reunión previa En el día señalado para la reunión previa, se informarán los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial, virtual o mixta), así como los requerimientos específicos necesarios para la realización de la propia auditoría. Efectuada la reunión previa, la referida Unidad de Transparencia elaborará una minuta en la que se precisará el desarrollo de la propia reunión, la cual deberá ser signada por los involucrados.

Acuerdo de inicio

En el día estipulado para el comienzo de la auditoría, el Oficial de Protección de Datos Personales de la Secretaría de Salud emitirá un acuerdo de inicio en el que deberá asentar lo siguiente:

· El servidor público designado por la instancia auditada para sustanciar la auditoría.
· Identificación del tratamiento o tratamientos de datos personales materia de la auditoría.
· El tipo de revisión que amerite el tratamiento (documental, presencial, virtual o mixta).
· La documentación, sistema o espacio físico que deberá estar plenamente disponible para ser examinado.
· Los datos de contacto de la UT ante los cuales podrán solventarse dudas relacionadas con el desarrollo de la auditoría. El acuerdo de inicio deberá ser notificado a la instancia respectiva y deberá obrar en el expediente que para esos efectos integre la Secretaría de Protección de Datos Personales.

Etapa de revisión

Esta etapa corresponde el escrutinio de la forma en que las instancias acreditan el cumplimiento de los principios de licitud, finalidad, lealtad,

consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad.

Examinación

En el marco de los estipulado en el acuerdo de inicio, la Unidad de Transparencia procederá a la revisión del tratamiento o tratamientos de datos personales, a efecto de corroborar que se encuentren apegados a los principios y deberes siguientes:

· Principio de licitud: el tratamiento de datos personales deberá tener sustento o estar relacionado con las facultades o atribuciones que la normatividad aplicable confiera a la instancia auditada.

· Principio de finalidad: el tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera a la instancia auditada.

· Principio de lealtad: que los datos personales no se hayan obtenido a través de medios engañosos o fraudulentos.

· Principio de consentimiento: cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la Ley General, la instancia auditada deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.

· Principio de calidad: que la Unidad Responsable auditada haya adoptado las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

· Principio de proporcionalidad: que la Unidad Responsable auditada sólo haya tratado los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad para la cual fueron recabados.

· Principio de información: que la Unidad Responsable auditada haya informado al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

· Principio de responsabilidad: que la instancia auditada haya adoptado la políticas y mecanismos necesarios para asegurar el cumplimiento de los principios, deberes y demás obligaciones

establecidas en la Ley General que establece las disposiciones en materia de protección de datos personales.

· Deber de seguridad: que la Unidad Responsable auditada haya establecido y mantenido medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión.
· Deber de confidencialidad: la Unidad Responsable auditada deberá demostrar la existencia de controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos.

Documento de conclusiones

La Unidad de Transparencia elaborará el documento de conclusiones, en el cual asentará la información que derive de la examinación realizada. Dicho documento, deberá exponer de manera clara lo siguiente:

· La estimación de cumplimiento correspondiente a cada principio y deber.
· Consideraciones que se estimen relevantes en cuanto al tratamiento de los datos personales.
· Recomendaciones en materia de seguridad de los datos personales.
· Observaciones y requerimientos que deban ser atendidos ante una deficiencia, desviación o mejora necesaria en el tratamiento de los datos personales, especificando el plazo en que las instancias deberán remitir las evidencias respectivas a la Unidad de Transparencia.
· Conclusiones generales de la auditoría.

Etapa conclusiva- Reunión final

El Oficial de Protección de Datos Personales convocará a la Unidad Responsable auditada a una reunión final, con el objetivo de hacerle entrega del documento de conclusiones. En tal reunión se explicarán a detalle las consideraciones efectuadas, se abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y se puntualizará el plazo y la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que las instancias deberán remitir las evidencias correspondientes. Efectuada la reunión final, la referida Secretaría elaborará una minuta en la que se concentrarán

las conclusiones alcanzadas, la cual deberá ser signada por los involucrados.

Cumplimiento de observaciones y requerimientos

Dentro del plazo otorgado en el documento de conclusiones, la instancia auditada deberá remitir a la UT las evidencias del cumplimiento de las observaciones y requerimientos que le hubieran sido realizados. Tales evidencias serán examinadas a efecto de dilucidar si cumplen con los extremos determinados y con ello, se atendió la deficiencia, desviación o mejora en el tratamiento de los datos personales. Si de su examen la UT corrobora que han sido adecuadamente cumplidas las observaciones y requerimientos, se procederá al cierre de la auditoría. Por el contrario, de concluir que existen extremos no cumplidos total o parcialmente, la UT realizará un único requerimiento adicional, reiterando la forma en que la instancia auditada debe demostrar su acatamiento. Si a pesar de ello persiste el incumplimiento, el Oficial de Protección de Datos Personales hará constar la persistencia de la deficiencia o desviación y procederá al cierre de la auditoría.

Informe de cierre de la auditoría

Teniendo a la vista la documentación generada en las etapas de la auditoría, la minuta de la reunión final y las evidencias que deriven del cumplimiento de observaciones y requerimientos, El Oficial de Protección de Datos Personales elaborará un informe final con el cual se dará por concluida la auditoría. Cabe precisar que, si del informe efectuado se advierte un incumplimiento a las observaciones y requerimientos efectuados, se dará cuenta al Comité de Transparencia a efecto de que tome conocimiento de tal inobservancia, así como de la deficiencia o desviación en el tratamiento respectivo. Dicho informe, deberá ser notificado a la Unidad Responsable auditada a más tardar dentro de los tres días hábiles siguientes a su emisión.

Selección de las instancias auditables

La programación de las auditorías se realizará a través de una selección de instancias basada en criterios aplicados al panorama general que guarda el tratamiento de los datos personales en la Secretaría de Salud. De

manera que, las auditorías a practicar se programarán analizando dicho panorama a la luz de criterios de selección específicos.

Panorama general

Del Inventario de Datos Personales y Sistemas, se tomará en consideración lo siguiente:

· El número de Unidades Responsables involucradas en el tratamiento de datos personales.
· El número de tratamientos que cada Unidad Responsable realiza, así como el resultado global de tal estadística.
· Los tratamientos se clasificarán en las categorías siguientes: Datos de carácter identificativo. Características personales. Circunstancias sociales. Datos académicos y profesionales. Detalles del empleo. Información comercial. Datos económicos. Financieros y de seguro.
· Instancias que operen uno o varios tratamientos que conlleven datos personales sensibles.

Criterios de selección

Ante el panorama general expuesto y atendiendo a los objetivos de este programa, los criterios de selección serán los siguientes:

· Tratamientos con un número considerable de riesgos.
· Tratamientos que, de ser objeto de una vulneración, tengan como consecuencia un impacto mayor al titular de los datos personales.
· Tratamientos prioritarios, especiales o estratégicos, que serán aquellos que conlleven un alto valor potencial cuantitativo y cualitativo para una tercera persona no autorizada para su posesión o que puedan causar un daño a la reputación del titular.
· Instancias cuyas funciones impliquen un alto número de tratamientos.
· Instancias cuyas funciones impliquen el tratamiento de datos sensibles.

En su análisis se considerarán los factores siguientes:

· El riesgo inherente a cada dato personal de acuerdo con su categoría.
· La sensibilidad del dato personal.

· El desarrollo tecnológico del sistema que opera el tratamiento.
· Posible impacto y consecuencias de la vulneración del dato personal.
· Número de titulares.
· Vulneraciones previas ocurridas en el sistema de datos.
· Valor y exposición de los activos3 involucrados con el tratamiento.

Para fijar el impacto, se considerará el tipo de riesgo existente (operativo, normativo o tecnológico), su probabilidad (muy poco probable, poco probable, probable o segura) y la proyección del daño que pueden producirse si la amenaza se concreta.

Programación

Una vez realizada la selección de las instancias bajo los criterios expuestos, la Unidad de Transparencia ponderará la cronología que deberá seguir la calendarización de las auditorías, lo cual deberá hacerse del conocimiento del Comité de Transparencia para su aprobación.

FECHA DE ÚLTIMA ACTUALIZACIÓN: 18-04-2023.