Mecanismos de monitoreo y revisión de las medidas de seguridad

Juan Badiano No, 1, Col. Belisario Domínguez Sección XVI, Alcaldía Tlalpan, C.P. 14080, CDMX Tel: (55) 5573 2911
www.cardiologia.org.mx

De acuerdo con lo dispuesto en el artículo 24, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), entre los mecanismos que deberán adoptarse para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Asimismo, el artículo 29, fracción VI de la Ley General, prevé que entre otros aspectos, el documento de seguridad deberá contener los mecanismos de monitoreo y revisión de las medidas de seguridad.

En ese sentido, en el artículo 27, fracción VII de la Ley General, se indica que se deben 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.

Aunado a lo anterior, el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) refiere 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.

Los mecanismos previstos en el presente documento serán aplicables específicamente al Sistema de Expediente Clínico Electrónico, así como a los sistemas, infraestructura tecnológica, bases de datos, aplicaciones, redes, equipos y procesos relacionados con el tratamiento de datos personales efectuado por este Instituto.

El monitoreo, supervisión y revisión de las medidas de seguridad se realizará bajo un enfoque de mejora continua, gestión de riesgos con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para cumplir con lo antes referido, el responsable deberá monitorear continuamente lo siguiente:

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 aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

Juan Badiano No, 1, Col. Belisario Domínguez Sección XVI, Alcaldía Tlalpan, C.P. 14080, CDMX Tel: (55) 5573 2911
www.cardiologia.org.mx

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

VII. Los incidentes y vulneraciones de seguridad ocurridas

En relación con lo anterior, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De acuerdo con lo anterior, este Instituto dará cumplimiento a dicha obligación a través de los mecanismos de monitoreo y supervisión, de actuación ante vulneraciones a la seguridad de los datos personales y de auditoría en materia de datos personales.

1. MECANISMO DE MONITOREO Y SUPERVISIÓN

La Unidad de Transparencia llevará a cabo el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, mediante las siguientes etapas:

I. Etapa de monitoreo

La Unidad de Transparencia realizará el monitoreo de manera cuatrimestral y podrá apoyarse de la Dirección de Administración, la Subdirección de Informática y las áreas responsables de los sistemas de tratamiento.

Las áreas deberán proporcionar evidencia documental que acredite el cumplimiento de las medidas de seguridad implementadas, y además, deberán elaborar un reporte, en el que deberán precisar:

	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.	☐	☐
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 Ley General 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 área.	☐	☐
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, 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: • 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.	☐	☐
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • 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 • 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.	☐	☐
9. Se monitorea y revisa 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: • 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 aceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.		

II. Etapa de Supervisión

La Unidad de Transparencia analizará los reportes emitidos por las áreas, identificando aquellos puntos en los que se hayan reportado:

- Nuevos activos;
- Incumplimientos;
- Controles insuficientes;
- Vulnerabilidades o riesgos;
- Migración tecnológica;
- Nuevas amenazas;
- Nuevas vulnerabilidades;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- Cambios en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos, y
- Incidentes y vulneraciones de seguridad ocurridas.

Derivado de lo anterior, emitirá una ficha de observaciones y acciones correctivas en la que se establecerán:

- Los hallazgos detectados;
- Las medidas correctivas requeridas;
- El área responsable;
- El plazo de atención, y
- La evidencia necesaria para acreditar su cumplimiento.

Las áreas deberán atender los requerimientos en un plazo no mayor a 30 días hábiles, salvo que exista justificación debidamente documentada.

La Unidad de Transparencia dará seguimiento hasta el cierre total de las observaciones emitidas.

2. MECANISMOS DE ACTUACIÓN ANTE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

El artículo 27, fracción VII prevé 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 relación con lo previsto en el artículo referido, el artículo 63, fracción VII de los Lineamientos Generales, refiere 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, deberán monitorearse continuamente los incidentes y vulneraciones de seguridad ocurridas.

Registro y atención de incidentes

Todo incidente o vulneración de seguridad relacionado con datos personales y datos personales sensibles deberá registrarse, clasificarse, analizarse, documentarse y atenderse oportunamente de acuerdo con lo establecido en la Guía para registrar y reportar vulneraciones de datos personales, disponible para su consulta en: .

Por lo anterior, las áreas deberán informar a la Unidad de Transparencia y a la Subdirección de Informática sobre cualquier incidente o vulneración de seguridad de forma inmediata, sin exceder de las veinticuatro horas siguientes a su detección.

La Unidad de Transparencia coordinará acciones con la Dirección de Administración y la Subdirección de Informática para el análisis técnico y seguimiento de los incidentes de seguridad.

3. MECANISMOS DE AUDITORÍA EN MATERIA DE DATOS PERSONALES

De conformidad con lo dispuesto en el artículo 24, fracción V de la Ley General, entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad, deberá establecerse un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Asimismo, el artículo 63 de los Lineamientos, establece que se deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Las auditorías en materia de datos personales tendrán por objeto analizar el cumplimiento de los deberes y principios previstos en la Ley General respecto de las áreas, mismos que fueron documentados a través de los cuestionarios sobre el tratamiento de datos personales y los inventarios y podrán incluir:

- Revisión documental;
- Validación de medidas de seguridad administrativas, físicas y técnicas;
- Revisión de controles de acceso;
- Análisis de vulnerabilidades;
- Revisión de bitácoras;
- Verificación de cumplimiento normativo, y
- Seguimiento de acciones correctivas derivadas de auditorías previas.

Las auditorías internas se realizarán de manera anual, mientras que las auditorías externas podrán realizarse cuando exista una modificación tecnológica relevante, una vulneración de seguridad, o cuando lo determine el Comité de Transparencia.

Por lo anterior, la Unidad de Transparencia realizará la propuesta al Comité de Transparencia respecto del inventario, deber o principio que deberá ser objeto de auditoría.

Evidencia documental

Como evidencia del cumplimiento de los mecanismos de monitoreo y revisión de las medidas de seguridad, deberán conservarse:

- Inventarios de tratamientos;
- Análisis de riesgos;
- Análisis de brecha;
- Bitácoras;
- Informes;
- Registros de incidentes;
- Evidencia de implementación de controles;
- Y cualquier documento generado en la atención del seguimiento de los mecanismos de monitoreo y revisión de las medidas de seguridad.

Tratándose del Sistema de Expediente Clínico Electrónico, se dará especial seguimiento a los accesos autorizados, privilegios de usuarios, transferencias de información, respaldos de información, disponibilidad de la información clínica y trazabilidad de operaciones realizadas en dicho Sistema.

Los mecanismos previstos en el presente documento estarán sujetos a revisión y actualización continua conforme a los cambios normativos, tecnológicos y operativos identificados por el Instituto, con el objeto de fortalecer permanentemente la seguridad del Sistema de Expediente Clínico Electrónico y la protección de los datos personales, de conformidad con lo dispuesto 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.

Juan Badiano No, 1, Col. Belisario Domínguez Sección XVI, Alcaldía Tlalpan, C.P. 14080, CDMX Tel: (55) 5573 2911
www.cardiologia.org.mx