

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Introducción

El presente documento contiene las medidas de seguridad administrativa, física y técnica aplicables a los datos personales en posesión del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Nuevo León (ISSSTELEON), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal de los usuarios de las prestaciones y servicios que este Instituto proporciona.

Objetivo

Identificar los datos personales que se obtienen en el ISSSTELEON clasificándolos y designando los responsables de su resguardo a fin de establecer las medidas de seguridad a implementar para su protección.

Alcance

El presente documento será de observancia obligatoria para todas las Unidades Administrativas del ISSSTELEON, las cuales deberán vigilar su correcta aplicación.

El inventario de datos personales y de los sistemas de tratamiento

El inventario de datos personales que son recabados a través de diversa documentación para la ejecución de los trámites y servicios proporcionados por el ISSSTELEON, se enlista en la siguiente tabla:

Consecutivo	Dato recabado	Tipo de Dato Personal		Forma en que se obtiene el dato		Estrictamente necesario para trámite/servicio
		Dato personal	Dato personal sensible	Recabado directamente	Recabado indirectamente	
1	Nombre	X	-	X	-	SÍ
2	Fotografía	X	-	X	-	SÍ
3	Firma	X	-	X	-	SÍ
4	Domicilio	X	-	X	-	SÍ
5	CURP	X	-	X	-	SÍ
6	Clave de elector	X	-	X	-	NO
7	Huella dactilar	-	X	X	-	SÍ
8	Número de seguridad social (NSS)	X	-	X	-	SÍ
9	RFC	X	-	X	-	SÍ




10	Correo electrónico	X	-	X	-	SÍ
11	Teléfono	X	-	X	-	SÍ
12	Número de afiliado	X	-	X	-	SÍ
13	Número de empleado	X	-	X	-	SÍ
14	Número de cédula profesional/maestría	X	-	X	-	SÍ
15	Número de registro del título profesional/maestría	X	-	X	-	SÍ
16	Número de licencia de conducir	X	-	X	-	NO
17	Número de cartilla militar	X	-	X	-	NO
18	Situación de salud	-	X	X	-	SÍ
19	CLABE interbancaria	X	-	X	-	SÍ
20	Número de cliente bancario	X	-	X	-	NO
21	Fecha de nacimiento	X	-	X	-	SÍ
22	Lugar de nacimiento	X	-	X	-	SÍ
23	Edad	X	-	X	-	SÍ
24	Sexo	X	-	X	-	SÍ
25	Estatura	X	-	X	-	SÍ
26	Peso	X	-	X	-	SÍ
27	Estado Civil	X	-	X	-	SÍ
28	Agrupaciones sindicales, sociales, etc.	-	X	X	-	SÍ
29	Antecedentes de procesos legales	-	X	X	-	SÍ

Las funciones y obligaciones de las personas que traten datos personales

Las funciones y obligaciones del personal se encuentran descritas en el perfil y en la descripción de puesto que se encuentra en posesión de la Dirección de Desarrollo Humano y publicadas en la Plataforma Nacional de Transparencia en lo correspondiente a la fracción II, inciso a) del artículo 95 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.

Además de lo establecido en cada perfil y descripción de puesto del personal, todo servidor público del ISSSTELEON que tenga acceso, trate, administre y/o maneje datos personales, deberá conocer y aplicar, como medidas de seguridad administrativa que serán de observancia obligatoria lo siguiente:

- I. Mantener el deber de confidencialidad respecto de los datos personales que se encuentren bajo su custodia o a los que tengas acceso o conocimiento con motivo de su empleo, cargo o comisión sin comunicarlos a quien no está legalmente autorizado, incluso después de que finalice su relación laboral en el ISSSTELEON;
- II. Resguardar en todo momento cualquier documento que contenga datos personales evitando que terceros no autorizados tengan acceso a los mismos;



- III. Queda prohibida la reutilización de hojas que contengan datos personales. En caso de que algún documento que contenga datos personales no sea entregado a su titular o, por alguna razón, no sea integrado al expediente personal del titular, este deberá ser destruido;
- IV. No utilizar ningún medio como celulares, cámaras fotográficas o cualquier otro dispositivo de uso personal, para captar, reproducir o difundir datos personales, aún si esto fuese para dar cumplimiento al ejercicio de los derechos ARCO por parte del titular, en su caso, deberá entregarse la información de manera impresa al titular o en su caso por los medios electrónicos autorizados y destinados para tal efecto;
- V. Solo el personal autorizado podrá acceder a documentos que contengan datos personales;
- VI. Cada servidor público, deberá registrar quién accede a los archivos bajo su custodia, especificando nombre, cargo, área de adscripción y motivo del acceso. Antes de permitir el acceso a los datos personales bajo su custodia deberá observarse el cumplimiento de la fracción anterior;
- VII. Bloquear el equipo de cómputo que le sea asignado cuando se encuentre ausente (Control + Alt + Supr) y apagarlo al terminar su jornada de trabajo con la finalidad de evitar el acceso al mismo de personas no autorizadas;
- VIII. Retirar los documentos que contengan datos personales que se encuentren a su resguardo de: impresoras, escáner y fotocopadoras;
- IX. Guardar bajo llave documentos o dispositivos que contengan datos personales que se encuentren bajo su custodia;
- X. Establecer y no compartir las contraseñas de los sistemas, equipos y demás dispositivos que se encuentren bajo su custodia, maneje y contengan datos personales;
- XI. Evita llevar fuera de tu lugar de trabajo datos personales en dispositivos electrónicos o papel. Si por el cumplimiento de sus funciones esto debiese ser necesario, deberá proteger esa información con contraseña o en sobre debidamente cerrado;
- XII. El servidor público deberá asegurar que los dispositivos móviles o portátiles que contenga datos personales, no se encuentren desatendidos en un lugar público; si por el cumplimiento de sus funciones es necesario separarse del dispositivo, deberá bloquearlo;
- XIII. Cumplir con las medidas de seguridad y normas internas que en materia de datos personales sean emitidas;
- XIV. Comunicar a su jefe inmediato cualquier incidencia que detecte en el tratamiento de datos personales sin importar si está corresponde o no a su área de adscripción;
- XV. Cuando sea necesario remitir datos personales a otras áreas del ISSSTELEON, comunicar por escrito la naturaleza de estos, especificando para qué finalidades pueden ser utilizados y la obligación que se tiene de guardar la confidencialidad respecto de los mismos.

Análisis de riesgos




El análisis de riesgos es el estudio que se debe de dar a todo nuevo tratamiento de datos personales con la principal finalidad de establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de las personas afectadas

Se considerará la siguiente tabla para determinar el nivel de riesgo:



isssteleon.gob.mx

Matamoros 319 Pte., Monterrey, Nuevo León. Tel. (81) 2033.9000

@gob_Nuevo León   

Valor de Gravedad (1-4)

4	8	12	16	ALTO (12-16)
3	6	9	12	
2	4	6	8	
1	2	3	4	

Valor de Probabilidad (1-4)

Matriz de análisis de riesgos						
Identificación		Probabilidad	Gravedad	Clasificación	Nivel de riesgo	Tratamiento o control operacional
Nombre	Riesgo					
Expediente físico de prestaciones sociales y económicas	Pérdida de información por incendio, inundación y/o roedores	2	3	6	Bajo	Verificar el correcto funcionamiento de los sistemas contra incendios. Verificar que la bomba de agua se encuentre en operación. Realizar periódicamente fumigaciones para el control de plagas de insectos y roedores.
	Robo/perdida/fuga de datos personales por acceso de personal no autorizado	1	4	4	Bajo	Resguardar bajo llave el acceso al archivo.




						<p>Establecer un libro de bitácora de acceso al archivo.</p> <p>Designar un encargado de resguardo y de control de acceso al archivo.</p>
Base de datos del ISSSTELEON	Pérdida de información por incendio	1	4	8	Medio	Verificar el correcto funcionamiento de los sistemas contra incendios.
	Pérdida de información por robo de hardware	1	1	1	Bajo	<p>Controles electrónico de acceso físico restringido únicamente para el personal autorizado al área de Administración General de Sistemas.</p> <p>Monitoreo continuo de cámaras de seguridad.</p>
	Robo de información por <i>hackeo</i>	1	4	4	Bajo	Equipo físico de firewall con Sistema de Prevención de Intrusión (IPS)

Análisis de brecha

Dirección de Prestaciones Sociales y Económicas			
Expediente de prestaciones sociales y económicas			
Pregunta de control	SI	NO	Observaciones
Medidas de seguridad basadas en la cultura del personal			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	X		
Política de escritorio limpio	X		
Hábitos de cierre y resguardo	X		
Impresoras, escáneres, copiadoras y buzones limpios	X		
¿Tienes mecanismos para eliminar de manera segura la información?	NA	NA	Por la naturaleza de los servicios prestados en el ISSSTELEON, la información recabada no es eliminada sino resguardada hasta en tanto se agoten los derechos a que pudiese ser sujeto tanto el derechohabiente como sus beneficiarios.
Destrucción segura de documentos	NA	NA	
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico	NA	NA	



Fijar periodos de retención y destrucción de información	NA	NA	
Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	X		
Fomentar la cultura de la seguridad de la información	X		
Asegurar la protección de datos personales en subcontrataciones	NA	NA	No se realizan procesos de subcontratación.
¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?		X	
¿Realizas respaldos periódicos de los datos personales?	X		Se realiza la digitalización de los documentos recibidos y se almacena en los servidores del área de Administración General de Sistemas.
Medidas de seguridad en el entorno de trabajo físico			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?		X	
Mantener registros del personal con acceso al entorno de trabajo		X	
¿Tienes medidas de seguridad para evitar el robo?	X		Se cuenta con un sistema de vigilancia de circuito cerrado, así como de guardias de seguridad tanto como personal del ISSSTELEON como el contratado como seguridad privada.
Cerraduras y candados	X		
¿Cuidas el movimiento de información en entornos de trabajo físicos?	X		
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico	NA	NA	Los equipos de cómputo son fijos y el acceso a la red para la consulta de información se realiza únicamente a través de la Red Local.
Mantener en movimiento sólo copias de la información, no el elemento original	X		

Administración General de Sistemas			
Base de datos de ISSSTELEON			
Pregunta de control	SI	NO	Observaciones
Medidas de seguridad basadas en la cultura del personal			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	X		
Política de escritorio limpio	X		
Hábitos de cierre y resguardo	X		



Impresoras, escáneres, copadoras y buzones limpios	X		
¿Tienes mecanismos para eliminar de manera segura la información?	NA	NA	Por la naturaleza de los servicios prestados en el ISSSTELEON, la información recabada no es eliminada sino resguardada hasta en tanto se agoten los derechos a que pudiese ser sujeto tanto el derechohabiente como sus beneficiarios.
Destrucción segura de documentos	NA	NA	
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico	NA	NA	
Fijar periodos de retención y destrucción de información	NA	NA	
Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	X		
Fomentar la cultura de la seguridad de la información	X		
Asegurar la protección de datos personales en subcontrataciones	NA	NA	No se realizan procesos de subcontratación.
¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?	X		
¿Realizas respaldos periódicos de los datos personales?	X		Se realiza respaldos de la información contenida en nuestros servidores en servidores externos para evitar pérdida de información.
Medidas de seguridad en el entorno de trabajo físico			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?	X		
Mantener registros del personal con acceso al entorno de trabajo		X	
¿Tienes medidas de seguridad para evitar el robo?	X		Se cuenta con un sistema de vigilancia de circuito cerrado, así como de guardias de seguridad tanto como personal del ISSSTELEON como el contratado como seguridad privada.
Cerraduras y candados	X		
¿Cuidas el movimiento de información en entornos de trabajo físicos?	NA	NA	La información solamente se almacena para su resguardo y protección.
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico		X	
Mantener en movimiento sólo copias de la información, no el elemento original	NA	NA	No se realizan copias de la información contenida en el servidor.
Medidas de seguridad en el entorno de trabajo digital			
¿Realizas actualizaciones al equipo de cómputo?	X		
¿Revisas periódicamente el software instalado en el equipo de cómputo?	X		




¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?	X		
Uso de contraseñas y/o cifrado	X		
Bloqueo y cierre de sesiones	X		
Administrar usuarios y accesos	X		
¿Revisas la configuración de seguridad del equipo de cómputo?	X		
¿Tienes medidas de seguridad para navegar en entornos digitales?	X		
Reglas de navegación segura	X		
Uso de conexiones seguras	X		
¿Cuidas el movimiento de información en entornos de trabajo digitales?	X		
Seguridad de la información enviada y recibida	X		

Plan de trabajo

1. Establecer y crear los procedimientos y mecanismos para actuar ante vulneraciones a la seguridad de los datos personales contenidos en los archivos físicos de la Dirección de Prestaciones Sociales y Económicas.
2. Delimitar los espacios físicos para dar acceso solo al personal autorizado, restringiendo así a aquellos ajenos al área responsable de salvaguardar la información.
3. Establecer y crear los procedimientos y mecanismos que aseguren que los equipos de cómputo portátiles, así como el uso de dispositivos de almacenamiento serán utilizados prioritariamente dentro del horario laboral establecido, conectados a la red de internet del ISSSTELEON y en sus instalaciones.
4. Designar un encargado responsable del acceso al archivo físico, formalizado mediante Carta Responsiva y para la aplicación y control de bitácoras de acceso del personal autorizado.

Medidas de seguridad en TIC's



En ISSSTELEON se cuenta con las siguientes medidas de seguridad para lo relacionado con equipos cómputo y servidores:

- Se cuentan con medidas técnicas para salvaguardar los datos e información que se almacena y maneja en el ISSSTELEON, asegurando su integridad, disponibilidad, confidencialidad y recuperación.
- El *site* de ISSSTELEON, en donde se encuentran nuestros equipos de *Data Center*, *Networking*, enlaces, conectividad, seguridad y respaldo de energía, se encuentra aislado y climatizado de acuerdo a normas establecidas y cuenta con acceso electrónico controlado, para lo cual se lleva una bitácora de actividades.
- El software y las aplicaciones de los equipos que se utilizan en ISSSTELEON cuentan con certificados y licenciamientos actualizados.
- Se cuenta con equipos de tecnología avanzada para realizar controles de seguridad en la red y en nuestros aplicativos, así como prevenir intrusiones a los mismos.



isssteleon.gob.mx


Matamoros 319 Pte., Monterrey, Nuevo León. Tel. (81) 2033.9000

@gob_Nuevo León   

Página 8 de 9

- Los datos se encuentran almacenados en servidores de alta gama y los accesos son administrados y monitoreados permanentemente.
- Se cuenta con procesos de respaldos de la información de alto nivel, establecidos en nuestro Plan de Respaldos de Datos, así como en nuestro Plan de Recuperación de Desastres (DRP) y en el Plan de Continuidad del Negocio (BCP).

El presente documento se elabora a los 19-diecinueve días del mes de enero del año 2024-dos mil veinticuatro en cumplimiento a lo establecido en el artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.



LIC. DANIEL FERNÁNDO MARTÍNEZ GARCÍA
RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA DEL
INSTITUTO DE SEGURIDAD Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO DE NUEVO LEÓN






**INSTITUTO DE SEGURIDAD Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO DE NUEVO LEÓN
(ISSSTELEON)**

**PROGRAMA ANUAL DE CAPACITACIÓN EN MATERIA DE
PROTECCIÓN DE DATOS PERSONALES
EJERCICIO 2024**



isssteleon.gob.mx

Matamoros 319 Pte., Monterrey, Nuevo León. Tel. (81) 2033.9000

@gob_Nuevo León   

Handwritten blue ink marks, including a large checkmark and several scribbles.

CONTENIDO

1. INTRODUCCIÓN

2. FUNDAMENTO LEGAL

3. OBJETIVO

4. ALCANCE

5. TEMARIO

6. CALENDARIO

7. EJECUCIÓN Y EVALUACIÓN



1. INTRODUCCIÓN

El Programa Anual de Capacitación en Materia de Protección de Datos Personales del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Nuevo León (ISSSTELEON), es un instrumento de gestión que contempla las acciones a desarrollar por parte de este organismo a efecto de que los servidores públicos que laboran al interior de este Instituto, se encuentren capacitados en materia de protección de datos personales, esto con la intención de brindarles de los conocimientos y las herramientas necesarias en el tratamientos de datos personales.

2. FUNDAMENTO LEGAL

El presente Programa se elabora de conformidad con lo establecido en el artículo 35, fracción III de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligado del Estado de Nuevo León y el artículo 44 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León.

3. OBJETIVO

La finalidad del presente Programa es dotar al personal que labora al interior del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Nuevo León (ISSSTELEON) de conocimiento, herramientas y aptitudes para lograr la homogeneidad al realizar el tratamiento de datos personales cumpliendo con el marco normativo en la materia.

4. ALCANCE

El presente programa se encuentra dirigido a las personas servidoras públicas involucradas en el tratamiento de los datos personales, adscritas a las diferentes Unidades Administrativas que conforman la estructura orgánica del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de Nuevo León.



5. TEMARIO

GENERALIDADES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Objetivo específico: Conocer los aspectos generales de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León respecto a definiciones, qué se considera un dato personal, importancia de su cuidado y resguardo, obligaciones de los responsables, entre otros.

DEL TRATAMIENTO DE LAS SOLICITUDES DE DERECHO ARCOP:

Objetivo específico: Conocer y operar conforme a la normativa conociendo quiénes tienen acceso a los datos personales, casos especiales para el ejercicio del derecho ARCOP, plazos de atención, tipos de respuestas a emitir, entre otros.

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES:

Objetivo específico: Conocer los principios y deberes establecidos en los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León, denotando su aplicación en la operación propia del ISSSTELEON.

6. CALENDARIO

La planificación de cada una del temario de capacitaciones a impartir se establece un calendario en el cual se fijan las fechas en que estos serán impartidos.

Las fechas y tiempos designados a cada temario referidos en el calendario mencionado son enunciativos más no limitativos, pueden modificarse, o reprogramarse.

El calendario de capacitación se ha programado de la siguiente manera:



Unidad Administrativa	Temas		
	Generalidades en materia de protección de datos personales (2 horas)	Del tratamiento de las solicitudes de derecho ARCO (2 horas)	Lineamientos de Protección de Datos Personales (2 horas)
Dirección de Prestaciones Sociales y Económicas	25 de abril	16 de mayo	6 de junio
Dirección de Servicios Médicos	26 de abril	17 de mayo	7 de junio
Dirección de Desarrollo Humano	2 de mayo	23 de mayo	13 de junio
Dirección Jurídica	3 de mayo	24 de mayo	14 de junio
Dirección de Administración	8 de mayo	30 de mayo	20 de junio
Dirección de Finanzas	9 de mayo	31 de mayo	21 de junio

7. EJECUCIÓN Y EVALUACIÓN

El contenido del temario será desarrollado e impartido por personal de la Unidad de Transparencia en conjunto con los miembros del Comité de Transparencia.

La evidencia respecto la impartición del temario contenido en el presente Programa se materializará mediante:

1. Lista de asistencia del personal asistente con fecha de impartición
2. Constancias de participación y conclusión de la capacitación (emitidas por el Comité de Transparencia)
3. Ficha de evaluación obtenida de las Encuestas de Evaluación de la Capacitación

El presente documento se emite a los 22-veintidós días del mes de febrero del año 2024-dos mil veinticuatro en cumplimiento a lo establecido en el artículo 35, fracción III de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y 44 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León.

