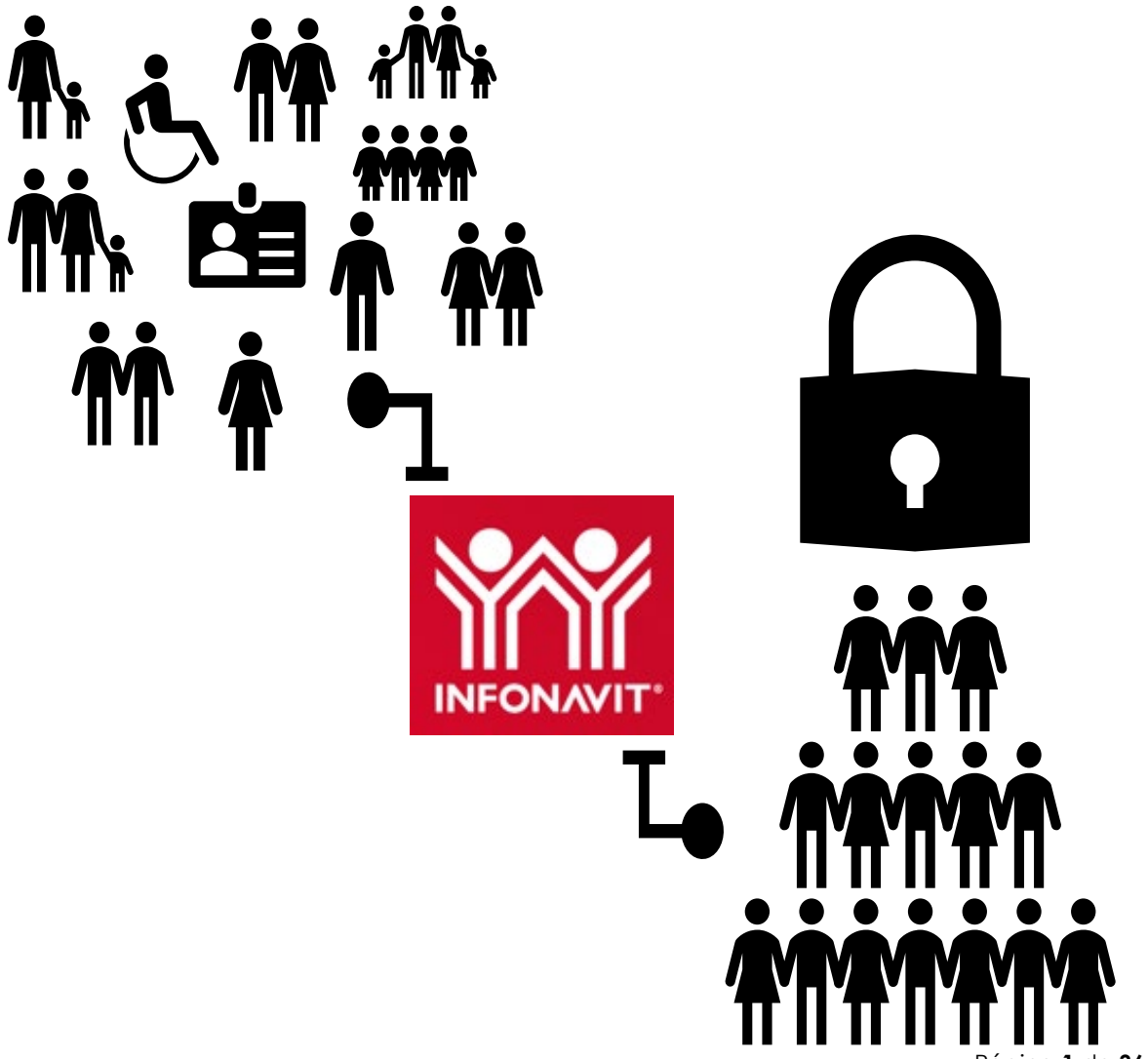
Documento de Seguridad del INFONAVIT

Protección de datos personales

Septiembre 2024



Control de versiones

Versión	Descripción	Fecha de creación/actualización
1	Creación del documento	10 de noviembre de 2021
2	Actualización	09 de octubre de 2024

Contenido

Antecedentes

El Instituto del Fondo Nacional de la Vivienda para los Trabajadores (Infonavit) como responsable, tiene el deber de proteger los datos personales en su posesión e implementar mecanismos que acrediten el cumplimiento de los principios, deberes, derechos y demás obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General de Datos), así como los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) de acuerdo con sus atribuciones.

Para ello el Infonavit, a través de las diversas unidades administrativas y las direcciones sectoriales empresarial y de los trabajadores que tratan datos personales en sus actividades cotidianas, ha establecido y mantenido a lo largo del tiempo medidas de seguridad físicas, técnicas y administrativas que permiten protegerlos de cualquier daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, atendiendo al riesgo inherente del dato personal.

En 2021, se elaboró un primer Documento de Seguridad el cual consideró los primeros esfuerzos institucionales para el cumplimiento de las obligaciones previstas en la Ley General de Datos y su normativa derivada, respecto de los deberes de seguridad y confidencialidad; así como la identificación, reconocimiento y agrupación de las acciones emprendidas al respecto, en un contexto de conformación inicial del sistema de gestión de seguridad en datos personales conforme lo previsto en la Ley General de Datos.

Introducción

El Infonavit comprometido con el camino de la mejora continua en protección de datos personales, en 2022 continuó realizando actividades para fortalecer la seguridad y confidencialidad de los datos personales de la derechohabiencia, por ejemplo, implementación de los Inventarios de datos personales por cada unidad administrativa; cursos de sensibilización sobre protección de datos personales; implementación de análisis normativos por tratamiento realizado; aprobación de la *Política de Tratamiento y Gestión de Datos Personales*, actualización de las *Políticas Institucionales para Seguridad de la Información;* desarrolló los *Lineamientos de Transparencia, Acceso a la Información y Protección de Datos Personales del Instituto del Fondo Nacional de la Vivienda para los Trabajadores*, el cual fue publicado en el Diario Oficial de la Federación el 03 de junio de 2024; implementó *nuevas tecnologías y sistemas*, en el trámite de créditos de Línea IV y los procesos operativos vinculados a éstos, así mismo, la designación de la Dirección General al *Oficial en Jefe de Seguridad de la Información* del Instituto el 10 de noviembre de 2017 el cual se encontraba adscrito a la Contraloría General; sin embargo, a partir de agosto de 2022 por decisión de la Dirección General fue trasladado a la Coordinación General de Riesgos; por último, el 9 de junio de 2021 se nombró al *Oficial de Protección de Datos Personales*.

Asimismo, se debe de considerar la dinámica operativa que ha tenido el Instituto, en la revisión y reorganización de los procesos institucionales; así como, la apertura de *Espacio Cultural Infonavit* el cual se compone del Museo Nacional de la Vivienda (Munavi) y del Centro de Información Documental-Biblioteca del Infonavit los cuales se articulan a través de un programa de actividades culturales y académicas diseñado por el área de Fomento Cultural y Académico, generando con ello un espacio de apertura institucional.

Considerando todo lo anterior y con fundamento en el artículo 36, fracción II de la Ley General de Datos, el Infonavit presenta la actualización de su Documento de Seguridad, el cual permite observar el avance de los esfuerzos colaborativos de los recursos humanos de las diferentes unidades administrativas, el monitoreo y revisión del sistema de gestión que opera en el Instituto, así como el fortalecimiento de la cultura de protección de datos personales y seguridad de la información a su interior, con el propósito de lograr el cumplimiento de las obligaciones institucionales previstas en la Ley General de Datos y su normativa derivada en beneficio de las personas titulares, el personal del Instituto y el propio Infonavit.

Marco normativo

Para los efectos del presente documento, se señala el siguiente sustento jurídico de manera enunciativa, mas no limitativa:

- Constitución Política de los Estados Unidos Mexicanos, artículo16, segundo párrafo
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Estatuto Orgánico del Infonavit
- Lineamientos de Transparencia, Acceso a la Información y Protección de Datos Personales del Infonavit
- Reglas de Operación de los Órganos Colegiados
- Lineamientos de Operación de las Delegaciones
- Políticas Institucionales para Seguridad de la Información
- Política de Tratamiento y Gestión de Datos Personales
- Código de ética del Infonavit
- Norma ISO 27005 "Gestión de riesgos de la seguridad de la información"
- Metodología de análisis de riesgos BAA[1] del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

[1] **B**eneficio para el atacante, la **A**ccesibilidad para el atacante y la **A**nonimidad del atacante

I. Metodología de gestión de riesgos de datos personales

Los artículos 33, fracción IV y 35, fracción III de la Ley General de Datos establecen dentro de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, respecto a ello, se dispone lo siguiente:

> *"Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> *I. […]*
>
> *IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
>
> *[…]"*

> Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:
> […]
> III. El análisis de riesgos;
> […]

Por su parte, el artículo 60, de los Lineamientos Generales establece lo siguiente:

> ***"Análisis de riesgos***
> *Artículo 60. Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*
>
> ***I.*** *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
> ***II.*** *El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
> ***III.*** *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
> ***IV.*** *Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
> ***V.*** *Los factores previstos en el artículo 32 de la Ley General."*

Conforme lo dispuesto por los artículos antes citados, el Infonavit, a través de la Coordinación General de Riesgos (CGR), en mayo de 2024 llevó a cabo un segundo ejercicio sobre análisis de riesgos enfocado al cumplimiento de las obligaciones establecidas en la Ley General de Datos lo que derivó en una nueva metodología de riesgos para datos personales y la aplicación de ésta por primera vez, al tratamiento de datos personales, aplicable a la Plataforma Biométrica Institucional (PBI).

Lo anterior en seguimiento al dictamen de la Evaluación de Impacto en la Protección de Datos Personales (EI) emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) derivado de la implementación de la PBI, misma que fue instruida en marzo de 2023 por Dirección General para su implementación.

En ese contexto, la CGR identificó la necesidad de modificar la metodología de análisis de riesgos para datos personales, alineándola con los requerimientos del INAI para el análisis de riesgos y de brecha.

Conforme lo anterior, el análisis de riesgos y brechas se basa en la Metodología de Gestión de Riesgos de Privacidad, la cual se encuentra apegada a estándares internacionales como la norma ISO 27005 "Gestión de riesgos de la Seguridad de la Información" y la metodología de análisis de riesgo BAA del INAI.

El objetivo de dicha metodología es definir el proceso de gestión de riesgos de datos personales para el Infonavit, que permita orientar sobre la identificación, análisis, evaluación, tratamiento y revisión de estos, proporcionando un marco conceptual y metodológico que facilite su gestión. De esta forma el Instituto asegura que los resultados de la apreciación de los riesgos de datos personales identificados sean consistentes, válidos y comparables.

El alcance de esta metodología fue exclusivamente para el Infonavit y aplica para gestionar los riesgos hasta su fase de plan de tratamiento de riesgos, asociados a los datos personales en los activos de información relacionados a los datos personales.

La metodología está compuesta por 7 fases, las cuales se ilustran en la siguiente figura:

Conforme lo anterior a continuación, se muestra de manera simplificada el contenido de cada etapa:

Fase 1: Establecimiento del contexto

En esta etapa se establece un contexto para la evaluación de riesgos el cual es proporcionado por políticas, procedimientos, criterios para seleccionar los riesgos a considerar, alcance de las evaluaciones, profundidad de los análisis, grado de formalidad y requisitos que faciliten determinaciones de riesgos coherentes y repetibles en todo el Instituto.

Las escalas que se utilizarán en esta metodología, para determinar la probabilidad y el impacto de los riesgos de datos personales de la información, son las siguientes:

Escala para determinar el nivel de probabilidad:

La escala que se utilizará para determinar la probabilidad de los riesgos de privacidad de la información es la siguiente:

Nivel de probabilidad	Descripción[2]	Frecuencia
1. REMOTA	Posibilidad muy baja de ocurrencia, es decir, presencia de forma fortuita, menor o igual al 5% de probabilidad.	0 veces en el último año.
2. POCO PROBABLE	Posibilidad baja de ocurrencia, es decir, presencia de forma ocasional, entre 6% y 20% de probabilidad.	De 1 a 2 veces al año.
3. PROBABLE	Posibilidad alta de ocurrencia, es decir, presencia con bastante frecuencia, entre 21% y 50% de probabilidad.	De 3 a 6 veces al año.
4. ALTAMENTE PROBABLE	Posibilidad muy elevada, es decir, presencia con mucha frecuencia, entre 51% y 80% de probabilidad.	De 7 a 9 veces al año.
5. ESPERADA	Posibilidad máxima, es decir, donde es casi un hecho que sucederá con más de 80% de probabilidad.	10 veces o más al año.

Escala para determinar el impacto:

El impacto se mide según el grado en que las consecuencias o efectos pueden afectar la consecución de los objetivos del Instituto, en este caso los objetivos en cuanto a la protección de datos personales.

La escala que se utilizará en esta metodología para determinar el impacto de los riesgos de datos personales es una escala semicuantitativa y se enfoca en las afectaciones o consecuencias que el evento pudiera ocasionar a los datos

[2] Fuente: Anexo 6g - Evaluación de los riesgos para el PRT, del Manual de Administración Integral de Riesgos (MAIR)

personales relacionados con el tratamiento de datos personales en el Instituto, considerando los siguientes niveles:

Nivel	Descripción
Menor	Consecuencias prácticamente despreciables para el Instituto y sin impacto a las personas derechohabientes, acreditados o empleados.
Bajo	Consecuencias menores para el Instituto y el impacto no relevante a las personas derechohabientes, acreditadas o personal.
Moderado	Consecuencias con daño medio para el Instituto y a las personas derechohabientes, acreditadas o personal.
Alto	Daño alto para el Instituto y a para las personas derechohabientes, acreditadas o personal.
Crítico	Daño severo para el Instituto y a las personas derechohabientes, acreditadas o personal.

Matriz para determinar el nivel de riesgo:

Para determinar el nivel de riesgo, se establece un método cualitativo, combinando los valores de probabilidad e impacto, teniendo en cuenta la siguiente matriz:

PROBABILIDAD	IMPACTO				
	Menor	Bajo	Moderado	Alto	Crítico
Remota	Bajo	Bajo	Moderado	Alto	Alto
Poco Probable	Bajo	Bajo	Moderado	Alto	Crítico
Probable	Bajo	Moderado	Moderado	Alto	Crítico
Altamente probable	Moderado	Moderado	Alto	Crítico	Crítico
Esperada	Moderado	Alto	Alto	Crítico	Crítico

Apetito de riesgo:

Con base en los niveles de riesgo establecidos en la tabla anterior y el apetito al riesgo del Infonavit se describen los criterios de aceptación de riesgos:

Nivel de riesgo	Descripción
Críticos y Altos	Son riesgos considerados inaceptables para el Instituto, por lo que supera el nivel de apetito de riesgo. Para cualquier riesgo que se

Nivel de riesgo	Descripción
	encuentre en estos niveles, se debe realizar un plan de tratamiento inmediato a corto plazo y con alta prioridad.
Moderados	Son riesgos considerados como elevados para el Instituto y dependiendo del riesgo, Infonavit decide si supera el nivel de apetito de riesgo aceptable, por ejemplo: • Riesgos con impacto moderado y probables podrían requerir algún tratamiento. • Riesgos con impacto bajo, pero altamente probables podrían requerir algún tratamiento. En caso de que Infonavit decida la aceptación del riesgo, se deberá realizar mediante una aprobación formal (mediante la firma de aceptación de dueño del riesgo y la Alta Dirección). En caso de que no se decida aceptar el nivel de riesgo, se debe realizar un plan de tratamiento a mediano o largo plazo.
Bajos	Son riesgos aceptables, es decir, están por debajo del apetito de riesgo aceptado por Infonavit, por lo que normalmente no se realiza ninguna acción especial requerida, excepto el mantenimiento de los controles actuales. Para este nivel de riesgo, se podría realizar un plan de tratamiento a largo plazo si así lo consideran los responsables del riesgo.

Fase 2: Identificación de activos de información dentro del alcance del ejercicio

Se procederá a identificar los procesos dentro del alcance del ejercicio y los diferentes tipos de activos de información relacionados, que para el caso de esta metodología se utilizarán los siguientes:

- Instalaciones.
- Equipo / Hardware.
- Aplicación / Software.
- Red de telecomunicaciones.
- Información personal.

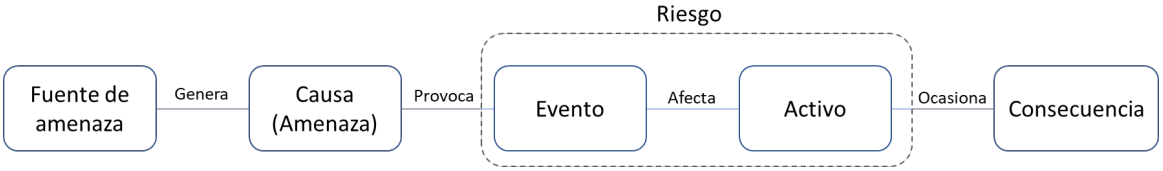
Como parte del levantamiento de riesgos, la metodología considera las siguientes actividades para la generación del inventario de activos de información:

- Identificar el flujo de los datos personales que utilizan los procesos en el alcance, independientemente del formato, proceso y medio.
- En caso de que el activo procese o almacene datos personales, identificar los tipos de datos involucrados y el nivel en el que se encuentran.
- En caso de que el proceso analizado utilice datos personales, se analizará el ciclo de vida de los datos personales.

Fase 3: Identificación de eventos de riesgos de datos personales

Se determinan aquellos eventos de riesgo que tendrán un impacto sobre los datos personales, y objetivos del Instituto o de sus procesos; definiendo en primera instancia sus causas con base en el contexto interno y externo y posteriormente, los posibles efectos (consecuencias) que se ocasionarían con la materialización del riesgo.

La siguiente figura muestra los componentes fundamentales del modelo de riesgos, componentes y sus relaciones:



En consecuencia, se debe realizar un análisis de riesgos de datos personales el cual implica la consideración del activo afectado, el tipo de evento, las causas, sus consecuencias y la probabilidad de ocurrencia de éstas, teniendo en cuenta la presencia (o no) de los controles existentes.

Fase 4: Análisis de riesgos de datos personales

El análisis de riesgos de datos personales implica la consideración del activo afectado, el tipo de evento, las causas, sus consecuencias y la probabilidad de ocurrencia de éstas, teniendo en cuenta la presencia (o no) de los controles existentes.

Fase 5: Valoración de riesgos de datos personales

La valoración del riesgo implica, comparar el nivel de riesgo encontrado durante el proceso de análisis con los criterios establecidos y el apetito de riesgos del Infonavit. Con base en los resultados del análisis de riesgos, la finalidad de la valoración es ayudar a la toma de decisiones determinando los riesgos a tratar y la prioridad para implementar el tratamiento.

De acuerdo con el resultado del nivel de riesgo residual, se debe determinar la prioridad de este, el cual puede ser, crítico y alto, moderado y bajo.

Fase 6: Tratamiento del riesgo

El tratamiento del riesgo implica la selección e implementación de una o varias opciones para modificar los riesgos. Una vez realizada la implementación, los tratamientos proporcionan o modifican los controles.

Las opciones que pueden ser seleccionadas por cada riesgo, son "evitar el riesgo", "mitigar el riesgo", "compartir el riesgo" o "aceptar el riesgo".

Fase 7: Comunicación y seguimiento

La CGR comunicará los resultados de la evaluación de riesgos a los responsables de la toma de decisiones del Instituto para definir Planes de Tratamiento de Riesgos.

En caso de existir, el Comité de Riesgos o el Comité de Transparencia deberá aprobar las acciones propuestas por los dueños de los procesos y controles en caso de que apliquen, verificando que estas acciones realmente minimicen los impactos de los riesgos críticos y altos.

La Unidad de Transparencia será la responsable de realizar el seguimiento y dar su visto bueno a los planes de tratamiento aprobados. Este seguimiento se realizará periódicamente, a través de un informe el cual se debe presentar al Comité de Riesgos o el Comité de Transparencia para su conocimiento.

II. Inventario de datos personales

El Infonavit gestiona su actuar cotidiano mediante un gobierno de procesos, la identificación de ello constituye la base a partir de la cual, se cuenta con un catálogo institucional de procesos que sirven de guía para la identificación y documentación normativa necesaria, así como para la administración de riesgos, el seguimiento, el control a nivel institucional y la mejora continua.

El modelo de gobierno de procesos del Instituto permite definir, modelar, documentar, medir y mejorar los procesos, así como homologar las capacidades en administración por procesos, fortalecimiento de las competencias y de los roles involucrados en la arquitectura de procesos.

El catálogo institucional de procesos busca determinar todos aquellos por medio de los cuales cada unidad administrativa da cumplimiento a sus atribuciones. Cada proceso incluye el marco normativo específico y los límites de los responsables de su ejecución.

Los procesos institucionales también cuentan con un proceso de actualización y mejora, por ello, el número de procesos reportados pueden variar entre una actualización y otra.

Al día de la presentación y aprobación del presente Documento de Seguridad, el Infonavit cuenta con un catálogo de procesos que tratan datos personales compuesto por **147 procesos**, de conformidad con lo reportado por las propias unidades administrativas, y las direcciones sectoriales empresarial y de los trabajadores a la Unidad de Transparencia.

Ahora bien, una vez identificados los procesos que tratan datos personales, los artículos 33, fracción III y 35, fracción I de la Ley General de Datos establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, contar con el inventario de datos personales y de los sistemas de tratamiento.

Para cumplir con lo anterior, el Infonavit cuenta con inventarios particulares organizados por unidades administrativas y direcciones sectoriales empresarial y de los trabajadores, que conforman el Inventario Institucional de Datos Personales (IIDP), el cual contempla los requerimientos previstos en los artículos 58 y 59 de los Lineamientos Generales.

En ese sentido, el IIDP cuenta con la información siguiente (la cual considera el ciclo de vida de los datos personales conforme lo previsto en el artículo 59 de los Lineamientos Generales):

1. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.
2. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.
3. Las finalidades de cada proceso de datos personales.
4. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.
5. Organización de la manera en que las y los empleados del Instituto tienen acceso a los sistemas de tratamiento.
6. Nombre completo o denominación o razón social de los encargados y el instrumento jurídico que formaliza la prestación de los servicios que brinda al Infonavit.
7. Terceros receptores de las transferencias que se efectúan, así como las finalidades que justifican éstas.
8. La obtención de los datos personales.
9. El almacenamiento de los datos personales.
10. 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.
11. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.
12. El bloqueo de los datos personales, en su caso, y
13. La cancelación, supresión o destrucción de los datos personales.

El IIDP que a continuación se describe, corresponde a los procesos sustantivos que tratan datos personales a cargo de la Contraloría General (CG), la Secretaría General y Jurídica (SGyJ), la Subdirección General de Planeación Financiera y Fiscalización (SGPFF), la Subdirección General de Crédito (SGC), la Subdirección General de Gestión de Cartera (SGGC), la Subdirección General de Operaciones (SGO), la Subdirección General de Administración y Recursos Humanos (SGARH), la Subdirección General de Comunicación (SGCom), la Subdirección General de Tecnologías de Información (SGTI) y la Coordinación General de Riesgos (CGR).

Es importante mencionar que para 2024, se sumó a este esfuerzo las direcciones sectoriales empresarial y de los trabajadores. De tal manera que la suma de los inventarios de datos personales particulares proporcionados por las unidades administrativas, y Direcciones Sectoriales conforman el IIDP.

En ese sentido, el IIDP se conforma de **147 procesos** que tratan datos personales, organizados de acuerdo con el artículo 9 referente a las Direcciones Sectoriales, y con la estructura prevista en el artículo 11, ambos del Estatuto Orgánico del Infonavit.

El Infonavit actualmente, con ayuda de la Subdirección General de Tecnologías de Información y la Unidad de Transparencia, está rediseñando la herramienta electrónica interna que alojará el IIDP[3], se espera que, para diciembre de 2024, ya se cuente con el aplicativo que facilite su registro y actualización.

A continuación, se enlistan los procesos de las unidades administrativas que tratan datos personales, vigentes al 30 de junio de 2024:

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
Contraloría General	11	GE.01.09	Gestión de la mejora continua del Sistema de Control Interno
		GO.04.02	Recepción de denuncias
		GO.04.04	Atención de quejas
		GO.04.11	Investigación de responsabilidades administrativas
		GO.04.13	Ejecución de auditorías del Sistema Integral de Gestión de Calidad
		GO.04.15	Gestión de la presentación de declaraciones de situación patrimonial
		GO.04.16	Atención a Denuncias Relacionadas con Posibles Fraudes o Conductas Indeseables
		GO.04.18	Gestión de Medidas y Controles de Cumplimiento Regulatorio
		GO.04.19	Atención de Recursos de Reconsideración

[3] El antecedente en 2021 fue la plataforma electrónica interna denominada Plataforma Integral de Control Interno (PICI).

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
		GO.04.20	Gestión de Recepción de Regalos, Cortesías u Obsequios
		GO.04.21	Gestión de Bases de Datos para Análisis de Posibles Fraudes o Conductas Indeseables
Secretaría General y Jurídica	30	AC.04.10	Entrega de vivienda con poder notarial
		AD.05.02	Aplicación de autoseguro por defunción, invalidez o incapacidad
		AC.06.02	Reactivación de Créditos Cerrados por Recuperación Judicial
		AC.06.03	Registro Avance Procesal
		AC.06.04	Borrón y cuenta nueva cobranza domiciliaria recuperación especializada
		AC.06.06	Adjudicación de vivienda recuperada por procesos judicial
		GO.02.01	Atención de denuncias
		GO.02.04	Regularización de escrituras 1972-2007
		GO.02.05	Mediación de controversias
		GO.02.06	Atención y previsión por contingencias laborales
		GO.02.10	Gestión de juicios
		GO.02.16	Otorgamiento y Revocación de Poderes
		GO.02.17	Convenios interinstitucionales
		GO.02.18	Atención a Solicitudes en Ejercicio de Derechos de ARCO
		GO.02.25	Administración de garantías
		GO.02.26	Seguimiento de las Relaciones Institucionales con Autoridades y Representantes Populares
		PR. SGAC.004	Liquidación del crédito al 75% del valor avalúo
		PR. SGAC.054	Gestión y seguimiento de cartera para productos INFONAVIT Total
		PR. SGAC.059	Devolución de documentos en solución de recuperación especializada
		PR. SGAC.060	Solución por convenio en ejecución de sentencia
		PR. SGAC.061	Solución de cartera vencida por convenio judicial o privado
		PR. SGAC.065	Seguimiento de solución a tu medida judicial
		PR. SGAC.085	Proceso de marca y liquidación de créditos COFINAVIT
		PR. SGAC.104	Borrón y cuenta nueva cobranza domiciliaria recuperación especializada
		PRO.SGJ.008	Gestión de requerimientos de la CNDH
		PR. SGARH.012	Formalización de contratos
		GO.02.21	Control y Seguimiento de Resoluciones de Órganos Colegiados
		GO.02.23	Elaboración del Acta de la Asamblea General
		GO.02.27	Elaboración de Actas de Órganos Colegiados
		GO.07.02	Gestión de las sesiones de Órganos Colegiados
Subdirección General de Planeación	11	AD.03.09	Atención solicitudes Registro y o corrección datos identificación trabajadores

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
Financiera y Fiscalización		PR. CGRF.008	Separación cuentas, marcas, desmarcas y saldos
		PR. CGRF.052	Unificación de cuentas NSS.IMSS. INFONAVIT
		SSV.03.03	Devolución del Fondo de Vivienda
		SV.01.01	Dispersión de Recursos de Vivienda
		SV.01.02	Individualización aportaciones extraordinarias a Subcuenta de Vivienda
		SV.01.03	Aclaratorio de aportaciones y amortizaciones en favor de trabajadores
		SV.01.04	Individualización de la recaudación patronal en SACI-SAFRE
		SV.03.02	Portabilidad del SSV INFONAVIT-FOVISSSTE
		SV.03.04	Administración de Transferencia del SSV
		SV.03.05	Restitución al saldo de la Subcuenta de Vivienda de TA y 43 bis
Subdirección General de Crédito	31	AC.02.01	Operación Canje del Monto de Crédito para Ecotecnologías
		AC.02.03	Otorgamiento de crédito Alternativa Financiamiento Mejora Directa INFONAVIT
		AC.02.04	Inscripción del Crédito Construyo Infonavit
		AC.02.05	Formalización del Crédito ConstruYO Infonavit
		AC.02.08	Precalificación, Perfilamiento y Asesoría del Crédito Infonavit de las Alternativas de Financiamiento
		AC.02.09	Titulación Notarial del Crédito Infonavit de las Alternativas de Financiamiento
		AC.02.10	Inscripción del Crédito Infonavit de las alternativas de financiamiento
		AC.02.18	Criterios de elegibilidad Mejora Directa Infonavit
		AC.02.21.008	Inscripción del Crédito Mejora Directa Infonavit en el sistema OCI
		AC.02.21.009	Formalización del Crédito Mejora Directa Infonavit en el sistema OCI
		AC.02.23	Otorgamiento de crédito para las alternativas de financiamiento Mejoravit Repara y Mejoravit Renueva
		AC.02.24	Operación Equipa tu casa
		AC.02.36	Otorgamiento de Crédito de Emergencia para Reparación y Mejora de Vivienda
		AC.03(2).06	Monitoreo a la operación del Aliado Estratégico que participa en Programas de Mejoramiento
		AC.03.10	Atención a Solicitudes de Servicio en la Originación de Crédito
		AC.03.17	Verificación del Programa Piloto Mejora Directa Infonavit
		AC.03.19	Administración del formato SIC
		AC.03.32	Monitoreo y Aclaración de Pagos a Favor del Vendedor Derivados de la Originación de Crédito
		AC.07.09	Administración del Aliado Estratégico Asesor Virtual de Programas de Mejoramiento

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
		AC.07.10	Administración del Aliado Estratégico Especializado en Promotoría de Programas de Mejoramiento
		AC.07.13	Administración del Aliado Estratégico Guarda Valores de Programas de Mejoramiento
		AC.07.20	Incorporación de Notarios
		AC.07.28	Administración de los Servicios de Notarios
		AC.07.41	Administración del Aliado Estratégico Validador de Destino de Programas de Mejoramiento
		PR.SGC.014	Resolución de Créditos Asignados Registrados en la BDA No Formalizados
		PR.SGC.017	Validación de la Identidad del Derechohabiente en la Inscripción de Crédito no Concluida
		PR.SGC.072	Canje del vale para la instalación del paquete Programa Hogar a tu Medida
		PR.SGC.076	Subproceso Atención de Incidentes en la Originación de Crédito
		PR.SGC.102	Verificación obra crédito ConstruYO
		PRO-SGC-018	Monitoreo de las Operaciones de Crédito de las Alternativas de Financiamiento
		RO.AC.02.17-025	Regla de Operación Equipa tu casa.
Subdirección General de Gestión de Cartera	22	AC.04.01	Emisión y distribución de los estados de Cuenta al acreditados
		AC.04.08	Asignación de Cuentas del Portafolio Hipotecario para la Cobranza Social
		AC.04.12	Generación de Constancias de Intereses de Créditos Hipotecarios
		AC.04.14	Generación de Reporte de Acreditados para las Sociedades de Información Crediticia Publicado
		AC.04.15	Ejecución de las Actividades Previas del Proceso Batch de Cartera y Aplicación de Pagos
		AC.04.16	Administración de Información de Créditos 43bis (Apoyo INFONAVIT y COFINAVIT)
		AC.04.22	Registro del Alta de Créditos en el Sistema ALS
		AC.05.01	Operación del Servicio de Mediación
		AC.05.02	Gestión de Estudio de Valoración Socioeconómica
		AC.05.03	Gestión de Apoyos de Reestructuras a Personas Acreditadas
		AC.05.05	Gestión de SSV para la aplicación de Garantías en el sistema ALS
		AC.05.06	Borrón y Cuenta Nueva por Aplicación Automática
		AC.06.07	Gestión de Soluciones para la Cobranza Social a través de los Agentes de Cobranza Extrajudicial
		AD.05.03	Devolución de Pagos en Exceso

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
		AD.05.06	Consulta de Información para pagos REA en Entidades Receptoras
		AD.05.07	Aplicación del Seguro de Daños para la Atención de las y los acreditados
		AD.05.08	Vinculación de NSS con Número de Crédito
		AD.05.10	Gestión de Apoyos por Paro Técnico y/o Disminución de Jornadas de Trabajo
		AD.05.11	Atención y Seguimiento a Créditos por Solicitud de grupos sociales y Cuentas Especiales
		AD.05.15	Devolución de Pagos en Exceso
		VR.01.01	ReEstrena con Infonavit
		VR.01.02	Renovación a tu medida Infonavit
Subdirección General de Operaciones	9	AD.02.03	Generación de conocimiento para el Soporte y Operación del Servicio
		AD.03.01	Atención al usuario
		AD.03.06	Gestión del Soporte del Centro de Contacto y Canales Digitales de Atención
		AD.02.01	Gestión del Conocimiento de Productos o Servicios
		AD.02.04	Gestión de los indicadores Operativos y del Servicio al Usuario (a)
		AD.02.05	Gestión del Monitoreo del Servicio
		AD.03.03	Administración de Datos de Contacto
		AD.03.07	Operación de Servicios de Soporte
		AD.03.08	Entrega de escrituras
Subdirección General de Administración y Recursos Humanos	25	CH.01.04	Contratación personal honorarios
		CH.03.02	Cálculo de Nómina de Activos
		CH.03.03	Cálculo de Nómina de Jubilados
		CH.03.04	Cálculo de Cuotas Obrero - Patronales
		CH.03.05	Gestión de Créditos Infonacot
		CH.03.06	Gestión de Vales de Despensa y Alimentos
		CH.03.07	Cálculo de Finiquitos y Liquidaciones
		CH.03.12	Gestión pago beneficios
		CH.03.20	Gestión del seguro de autos de los trabajadores
		CH.03.21	Administración de movimientos de personal, posiciones y unidades organizativas
		RM.01.02	Proceso de contratos y pedidos
		RM.01.04	Gestión de excepciones a la licitación abierta y compras menores
		RM.01.05	Administración de Registros de Proveedores
		RM.01.07	Investigación de mercado
		RM.01.08	Formalización de contratos
		RM.01.09	Licitación abierta
		RM.01.10	Integración de expedientes del proceso de adquisiciones de bienes y servicios
		RM.01.11	Gestión de Informes de Transparencia fracciones XXVIII y XXXII del artículo 70 de la LGTAIP
		RM.02.02	Administración del Archivo de Trámite
		RM.02.03	Administración de Archivo de Concentración
		RM.02.04	Administración de Archivo Histórico

Catálogo de Procesos que Tratan Datos Personales			
Unidad administrativa/Órgano Colegiado /Sector	**Número de inventarios**	**Clave del proceso**	**Nombre del proceso**
		RM.02.06	Gestión de Baja Documental
		RM.02.07	Gestión de Préstamo de Expedientes
		RM.02.08	Administración de la Guarda y Custodia de los expedientes de crédito en el ANEC
		RM.03.03	Levantamiento de inventario de activo de fijo
Subdirección General de Comunicación	2	GO.09.02	Investigación de Comunicación
		GO.10.11	Infonavit te escucha
Subdirección General de Tecnologías de Información	1	PRO-SGTI-024	Desarrollar soluciones tecnológicas
Coordinación General de Riesgos	5	GO.02.01	Atención a denuncias
		GO.02.06	Atención y Previsión por Contingencias Legales
		GO.03.02	Monitoreo de Riesgos Clave
		GO.06.02	Análisis de Impacto al Negocio
		SV.03.04	Administración de Transferencias del SSV
Total	**147**		

Es importante precisar que, durante la identificación de los tratamientos de datos personales, las unidades administrativas, y las direcciones sectoriales empresarial y de los trabajadores identificaron actividades que, si bien no son un proceso de manera formal, sí son actividades que implican el tratamiento de datos personales. En ese sentido, dichas actividades también se suman al inventario a fin de que se protejan y se encuentren alineados a los principios, deberes y demás obligaciones previstas en la Ley General de Datos y su normativa:

Actividades (vigentes al 30 de junio de 2024)		
Unidad administrativa/Sector	**Número de inventarios**	**Nombre de la actividad**
Dirección General	2	Atención ciudadana
		Gestión de asuntos de Dirección General
Contraloría General	1	Reglas de contacto con externos
Secretaría General y Jurídica	15	Capacitación por la Unidad de Transparencia
		Procesos de investigación y verificación a cargo de la Unidad de Transparencia - INAI
		Aplicativo APRE
		Asuntos legislativos
		CNDH
		Denuncia
		Dirección Sectorial Empresarial
		Inconformidades
		Peticiones DG- Presidencia
		Poderes
		Quejas CRM
		Quejas responsabilidad
		Transparencia
		SAM requerimientos ministeriales

		SICJ GAP
Subdirección General de Crédito	4	Dictamen Anteproyecto Suelo + Construcción
		Revisiones Proyecto e Instrucción Ministraciones- Créditerreno Mi hogar
		Repositorio Avalúos
		Revisión Avalúos Mercado Abierto Individual
Subdirección General de Administración y Recursos Humanos	1	Control de accesos institucionales
Coordinación General de Riesgos	10	Cierre de Cifras Mensuales
		Avalúos
		Identificación de género
		Rompimiento de límites
		Modelos de originación
		Imor por industria
		Puntaje obtenido en los modelos de originación
		Ajuste de Modelos de Originación
		Atención al requerimiento de Transparencia en materia de Adquisiciones
		Estrategia Institucional de Seguridad de la Información – Verificación de las PISI
Dirección Sectorial Empresarial	1	Directorio de Órganos Colegiados
Dirección Sectorial Trabajadores	2	Atención a centrales sindicales
		Programa de asesor sindical certificado
Total	**36**	

Los procesos y actividades enlistados están en revisión por la Unidad de Transparencia, a través de la Oficial de Protección de Datos Personales, a fin de identificar áreas de oportunidad en la descripción de sus componentes o en obligaciones en la materia a cargo del área competente.

1. Titulares y datos personales tratados

El Infonavit recaba distintos datos personales dependiendo del tipo de persona de que se trate y de las finalidades de su tratamiento, en ese sentido nuestros titulares tienen las siguientes categorías de personas: acreditadas, derechohabientes, patrones, jubiladas, personal del propio Instituto, miembros de órganos colegiados, proveedores y público en general.

Es necesario precisar que, respecto a los datos personales de las y los proveedores, el Instituto ha adoptado como una buena práctica, el identificar los datos personales que corresponden a proveedores personas físicas y en su caso a los datos personales del representante legal de la persona jurídica, con la que el Instituto tiene relaciones jurídicas, comerciales o de servicios[4], a fin de procurar su seguridad y cumplir con otras obligaciones legales.

[4] Independientemente de que los datos personales tengan la calidad de públicos o privados.

A continuación, se muestra las categorías de personas titulares y los datos personales que se tratan, los cuales pueden modificarse conforme a las necesidades institucionales y el marco normativo al que está sujeto el Instituto:

Titulares	Tipología de datos personales
La o él acreditado La o él derechohabiente	• Identificación • Contacto • Localización • Laborales • Patrimoniales (en su caso del cónyuge) • Salud • Familiares • Bancarios • Beneficiarios • Procedimientos judiciales
La o él jubilado	• Identificación • Localización • Patrimoniales • Salud • Familiares • Beneficiarios • Bancarios
Miembros de Órganos Colegiados	• Identificación • Contacto • Financieros

Titulares	Tipología de datos personales
La o él patrón	• Identificación • Localización • Contacto • Procedimientos judiciales • Bancarios
La o él proveedor	• Identificación • Contacto • Ubicación • Bancarios • Procedimientos judiciales
La o él empleado del Infonavit	• Identificación • Contacto • Localización • Laborales • Patrimoniales (en su caso del cónyuge) • Académicos • Salud • Familiares • Bancarios • Beneficiarios • Expedientes de responsabilidad administrativa

	• Procedimientos judiciales
Público en general	• Identificación • Contacto • Intereses personales relativos a los temas del Espacio Cultural Infonavit (académicos, artísticos y culturales). • Nivel académico

Al respecto, es conveniente manifestar que el Instituto tiene identificado, incluso, en la descripción documental de cada uno de sus procesos institucionales, los documentos soporte que dan sustento a dichos procesos y en ellos, es posible observar los datos personales que se tratan, a fin de que el personal del Instituto cumpla los procesos con legalidad e integridad.

2. *Obtención de datos personales*

El Infonavit, para cumplir con sus funciones eficientemente, recaba datos personales de manera directa e indirecta de sus diversos titulares, en este contexto de deberá entender por:

- **Obtención de datos personales de forma directa de su titular:** Al acto en el cual el propio titular proporciona los datos personales, personalmente o por algún medio que permite su entrega directa al Infonavit, como podrían ser, medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio.

- **Obtención de datos personales de manera indirecta del titular:** Al acto en el cual el Infonavit obtiene los datos personales del titular, sin que éste lo haya proporcionado de forma personal o directa, por ejemplo, a través de una fuente de acceso público o una transferencia.

Conforme lo anterior, el Infonavit obtiene los datos personales de las siguientes formas:

Modalidad directa	
Presencial	• CESI: Centro de Servicio Infonavit • Oficinas del Instituto que prestan atención personal • Unidad de Transparencia • Ferias y eventos institucionales • Infomóvil • Kioskos de autoservicio
Portal electrónico institucional	• Mi Cuenta Infonavit • Portal empresarial
Teléfono institucional	• Infonatel • Teléfono institucional del personal del Infonavit
Correo electrónico institucional	

Modalidad directa	
Ventanilla única	Servicio Postal Mexicano (SEPOMEX)
Mensajería ordinaria	Valija institucional
Mensajería electrónica SMS	
Aplicaciones electrónicas	Aplicación móvil Infonavit

Modalidad indirecta	
Transferencias	Instituto Mexicano del Seguro Social – IMSS
	Servicio de Administración Tributaria- SAT
	Fiscalía General de la República -FGR
	Comisión Nacional de Derechos Humanos- CNDH
	Comisión Ejecutiva de Atención a Víctimas - CEAV
	Comisión Nacional de Sistemas de Ahorro para el Retiro - CONSAR
	Tribunales del Poder Judicial de la Federación - PJF
	Autoridades jurisdiccionales
	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales- INAI
	Secretaría de la Función Pública- SFP
	Fondo de la Vivienda del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado – FOVISSSTE
	Empresa Operadora de la Base de Datos Nacional del Sistema de Ahorro para el Retiro -PROCESAR
	Institutos de Seguridad Social Estatales
	Notarias a nivel nacional
	Aseguradoras
	Afores
	Patrones
	Sociedades de Información Crediticia

3. *Catálogo de formatos de almacenamiento*

Los datos personales tratados en los procesos y actividades institucionales son almacenados en diferentes tipos de repositorios, tales como archivos físicos (en menor número), archivos electrónicos, sistemas y servidores que se van ajustando conforme a las necesidades operativas y de seguridad del Infonavit.

Tipo de soporte	Formato de almacenamiento	
Físicos	Archiveros en oficinas identificadas por número	Expedientes que contienen las actuaciones impresas de cada uno de los o las titulares, según el proceso y la finalidad.
Electrónicos	Computadoras del personal del Instituto	Expedientes o bases de datos que contienen los datos

Tipo de soporte	Formato de almacenamiento	
		personales de cada uno de los o las titulares, según el proceso y/o actividades, así como sus finalidades.
	Sistemas y aplicaciones electrónicos	Serie de programas informáticos operados por el Instituto para procesar, obtener, administrar, controlar tareas específicas, con la finalidad de cumplir con las especificaciones y necesidades operativas de los procesos y actividades, así como sus finalidades.
	Sistemas electrónicos de encargados	Serie de programas informáticos operados por un encargado para procesar, obtener, manipular, administrar, controlar tareas específicas, con la finalidad de cumplir con las especificaciones y necesidades operativas de los procesos, actividades, así como sus finalidades.
	Servidores institucionales	Equipo informático que forma parte de la red del Instituto.

4. Encargados y medios de formalización

Dentro de las actividades que realiza el Infonavit, algunas se ejecutan mediante la contratación de encargados (proveedores). En el caso particular de actividades que involucran el tratamiento de datos personales, a través de los servicios de éstos, el Infonavit ha previsto controles de seguridad y confidencialidad siguientes:

- ✓ Firma de contratos con cláusula de confidencialidad.
- ✓ Firma de contratos con cláusulas específicas donde se advierten las obligaciones y prohibiciones del encargado.
- ✓ Firma de la *Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales*.
- ✓ Firma de la *Política de Tratamiento y Gestión de Datos Personales.*
- ✓ Firma de las *Políticas Institucionales para Seguridad de la Información*.
- ✓ Clasificación de los encargados, conforme lo siguiente:

- ***Tipo A***: Proveedores que tratan datos personales y que cuentan con una interrelación con los procesos institucionales y que operan usando directamente la infraestructura del Instituto.
- ***Tipo B:*** Proveedores que generan un producto o servicio el cual no está interrelacionado con los procesos institucionales, utilizando infraestructura propia; pueden tener acceso a información operativa, sensible del Instituto.
- ***Tipo C:*** Proveedores que generan un producto o servicio que interrelaciona con los procesos institucionales, utilizando infraestructura propia; por la naturaleza del producto o servicio que desempeñan tienen acceso a información operativa, sensible del Instituto.

Considerando lo anterior, se aplican las cláusulas en materia de protección de datos personales que correspondan, de conformidad con lo previsto en los artículos 59 de la Ley General de Datos y 109 de los Lineamientos Generales.

De manera general, el Infonavit cuenta con los siguientes tipos de encargados:

- Empresas habilitadas para captura remota de inscripción de créditos hipotecarios.
- Empresas verificadoras.
- Empresas de cobranza.
- Unidades de valuación.
- Despachos para notificación fiscal.
- Despachos de ajustadores.

5. Terceros receptores de datos personales

El Instituto lleva a cabo transferencias nacionales de datos personales, de conformidad con los artículos 3, fracción XXXII, 65 y 70 de la Ley General de Datos, por lo que comparte información de sus titulares, principalmente a autoridades, ya sea por mandato legal; para el ejercicio de facultades propias; para la investigación o persecución de delitos; para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente o cuando es necesario para mantener o cumplir una relación jurídica entre el Infonavit y la o el titular.

Nuestros terceros receptores son:

- Instituto Nacional Electoral- INE
- Instituto Mexicano del Seguro Social – IMSS
- Servicio de Administración Tributaria- SAT
- Fiscalía General de la República -FGR

- Comisión Nacional de Derechos Humanos- CNDH
- Comisión Nacional de Sistemas de Ahorro para el Retiro – CONSAR
- Tribunales del Poder Judicial de la Federación - PJF
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales- INAI
- Fondo de la Vivienda del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado – FOVISSSTE
- Institutos de Seguridad Social Estatales
- Sociedades de Información Crediticia.
- Universidad Nacional Autónoma de México -UNAM
- Empresa Operadora de la Base de Datos Nacional del Sistema de Ahorro para el Retiro -PROCESAR
- Fondo Nacional para el Consumo de los Trabajadores – FONACOT
- Catastro
- Notarias a nivel nacional
- Aseguradoras
- Afores
- Patrones

III. Funciones y obligaciones de las personas que hacen tratamientos

El artículo 33, fracción II, así como el 35, fracción II de la Ley General de Datos, establecen dentro de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de los datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales, como a continuación se observa:

> **"Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:
> **[…]**
> **II.** Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
> […]"
>
> **"Artículo 35.** De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:
> **I.** El inventario de datos personales y de los sistemas de tratamiento;
> **II.** Las funciones y obligaciones de las personas que traten datos personales;
> **III.** El análisis de riesgos;
> **IV.** El análisis de brecha;
> **V.** El plan de trabajo;
> **VI.** Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
> **VII.** El programa general de capacitación."

Sobre el particular, el artículo 57 de los Lineamientos Generales señala lo siguiente:

> ***"Funciones y obligaciones***
> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento."*

En este contexto, las funciones y obligaciones del personal del Infonavit que trata datos personales se han identificado en dos niveles:

- A *nivel macro*, en la Ley General de Datos, Lineamientos Generales de Protección de Datos Personales para el Sector Público, Lineamientos de Transparencia, Acceso a la Información y Protección de Datos Personales del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, el Estatuto Orgánico, las Reglas de Operación de los Órganos Colegiados, el Manual General de Organización, los Manuales de organización específicos, así como los Lineamientos de Operación de las Delegaciones y al Código de ética, en los cuales se describen las funciones asignadas al personal,

- A *nivel micro*, se trata a nivel de empleado (a), a través de dos vertientes, la primera se refiere a lo previsto en los inventarios de datos personales que se registraron por cada uno de los procesos institucionales, en los cuales se identifica el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento. La segunda vertiente es a través de las descripciones de puestos del personal y conforme a la Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales.

Asimismo, el Instituto cuenta con la **Política de Tratamiento y Gestión de Datos Personales** (PTGDP) aprobadas en abril de 2022, cuyo objetivo es establecer la política de datos personales, la cual contiene las bases, principios y procedimientos para el tratamiento y gestión de los datos personales en posesión del Infonavit. La PTGDP es de observancia obligatoria para el personal del Instituto y sus Órganos Colegiados, así como para sus proveedores cuyas funciones y actividades impliquen realizar cualquier tratamiento de datos personales.

El compromiso del Infonavit es garantizar el derecho a la protección de los datos personales crucial en sus acciones, operaciones y funciones, al proporcionar sus servicios y productos, salvaguardando en todo momento el cumplimiento de los

ocho principios y dos deberes en materia de datos personales, previstos en los artículos 16, 31 y 42 previstos en la Ley General de Datos, para evitar que las y los titulares sufran consecuencias adversas, así como riesgos o daños a su persona vinculados con tratamiento indebido de sus datos personales.

Al respecto, se destacan las siguientes atribuciones:

El **Comité de Transparencia** debe:

- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales al interior del Infonavit, de conformidad con las disposiciones previstas en la Ley General Datos y en aquellas disposiciones que resulten aplicables en la materia.

La **Unidad de Transparencia**, tendrá las siguientes funciones:

- Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
- Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Igualmente, con colaboración del **Oficial de Protección de Datos Personales,** debe:

- Proponer al Comité de Transparencia las políticas de datos personales para dar cumplimiento a la Ley General de Datos y su normativa derivada.

- Coordinar la elaboración de la Evaluación de Impacto en la Protección de Datos Personales cuando se pretenda poner en operación o modificar sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, de conformidad con la Ley General de Datos, implique el tratamiento intensivo o relevante de datos personales.

- Coordinar, recabar y resguardar el Inventario Institucional de Datos Personales.

Las **unidades administrativas** deben:

- Colaborar en el ámbito de su competencia con el diseño, la implementación y la mejora continua del Sistema de gestión de seguridad de datos personales.

- Colaborar en la actualización del Documento de Seguridad en materia de datos personales.

- Cooperar y facilitar la información que sea necesaria, conforme a sus atribuciones y funciones, para la elaboración del análisis de riesgos a la Coordinación General de Riesgos.

- Informar a su superior jerárquico y notificar a la Contraloría General, a la Unidad de Transparencia, al Oficial de Protección de Datos Personales, y al Oficial en Jefe de Seguridad de la Información sobre cualquier incumplimiento de la Política de Tratamiento y Gestión de Datos Personales (PTGDP) o de las Políticas Institucionales para la Seguridad de la Información (PISI) a efecto de que cada uno de ellos, actúen en consecuencia conforme a sus atribuciones.

- Proporcionar, a la Unidad de Transparencia y al Oficial de Protección de Datos Personales, la documentación que acredite el cumplimiento de los principios, deberes y demás obligaciones en materia de protección de datos personales.

- Cooperar y facilitar la información que sea necesaria, conforme a sus atribuciones y funciones, para atender las investigaciones y/o verificaciones en materia de datos personales en las que se vean involucradas, a la Unidad de Transparencia, el Oficial de Protección de Datos Personales, el Oficial en Jefe de Seguridad de la Información y/o la Contraloría General, según sea el caso.

- Actualizar anualmente el Registro de bases de datos con datos personales, así como el Inventario de datos personales que fundamental y estratégicamente le sirven para cumplir con sus finalidades conforme a sus atribuciones y funciones.

- Contactar a la Contraloría General, el Oficial en Jefe de Seguridad de la Información y el Oficial de Protección de Datos Personales cuando requieran realizar transferencias y/o remisiones de datos personales para

que en conjunto se definan y/o revisen las condiciones para llevarlas a cabo en apego al marco normativo que, a cada una de las áreas y puestos mencionados, les competa.

La **Coordinación General de Riesgos** debe:

- Coordinar la ejecución del análisis de riesgos en materia de datos personales.

La **Contraloría General** debe:

- Dar seguimiento a la atención de hallazgos, planes de mitigación e implantación de controles relacionados a los riesgos a los que se encuentra expuesto el Infonavit.

Por su parte, el Instituto también cuenta con las **Políticas Institucionales para Seguridad de la Información (PISI),** actualizadas en agosto de 2023, las cuales tienen como objetivo proporcionar las directrices para la protección de la información de las personas derechohabientes, acreditados(as), jubilados(as), patrones(as), proveedores(as), personal del Instituto, miembros de Órganos Colegiados y público en general, así como de la información financiera Institucional.

En particular las PISI en la política *14.4 Protección de Datos Personales* establecen las directrices generales sobre la materia.

Por otro lado, el Infonavit cuenta con la descripción y perfil del puesto de cada uno de sus empleados y empleadas, con un nivel estratégico y táctico, el cual incluye el tipo de relaciones internas y externas que debe de cumplir, así como los activos de información de los cuales es dueño y el perfil de seguridad de la información que le corresponde, considerando sus actividades cotidianas y el tipo de información que maneja.

Es importante precisar que el incumplimiento de los principios, deberes y obligaciones establecidos en la PTGDP o en las PISI, respecto de seguridad en donde se afecte a los datos personales, tienen consecuencias.

En el caso de datos personales la PTGDP prevé que el incumplimiento será sancionado de conformidad con lo establecido en la Ley General de Datos, artículos 163, 164 y 165, y conforme los procedimientos previstos por la Contraloría General del Instituto y demás normativa interna, sin perjuicio de las sanciones del orden civil, penal o de cualquier otro tipo que pudieran derivarse de los mismos hechos.

Por su parte, las PISI, prevén el establecimiento de las medidas de control preventivas, de detección y correctivas para definir y documentar los requisitos estatutarios, regulatorios y contractuales para la protección de los datos personales que maneja el Instituto.

Todo el personal del Instituto es responsable de notificar ante el Oficial en Jefe de Seguridad de la Información y a la Contraloría General cualquier omisión o incumplimiento a las PISI, las anteriores notificaciones podrían derivar acciones de control interno o de reforzamiento de controles internos, pero también en procesos de responsabilidades administrativas o de acciones legales por parte del Instituto.

Lo anterior permite tener control de las actividades de las y los empleados vinculadas con el tipo de información y datos personales que trata, atendiendo a sus funciones, ello permite identificar e implementar las medidas de seguridad que correspondan a cada caso.

IV. Mecanismos de monitoreo y revisión de medidas de seguridad

El artículo 33, fracción VII de la Ley General de Datos establece como otra de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***"Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, 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 dispuesto en el párrafo anterior del presente artículo, 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;*

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.*

Aunado a lo previsto en las fracciones anteriores del presente artículo, 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 lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Instituto.

Para los tratamientos de datos personales del Infonavit, considera los siguientes tipos de monitoreo:

1) **Revisión del cumplimiento de la Política de Tratamiento y Gestión de Datos Personales.** El Comité de Transparencia**,** la Unidad de Transparencia y la Oficial de Protección de Datos Personales, deberán supervisar la PTGDP, al menos cada dos años, o bien, cuando ocurra cualquiera de los supuestos siguientes:

- Modificación al alcance de la PTGDP.
- Modificación a la legislación aplicable al Infonavit, o a su normativa o políticas institucionales.
- Modificación a los servicios y productos ofrecidos por el Infonavit.
- Actualización o cambio en las tecnologías utilizadas por el Infonavit.
- Identificación de riesgos en los procesos de remisión y transferencias de datos personales.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
- Implementación de acciones derivadas de una revisión o auditoria de cumplimiento a la PTGDP.
- Actualización o adopción de nuevos estándares nacionales o internacionales aplicables al Infonavit o en materia de protección de datos personales.
- Retroalimentación de las unidades administrativas y Órganos Colegiados que ameriten cambios a la PTGDP.

2) **Revisión de cumplimiento de las Políticas Institucionales para Seguridad de la información.** Tiene el objetivo de asegurar que las y los empleados realicen los tratamientos de datos personales en concordancia con lo dispuesto en las políticas, los manuales de organización, las guías, y demás normatividad que resulte aplicable. Lo anterior es así ya que el alcance de éstas aplica a todas las áreas del Instituto, sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal del Instituto en el ejercicio de sus funciones, a los proveedores vinculados a

través de instrumentos jurídicos y a los terceros. Es de señalar que el presente tipo de monitoreo incluye el acceso y procesamiento de información fuera de las instalaciones del Instituto, así como el uso de dispositivos móviles con acceso autorizado a la información del Instituto.

3) **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: personal de vigilancia en los accesos al edificio del Infonavit, control de acceso del personal con tarjeta de proximidad, y circuito cerrado de cámaras de vigilancia.

4) **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, se cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del Infonavit.

   - **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el Oficial en Jefe de Seguridad de la Información, la Unidad de Transparencia, la Oficial de Protección de Datos Personales, la SGTI y las unidades administrativas involucradas, se coordinan, en atención a sus competencias, para decidir sobre las acciones pertinentes para la identificación, contención, mitigación, recuperación, en su caso y mejora continua, según les corresponda, hasta que se concluya el asunto.

V. Programa General de Capacitación

Finalmente, al referirnos al Programa de capacitación, previsto en artículo 33, fracción VIII de la Ley General de Datos, que dispone que se deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales. Así como lo previsto en el artículo 35, fracción VII de la Ley General de Datos, el programa de capacitación del Infonavit forma parte del Documento de Seguridad.

En ese sentido, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> "***Capacitación***
> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

- ***I.*** *Los requerimientos y actualizaciones del sistema de gestión;*
- ***II.*** *La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
- ***III.*** *Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
- ***IV.*** *Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad."*

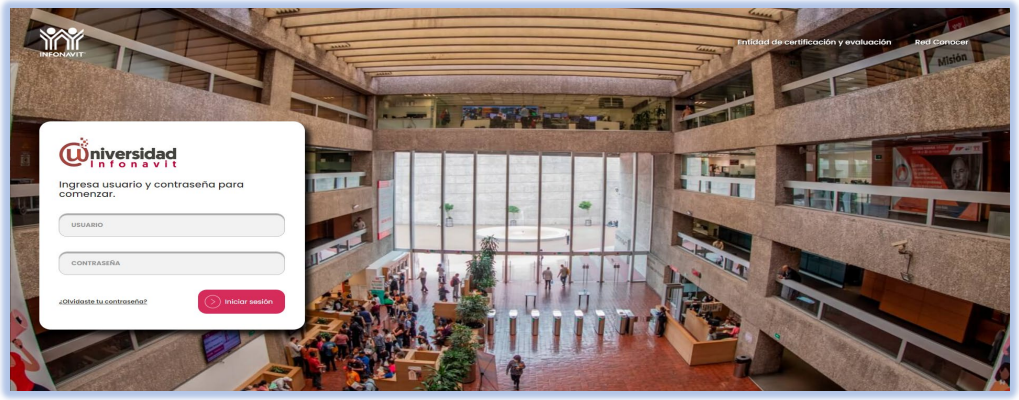
Al respecto, el Infonavit instrumentó programas transversales con el objetivo de reforzar la protección de datos personales, así como la seguridad de la información que, en conjunto con las otras medidas de seguridad, suman al sistema de gestión.

Como parte de dichos programas, se impulsó y fortaleció la cultura organizacional en materia de protección de datos personales y de seguridad de la información a fin de que cada trabajador(a) esté sensibilizado y comprometido con el cumplimiento de la Ley General de Datos, las Políticas Institucionales para Seguridad de la Información y la Política de Tratamiento y Gestión de Datos Personales.

A partir de lo anterior, el Instituto diseñó e implementó cursos en su plataforma específica de capacitación denominada **Universidad Infonavit** tanto en protección de datos personales como en seguridad de la información.

Dichas acciones de capacitación arrojan resultados importantes para las medidas de seguridad administrativas y técnicas, ya que el Instituto cuenta con una plantilla de personal de casi 6,000 trabajadores, siendo los avances los siguientes:

Curso	Porcentaje de avance
Derecho a la protección de datos personales	94%
Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	90%
Riesgos, amenazas y medidas de seguridad de la información	71%
Seguridad de la información	62%



Finalmente, es importante precisar que la CGR, mediante el Oficial en Jefe de Seguridad de la Información, lleva a cabo continuamente campañas de difusión sobre seguridad de la información, así como ejercicios para que el personal comprenda fácilmente el importante papel que tiene en este rubro.

En el Infonavit, conscientes de que la seguridad la hacemos todas y todos, seguiremos trabajando para fortalecer la seguridad y confidencialidad de los datos personales que posee, en el ejercicio de sus funciones, en un contexto de cumplimiento normativo y operativo de mejora continua.