

# MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS



## CONTENIDO

I. Aprobación.....	3
II. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad Implementadas.....	4
A. Mecanismos de monitoreo y revisión de carácter general.....	4
B. Mecanismos de monitoreo y revisión de las medidas de seguridad técnicas implementadas.....	6
C. Mecanismos de monitoreo y revisión de las medidas de seguridad administrativas y físicas implementadas.....	9
D. Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones.....	10



# MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS

## I. Aprobación

Los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad Implementadas (Mecanismos de Monitoreo y Revisión) se adoptaron en cumplimiento a lo dispuesto en los artículos 33, fracción VII y 35, fracción VI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; como parte integrante del Documento de Seguridad para la Protección de los Datos Personales en Posesión del Instituto Federal de Telecomunicaciones (Documento de Seguridad) cuya última actualización se aprobó mediante Acuerdo 19/SO/28//24, del Comité de Transparencia del Instituto Federal de Telecomunicaciones (Comité u Órgano Colegiado), en la Décima Novena Sesión Ordinaria, celebrada el 20 de mayo de 2024. Los Mecanismos de Monitoreo y Revisión se encuentran contenidos en el Capítulo IX del Documento de Seguridad.

Mediante Acuerdo 07/SO/10/2025 emitido por el Órgano Colegiado el 27 de febrero de 2025, se propuso la actualización del presente documento con la finalidad de ser acorde con el Documento de Seguridad Vigente y las Reglas de Operación del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones.

### A. Mecanismos de monitoreo y revisión de carácter general

En cumplimiento a lo dispuesto en los artículos 33, fracción VII, 35, fracción VI, de la LGPDPPSO, y 63 de los Lineamientos Generales, como parte de los mecanismos para 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, se proponen algunos mecanismos de supervisión interna y externa, basados en los principios de (1) participación, (2) evaluación continua, y (3) evaluación y comunicación de deficiencias, requisitos institucionales establecidos para el “Principio de supervisión” del Sistema de Control Interno del Instituto. De manera particular, se proponen las siguientes acciones:

Internos	Externos
<p>Supervisión por parte del Comité de Transparencia, en coordinación con las Áreas o Unidades Administrativas competentes del IFT, a través del Grupo de Trabajo de Protección de Datos Personales del Instituto Federal de Telecomunicaciones y de las acciones relacionadas con el Sistema de Control Interno Institucional, para el cumplimiento de las medidas, controles y acciones previstas en el Documento de Seguridad.</p>	<p>Auditorías y revisiones voluntarias a cargo del INAI, en términos de lo dispuesto por el artículo 151 de la LGPDPSO.</p>
<p>Supervisión directa por parte de las personas servidoras públicas en sus respectivos niveles de competencia, respecto al funcionamiento y operación de las medidas de seguridad físicas, administrativas y técnicas, con el objetivo de identificar áreas de mejora y oportunidad para proteger de una manera más adecuada los datos personales en posesión del Instituto.</p>	
<p>Acciones del Grupo de Trabajo de Protección de Datos Personales del Instituto, con el objetivo de revisar de manera periódica la efectividad de las medidas de seguridad existentes y faltantes.</p>	
<p>Elaboración de un <b>Informe anual</b> por parte de la Unidad de Transparencia, que incluya la información relativa al cumplimiento de la normativa en la materia, con el objetivo de contar con un referente cuantitativo y</p>	



Internos	Externos
<p>cualitativo que permita determinar lo siguiente:</p> <ul style="list-style-type: none"><li>• Personal capacitado en el Instituto respecto a los conceptos, principios, deberes y derechos contenidos en la LGPDPPSO y sus Lineamientos Generales, a partir de la oferta de acciones de capacitación impartidas por el INAI en las modalidades virtual y/o presencial a distancia, así como las acciones de capacitación impartidas a las personas servidoras públicas del Instituto en materia de protección de datos personales con recursos propios.</li></ul> <p>En términos de lo dispuesto por el numeral Décimo Tercero de la Política de Protección de Datos Personales del Instituto, la Unidad de Transparencia deberá presentar anualmente al Comité de Transparencia, el programa de capacitación del personal en materia de protección de datos personales, considerando el perfil de puesto, sus roles y responsabilidades asignadas para el tratamiento, seguridad y resguardo de los datos personales.</p> <p>La Unidad de Transparencia presentará al INAI, a más tardar el primer trimestre de cada año, la detección de necesidades de capacitación especializada en materia de protección de datos personales, misma que se encontrará alineada al Programa Anual de Capacitación que el INAI al efecto establezca.</p> <ul style="list-style-type: none"><li>• Acciones realizadas durante el periodo a reportar en materia de protección de datos</li></ul>	



Internos	Externos
<p>personales, para dar cumplimiento a la legislación aplicable.</p> <ul style="list-style-type: none"><li>• Acciones y reuniones realizadas por el Grupo de Trabajo de Protección de Datos Personales del Instituto, como parte de los mecanismos de monitoreo y revisión de las medidas de seguridad implementadas, así como de las amenazas y vulneraciones a las que están sujetos los datos personales.</li><li>• En su caso, la referencia a las actividades del Comité de Transparencia que, en su carácter de autoridad máxima en la materia, tengan como objeto coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el Instituto, de conformidad con las disposiciones previstas en la LGPDPSO, los Lineamientos Generales y en aquellas disposiciones que resulten aplicables en la materia.</li></ul>	

## B. Monitoreo y revisión de las medidas de seguridad técnicas implementadas

De conformidad con lo dispuesto en los artículos 33, fracción VII, 35, fracción VI, de la LGPDPSO y 63 de los Lineamientos Generales, a continuación, se presentan los mecanismos para monitorear y revisar de manera periódica, las medidas de seguridad técnicas implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Control de seguridad	Acciones específicas
Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así	Los controles técnicos de seguridad se encuentran implementados a través de



Control de seguridad	Acciones específicas
como las amenazas y vulneraciones a las que están sujetos los datos personales.	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED] para identificar de manera oportuna los ataques que pudieran generarse.</p> <p>Previo a la actualización o salida a producción de una solución tecnología, se realizan los análisis de vulnerabilidades correspondientes para identificar las brechas de seguridad existentes; [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED] en las aplicaciones Web. En el mismo sentido, toda la infraestructura involucrada en la operación de las soluciones tecnológicas y las comunicaciones electrónicas, así como la infraestructura de seguridad, se analiza periódicamente para identificar vulnerabilidades y/o configuraciones deficientes.</p> <p>[REDACTED] se realizan pruebas [REDACTED] ético o [REDACTED] con el objetivo de [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED] Dentro de estas pruebas se realizan actividades para [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

<sup>1</sup> <https://www.imatech.com/blog/2019/04/01/riesgos-de-seguridad-owasp/>



Control de seguridad	Acciones específicas
	<p>El SGSI, del Instituto contempla un proceso de gestión de riesgos que es ejecutado de [REDACTED]</p> <p>[REDACTED] El objetivo de dicho proceso es [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>Asimismo, el SGSI cuenta con [REDACTED] establecidos, los cuales son medidos periódicamente para medir la eficacia de los controles de seguridad implementados.</p> <p>Para garantizar que el SGSI y los controles de seguridad de la información operen de acuerdo con las políticas, los procesos y procedimientos establecidos, [REDACTED] se realizan una auditoría interna y una auditoría por parte de la [REDACTED] que certificó el Sistema de Gestión de Seguridad de la Información bajo [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>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. En particular, deberá</p>	<p>Los controles administrativos relacionados con la seguridad tales como las Políticas específicas de seguridad de la información y la Política para el uso de recursos de las TIC, son monitorizados a través de un proceso disciplinario preestablecido y se encuentran bajo un esquema de mejora continua que considera su revisión y en su caso adecuación periódica.</p>





Control de seguridad	Acciones específicas
<p>monitorearse continuamente lo siguiente:</p> <ul style="list-style-type: none"><li>• Los nuevos activos que se incluyan en la gestión de riesgos.</li><li>• Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.</li><li>• Las <b>nuevas amenazas</b> que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.</li><li>• La posibilidad de que <b>vulnerabilidades nuevas o incrementadas</b> sean <b>explotadas</b> por las amenazas correspondientes.</li><li>• Las <b>vulnerabilidades identificadas</b> para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.</li><li>• El cambio en el impacto o consecuencias de amenazas valoradas, <b>vulnerabilidades y riesgos</b> en conjunto, que resulten en un nivel inaceptable de riesgo, y</li><li>• Los <b>incidentes</b> y <b>vulneraciones de seguridad</b> ocurridas.</li></ul>	

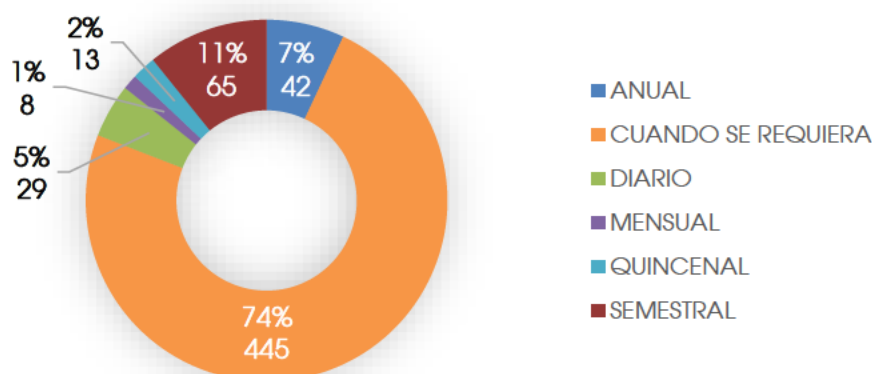


### C. Mecanismos de Monitoreo y revisión de las medidas de seguridad administrativas y físicas implementadas

La frecuencia de monitoreo o seguimiento de la efectividad de los controles implementados por las Unidades Administrativas corresponde a la periodicidad con que son revisados en su diseño contra la materialización de riesgos, arrojando como principal resultado la efectividad o insuficiencia de los controles y por ende un rediseño de estos.

El 74% de las medidas de seguridad implementadas en el Instituto son ejecutadas cada vez que son requeridas; por otro lado, las frecuencias de monitoreo semestral y anual son la segunda opción de ejecución con el 8% y el 4% respectivamente. Finalmente, el 7% de las medidas de seguridad son utilizadas en periodos menores.

FRECUENCIA DE MONITOREO DE LA EFECTIVIDAD DE CONTROLES



FUENTE: Elaborado por el IFT, con base en el inventario de riesgos de datos personales.

### D. Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones

El monitoreo y supervisión de las medidas de seguridad implementadas en el Instituto tiene como base el principio de **responsabilidad**, al que hace referencia el artículo 30 de la LGPDPSO, pero incluyendo el componente “proactivo”, que permitirá cumplir de manera más adecuada no sólo con el deber de seguridad, sino con los principios, deberes y derechos establecidos en este ordenamiento y en sus Lineamientos Generales.

De esta manera, con el fin de monitorear y supervisar de manera permanente el cumplimiento de los principios y deberes en el tratamiento de datos, así como las medidas de seguridad administrativas, físicas y técnicas en el IFT, y de conformidad con lo previsto en el artículo 35, fracciones V y VI, de la LGPDPSO, se creó el “Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones” (Grupo de Trabajo).



Las “Reglas de Integración y Operación del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones”, fueron aprobadas por el Comité de Transparencia del IFT, mediante Acuerdo 17/SE/04/20, adoptado en su Décimo Séptima Sesión Extraordinaria, celebrada el 06 de noviembre de 2020, las cuales regulan, de manera general, la integración y operación del Grupo de Trabajo.

En términos de la **TERCERA** disposición general de las Reglas de Integración y Operación del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones, el Grupo de Trabajo tiene los objetivos siguientes:

- Analizar la situación actual del cumplimiento de los principios y deberes establecidos en la LGPDPPSO y los Lineamientos Generales;
- Monitorear el funcionamiento de las medidas de seguridad administrativas, físicas y técnicas, implementadas para proteger la confidencialidad, integridad y disponibilidad de los datos personales en posesión del Instituto;
- Proponer medidas de seguridad administrativas, físicas y técnicas adicionales que puedan incluirse en las políticas de seguridad de la información o en un programa de protección de datos personales institucional;
- Identificar posibles riesgos y amenazas que requieran la adopción de estrategias organizacionales para mitigarlas, con el objetivo de disminuir el impacto en los activos de información en posesión del Instituto;
- Identificar y diseñar soluciones prácticas a problemas, complicaciones y/o contrariedades, entre otras, que dificulten la aplicación y/o cumplimiento de la normatividad en la materia, a efecto de adoptar o estandarizar criterios de control interno para cumplir con los principios de protección de datos personales;
- Detectar y solicitar a las instancias correspondientes capacitación en temas específicos del derecho a la protección de datos personales en atención a las necesidades que se identifiquen al interior del Instituto;
- Aplicar herramientas y metodologías especializadas de control interno y administración de riesgos que promuevan una cultura institucional de protección de datos Personales;
- Fungir como un foro para el intercambio de información, apreciaciones o propuestas respecto al cumplimiento de los objetivos previstos en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable, la Política de Datos Personales, el Documento de Seguridad, y cualquier instrumento relativo y derivado de dichos ordenamientos;
- Llevar a cabo reuniones de trabajo, cuando las circunstancias específicas así lo ameriten, conforme a la convocatoria, calendario y dinámica acordados previamente por el Comité, y remitidas por la Secretaría, las cuales tendrán como objeto planear, diseñar, elaborar, instituir, coordinar y supervisar, en tiempo real, las acciones y los procedimientos para garantizar el derecho a la protección de los datos personales en posesión del IFT, de conformidad con las disposiciones previstas en la LGPDPPSO, los



Lineamientos Generales y demás normativa aplicable, la Política de Datos Personales, el Documento de Seguridad, y cualquier instrumento relativo y derivado de dichos ordenamientos, y

- Coadyuvar con las unidades administrativas del Instituto, que así lo requieran, para la elaboración del informe al Comité, indicado en el primer párrafo del numeral Octavo de la Política de Datos Personales, en cuanto a la posible adopción de las medidas que correspondan, con base en los insumos recabados y proporcionados por las áreas.

En relación con lo anterior, teniendo en cuenta que el cumplimiento de los principios y deberes en el tratamiento de los datos personales previstos en la LGPDPPSO, los Lineamientos Generales y en la Política de Protección de Datos Personales del Instituto, es un proceso que requiere de la participación activa y continua de las personas servidoras públicas del Instituto, el Grupo de Trabajo se conforma de la manera siguiente:

Mecanismo	Integración
"Grupo de Trabajo de Protección de Datos Personales en posesión del Instituto Federal de Telecomunicaciones"	<ol style="list-style-type: none"><li>1. Comité de Transparencia;</li><li>2. Unidad de Transparencia, a través de:<ul style="list-style-type: none"><li>- La Dirección de Clasificación y Datos Personales;</li></ul></li><li>3. Unidad de Administración, a través de:<ul style="list-style-type: none"><li>- La Dirección de Control Interno y Administración de Riesgos;</li><li>- La Dirección de Seguridad de la Información;</li><li>- El Área Coordinadora de Archivos;</li></ul></li><li>4. Las personas Subenlaces de Transparencia y Protección de Datos Personales de las Unidades Administrativas del IFT y,</li><li>5. Las personas servidoras públicas involucrados en el tratamiento de los datos personales de que se trate (en caso de ser necesario).</li></ol>

El Grupo de Trabajo funge como un mecanismo permanente de monitoreo no sólo de las medidas de seguridad implementadas en el Instituto, sino de las obligaciones y



deberes establecidos en los ordenamientos en la materia, en sus respectivas Áreas. Lo anterior, con independencia de la participación oportuna de la Unidad de Transparencia del Instituto, como coordinadora de las actividades del Grupo de Trabajo.

De conformidad con la regla NOVENA de las “Reglas del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones”, se prevén 2 reuniones anuales, distribuidas en los meses de mayo, y noviembre.

Al día de hoy, el Grupo de Trabajo se constituye como un elemento fundamental que coadyuva con la Unidad de Transparencia y el propio Comité de Transparencia (en su carácter de autoridad máxima en materia de protección de datos personales, en términos de lo dispuesto por el artículo 83, segundo párrafo, de la LGPDPPSO), para impulsar acciones mejor orientadas hacia la problemática y situación real del derecho a la protección de datos personales en el Instituto.

Control de cambios			
Fecha	Autor	Versión	Referencia del cambio
27 de febrero de 2025 <sup>3</sup>	Comité de Transparencia	2.0	Actualización del Documento

Actualiza	Revisa	Autoriza
<b>Tania Jacqueline Leal Tapla</b> Directora de Clasificación y Datos Personales	<b>Alejandra Martínez Morales</b> Coordinadora de Transparencia, Acceso a la Información y Gobierno Abierto	<b>Alejandra Martínez Morales</b> Coordinadora de Transparencia, Acceso a la Información y Gobierno Abierto, Presidenta del Comité de Transparencia del Instituto Federal de Telecomunicaciones

<sup>3</sup> Aprobada en la Séptima Sesión Ordinaria del Comité de Transparencia celebrada el 27 de febrero de 2025 mediante el Acuerdo número 07/SO/10/25.



Actualiza	Revisa	Autoriza
		<hr/> <p><b>Adriana de León Paz</b></p> <p>Directora General de Finanzas Presupuesto y Contabilidad de la Unidad de Administración, Integrante del Comité de Transparencia del Instituto Federal de Telecomunicaciones</p> <hr/> <p><b>José Luis Mancilla Rosales</b></p> <p>Director General de Instrumentación de la Unidad de Asuntos Jurídicos, Integrante del Comité de Transparencia del Instituto Federal de Telecomunicaciones</p>

