



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"



COFAA
COMISIÓN DE OPERACIÓN Y FOMENTO
DE ACTIVIDADES ACADÉMICAS DEL
INSTITUTO POLITÉCNICO NACIONAL

2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

SISTEMAS DE SUPERVISIÓN Y VIGILANCIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES 2024

1 de

Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional.
Tresguerras No. 27, Esq. M. Tolsá, Col. Centro, Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06040.
Conmutador 5729 6000, extensiones 65103, 65020, 65041 y 65097.

www.cofaa.ipn.mx





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

CONTENDIO

1. Mecanismo de monitoreo y supervisión
2. Etapa de Monitoreo.
3. Etapa de Supervisión
4. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

INTRODUCCIÓN

El artículo **30**, fracción **V**, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que, entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de implementar un sistema de supervisión y vigilancia, 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 artículo **33**, fracción **VII**, de la Ley General, 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

En ese contexto, el artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece 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, se deberá monitorear continuamente 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 del sujeto obligado 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,





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

- ✓ Los incidentes y vulneraciones de seguridad ocurridos.

En ese sentido, la Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional (COFAA-IPN), desarrollará el cumplimiento de dicha obligación a través de un mecanismo de monitoreo y supervisión; y el Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales.

Mecanismo de monitoreo y supervisión

La Unidad de Transparencia será la encargada 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:

Etapas 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.



2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECYT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

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 Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

	si	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 LGPDPSO 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 persona que trata datos personales		
4. Se ha comunicado a cada integrante de las áreas de la comisión que realice tratamiento de datos personales 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: <ul style="list-style-type: none"> ● Los medios físicos y electrónicos a través de los cuales se obtienen los datos personales; ● Las finalidades de cada tratamiento de datos personales; 		





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

<ul style="list-style-type: none"> ● El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
<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 ● Criterios emitidos por el INAI que coadyuvaran al comité de Transparencia y a los responsables del tratamiento de datos personales a un correcto manejo y clasificación de la información
<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. ● El desarrollo tecnológico; ● 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.
<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





reemplazar a uno o más controles implementados actualmente.
<p>10. 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:</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.

Etapas 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 plasmarán 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





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

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 COFAA-IPN, 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.

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.

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.





2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab
100 Aniversario del CECyT "Gonzalo Vázquez Vela"
60 Aniversario del Centro Cultural "Jaime Torres Bodet"
50 Aniversario de la ESIME Unidad Culhuacán,
ESIA Unidad Tecamachalco y de la Escuela Superior de Turismo
40 Aniversario del CIEMAD, CEPROBI y del CITEDI

- ✓ 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.

