

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES DEL SISTEMA 2 (S2) DE LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS DEL SISTEMA ESTATAL DE INFORMACIÓN (SEI).

INTRODUCCIÓN

La presente Evaluación de Impacto en la Protección de Datos Personales tiene como propósito identificar, analizar y mitigar los riesgos inherentes al tratamiento de datos personales que se realiza a través del ***Sistema 2 (S2) de los servidores públicos que intervengan en procedimientos de contrataciones públicas*** desarrollado e implementado como un subsistema del Sistema Estatal de Información (SEI) del Sistema Estatal Anticorrupción de Nuevo León (SEA-NL).

El Sistema 2 (S2) tiene por objeto registrar, sistematizar y poner a disposición pública la información relativa a las personas servidoras públicas que participan en cualquiera de las etapas del procedimiento de contratación pública, desde la planeación hasta el cierre, permitiendo identificar su nivel de intervención y adscripción institucional. Este sistema forma parte de la estrategia de interoperabilidad con la Plataforma Digital Nacional (PDN), promovida por el Comité Coordinador del Sistema Nacional Anticorrupción y replicada por el SEA-NL en el ámbito estatal y municipal.

Su implementación responde a un enfoque preventivo en materia de combate a la corrupción, al permitir detectar posibles conflictos de interés, dar seguimiento a la actuación de las personas servidoras públicas involucradas en las contrataciones, y contribuir a la integridad en el ejercicio del gasto público. Asimismo, fortalece los principios de transparencia, rendición de

cuentas y máxima publicidad en los procesos administrativos, conforme al marco normativo aplicable.

La Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León (SESEA-NL), como organismo con autonomía técnica y de gestión, actúa como responsable del tratamiento de los datos personales que se integran en el S2, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL), así como en los Lineamientos de Protección de Datos Personales del INFONL¹.

El tratamiento de datos personales en el S2 se limita exclusivamente a información necesaria, pertinente y proporcional para el cumplimiento de sus finalidades, evitando la incorporación de datos sensibles o excesivos. Entre los datos que se recaban y sistematizan se encuentran el nombre, cargo, clave o número de servidor público, unidad administrativa de adscripción, y el procedimiento de contratación en que interviene. La fuente primaria de estos datos son los entes públicos obligados a reportar información en términos de las Bases para el Funcionamiento del SEI² y de los lineamientos de la PDN³.

En cumplimiento de sus obligaciones como responsable, la SESEA-NL ha desarrollado esta Evaluación de Impacto como una herramienta preventiva que permite valorar la licitud, proporcionalidad y seguridad del tratamiento de los datos personales en el S2, estableciendo medidas técnicas, administrativas y organizativas orientadas a garantizar la confidencialidad, integridad y

¹ Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales.

² Sistema Estatal de Información.

³ Plataforma Digital Nacional.

disponibilidad de la información, así como a proteger los derechos de los titulares.

A través de este instrumento, la SESEA-NL reafirma su compromiso con la protección de los datos personales, la innovación institucional responsable, y el fortalecimiento de los mecanismos de control, supervisión y prevención de riesgos en los procedimientos de contratación pública en el Estado de Nuevo León.

MARCO NORMATIVO

La presente evaluación se sustenta en un conjunto de disposiciones constitucionales y legales que rigen el tratamiento de datos personales en posesión de sujetos obligados en México, así como en las normas específicas que regulan la actuación del Sistema Estatal Anticorrupción de Nuevo León.

- Constitución Política de los Estados Unidos Mexicanos,
- Constitución Política del Estado Libre y Soberano de Nuevo León,
- Ley General del Sistema Nacional Anticorrupción,
- Ley General de Responsabilidades Administrativas
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León,
- Ley del Sistema Estatal Anticorrupción para el Estado de Nuevo León,
- Ley de Responsabilidades Administrativas del Estado de Nuevo León
- Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León
- Bases para el funcionamiento de la Plataforma Digital Nacional,
- Bases para el funcionamiento del Sistema Estatal de Información (SEI),

- Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales,
- Acuerdo mediante el cual se aprueban los lineamientos sobre los principios y deberes de protección de datos personales en posesión de los sujetos obligados, emitido por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León,
- Lineamientos de protección de datos personales para los sujetos obligados del Estado de Nuevo León, emitido por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León, y
- Guía de Evaluación de Impacto de Privacidad, emitida por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León,

1. DESCRIPCIÓN DE LA POLÍTICA PÚBLICA, PROGRAMA, SISTEMA O PLATAFORMA INFORMÁTICA, APLICACIÓN ELECTRÓNICA O CUALQUIER OTRA TECNOLOGÍA QUE IMPLIQUE UN TRATAMIENTO INTENSIVO O RELEVANTE DE DATOS PERSONALES QUE PRETENDA PONER EN OPERACIÓN O MODIFICAR.

De conformidad con lo dispuesto en los artículos 76 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 14 fracción XIX, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, así como de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, se proporciona la siguiente información:

sl

A. Denominación del Sujeto Obligado Responsable del Tratamiento:

Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León (SESEANL).

B. Nombre del Proyecto:

Sistema 2 (S2) de los servidores públicos que intervengan en procedimientos de contrataciones públicas del Sistema Estatal de Información (SEI).

C. Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales:

Objetivo general.

El objetivo general del Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas del Sistema Estatal de Información (SEI) es permitir el registro, sistematización, consulta y validación de la información relativa a las personas servidoras públicas que participan en las distintas fases de los procedimientos de contratación pública, en cumplimiento de lo dispuesto por la Ley General de Responsabilidades Administrativas, la Ley General del Sistema Nacional Anticorrupción, la Ley de Responsabilidades Administrativas del Estado de Nuevo León, la Ley del Sistema Estatal Anticorrupción del Estado de Nuevo León, y demás disposiciones legales aplicables.

El Sistema 2 (S2) opera como un subsistema interoperable del Sistema Estatal de Información, lo que permite la actualización y consulta en tiempo real de datos públicos mediante interfaces de programación de aplicaciones (API) con

la Plataforma Digital Nacional (PDN). Este mecanismo fortalece la prevención de conflictos de interés, la transparencia en la gestión de recursos públicos y la integridad en los procedimientos de contratación, conforme a los principios constitucionales de legalidad, eficiencia, honradez, transparencia y máxima publicidad, previstos en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos y el artículo 201 de la Constitución Política del Estado de Nuevo León.

Objetivos específicos:

1. Registrar, validar, sistematizar y conservar la información relativa a las personas servidoras públicas que participan en procedimientos de contratación pública, incluyendo su identidad, cargo, unidad administrativa de adscripción y nivel de intervención, conforme a los formatos y criterios establecidos por la PDN y el Comité Coordinador del SEA-NL.
2. Garantizar el acceso público, oportuno y verificable a la información sobre los servidores públicos involucrados en contrataciones, asegurando su interoperabilidad con la Plataforma Digital Nacional (PDN), bajo los principios de transparencia, rendición de cuentas y protección de datos personales.
3. Prevenir posibles conflictos de interés y prácticas indebidas mediante el seguimiento institucional a las personas que participan en la toma de decisiones durante procesos de contratación, y facilitar la detección de patrones de riesgo.
4. Fortalecer los mecanismos institucionales de vigilancia, control interno y fiscalización, proporcionando a los entes públicos herramientas para monitorear y documentar la participación de su personal en las contrataciones públicas.

5. Dar cumplimiento a las obligaciones normativas en materia de responsabilidades administrativas, transparencia y protección de datos personales, conforme a las leyes generales y estatales aplicables, así como a los lineamientos del INFONL.
6. Facilitar la generación de reportes, análisis, visualizaciones y estadísticas sobre participación de servidores públicos en contrataciones, contribuyendo a la formulación de políticas públicas, estudios técnicos, investigaciones administrativas y acciones de mejora institucional.

D. FUNDAMENTO LEGAL DE LA PLATAFORMA INFORMÁTICA QUE IMPLIQUE UN TRATAMIENTO INTENSIVO DE DATOS PERSONALES.

El fundamento legal del Sistema 2 (S2) de los Servidores Públicos que Intervienen en Contrataciones Públicas se encuentra distribuido entre diversos ordenamientos jurídicos de carácter general y local.

A nivel nacional, la Ley General del Sistema Nacional Anticorrupción en sus artículos 9, fracción XIII; 36, fracción I; 49, fracción II; y 51, establece la creación y operación de la Plataforma Digital Nacional, incluyendo el sistema específico de contrataciones públicas. Complementariamente, la Ley General de Responsabilidades Administrativas, en su artículo 3, fracción XXII, y el artículo 43, detalla los elementos y actualizaciones que deberá contener dicho sistema, así como la disponibilidad pública de la información.

En el ámbito estatal, el artículo 43 de la Ley de Responsabilidades Administrativas del Estado de Nuevo León y el artículo 49 de la Ley del Sistema Estatal Anticorrupción refuerzan la obligación de incluir en el Sistema Estatal de Información los datos relativos a los servidores públicos que intervienen en procedimientos de contrataciones.

Asimismo, las Bases para el Funcionamiento de la Plataforma Digital Nacional, en su artículo 46, establecen que el objeto del sistema es permitir el acceso a dicha información para fines de fiscalización, prevención y combate a la corrupción. Por su parte, el Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, en su artículo 27, fracciones III y IV, señala las atribuciones del Titular de la Dirección de Tecnologías de la Información en cuanto a la implementación y coordinación de las plataformas digitales responsables de esta información.

Todo lo anterior conforma un marco normativo integral que sustenta la existencia, operación y objetivos del Sistema 2 (S2) como parte fundamental de la Plataforma Digital Nacional y su réplica en el ámbito estatal.

Ley General del Sistema Nacional Anticorrupción

“Artículo 9. El Comité Coordinador tendrá las siguientes facultades:

XIII. Establecer una Plataforma Digital Nacional que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que se refiere el Título Cuarto de esta Ley;

...

“Artículo 36. Las leyes de las entidades federativas desarrollarán la integración, atribuciones, funcionamiento de los Sistemas Locales atendiendo a las siguientes bases:

I. Deberán contar con una integración y atribuciones equivalentes a las que esta Ley otorga al Sistema Nacional;”

...

Artículo 49. La Plataforma Digital Nacional del Sistema Nacional estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los siguientes sistemas electrónicos: I. Sistema de evolución



patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;

II. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;

...

Artículo 51. Los sistemas de evolución patrimonial y de declaración de intereses, así como de los Servidores públicos que intervengan en procedimientos de contrataciones públicas, operarán en los términos de la Ley General de Responsabilidades Administrativas. “

Ley General de Responsabilidades Administrativas:

“Artículo 3. Para efectos de esta Ley se entenderá por:

XXII. Plataforma digital nacional: La plataforma a que se refiere la Ley General del Sistema Nacional Anticorrupción, que contará con los sistemas que establece la referida ley, así como los contenidos previstos en la presente Ley;

...

Artículo 43. La Plataforma digital nacional incluirá, en un sistema específico, los nombres y adscripción de los Servidores Públicos que intervengan en procedimientos para contrataciones públicas, ya sea en la tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, el cual será actualizado quincenalmente.

Los formatos y mecanismos para registrar la información serán determinados por el Comité Coordinador.

La información a que se refiere el presente artículo deberá ser puesta a disposición de todo público a través de un portal de Internet.”

Ley del Sistema Estatal Anticorrupción del Estado de Nuevo León:

“Artículo 42. Corresponde al Secretario Técnico ejercer la dirección de la Secretaría Ejecutiva, por lo que contará con las siguientes facultades:

X. Administrar el Sistema de Información Estatal que establecerá el Comité Coordinador, en términos de esta Ley y asegurar el acceso a las mismas de los miembros del Comité Coordinador y la Comisión Ejecutiva;

...

Artículo 49. *El Comité Coordinador emitirá las bases que regulen el acceso, recepción e integración de los datos que deberán proporcionar los sujetos obligados del Estado de Nuevo León y que deban ser incorporados a la Plataforma Digital Nacional que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la presente Ley, la Ley General del Sistema Nacional Anticorrupción y la Ley General de Responsabilidades Administrativas, así como para los sujetos de esta Ley, atendiendo a las necesidades de accesibilidad de los usuarios.*

Por parte del Sistema Estatal Anticorrupción, el Secretario Técnico será el encargado de coordinar el acceso y alimentación de la Plataforma Digital Nacional con la información que los sujetos obligados deban presentar en sus declaraciones, en términos de la Ley General de Responsabilidades de Servidores Públicos.

Para ello, el Secretario Técnico promoverá la administración y publicación de la información en formato de datos abiertos, en todas aquellas dependencias y entidades locales que deban brindarle información conforme a la Ley General de Transparencia y Acceso a la Información Pública y la demás normatividad aplicable.

Asimismo, el Secretario Técnico estará facultado para que en concordancia con las bases que al efecto haya emitido el Comité Coordinador del Sistema Estatal Anticorrupción, establecer formatos, criterios, políticas y protocolos a los Entes públicos del Estado que

tengan a su disposición, información, datos y documentos que sean pertinentes y necesarios para ser incorporados al Sistema Estatal de Información y que en su caso, deban ser incorporados a la Plataforma Digital Nacional en sus diferentes sistemas electrónicos.”

Ley de Responsabilidades Administrativas del Estado de Nuevo León:

“Artículo 3. Para efectos de esta Ley se entenderá por:

XXIII. Plataforma digital nacional: La plataforma a que se refiere la Ley General del Sistema Nacional Anticorrupción, que contará con los sistemas que establece la referida ley, así como los contenidos previstos en la Ley General de Responsabilidades Administrativas;

...

Artículo 43. *El Sistema Estatal de Información y la Plataforma Digital Nacional incluirán, en un sistema específico, los nombres y adscripción de los Servidores Públicos que intervengan en procedimientos para contrataciones públicas, ya sea en la tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, el cual será actualizado quincenalmente.*

Los formatos y mecanismos para registrar la información serán determinados por el Comité Coordinador.

La información a que se refiere el presente artículo, deberá ser puesta a disposición de todo público a través de un portal de Internet.”

Artículo 46 de las Bases para el Funcionamiento de la Plataforma Digital Nacional:

“Artículo 46. *El objeto del sistema es permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus*

prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.”

Artículo 27 fracciones III y IV del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León:

ARTÍCULO 27. Para el desahogo de los asuntos de su competencia, el Titular de la Dirección de Tecnologías de la Información contará con las siguientes facultades:

III. Implementar, mantener, actualizar y evaluar los servicios de las plataformas digitales cuya administración son responsabilidad de la Secretaría Ejecutiva;

IV. Proponer la instauración de mecanismos de organización de la información que permitan la adecuada interacción entre los diversos sistemas de las entidades miembros del Sistema Estatal Anticorrupción;”

Lo dispuesto en los artículos 5, fracción II; 17; 18; 41; 42 y 43 de las Bases para el Funcionamiento del Sistema Estatal de Información (SEI) establece lineamientos fundamentales para el diseño y operación del Sistema Estatal.

El artículo 5, fracción II, señala que:

“Artículo 5. De conformidad con el artículo 49 de la Ley General del Sistema Nacional Anticorrupción y el artículo 27 de la Ley General de Responsabilidades Administrativas, el Sistema Estatal de Información estará conformada por, al menos los siguientes sistemas:

II. Sistema de los servidores públicos;

Asimismo, el artículo 17 establece que:

Artículo 17. *La Secretaría Ejecutiva previa aprobación del Comité Coordinador elaborará y publicará un catálogo de perfiles, en el cual se establezcan las facultades, obligaciones, y/o atribuciones que les sean aplicables a cada uno de los usuarios de manera genérica.*

Por su parte, el artículo 18 dispone:

Artículo 18. *Para el acceso restringido de la información, la Secretaría Ejecutiva establecerá los mecanismos de seguridad necesarios que emita el Comité Coordinador y que para efecto garanticen la confidencialidad, integridad y disponibilidad de la información.”*

Este marco jurídico establece la obligación de los entes públicos de registrar, sistematizar y poner a disposición pública la información relativa a las personas servidoras públicas que intervienen en los procedimientos de contratación pública, conforme a los formatos y especificaciones establecidos por el Comité Coordinador del Sistema Nacional Anticorrupción y reflejados en la Plataforma Digital Nacional. El S2 opera bajo un esquema de interoperabilidad y consulta en tiempo real mediante interfaces de programación de aplicaciones (API), garantizando la trazabilidad, verificabilidad y actualidad de la información.

Asimismo, este fundamento faculta a la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León (SESEA-NL) para coordinar el funcionamiento del Sistema Estatal de Información (SEI), del cual forma parte el S2, garantizando la legalidad del tratamiento de los datos

personales contenidos en dicho sistema. El referido tratamiento se encuentra alineado con los principios de licitud, finalidad, proporcionalidad, seguridad, calidad, responsabilidad y transparencia, establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, y los Lineamientos emitidos por el INFONL.

E. Categorías de los titulares de los datos personales y datos personales que serán objeto de tratamiento distinguiendo los datos sensibles.

En el marco del funcionamiento del Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, subsistema del Sistema Estatal de Información (SEI) del Estado de Nuevo León, se identifican y documentan las categorías de titulares de datos personales cuyos datos son objeto de tratamiento, en apego a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL) y demás normatividad aplicable.

El tratamiento de datos personales en el S2 se limita a información estrictamente necesaria, pertinente y relacionada con el ejercicio de funciones públicas, sin que se recaben ni almacenen datos personales sensibles.

a) Categorías de titulares

El tratamiento de datos personales en el Sistema S2 se refiere a las siguientes categorías de titulares:

1. Personas servidoras públicas adscritas a entes públicos estatales y municipales que intervienen en procedimientos de contratación pública, en cualquiera de sus fases: planeación, preparación, adjudicación, ejecución o cierre.
2. Personas servidoras públicas superiores jerárquicas de quienes participan directamente en los procesos de contratación, cuando sean responsables de autorizar, supervisar o validar dichos procedimientos.
3. Personas servidoras públicas facultadas para firmar, aprobar o autorizar actos administrativos vinculados a contrataciones públicas, incluyendo contratos, convenios o modificaciones contractuales.
4. Personas servidoras públicas encargadas de los órganos internos de control que intervienen en la validación, auditoría o revisión posterior de los procesos de contratación.

b) Datos personales objeto de tratamiento.

Los datos personales tratados por el **Sistema 2 (S2)** son aquellos estrictamente necesarios para identificar, verificar y sistematizar la participación de personas servidoras públicas en los procedimientos de contratación pública, conforme a las obligaciones previstas en el marco legal anticorrupción. Dichos datos son exclusivamente de carácter identificativo, institucional y funcional, y se limitan a los siguientes, conforme a cada categoría:

22

1. Personas servidoras públicas adscritas a entes públicos estatales y municipales que intervienen en procedimientos de contratación pública, en cualquiera de sus fases: planeación, preparación, adjudicación, ejecución o cierre:

- Nombre completo,
- Genero,
- RFC,
- CURP,
- Nombre del puesto,
- Nivel del puesto,
- Ejercicio fiscal,
- Ramo,
- Nombre de la institución o dependencia,
- Siglas de la institución o dependencia,
- Clave de la institución o dependencia,

2. Personas servidoras públicas superiores jerárquicas de quienes participan directamente en los procesos de contratación, cuando sean responsables de autorizar, supervisar o validar dichos procedimientos:

- Nombre completo,
- RFC,
- CURP,
- Nombre del puesto,
- Nivel del puesto,
- Tipo de procedimiento,
- Tipo de área, y
- Nivel de responsabilidad.

sl

3. Relación de Particulares Inhabilitados. Esta información se integra conforme a lo dispuesto en el artículo 44, párrafo tercero, de la Ley General de Responsabilidades Administrativas (LGRA) y el artículo 44, párrafo tercero, de la Ley Local de Responsabilidades. De acuerdo con dichos preceptos, y en relación con los artículos 43, párrafo tercero, de la LGRA y 43, párrafo tercero, de la Ley Local, esta información no será pública en el Sistema 2 (S2) de la Plataforma Digital, sino que estará disponible únicamente para los servidores públicos autorizados, conforme al Catálogo de Perfiles del S2.

Los datos que obran en dicha relación son los siguientes:

1. Nombres y apellidos de la persona física, o bien, razón social de la persona moral, que se encuentre inhabilitada para celebrar contratos con entes públicos derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades.
2. Periodo de la inhabilitación.
3. Ente público al que pertenece la autoridad que impuso la inhabilitación.
4. Autoridad que impuso la inhabilitación.

c) Datos sensibles.

El Sistema 2 (S2) no trata datos personales sensibles, en los términos del artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y del artículo 3, fracción IX de

la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL). La información contenida en este sistema se limita a datos de identificación institucional y funcional de personas servidoras públicas en ejercicio de sus atribuciones, y se integra a partir de los registros y reportes oficiales generados por los entes públicos obligados, conforme a los criterios establecidos en los Lineamientos Técnicos de la Plataforma Digital Nacional (PDN).

No obstante, se implementan medidas técnicas, administrativas y organizativas adecuadas para garantizar que el tratamiento de los datos personales —aun cuando no sean sensibles— cumpla con los principios de licitud, finalidad, proporcionalidad, seguridad y responsabilidad, minimizando los riesgos de uso indebido, alteración, pérdida, destrucción o acceso no autorizado. Estas medidas se encuentran alineadas con los estándares previstos en la legislación aplicable, así como en las mejores prácticas nacionales e internacionales en materia de protección de datos personales.

De conformidad con lo dispuesto en el artículo 3, fracción X de la Ley General de Protección de Datos Personales, y el artículo 3, fracción XI de la Ley Local de Protección de Datos, se consideran datos sensibles aquellos que se relacionan con la esfera más íntima de su titular, o cuya utilización pueda dar lugar a discriminación o implique un riesgo grave para éste.

En este contexto, se consideran datos sensibles aquellos que se recaban como parte de la relación con personas físicas que se encuentren inhabilitadas para celebrar contratos con entes públicos, derivado de procedimientos administrativos distintos a los previstos en la Ley General de Responsabilidades Administrativas (LGRA) y en la Ley Local de Responsabilidades. Tal como se describió en el numeral III anterior, esta



información reviste carácter sensible, ya que su divulgación podría propiciar un trato diferenciado e injustificado, derivando en actos de discriminación por parte de particulares que, al conocer dicha sanción, podrían negar o dificultar su contratación en el ámbito privado.

Además, la publicidad de dicha información podría implicar una afectación injustificada a los derechos de la persona inhabilitada, al configurarse en los hechos una sanción no prevista expresamente en la ley, con efectos infamantes, lo cual contravendría lo dispuesto en los artículos 14, párrafo tercero, y 20, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos.

Es importante precisar que, conforme a los artículos 43, párrafo tercero, en relación con el 44, párrafo tercero de la LGRA, así como de la Ley Local de Responsabilidades, los datos sensibles en cuestión no deberán ser objeto de publicidad. Su acceso estará restringido exclusivamente a los servidores públicos autorizados conforme al Catálogo de Perfiles del Sistema 2 (S2), para fines de prevención, investigación y sanción de faltas administrativas y hechos de corrupción, así como para garantizar el cumplimiento de los principios y condiciones establecidos en el artículo 134, párrafos primero, tercero y cuarto de la Constitución Federal.

F. Finalidades del tratamiento de los datos personales

El tratamiento de datos personales en el Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, como parte del Sistema Estatal de Información (SEI) del Estado de Nuevo León, obedece a finalidades determinadas, explícitas y legítimas, en apego a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

(LGPDPESO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL), y los Lineamientos aplicables emitidos por el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL).

1. Finalidades primarias

Las siguientes finalidades son indispensables para el funcionamiento del sistema, el cumplimiento de obligaciones legales y la colaboración institucional con la Plataforma Digital Nacional:

- Registrar, sistematizar y poner a disposición pública la información relativa a personas servidoras públicas que intervengan en cualquiera de las fases de los procedimientos de contratación pública, conforme a los lineamientos técnicos de la PDN y los principios del Sistema Nacional Anticorrupción.
 - a) Garantizar la interoperabilidad del Sistema 2 (S2) con la Plataforma Digital Nacional (PDN), mediante el envío y actualización periódica de los datos públicos, a través de mecanismos electrónicos de consulta en tiempo real (API).
 - b) Prevenir conflictos de interés, favoreciendo la transparencia en los procesos de contratación pública, mediante la consulta automatizada del personal involucrado en cada etapa del procedimiento.
 - c) Fortalecer los mecanismos institucionales de control, vigilancia, rendición de cuentas y combate a la corrupción, brindando a los

órganos internos de control, entes fiscalizadores y órganos de gobierno una herramienta para la trazabilidad de las decisiones administrativas.

- d) Facilitar la consulta pública y verificable sobre la participación de servidores públicos en contrataciones, en cumplimiento del principio de máxima publicidad establecido en la legislación en materia de transparencia y responsabilidades administrativas.
- e) Atender requerimientos institucionales derivados de auditorías, revisiones, investigaciones, solicitudes de información, acciones de control interno, o procedimientos administrativos o legales.

2. Finalidades secundarias (*cuando aplique*)

En caso de autorización expresa de los titulares o si resultan compatibles con las finalidades primarias, podrán llevarse a cabo los siguientes tratamientos adicionales:

- a) Elaboración de estadísticas, reportes y productos analíticos para evaluar el comportamiento institucional en materia de integridad en las contrataciones públicas.
- b) Desarrollo de herramientas de análisis que permitan identificar patrones, riesgos o áreas críticas en los procesos de contratación, así como posibles focos de conflicto de interés.



- c) Generación de insumos para el diseño, seguimiento y evaluación de políticas públicas orientadas al fortalecimiento de la legalidad, la eficiencia administrativa y la integridad pública.

La ejecución de estas finalidades secundarias se realizará conforme a lo establecido en el Aviso de Privacidad Integral correspondiente, asegurando que en ningún caso se vulneren los derechos de los titulares ni se contravengan los principios de finalidad, proporcionalidad y lealtad en el tratamiento de los datos personales.

G. SUJETOS RESPONSABLES DEL TRATAMIENTO DE LOS DATOS PERSONALES

1. Responsable del Tratamiento

La Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Nuevo León (SESEA-NL) será la responsable del tratamiento de los datos personales en el Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, en virtud de que:

- a) Administra y coordina el funcionamiento del sistema como parte del Sistema Estatal de Información (SEI);
- b) Determina los fines y medios del tratamiento de los datos personales contenidos en el sistema;
- c) Supervisa la correcta operación del sistema y el cumplimiento de las medidas técnicas, organizativas y administrativas de protección de datos;

- d) Garantiza el cumplimiento de los principios, deberes y derechos previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en la legislación estatal aplicable.

2. Encargados del tratamiento

Se considerarán encargados del tratamiento aquellos entes públicos, unidades administrativas u operadores técnicos que:

- a) Actúen bajo las instrucciones de la SESEA-NL para el tratamiento de datos personales, en términos del contrato, convenio o designación correspondiente;
- b) Brinden servicios especializados relacionados con el desarrollo, mantenimiento, soporte, interoperabilidad, seguridad o infraestructura del Sistema S2;
- c) Cumplan con las cláusulas de confidencialidad, integridad, disponibilidad y no reutilización de los datos personales con fines distintos a los autorizados.

H. TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES.

En cumplimiento con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL), así como los Lineamientos emitidos por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Nuevo León (INFONL), se establecen las

siguientes disposiciones relativas a las transferencias y remisiones de datos personales efectuadas en el Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, parte del Sistema Estatal de Información (SEI).

1. Definición y alcance

Las transferencias y remisiones de datos personales se entienden como los actos mediante los cuales se comunican, transmiten o ceden datos personales a un tercero, sea éste una autoridad pública o un particular, para su tratamiento conforme a los fines del Sistema S2 y a lo establecido en el marco jurídico vigente.

Estas acciones se ejecutan con el propósito de permitir la interoperabilidad, fiscalización, verificación administrativa, difusión pública o colaboración institucional, en el marco de las obligaciones de transparencia, integridad pública y rendición de cuentas en los procedimientos de contratación.

2. Criterios para la transferencia

- Las transferencias se realizarán únicamente cuando sean necesarias, pertinentes y proporcionales para el cumplimiento de las finalidades del Sistema S2.
- Se garantizará que los destinatarios de la información cumplan con las medidas legales, técnicas y administrativas necesarias para proteger los datos personales transferidos.
- Las transferencias se limitarán a los datos estrictamente necesarios, conforme a los principios de proporcionalidad y minimización del tratamiento.

- Las finalidades de la transferencia deberán ser compatibles con las finalidades originales del tratamiento en el Sistema S2.
- Los titulares de los datos serán informados sobre las transferencias mediante el Aviso de Privacidad Integral correspondiente.

3. Categorías de terceros receptores

- La Plataforma Digital Nacional (PDN), para efectos de consulta e interoperabilidad conforme al artículo 49 de la Ley del Sistema Estatal Anticorrupción y los Lineamientos Técnicos de la Plataforma.
- Entes públicos estatales y municipales con atribuciones de control interno, auditoría, fiscalización o contratación pública, que requieran consultar o verificar la participación de servidores públicos en procedimientos de contratación.
- Autoridades jurisdiccionales o administrativas, cuando la información sea requerida en el marco de investigaciones, procedimientos legales o revisiones institucionales.
- Proveedores de servicios tecnológicos, en su carácter de encargados del tratamiento, que brinden servicios de desarrollo, mantenimiento, alojamiento o soporte técnico del sistema.
- Órganos garantes en materia de transparencia y protección de datos personales, para la atención de recursos, verificaciones o procedimientos legales.

sl

4. Medidas para garantizar la protección en las transferencias

- Celebración de convenios, contratos o cláusulas de corresponsabilidad y confidencialidad, que regulen el uso, resguardo y limitaciones en el tratamiento de los datos transferidos.

- Implementación de protocolos de verificación, seguimiento y supervisión sobre las condiciones bajo las cuales se efectúan las transferencias y remisiones.
- Establecimiento de procedimientos para restringir, suspender o revocar el acceso a datos, en caso de incumplimiento contractual, incidente de seguridad o riesgo para los derechos de los titulares.
- Ejecución de acciones de capacitación continua a los terceros receptores, respecto a las obligaciones derivadas de la legislación aplicable en materia de protección de datos personales.

I. DERECHOS ARCO Y PROCEDIMIENTOS PARA SU EJERCICIO

En cumplimiento con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSO), así como en los Lineamientos emitidos por el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales, se garantiza a los titulares de los datos personales tratados en el Sistema Estatal de Información de Servidores Públicos que intervengan en procedimientos de contrataciones públicas (S2) el ejercicio de sus derechos ARCO: Acceso, Rectificación, Cancelación y Oposición.

1. Derecho de Acceso

Los titulares tienen derecho a conocer qué datos personales están siendo tratados, así como las finalidades, las personas o entidades a quienes se han transferido, y las medidas de seguridad aplicadas.



2. Derecho de Rectificación

Los titulares pueden solicitar la corrección de datos personales inexactos o incompletos, con la finalidad de que la información sea veraz y actualizada.

3. Derecho de Cancelación

Los titulares pueden solicitar la supresión de sus datos personales cuando consideren que no están siendo tratados conforme a la normativa aplicable o cuando hayan dejado de ser necesarios para la finalidad por la cual fueron recabados.

4. Derecho de Oposición

Los titulares pueden oponerse al tratamiento de sus datos personales en casos específicos, conforme a lo previsto en la ley y siempre que existan motivos legítimos.

Procedimientos para el Ejercicio de Derechos ARCO

El titular de los datos personales cuenta con la posibilidad de ejercer en todo momento los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), así como el de portabilidad de los datos, ya sea por su propia cuenta o por medio de su representante.

Cuando los ejerza directamente, deberá acreditar su identidad. Cuando los ejerza a través de un representante, este último deberá acreditar tanto su identidad, así como la del titular, y su personalidad (mediante instrumento público o carta poder simple, firmada ante dos testigos, anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción de



este, o declaración en comparecencia personal del titular ante la Unidad Transparencia).

En ese sentido, el titular tiene el derecho a acceder a los datos personales que obren en posesión del área administrativa correspondiente y a conocer la información relacionada con las condiciones y generalidades de su tratamiento (*Acceso*).

Asimismo, los titulares de datos personales cuentan en todo momento con la posibilidad legal de solicitar la corrección de su información personal, en caso de que este desactualizada, sea inexacta o incompleta (*Rectificación*).

Igualmente, puede solicitar que se elimine su información de los registros o bases de datos, cuando consideren que la misma no está siendo utilizada conforme a los principios, deberes previstos en los Lineamientos sobre principios y deberes de protección de datos personales en posesión de los sujetos obligados, así como en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. También, cuando hayan dejado de ser necesarios para la finalidad para la cual fueron recabados (*Cancelación*).

Finalmente, pueden oponerse al uso de sus datos personales para fines específicos cuando se cause un daño o perjuicio al titular, o estos produzcan efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades (*Oposición*). Estos derechos se encuentran ligados al tratamiento de sus datos personales, y se conocen comúnmente como derechos ARCO.

sl

En atención al artículo 63 de la Ley de Protección Datos Personales en Posesión de Sujetos Obligados, la solicitud de derechos ARCO, deberá contener los requisitos mínimos que se detallan a continuación:

- I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
- IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular;
- VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Las solicitudes pueden presentarse de forma presencial en la Unidad de Transparencia de la SESEANL, ubicada en Escobedo 637, zona Centro, Monterrey, N.L., C.P. 64000, teléfono 81 3143 7710, en un horario de lunes a viernes de 9:00 a 17:00 horas; o a través de la Plataforma Nacional de Transparencia: <http://www.plataformadetransparencia.org.mx> o en su caso, a través del siguiente correo electrónico: transparencia@seseanl.gob.mx



J. Conservación y plazos de retención de datos.

En cumplimiento con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSOENL), y los Lineamientos emitidos por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Nuevo León (INFONL), se establecen las siguientes políticas y procedimientos respecto a la conservación y retención de los datos personales tratados en el Sistema 2 (S2) del Sistema Estatal de Información (SEI):

1. Principios rectores

- **Limitación en el tiempo:** Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades legales, administrativas y de transparencia pública, incluyendo las obligaciones de interoperabilidad con la Plataforma Digital Nacional.
- **Seguridad y confidencialidad:** Durante el periodo de conservación, los datos estarán protegidos mediante medidas de seguridad técnicas, físicas y administrativas que prevengan su pérdida, acceso no autorizado, uso indebido o alteración.
- **Minimización:** Solo se conservarán los datos pertinentes, adecuados y estrictamente necesarios en función de las finalidades del Sistema S2, en apego a los principios establecidos en la legislación aplicable en materia de protección de datos personales.

2. Plazos específicos de conservación

- **Datos de personas servidoras públicas que intervienen en procedimientos de contratación:** Serán conservados por un periodo mínimo de cinco años, contados a partir de la conclusión del procedimiento de contratación correspondiente o de la última intervención registrada de la persona servidora pública. Este plazo podrá extenderse en caso de que existan disposiciones específicas en materia de archivos, responsabilidades administrativas o fiscalización.
- **Datos vinculados con procedimientos de contratación en curso:** Permanecerán activos en el sistema hasta que dichos procedimientos concluyan formalmente y se hayan agotado los plazos de revisión o prescripción establecidos en la legislación aplicable.
- **Datos cuya conservación ya no sea necesaria:** Una vez cumplida la finalidad del tratamiento, los datos serán eliminados o anonimizados conforme a procedimientos institucionales que garanticen la seguridad y legalidad de la supresión, de acuerdo con la normativa de protección de datos y gestión documental.

3. Procedimientos para la conservación, revisión y eliminación

- **Almacenamiento seguro:** Los datos serán almacenados en plataformas tecnológicas seguras, con mecanismos de respaldo, control de acceso y trazabilidad conforme a estándares técnicos y normativos.

2

- **Revisión periódica:** Se realizarán auditorías internas y revisiones al menos una vez al año, para identificar datos que deban ser depurados, eliminados o anonimizados conforme a los criterios de la política vigente.
- **Eliminación y anonimización:** Se aplicarán métodos seguros e irreversibles de destrucción o anonimización, como el borrado seguro en medios digitales o la destrucción física de registros impresos, garantizando que no sea posible su reconstrucción o identificación.
- **Registro de acciones:** Todas las actividades relacionadas con la supresión, modificación o depuración de datos serán documentadas mediante bitácoras o registros de control para fines de auditoría y rendición de cuentas.

4. Responsabilidades

- La Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León (SESEA-NL), en su calidad de responsable del tratamiento, será la encargada de implementar, actualizar y supervisar el cumplimiento de esta política de conservación.
- El Responsable de Protección de Datos Personales (RPD) de la SESEA-NL será responsable de verificar el cumplimiento de los plazos establecidos, así como de supervisar los procesos de eliminación o anonimización, conforme a las disposiciones legales, los principios rectores y las mejores prácticas en la materia.

K. EVALUACIÓN DE RIESGOS Y MEDIDAS DE MITIGACIÓN

Conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los artículos correlativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, así como en cumplimiento de los Lineamientos emitidos por el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León (INFONL), se realiza la presente evaluación de riesgos inherentes y se establecen las medidas preventivas, correctivas y de mitigación necesarias, con el fin de salvaguardar los derechos y libertades de los titulares cuyos datos personales son tratados en el Sistema 2 (S2) de Personas Servidoras Públicas que intervienen en contrataciones públicas del Sistema Estatal de Información (SEI).

Dado que este sistema implica el tratamiento intensivo y sistemático de datos personales relacionados con sanciones administrativas definitivas —por faltas graves y no graves— impuestas a personas físicas, morales y servidores públicos, su análisis de riesgos se orienta a garantizar la seguridad, legalidad, proporcionalidad, confidencialidad, transparencia y responsabilidad en el tratamiento, publicación e interoperabilidad de dicha información, especialmente por su carácter sensible y su potencial impacto reputacional, jurídico y social sobre los titulares involucrados.

sl

Identificación y Análisis de Riesgos

Se identifican los siguientes riesgos inherentes al tratamiento de datos personales en el S2, considerando la naturaleza, volumen, sensibilidad y finalidad del tratamiento:

Riesgo	Descripción	Impacto Potencial	Probabilidad	Nivel de Riesgo
Acceso no autorizado	Posible acceso al sistema o base de datos por personas no autorizadas	Divulgación indebida, pérdida de confidencialidad	Media	Alto
Pérdida o destrucción accidental	Fallas técnicas, incidentes de hardware o software que provoquen pérdida de datos	Interrupción del servicio, pérdida de información	Baja	Medio
Modificación no autorizada	Alteración o manipulación de datos personales sin autorización	Dato inexacto o alterado, afectación a la integridad	Media	Alto
Divulgación indebida	Publicación o transmisión de	Violación a la privacidad y	Baja	Alto

sl

Riesgo	Descripción	Impacto Potencial	Probabilidad	Nivel de Riesgo
	datos personales fuera del marco legal	derechos de los titulares		
Uso indebido por terceros	Tratamiento de datos por encargados o terceros no conforme	Vulneración de derechos y sanciones legales	Baja	Medio
Incumplimiento normativo	Falta de cumplimiento de obligaciones legales y reglamentarias	Sanciones administrativas y daño reputacional	Baja	Alto

Medidas de Mitigación

Para minimizar y controlar los riesgos identificados, la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León implementa las siguientes medidas, alineadas con el principio de responsabilidad proactiva:



1. Medidas Administrativas

- Capacitación continua al personal sobre protección de datos y obligaciones legales.

- Designación de responsables y enlaces en materia de protección de datos.
- Protocolos de autorización y control para accesos y modificaciones.
- Elaboración y actualización periódica de políticas y lineamientos internos.

2. Medidas Técnicas

- Implementación de sistemas de autenticación robusta.
- Cifrado de datos en tránsito y en reposo con estándares criptográficos vigentes.
- Monitoreo constante de accesos y actividades en el sistema.
- Respaldo periódico de información con almacenamiento seguro y recuperación ante desastres.
- Realización de pruebas de vulnerabilidades y auditorías de seguridad regulares.

3. Medidas Físicas

- Control de acceso físico a instalaciones y servidores.
- Seguridad en la custodia de medios físicos y documentos que contengan datos personales.
- Protocolos para disposición segura y destrucción de documentos y soportes electrónicos.

4. Medidas Contractuales

- Inclusión de cláusulas de confidencialidad y protección de datos en contratos con proveedores, encargados y terceros.
- Evaluación y supervisión del cumplimiento de obligaciones por parte de encargados y terceros relacionados.

Monitoreo y Revisión Continua

La SESEA-NL establece un mecanismo permanente de monitoreo y evaluación para verificar la eficacia de las medidas implementadas, así como la identificación temprana de nuevas amenazas y vulnerabilidades, adaptándose a los cambios tecnológicos, normativos y operativos.

Se realizarán revisiones anuales o cuando circunstancias extraordinarias lo requieran, asegurando la mejora continua del programa de protección de datos personales y el cumplimiento estricto del marco jurídico vigente.

PROCEDIMIENTOS DE ATENCIÓN A INCIDENTES

Con el fin de garantizar la protección y seguridad de los datos personales tratados en (S2), se establecen los siguientes procedimientos para la atención oportuna y adecuada de incidentes relacionados con la seguridad de la información:

a) Identificación y notificación

- Cualquier sospecha o detección de incidente de seguridad deberá ser reportada inmediatamente al responsable de la protección de datos personales o al área de seguridad informática.
- Se establecerán canales claros para la notificación interna de incidentes.



b) Evaluación del incidente

- Se realizará una evaluación rápida para determinar el alcance, gravedad y posible impacto del incidente sobre los datos personales y los derechos de los titulares.
- Se clasificará el incidente según su nivel de riesgo (bajo, medio, alto).

c) Contención y mitigación

- Se tomarán medidas inmediatas para contener el incidente y evitar su propagación o escalamiento.
- Se implementarán acciones correctivas para mitigar los daños ocasionados.

d) Comunicación a las autoridades y titulares

- En caso de incidentes con impacto significativo, se notificará al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León (INFONL), conforme a los plazos y procedimientos establecidos en la normatividad aplicable.
- Se informará a los titulares afectados, cuando exista un riesgo real para sus derechos y libertades, proporcionando las recomendaciones necesarias para protegerse.

e) Registro y documentación

- Todos los incidentes deberán ser documentados en un registro interno que incluya detalles del suceso, acciones tomadas, resultados y lecciones aprendidas.

- Esta documentación será base para la revisión y mejora continua de los controles de seguridad.

f) Revisión y mejora

- Después de la atención del incidente, se realizará un análisis para identificar causas raíz y fortalecer las medidas preventivas y correctivas del sistema.
- Se promoverá la capacitación continua del personal sobre manejo y prevención de incidentes de seguridad.

L. Medidas de seguridad.

En cumplimiento con lo dispuesto en los artículos 25, 26 y 27 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y los artículos correlativos de la Ley local del Estado de Nuevo León, así como conforme a los Lineamientos emitidos por el Instituto de Transparencia y Acceso a la Información Pública del Estado de Nuevo León, se describen a continuación las medidas de seguridad implementadas para proteger los datos personales tratados en el (S2).

Estas medidas están orientadas a garantizar la confidencialidad, integridad y disponibilidad de los datos personales, en atención a su nivel de sensibilidad, volumen, tratamiento y riesgo asociado.

1. Medidas Administrativas

- Designación de un Enlace de Protección de Datos Personales dentro de la SESEA-NL.
- Elaboración y difusión del Aviso de Privacidad Integral del sistema S2.

- Capacitación periódica al personal sobre el tratamiento adecuado de datos personales.
- Protocolos de actuación en caso de vulneraciones a la seguridad.
- Control de acceso basado en roles al sistema S2 para usuarios internos y externos.
- Clausulado de confidencialidad en contratos con encargados o desarrolladores tecnológicos.
- Bitácoras de registro de accesos y modificaciones a los datos dentro del sistema.

2. Medidas Físicas

- Instalaciones con acceso controlado y vigilancia para el resguardo de servidores físicos (si aplica).
- Controles de ingreso a centros de datos o salas técnicas restringidas exclusivamente a personal autorizado.
- Políticas de resguardo de documentos en medios físicos, bajo llave y con control de acceso.
- Protocolo de disposición segura de documentos físicos y medios electrónicos obsoletos.

3. Medidas Técnicas

- Cifrado de la información en tránsito mediante protocolos SSL/TLS.
- Cifrado de base de datos en reposo con estándares AES-256 o equivalentes.
- Segmentación de redes internas y control de tráfico para prevenir accesos no autorizados.
- Respaldos automáticos y periódicos de la base de datos, con recuperación ante desastres.



- Registro de eventos de seguridad y monitoreo constante del sistema.
- Pruebas periódicas de vulnerabilidad y cumplimiento de parches de seguridad.

Estas medidas se determinan con base en el resultado del análisis de riesgo previsto en los artículos 27 y 29 de la LGPDPPSO, 38 y 41 de la LPDPPSONL y serán actualizadas conforme evolucionen las amenazas tecnológicas, los tratamientos realizados y los avances normativos aplicables.

Asimismo, la SESEA-NL se compromete a revisar anualmente la política de seguridad de la información del sistema S2 y realizar auditorías internas o externas en cumplimiento con el principio de responsabilidad proactiva y rendición de cuentas institucional.

M. Responsabilidades y roles.

Para asegurar una adecuada protección de los datos personales en (S2), se definen las siguientes responsabilidades y roles dentro del marco institucional:

a) Responsable del Tratamiento de Datos Personales

- Es la entidad o área que determina las finalidades y medios del tratamiento de datos personales dentro del S2.
- Tiene la obligación de garantizar el cumplimiento de la normativa aplicable en materia de protección de datos, supervisar las actividades de tratamiento y responder por cualquier incumplimiento.



b) Encargado del Tratamiento

- Es la persona o área designada para llevar a cabo las operaciones de tratamiento de datos personales bajo las instrucciones del responsable.
- Debe asegurar la correcta ejecución de las medidas de seguridad y confidencialidad establecidas.

c) Delegado o Enlace de Protección de Datos Personales

- Funciona como intermediario entre el responsable, los titulares de los datos y las autoridades en materia de protección de datos.
- Atiende las solicitudes y derechos ARCO de los titulares, así como las consultas y requerimientos del INFONL.
- Supervisa el cumplimiento de las políticas y procedimientos internos relacionados con la protección de datos.

d) Usuarios y Personal Operativo

- Todo el personal que tenga acceso al S2 debe cumplir con las políticas internas de protección de datos, así como con las medidas de seguridad establecidas.
- Deben reportar cualquier incidente o vulneración de seguridad y participar en programas de capacitación.

N. Nombre y cargo de los servidores públicos que autorizan la operación o modificación de la operación de la plataforma informática.

1. Mtro. Bernardo Sierra Gómez, Coordinador Ejecutivo encargado del despacho de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción

del Estado de Nuevo León, en calidad de administrador del Sistema Estatal de Información previsto en la Ley del Sistema Estatal, a la cual pertenece el S2.

2. Ing. Luis Antonio López García, Coordinador de Tecnologías de la Información, en calidad de responsable del funcionamiento y operación del Sistema Estatal de Información previsto en la Ley del Sistema Estatal, a la cual pertenece el S2.

2. JUSTIFICACIÓN DE LA NECESIDAD DE IMPLEMENTACIÓN DEL SISTEMA DE LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN CONTRATACIONES PÚBLICAS (S2)

La implementación del Sistema de los Servidores Públicos que Intervengan en Contrataciones Públicas (S2), como parte del Sistema Estatal de Información (SEI), se justifica en la necesidad de fortalecer los mecanismos de integridad, transparencia, control preventivo y rendición de cuentas en el ámbito de las contrataciones públicas, tanto a nivel estatal como municipal. Este sistema constituye un subsistema estratégico del SEI y es clave para el funcionamiento coordinado del Sistema Estatal Anticorrupción de Nuevo León (SEA-NL), así como para la interoperabilidad con la Plataforma Digital Nacional (PDN).

Su operación se sustenta en los principios constitucionales de legalidad, transparencia, rendición de cuentas, debida diligencia y protección de datos personales, previstos en la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política del Estado de Nuevo León, la Ley General de Responsabilidades Administrativas, la Ley General del Sistema Nacional Anticorrupción, la Ley del Sistema Estatal Anticorrupción de Nuevo León, y en

sl

las leyes general y local en materia de protección de datos personales en posesión de sujetos obligados.

La necesidad de este sistema se justifica por las siguientes consideraciones:

1. **Visibilización y trazabilidad de la participación de servidores públicos en contrataciones.** El S2 permite identificar con precisión a las personas servidoras públicas que participan en los procedimientos de contratación pública, en cualquiera de sus fases (planeación, preparación, adjudicación, ejecución o cierre), fortaleciendo la trazabilidad de las decisiones administrativas.
2. **Prevención de conflictos de interés y responsabilidades ocultas.** Contar con un registro estructurado de los funcionarios involucrados en las contrataciones permite detectar oportunamente conflictos de interés y evitar simulaciones, duplicidades o prácticas indebidas en el ejercicio de funciones.
3. **Instrumento clave para el control interno y la fiscalización.** El S2 dota a los órganos internos de control, auditorías superiores y entes fiscalizadores de una herramienta tecnológica que permite verificar la correcta participación y legalidad de las actuaciones de los servidores públicos involucrados en contrataciones.
4. **Cumplimiento de obligaciones derivadas del Sistema Nacional Anticorrupción.** El sistema responde a los lineamientos y criterios del Comité Coordinador del SNA y permite alimentar de manera automatizada la Plataforma Digital Nacional con información sobre los servidores públicos participantes en procesos contractuales.
5. **Fortalecimiento del derecho de acceso a la información pública.** La publicación sistemática de la participación de servidores públicos en

procedimientos de contratación pública permite a la ciudadanía ejercer una vigilancia informada sobre las decisiones gubernamentales.

6. **Mejora de la integridad y confianza institucional.**

La implementación del S2 promueve prácticas de gestión pública más abiertas, responsables y orientadas a la prevención de riesgos de corrupción, lo cual incrementa la confianza ciudadana en la administración pública.

7. **Cumplimiento de estándares internacionales en materia de contrataciones abiertas.** El S2 contribuye al cumplimiento de compromisos internacionales como los establecidos por la Alianza para el Gobierno Abierto, la OCDE y la Convención de las Naciones Unidas contra la Corrupción, en lo relativo a la integridad y transparencia en compras públicas.

8. **Apoyo a la generación de inteligencia institucional.** La información registrada por el sistema puede utilizarse para generar indicadores, estadísticas y reportes institucionales, que permitan orientar políticas públicas de integridad, eficiencia administrativa y profesionalización del servicio público.

9. **Interoperabilidad y modernización tecnológica.** Su diseño permite su articulación con otros sistemas del SEI, así como con la Plataforma Digital Nacional, garantizando eficiencia, consistencia y reutilización de datos institucionales a través de mecanismos interoperables.

10. **Protección adecuada de los datos personales tratados.** El tratamiento de datos personales dentro del S2 se realiza conforme a los principios de licitud, finalidad, proporcionalidad, calidad y responsabilidad, sin tratar datos sensibles ni realizar usos no autorizados, garantizando los derechos de los titulares.



En su conjunto, el Sistema 2 (S2) representa una pieza clave en el fortalecimiento del ecosistema estatal de integridad y contrataciones públicas abiertas, cuya implementación es indispensable para avanzar en el combate preventivo a la corrupción, el cumplimiento de la normatividad en materia de responsabilidades administrativas, y la consolidación de un gobierno más transparente y confiable en el Estado de Nuevo León.

3. REPRESENTACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES A TRATAR

Conforme a los principios establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Nuevo León (LPDPOSONL), los responsables del tratamiento deben identificar de manera clara y precisa las fases en que los datos personales serán recabados, tratados, conservados y, en su caso, suprimidos. Este mapeo del ciclo de vida de los datos es esencial para asegurar el cumplimiento del principio de responsabilidad.

En el caso del Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, el tratamiento de datos personales se da en el contexto de la identificación, registro, validación, consulta y seguimiento de las personas servidoras públicas que participan en las diversas etapas del procedimiento de contratación pública (planeación, preparación, adjudicación, ejecución o cierre).

a) Fases del ciclo de vida de los datos personales

1. Obtención

Los datos personales integrados en el Sistema 2 (S2) de los Servidores Públicos que Intervienen en Contrataciones Públicas son obtenidos de diversas fuentes documentales, electrónicas o digitales, proporcionadas por los entes públicos estatales y municipales que llevan a cabo procedimientos de contratación pública, en cualquiera de sus fases: planeación, preparación, adjudicación, ejecución o cierre.

La información es recabada directamente por las unidades administrativas responsables de los procedimientos de contratación, los órganos internos de control, u otras áreas designadas conforme a sus atribuciones. Esta recolección puede realizarse mediante plataformas de carga institucional, formularios estructurados conforme a los lineamientos del Catálogo de Datos del S2, o por mecanismos de interoperabilidad con otros sistemas del propio ente público o del Sistema Estatal de Información (SEI).

Conforme a lo establecido en el Capítulo II de las Bases para el funcionamiento del Sistema Estatal de Información y en las Bases para la Plataforma Digital Nacional, los datos personales pueden ser recabados por proveedores autorizados, quienes a su vez obtienen la información de las fuentes previamente mencionadas, garantizando su autenticidad y seguridad en la transferencia.

En los casos en que exista conexión con la Plataforma Digital Nacional (PDN), la integración de datos se realiza mediante mecanismos de transferencia segura y autenticada, en cumplimiento de las especificaciones técnicas del S2 y de las Bases del SEI.

2. Registro e ingreso al sistema

Los datos se capturan o integran en los formatos establecidos por el SEI, mediante interfaces electrónicas, integraciones automatizadas o carga documental, y se alojan en bases de datos estructuradas.

3. Almacenamiento y conservación

Los datos se resguardan en servidores seguros del SEA-NL bajo medidas técnicas y organizativas que garantizan su integridad, disponibilidad y confidencialidad. El almacenamiento se realiza conforme a los plazos legales de conservación de documentos administrativos y contratos.

4. Uso y tratamiento

Los datos personales integrados en el Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas son tratados exclusivamente para registrar, validar, sistematizar y consultar la información relativa a las personas servidoras públicas que participan en cualquiera de las fases de los procedimientos de contratación pública en el ámbito estatal y municipal.

Su uso se limita a:

- Dar cumplimiento a las obligaciones legales en materia de contrataciones públicas, transparencia, integridad y rendición de cuentas.

- Prevenir conflictos de interés y contrataciones indebidas, mediante la identificación y seguimiento de los servidores públicos que intervengan en los procedimientos.
- Facilitar la interoperabilidad con la Plataforma Digital Nacional (PDN) y otros subsistemas del Sistema Estatal de Información (SEI).
- Fortalecer los mecanismos institucionales de control, vigilancia, auditoría y fiscalización en los entes públicos.
- Contribuir a la generación de análisis, reportes y visualizaciones institucionales o públicas para el monitoreo de prácticas de integridad y cumplimiento normativo.

El tratamiento se lleva a cabo bajo los principios de licitud, finalidad, lealtad, proporcionalidad, calidad y responsabilidad, conforme a lo dispuesto en la LGPDPPSO, la LPDPPSOENL, y los Lineamientos Técnicos emitidos por el INFONL, garantizando en todo momento la protección de los derechos de los titulares.

5. Difusión y acceso público

En cumplimiento de la Ley de Transparencia, ciertos datos se hacen públicos en la Plataforma, previa aplicación de criterios de disociación, testado o clasificación, en caso de contener información confidencial o sensible.

6. Actualización y rectificación

Los datos pueden ser modificados o rectificados a solicitud del titular o por disposición de autoridad competente, conforme al procedimiento legal correspondiente.

7. Supresión o baja

Una vez cumplido el ciclo legal de conservación o cuando se declare su baja por obsolescencia, los datos se suprimen de forma segura mediante mecanismos técnicos que impidan su recuperación o reconstrucción no autorizada.

b) Fuentes internas y/o externas:

- Registros administrativos internos de los entes públicos estatales y municipales que documentan la participación de servidores públicos en cualquiera de las fases del procedimiento de contratación pública (planeación, preparación, adjudicación, ejecución o cierre).
- Sistemas institucionales de control interno, plataformas de gestión de contrataciones, módulos de planeación o seguimiento presupuestal, y otros sistemas de apoyo administrativo donde se documenten perfiles, atribuciones o actos relacionados con la intervención de servidores públicos en contrataciones.
- Reportes o validaciones emitidas por órganos internos de control, contralorías o unidades jurídicas responsables de verificar la legalidad de los procedimientos de contratación.
- Bases de datos y sistemas interoperables, incluyendo el Sistema Electrónico de Contrataciones Gubernamentales, plataformas estatales de transparencia o rendición de cuentas, así como la Plataforma Digital Nacional (PDN), en los módulos relacionados con contrataciones públicas.



c) Medios y procedimientos por los cuales se recabarán los datos personales, o que ya han sido recabados:

- Carga de información por parte de los entes públicos obligados (estatales y municipales) mediante formularios electrónicos habilitados en el Sistema Estatal de Información, conforme a las estructuras y campos establecidos por el formato S2 de la Plataforma Digital Nacional (PDN).
- Integración automatizada a través de interfaces de programación de aplicaciones (API) que permiten la interoperabilidad del S2 estatal con la PDN, asegurando el registro y actualización automática de los datos correspondientes.
- Captura directa de información contenida en actos administrativos, tales como oficios de designación, contratos, actas de adjudicación, resoluciones internas o dictámenes que acrediten la intervención de personas servidoras públicas en procedimientos de contratación pública.
- Remisión oficial de información por medios físicos o electrónicos institucionales, validada por los órganos internos de control o unidades administrativas responsables de las contrataciones, conforme a sus atribuciones y a los lineamientos técnicos del Sistema Estatal de Información.

d) Áreas, grupos o personas que llevarán a cabo procesos de tratamiento con los datos:

- **Unidades administrativas responsables de contrataciones públicas** en los entes obligados (estatales y municipales), encargadas

de registrar, cargar o validar la información de las personas servidoras públicas que intervienen en los procedimientos de contratación en cualquiera de sus fases.

- **Órganos internos de control y contralorías**, que verifican y supervisan la legalidad y validez de la información remitida, así como el cumplimiento de las obligaciones normativas en materia de integridad, transparencia y prevención de conflictos de interés.
- **Unidades de tecnologías de la información de los entes públicos**, responsables del soporte técnico, infraestructura, seguridad informática y operación de los módulos institucionales conectados al Sistema Estatal de Información (SEI) y su interoperabilidad con la Plataforma Digital Nacional (PDN).
- **La Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Nuevo León (SESEA-NL)**, como instancia responsable del tratamiento, resguardo, administración, coordinación e interoperabilidad del Sistema 2 (S2), en cumplimiento de lo dispuesto por las Bases del SEI y su Estatuto Orgánico.

e) Plazos de conservación o eliminación de los datos personales:

- Los datos personales recabados en el Sistema 2 (S2) serán conservados durante un periodo mínimo de **cinco años**, contados a partir de la fecha en que concluya el procedimiento de contratación pública en el que haya intervenido la persona servidora pública correspondiente, conforme a lo dispuesto en la Ley General de Archivos, la Ley de Archivos para el Estado de Nuevo León, y la normativa aplicable en materia de responsabilidades administrativas y fiscalización.



- En caso de que subsista un procedimiento legal, administrativo, de auditoría o fiscalización en curso relacionado con la contratación en cuestión, la conservación se extenderá hasta que se resuelva de forma definitiva la situación jurídica del acto.
- Una vez cumplido el plazo legal y si no existe una causa que justifique su conservación, los datos personales serán eliminados o anonimizados conforme a procedimientos institucionales seguros, respetando los principios de proporcionalidad, minimización y licitud del tratamiento.
- La **eliminación o anonimización** de datos se realizará bajo mecanismos que garanticen la **irreversibilidad** del tratamiento, evitando su recuperación, reproducción o reutilización indebida.

f) Técnicas que se utilizarán para garantizar el resguardo seguro de los datos personales:

- Cifrado de bases de datos.
- Control de accesos basado en roles.
- Auditorías y bitácoras de acceso.
- Respaldo y recuperación ante desastres.
- Pruebas de penetración y revisión continua de vulnerabilidades.
- Medidas de disociación para los datos publicados.

g) Técnicas que se utilizarán para garantizar el borrado seguro de los datos personales:

- Borrado lógico seguro (software).
- Borrado físico.

- Cifrado previo más destrucción de claves.
- Auditorías periódicas.
- Registros y validación de destrucción.
- Formación de personal sobre gestión de la información.

4. IDENTIFICACIÓN, ANÁLISIS Y DESCRIPCIÓN DE LA GESTIÓN DE LOS RIESGOS INHERENTES PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

1. Identificación y descripción de los riesgos administrativos, físicos o tecnológicos

En esta etapa se identifican los riesgos inherentes asociados a la operación del Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas, considerando la posibilidad de que comprometan la confidencialidad, integridad o disponibilidad de los datos personales tratados, ya sea por vulnerabilidades técnicas, errores humanos, accesos indebidos, fugas de información o actos maliciosos.

El tratamiento de datos en este sistema implica la recopilación, validación, sistematización e interoperabilidad de información que identifica a personas servidoras públicas que participan en procedimientos de contratación en cualquiera de sus fases. Dado que esta información puede tener implicaciones reputacionales, administrativas o incluso legales, el sistema debe prever los escenarios de riesgo más relevantes en el entorno institucional y tecnológico.



1.1 Riesgos administrativos identificados:

- Accesos no autorizados por ausencia de controles de roles y privilegios.
- Uso indebido de información por parte del personal con acceso a datos sensibles.
- Ausencia de políticas internas de privacidad o desconocimiento del personal sobre ellas.
- Falta de capacitación periódica sobre tratamiento adecuado de datos personales.
- Deficiencia en el registro y documentación de actividades de tratamiento de datos.

1.2 Riesgos físicos identificados:

- Acceso físico no controlado a instalaciones donde se almacenan datos o servidores.
- Robo, extravío o destrucción accidental de dispositivos de almacenamiento (USB, laptops, discos duros).
- Falta de sistemas de respaldo físico y control de acceso biométrico o con tarjeta.
- Riesgos de desastres naturales (incendio, inundación) sin planes de contingencia física.

1.3 Riesgos tecnológicos identificados:

- Vulnerabilidades en la aplicación web del sistema (ej. ataques de inyección SQL, XSS, CSRF).
- Deficiente cifrado de datos personales en tránsito o en reposo.
- Fallos en el control de sesiones y autenticación de usuarios.

- Ausencia de pruebas de seguridad (pentesting) periódicas.
- Integración con terceros sin mecanismos de aseguramiento contractual sobre el uso de datos.
- Uso de software obsoleto o sin actualizaciones de seguridad.
- Acceso remoto a sistemas sin autenticación robusta.
- Ausencia de respaldo de información y de protocolos de recuperación ante fallos o ataques cibernéticos.

2. Ponderación cuantitativa y/o cualitativa de la probabilidad e impacto

El responsable debe realizar un análisis de riesgos bajo criterios objetivos y sistemáticos que permitan determinar:

- **La probabilidad** de que cada riesgo identificado ocurra, usando escalas como: baja, media o alta.
- **El impacto** que tendría sobre la privacidad de los titulares si dicho riesgo se materializara, considerando: pérdida de confidencialidad, afectación a la integridad, acceso no autorizado, pérdida del control sobre los datos, afectaciones reputacionales o discriminación.

2.1 Metodología empleada para la valoración

Se utiliza una matriz de riesgos en donde se cruzan dos variables clave:



Variable	Escala utilizada	Criterios de referencia
Probabilidad de ocurrencia	Baja, Media, Alta	Con base en la frecuencia histórica, facilidad de explotación, nivel de exposición del sistema, controles existentes
Nivel de impacto	Bajo, Medio, Alto	En función del daño posible al titular, el volumen de datos afectados, el tipo de dato (identificativos, sensibles), consecuencias legales y reputacionales

El resultado de la ponderación determina el **nivel de riesgo residual** y sirve de base para seleccionar medidas de mitigación proporcionales.

2.2 Criterios específicos de análisis

Se adoptan los siguientes criterios de interpretación para cada variable:

- **Probabilidad Alta:** El riesgo es inminente o probable a corto plazo si no se implementan medidas adicionales.
- **Probabilidad Media:** El riesgo puede ocurrir bajo determinadas condiciones, o se ha presentado con baja frecuencia.
- **Probabilidad Baja:** El riesgo es excepcional o remoto, bajo un entorno de control maduro.
- **Impacto Alto:** Compromete datos sensibles, involucra a un gran número de titulares o tiene consecuencias legales o reputacionales graves.
- **Impacto Medio:** Puede afectar derechos de algunos titulares o generar sanciones menores.

- **Impacto Bajo:** Afecta datos no sensibles o el impacto es contenido fácilmente por las medidas implementadas.

2.3 Matriz de valoración de riesgos

A continuación, se presentan algunos de los riesgos previamente identificados, con su respectiva ponderación:

Riesgo identificado	Probabilidad	Impacto	Nivel de riesgo
Acceso no autorizado por personal interno	Alta	Alto	Crítico
Fugas de datos por errores de configuración	Media	Alto	Alto
Robo de dispositivos con datos	Media	Medio	Medio
Ausencia de política de privacidad institucional	Alta	Medio	Alto
Ataques de inyección SQL en plataforma	Alta	Alto	Crítico
Ausencia de respaldo cifrado y automatizado	Media	Alto	Alto
Fallas en control de sesiones	Media	Medio	Medio
Accesos físicos no controlados a servidores	Baja	Medio	Bajo/Medio

Esta clasificación permite establecer prioridades en la implementación de controles y dar cumplimiento al principio de responsabilidad proactiva (accountability).

2.4 Conclusión de la ponderación

Del análisis efectuado se concluye que:

- **Existen riesgos críticos y altos que deben ser mitigados de forma inmediata**, especialmente los relacionados con accesos indebidos, vulnerabilidades tecnológicas, y ausencia de controles internos documentados.
- La mayoría de los riesgos identificados **pueden reducirse a un nivel aceptable** mediante la implementación o fortalecimiento de medidas de seguridad administrativas, físicas y tecnológicas.
- Se recomienda realizar revisiones periódicas del análisis de riesgo y mantener actualizada la matriz de riesgos conforme evolucionen el sistema y sus funcionalidades.

3. Medidas y controles para eliminar, mitigar, transferir o retener los riesgos detectados

Una vez identificados y valorados los riesgos, el responsable deberá documentar y aplicar **controles organizacionales, físicos y técnicos** que reduzcan la probabilidad de ocurrencia o el impacto en caso de materialización. Las acciones deben ser proporcionales y adecuadas.

3.1 Tipología de medidas aplicadas por tipo de riesgo

A. Riesgos tecnológicos y de ciberseguridad

Estos riesgos representan la mayor concentración de exposición y se mitigan mediante:

Riesgo	Medidas técnicas de mitigación
Acceso no autorizado por terceros o personal interno	Implementación de control de acceso basado en roles (RBAC), autenticación multifactor (MFA) y bitácoras de acceso con análisis periódico.
Inyección NoSQL u otras vulnerabilidades	Validación estricta de entradas, uso de consultas parametrizadas o APIS seguras, sanitización de los datos, validaciones de tipo en el back-end, principio de menor privilegio, auditoría y monitoreo, cifrado y autenticación, actualización y parches.
Pérdida de disponibilidad de información	Respaldos automáticos, almacenados en sitios redundantes con cifrado AES-256 y políticas de restauración probadas periódicamente.
Fugas por dispositivos externos	Política de uso restringido de USB y cifrado en reposo de la información en equipos portátiles.
Uso de contraseñas débiles	Implementación de políticas robustas de contraseñas, rotación periódica y sistemas de bloqueo por intentos fallidos.

B. Riesgos organizacionales y administrativos

Estos se controlan a través de políticas, procedimientos y formación continua:

Riesgo	Medidas administrativas de mitigación
Falta de políticas institucionales	Desarrollo y difusión de políticas de privacidad, seguridad de la información, retención y destrucción segura de datos.
Capacitación insuficiente	Programas anuales obligatorios de capacitación en protección de datos personales y seguridad de la información para todo el personal.
Gestión deficiente de incidentes	Establecimiento de un protocolo de respuesta ante incidentes de seguridad, conforme al artículo 40 de la LGPDPSO.
Falta de control sobre encargados o terceros	Cláusulas contractuales con obligaciones específicas en materia de confidencialidad y seguridad, conforme al artículo 28.

C. Riesgos físicos y de infraestructura

Mitigados a través de controles físicos y operativos:

Riesgo	Medidas físicas de mitigación
Accesos no autorizados a servidores	Instalación en cuartos de servidores con control de acceso biométrico y video vigilancia.
Robo de dispositivos	Inventario controlado, señalización visible de confidencialidad y software de geolocalización/borrado remoto.

Riesgo	Medidas físicas de mitigación
Daños por siniestros	Plan de continuidad de operaciones (BCP), control de humedad, temperatura y protección contra incendios en infraestructura crítica.

3.2 Tratamiento de riesgos residuales: aceptar, transferir o eliminar

Algunos riesgos no pueden eliminarse completamente; por ello se aplican criterios de gestión residual:

- **Eliminar el riesgo:** En casos donde el tratamiento de ciertos datos no es indispensable, se aplica el principio de minimización, suprimiendo su recolección o conservación.
- **Mitigar el riesgo:** Implementando controles adicionales o redundantes que reduzcan la probabilidad de ocurrencia o su impacto.
- **Transferir el riesgo:** Mediante contratación de seguros de ciberseguridad o convenios con encargados que asuman parte de la responsabilidad bajo cláusulas específicas.
- **Aceptar el riesgo:** Solo cuando su nivel es **bajo** y cuenta con medidas de vigilancia continua, bajo evidencia documental que justifique la decisión ante el INFONL.



3.3 Instrumentación, seguimiento y evidencia documental

Para garantizar la trazabilidad, los controles implementados deben:

- Integrarse en un **Plan de Seguridad de la Información y Protección de Datos Personales**;
- Ser verificados periódicamente mediante auditorías internas;
- Contar con evidencia documental para su presentación ante el INFONL (bitácoras, políticas firmadas, reportes de prueba, capacitaciones, etc.);
- Ser revisados y actualizados conforme evolucionen las tecnologías o los tratamientos realizados por el sistema S2.

5. MECANISMOS Y PROCEDIMIENTOS QUE SERÁN ADOPTADOS PARA GARANTIZAR EL CUMPLIMIENTO NORMATIVO EN EL TRATAMIENTO MASIVO O RELEVANTE DE DATOS PERSONALES.

El Sistema (S2) del Sistema Estatal de Información adopta los siguientes mecanismos y procedimientos para asegurar que el tratamiento masivo y relevante de datos personales cumpla con el marco normativo vigente:

1. Designación del Responsable de Protección de Datos Personales (RPD) del Sistema:

Designar un responsable con autonomía técnica y operativa específico para el Sistema, encargado de coordinar, supervisar y garantizar el cumplimiento de la normativa en materia de protección de datos personales en todos los procesos relacionados con la operación y gestión del Sistema Estatal de Información.

2. Políticas, protocolos y procedimientos internos específicos para el Sistema:

Contar con políticas institucionales formalizadas y protocolos detallados que regulan el manejo, almacenamiento, procesamiento y difusión de datos personales contenidos en el Sistema (S2), asegurando medidas técnicas y organizativas adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos.

3. Evaluación de Impacto en la Protección de Datos Personales (EIPDP) aplicada al Sistema:

Realizar una evaluación exhaustiva que identifica los riesgos inherentes al tratamiento masivo de datos personales dentro del Sistema, evaluando su probabilidad e impacto, y definiendo las medidas preventivas, correctivas y mitigantes necesarias para minimizar dichos riesgos, conforme a los Lineamientos del INFONL y demás normativas aplicables.

4. Capacitación y sensibilización del personal involucrado en el Sistema:

Implementar programas de formación continua dirigidos a los operadores, administradores y demás personal relacionado con el Sistema, con la finalidad de fortalecer la cultura de protección de datos personales y asegurar el cumplimiento de las obligaciones legales específicas al manejo de información contenida en la Plataforma.



5. Procedimientos para la atención de derechos ARCO de los titulares de datos contenidos en el Sistema:

Establecer canales accesibles y procedimientos claros para que los titulares puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición respecto de sus datos personales almacenados en el Sistema, garantizando la respuesta en los plazos legales establecidos.

6. Mecanismos de supervisión, auditoría y control del Sistema:

Efectuar auditorías internas y revisiones periódicas para verificar el cumplimiento normativo y la efectividad de las medidas implementadas en el Sistema, asegurando la detección y corrección oportuna de posibles incumplimientos o vulnerabilidades.

7. Gestión de incidentes y brechas de seguridad en el Sistema:

Disponer de protocolos para la detección, registro, análisis, atención y notificación de incidentes que puedan afectar la seguridad de los datos personales tratados en el Sistema, incluyendo la obligación de informar a la autoridad competente conforme a la legislación vigente.

8. Actualización normativa y mejora continua del Sistema:

Mantener un proceso constante de revisión y actualización de políticas, protocolos y medidas técnicas del Sistema, acorde con los cambios legislativos, avances tecnológicos y mejores prácticas internacionales,

garantizando la protección adecuada de los datos personales a lo largo del tiempo.

9. Documentación, registro y conservación de evidencias relativas al Sistema:

Asegurar la conservación y disponibilidad de toda la documentación que demuestre el cumplimiento de los procesos y medidas implementadas en el Sistema, facilitando la validación y auditoría por parte del INFONL y otras autoridades competentes.

10. Cumplimiento normativo y rol del Oficial de Protección de Datos Personales

El responsable debe asegurar que todo el tratamiento de datos cumpla con:

- Principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales,
- Los derechos ARCO de los titulares,
- Y contar con la opinión del **Oficial de Protección de Datos Personales**, quien debe pronunciarse sobre la viabilidad del tratamiento, la suficiencia de las medidas de seguridad y la mitigación de riesgos.



6. LOS RESULTADOS DE LA O LAS CONSULTAS EXTERNAS QUE, EN SU CASO, SE EFECTÚEN.

De conformidad con lo dispuesto en los artículos 74 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 14, fracción VI y 21 de las Disposiciones administrativas del carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, no se realizaron consultas externas.

7. OPINIÓN DEL RESPONSABLE DE PROTECCIÓN DE DATOS PERSONALES (RPD)

Como Responsable de Protección de Datos Personales del Sistema 2 (S2) de los Servidores Públicos que Intervengan en Contrataciones Públicas del Sistema Estatal de Información del SEA-NL, y en ejercicio de mi autonomía técnica y operativa, manifiesto que he participado activamente en la elaboración y revisión integral de la presente Evaluación de Impacto en la Protección de Datos Personales (EIPDP).

He examinado los documentos normativos, operativos y técnicos que sustentan el tratamiento masivo y relevante de datos personales en el marco del funcionamiento del Sistema S2, incluyendo políticas institucionales, controles de seguridad implementados, bitácoras de auditoría, protocolos de interoperabilidad con la Plataforma Digital Nacional, y registros de cumplimiento normativo.

Con base en esta revisión, confirmo que:

- Se han identificado de forma clara y precisa los riesgos inherentes al tratamiento de datos personales que realiza el Sistema S2.
- Se han establecido medidas técnicas y organizativas adecuadas para mitigar dichos riesgos, conforme a los principios y deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la legislación local del Estado de Nuevo León.
- El tratamiento cumple con los principios de licitud, finalidad, proporcionalidad, seguridad, y responsabilidad, garantizando el respeto a los derechos de los titulares de los datos personales.
- Se ha integrado un esquema de mejora continua que contempla mecanismos de actualización normativa, revisión de procedimientos, y fortalecimiento de capacidades del personal.

Adicionalmente, se recomienda mantener y fortalecer las estrategias de capacitación continua al personal involucrado, así como revisar periódicamente los acuerdos de interoperabilidad, políticas de minimización de datos y protocolos de atención ante incidentes de seguridad.

Por lo anterior, emito opinión favorable para la validación y aprobación de la presente Evaluación de Impacto en la Protección de Datos Personales correspondiente al Sistema 2 (S2).

Fecha: 12 de agosto de 2025

Nombre y firma: Mtro. Bernardo Sierra Gómez

Coordinador Ejecutivo encargado del despacho de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León

8. CUALQUIER OTRA INFORMACIÓN O DOCUMENTOS QUE CONSIDERE CONVENIENTE HACER DEL CONOCIMIENTO DE LA COMISIÓN.

Adicionalmente a lo señalado en los apartados precedentes y documentación requisitada, se considera importante remitir en la presente evaluación de impacto respecto al sistema 2 del Sistema Estatal de Información, los siguiente:

Constitución Política de los Estados Unidos Mexicanos

<https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>

Constitución Política del Estado Libre y Soberano de Nuevo León

https://www.hcnl.gob.mx/trabajo_legislativo/leyes/pdf/CONSTITUCION%20POLITICA%20DEL%20ESTADO%20LIBRE%20Y%20SOBERANO%20DE%20NUEVO%20LEON.pdf?2023-05-29

Ley General del Sistema Nacional Anticorrupción

https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNA_200521.pdf

Ley General de Responsabilidades Administrativas

<https://www.diputados.gob.mx/LeyesBiblio/pdf/LGRA.pdf>

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

<https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

Ley del Sistema Estatal Anticorrupción para el Estado de Nuevo León

https://www.hcnl.gob.mx/trabajo_legislativo/leyes/

Ley de Responsabilidades Administrativas del Estado de Nuevo León

https://www.hcnl.gob.mx/trabajo_legislativo/leyes/pdf/LEY%20DE%20RESPONSABILIDADES%20ADMINISTRATIVAS%20DEL%20ESTADO%20DE%20NUEVO%20LEON.pdf?2023-01-27

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León

https://www.hcnl.gob.mx/trabajo_legislativo/leyes/pdf/LEY%20DE%20PROTECCION%20DE%20DATOS%20PERSONALES%20EN%20POSESION%20DE%20SUJETOS%20OBLIGADOS%20DEL%20ESTADO%20DE%20NUEVO%20LEON.pdf?2019-12-11

Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León

<https://seseanl.gob.mx/wp-content/uploads/ESTATUTO-ORGANICO-DE-LA-SECRETARIA-EJECUTIVA-DEL-SISTEMA-ESTATAL-ANTICORRUPCION.pdf>

Bases para el funcionamiento de la Plataforma Digital Nacional

https://www.dof.gob.mx/nota_detalle.php?codigo=5541802&fecha=23/10/2018#gsc.tab=0

Bases para el funcionamiento del Sistema Estatal de Información (SEI)

<https://seseanl.gob.mx/wp-content/uploads/DICTAMEN-QUE-CONTIENE-LAS-BASES-PARA-EL-FUNCIONAMIENTO-DEL-SISTEMA-ESTATAL-DE-INFORMACION-SEI.pdf>

Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales

https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018#gsc.tab=0

Acuerdo mediante el cual se aprueban los lineamientos sobre los principios y deberes de protección de datos personales en posesión de los sujetos obligados, emitido por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León

https://cotai.org.mx/descargas/mn/Acuerdo_Lineamientos_principios_deberes_DP_02_05_2019.pdf

Lineamientos de protección de datos personales para los sujetos obligados del Estado de Nuevo León, emitido por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León

https://cotai.org.mx/descargas/mn/Lineamientos_Proteccion_Datos_Personales_20_08_2020.pdf

Guía de Evaluación de Impacto de Privacidad, emitida por el Instituto de Transparencia y Acceso a la Información del Estado de Nuevo León
https://www.cotai.org.mx/descargas/mn/Guia_evaluacion_impacto_privacidad_05_10_2018.pdf

Monterrey, Nuevo León, a 13 de agosto de 2025.

Atentamente



SECRETARÍA
EJECUTIVA DEL
SISTEMA ESTATAL
ANTICORRUPCIÓN

Mtro. Bernardo Sierra Gómez

**Coordinador Ejecutivo Encargado del Despacho
de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción
del Estado de Nuevo León**