Elaboró: CSG
Fecha emisión: Junio 2021
Última revisión: Octubre 2025
Código: LIS GSI 009
Versión: 02

Matriz de Partes Interesadas del SGSI

La impresión en papel de este DOCUMENTO, o su consulta en cualquier otro medio diferente a Intranet, no es válida como documento oficial de nuestra Organización. por lo que su uso es responsabilidad de la persona que lo imprima o consulte.

No.	Partes Interesada	Grupo	Contexto	Requisitos		Proceso de la Organización en el que tiene impacto								Total Procesos	Seguimiento (Retroalimentación)	Método de Comunicación
				Necesidades	Expectativas	Cobranza Punta-Punta	Investigación de Crédito	Recuperación de Cartera	Gestión Domiciliaria	Sistemas	Recursos Humanos	Contabilidad y Tesorería	Compras			
1	Infonavit	Clientes	Externo	Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y específica a los artículos aplicables para el tratamiento de los datos personales de los Acreditados. Firma los acuerdos para la transferencia de información y cadena de custodia a efecto de evitar pérdidas de información, en términos de la Política de Gestión de Activos del INFONAVIT. Contar con las licencias, usuarios y contraseñas para el acceso a las plataformas de gestión que el INFONAVIT determine. Garantizar el cumplimiento de las siguientes Políticas del Manual General de Políticas de Seguridad de la Información del INFONAVIT: Manejo de medios, Control de accesos, Cifrado, Áreas seguras, Transferencia de información, Adquisición, desarrollo y mantenimiento de sistemas y aplicaciones, Entrenamiento y conciencia en materia de seguridad de la información, Gestión de activos, Gestión de incidentes, Seguridad de las operaciones y Seguridad de las comunicaciones. En caso de que la organización haga uso de un dispositivo de su propiedad para el almacenamiento y utilización de información del INFONAVIT, deberá realizar un borrado seguro utilizando el estándar NIST 800-88 REV 1. Impartir capacitación en materia de seguridad de la información a los empleados de la organización por lo menos una vez al año y cada ve que exista rotación de personal. Ubicarse en un lugar seguro y de fácil acceso para los Acreditados y que cuenten con protocolos de seguridad COVID y respeten los Programas de Protección Civil	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Estar certificado en la norma UNE-ISO/IEC 27001:2022 Contar con un plan de continuidad en los servicios, con la finalidad de garantizar el servicio en los sistemas de información en caso de eventos de desastre, contingencia, fallas o interrupciones en las telecomunicaciones y/o en sus equipos de cómputo y otros que estén involucrados en el servicio.	x	x			x	x			4	Encuestas de Satisfacción al Cliente. Supervisiones de gabinete y de campo mensuales. Control de quejas.	Juntas de trabajo presenciales y/o virtuales. Evidencia de los planes de trabajo Correo electrónico y llamadas telefónicas
2	CitiBanamex	Clientes	Externo	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Contar con infraestructura necesarias para garantizar la seguridad de la información en relación con el acceso, almacenamiento, y/o procesamiento de la información de su propiedad. la organización debe de poner a disposición del cliente infraestructura no externalizada o con acceso remoto o web. Cumplir con el Assessment de TPISA de seguridad de la información. Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos aplicables. Realizar toda la gestión necesaria para asegurar que los datos que nos proporciona el Cliente y los que se le entregan no se verán vulnerados en cuanto a su confidencialidad, integridad y disponibilidad.	Estar certificado en la norma UNE-ISO/IEC 27001:2022		x		x	x	x			3	Encuestas de Satisfacción al Cliente. Auditorías anuales de Seguridad de la Información	Juntas de trabajo mensuales presenciales y/o virtuales. Correo electrónico y llamadas telefónicas
3	Banco Afirme	Clientes	Externo	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Contar con infraestructura necesarias para garantizar la seguridad de la información en relación con el acceso, almacenamiento, y/o procesamiento de la información de su propiedad. la organización debe de poner a disposición del cliente infraestructura no externalizada o con acceso remoto o web. Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos aplicables. Realizar toda la gestión necesaria para asegurar que los datos que nos proporciona el Cliente y los que se le entregan no se verán vulnerados en cuanto a su confidencialidad, integridad y disponibilidad.	Estar certificado en la norma UNE-ISO/IEC 27001:2022				x	x	x			3	Encuestas de Satisfacción al Cliente. Auditorías anuales de Seguridad de la Información	Juntas de trabajo mensuales presenciales y/o virtuales. Correo electrónico y llamadas telefónicas

4	CrediMovil	Clientes	Externo	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Contar con infraestructura necesarias para garantizar la seguridad de la información en relación con el acceso, almacenamiento, y/o procesamiento de la información de su propiedad. la organización debe de poner a disposición del cliente infraestructura no externalizada o con acceso remoto o web. Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos aplicables. Realizar toda la gestión necesaria para asegurar que los datos que nos proporciona el Cliente y los que se le entregan no se verán vulnerados en cuanto a su confidencialidad, integridad y disponibilidad.	Estar certificado en la norma UNE-ISO/IEC 27001:2022				x	x	x			3	Encuestas de Satisfacción al Cliente. Auditorías anuales de Seguridad de la Información	Juntas de trabajo mensuales presenciales y/o virtuales. Correo electrónico y llamadas telefónicas
5	BBVA Bancomer, Banca Empresarial, Multiva ION, Scotiabank, Afirme Sadabell, Unión de Crédito, Monex, Ve por Más, SIMSA, REYMSA, Santander, Sabcapital,	Clientes	Externo	Contar con infraestructura necesarias para garantizar la seguridad de la información en relación con el acceso, almacenamiento, y/o procesamiento de la información de su propiedad. Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos aplicables. Realizar toda la gestión necesaria para asegurar que los datos que nos proporciona el Cliente y los que se le entregan no se verán vulnerados en cuanto a su confidencialidad, integridad y disponibilidad. Contar con un plan de continuidad en los servicios, con la finalidad de garantizar el servicio en los sistemas de información en caso de eventos de desastre, contingencia, fallas o interrupciones en las telecomunicaciones y/o en sus equipos de cómputo y otros que estén involucrados en el servicio.	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Estar certificado en la norma UNE-ISO/IEC 27001:2022		x			X				2	Encuestas de Satisfacción al Cliente. Atención de aclaraciones por parte de la Supervisora de Atención a Clientes. Juntas de seguimiento trimestrales (aplica solo con algunos clientes)	Correo electrónico y llamadas telefónicas
6	SEARS SANBORNS MULTIVA	Clientes	Externo	Contar con infraestructura necesarias para garantizar la seguridad de la información en relación con el acceso, almacenamiento, y/o procesamiento de la información de su propiedad. Apegarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos aplicables. Realizar toda la gestión necesaria para asegurar que los datos que nos proporciona el Cliente y los que se le entregan no se verán vulnerados en cuanto a su confidencialidad, integridad y disponibilidad. Contar con un plan de continuidad en los servicios, con la finalidad de garantizar el servicio en los sistemas de información en caso de eventos de desastre, contingencia, fallas o interrupciones en las telecomunicaciones y/o en sus equipos de cómputo y otros que estén involucrados en el servicio.	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Estar certificado en la norma UNE-ISO/IEC 27001:2022			x		X				2	Encuestas de Satisfacción al Cliente. Reportes de REDECO.	Correo electrónico y llamadas telefónicas
7	Deudores	Terceras partes	Externo	El tratamiento de los datos personales de los Deudores acreditados se apeguen a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos 19, 20 y 21. El tratamiento de los datos personales de terceros se apegue a Ley Federal de Protección de Datos Personales en Posesión de Autoridades, Órganos y Organismos de Gobierno (sujetos obligados).	No hacer mal uso de los datos personales y sensibles de los Deudores.			X		X				2	Quejas y/o comentarios de los Deudores. Reportes de REDECO.	Atención presencial, llamada telefónica y/o correo electrónico.
8	Acreditados	Terceras partes	Externo	El tratamiento de los datos personales de los Acreditados se apeguen a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma específica a los artículos 19, 20 y 21. El tratamiento de los datos personales de terceros se apegue a Ley Federal de Protección de Datos Personales en Posesión de Autoridades, Órganos y Organismos de Gobierno (sujetos obligados).	No hacer mal uso de los datos personales y sensibles de los Acreditados.	x				X				2	Buzón de quejas y sugerencias en las sucursales. Encuesta de Satisfacción.	Atención presencial, llamada telefónica y/o correo electrónico.

9	Sujetos de Investigación	Terceras partes	Externo	El tratamiento de los datos personales de los Acreditados se apeguen a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma especifica a los artículos 19, 20 y 21. El tratamiento de los datos personales de terceros se apegue a Ley Federal de Protección de Datos Personales en Posesión de Autoridades, Órganos y Organismos de Gobierno (sujetos obligados).	No hacer mal uso de los datos personales y sensibles de los Sujetos de investigación.		x		x	X				3	Formato de Atención al Cliente Formato de quejas	Atención presencial, llamada telefónica y/o correo electrónico.
10	INAI	Autoridades regulatorias	Externo	Cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización. Estar certificado en la norma UNE-ISO/IEC 27001:2022	x	x	x	x	x	x	x	x	8	Resultado de la verificación por parte del INAI en la organización para determinar el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (cuando aplique)	Atención presencial, llamada telefónica y/o correo electrónico.
11	RPPyC	Autoridades regulatorias	Externo	Cumplimiento de los Reglamentos de los Registros Públicos del estado de México y de la Ciudad de México Contar con la firma electrónica de autentificación para la plataforma SIGER y así poder acceder a la consulta en línea de la información disponible de los RPPyC	Hacer buen uso de la información electrónica obtenida.		x							1	Verbal en caso de incumplir un lineamiento de seguridad al visitar de manera física algún Registro Público del estado de México y de la Ciudad de México. Correo electrónico en caso de incumplir un lineamiento de seguridad al realizar un trámite en línea en los Registros Públicos del estado de México y de la Ciudad de México.	Atención presencial, llamada telefónica y/o correo electrónico.
12	Juzgados Civiles de la Ciudad de México y/o Estado de México	Autoridades regulatorias	Externo	Cumplimiento de los Reglamentos de los Juzgados Civiles de la Ciudad de México y del estado de México. Contar con las firmas electrónicas de autentificación para el acceso a la información y realizar trámites en línea disponible de los juzgados civiles (Certificado digital de firma electrónica FIREL para la Cdmx y Firma electrónica para el Estado de México)	Hacer buen uso de la información electrónica obtenida.	x								1	Verbal en caso de incumplir un lineamiento de seguridad al visitar de manera física algún juzgado civil del estado de México y de la Ciudad de México. Correo electrónico en caso de incumplir un lineamiento de seguridad al realizar un trámite en línea en algún juzgado civil del estado de México y de la Ciudad de México.	Atención presencial, llamada telefónica y/o correo electrónico.
13	Municipio de Nezahualcóyotl	Autoridades regulatorias	Externo	Cumplimiento del Reglamento de Protección Civil del municipio de Nezahualcóyotl Edo. de México	Registro del Programa Interno de Protección Civil de la organización en la Coordinación de Protección Civil del municipio de Nezahualcóyotl para su autorización.		x	x	x		x			4	Resultado de la verificación de la Coordinación de Protección Civil del municipio de Nezahualcóyotl (cuando aplique)	Atención presencial (cuando aplique)
14	Municipio de Toluca	Autoridades regulatorias	Externo	Cumplimiento del Reglamento de Protección Civil del municipio de Toluca Edo. de México	Registro del Programa Interno de Protección Civil de la organización en la Coordinación de Protección Civil y Bomberos del municipio de Toluca del municipio de Toluca para su autorización.	x					x			2	Resultado de la verificación de la Coordinación de Protección Civil y Bomberos del municipio de Toluca (cuando aplique)	Atención presencial (cuando aplique)
15	Alcaldía Benito Juárez de la CDMX	Autoridades regulatorias	Externo	Cumplimiento de la Ley de Gestión Integral de Riesgos y de Protección Civil de la Ciudad de México.	Registro del Programa Interno de Protección Civil de la organización en la Dirección General de Prevención del Delito y Protección Civil de la Deleg. Benito Juárez de la Cdmx para su autorización.	x					x			2	Resultado de la verificación de la Dirección General de Prevención del Delito y Protección Civil de la Deleg. Benito Juárez de la Cdmx (cuando aplique)	Atención presencial (cuando aplique)
16	Colaboradores	Colaboradores	Interno	El tratamiento de los datos personales de los empleados se apegue a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en forma general y de forma especifica a los artículos 19, 20 y 21 por parte de la Organización. La información contenida en el expediente del personal, sea debidamente resguardada y se mantenga de manera íntegra y confidencial.	Capacitación y sensibilización respecto a la seguridad de la información que se maneja en la organización.	x	x	x	x	x	x	x	x	8	Encuestas del clima laboral Buzón CIA Encuesta de Salida (En caso de renuncia voluntaria)	Atención presencial, llamada telefónica y/o correo electrónico.
17	Proveedores	Proveedores	Externo	La información contenida en los contratos se mantenga de manera confidencial e integra. Cumplir con los acuerdos contractuales. Cumplir con los acuerdos de confidencialidad firmados.	No hacer mal uso de los datos proporcionados a la organización.	x				x			x	3	Contacto con el Responsable del proceso de Compras en caso de que se haga mal uso de la información y/o datos proporcionados por los proveedores.	Llamada telefónica y/o correo electrónico.
18	Organismo de Certificación	Proveedores	Externo	Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización.	Certificarse en la norma UNE-ISO/IEC 27001:2022	x	x	x	x	x	x	x	x	8	Informe de auditoría externa del SGSI de la organización. Atención y seguimiento de los hallazgos detectados en la auditoría (NC y observaciones)	Atención presencial, llamada telefónica y/o correo electrónico.
19	Socios de la Organización	Socios de la Organización	Interno	El uso de los datos personales de los socios se apegue a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares por parte de la Organización. Contar con un Sistema de Gestión de Seguridad de la Información implementado en la organización y estar certificado en la norma UNE-ISO/IEC 27001:2022	Disponibilidad oportuna de la información de la organización.	x	x	x	x	x	x	x	x	8	Informes ejecutivos de las áreas de la organización Revisión por la Dirección del SGSI	Atención presencial, llamada telefónica y/o correo electrónico.