

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES DEL SISTEMA DE INFORMACIÓN PÚBLICA DE CONTRATACIONES (S6) 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 de Información Pública de Contrataciones (S6), como subsistema del Sistema Estatal de Información (SEI) del Sistema Estatal Anticorrupción del Estado de Nuevo León.

El Sistema de Información Pública de Contrataciones (S6) tiene por objeto registrar, sistematizar, actualizar, consultar, publicar e interoperar información pública relacionada con los procedimientos de contratación pública que realizan los entes públicos del Estado de Nuevo León y sus municipios, incluyendo las etapas de planeación, contratación pública, adjudicación, contrato y ejecución, así como la identificación de los actores involucrados en dichos procedimientos.

Su implementación responde a un enfoque de contrataciones abiertas, transparencia, rendición de cuentas, integridad pública y prevención de riesgos de corrupción, al permitir la trazabilidad de las decisiones y actuaciones relacionadas con los procedimientos de contratación pública, así como la disponibilidad de información útil, verificable e interoperable con la Plataforma Digital Nacional.

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 S6, conforme a 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 demás disposiciones aplicables en materia de protección de datos personales, transparencia, archivos, responsabilidades administrativas y contrataciones públicas.

El tratamiento de datos personales en el S6 se limita a la información necesaria, adecuada y proporcional para el cumplimiento de sus finalidades legales y operativas. La mayor parte de la información del sistema corresponde a información pública de procedimientos de contratación, datos institucionales, información económica, presupuestal, contractual y documental. En particular, la información relativa al nombre, cargo, función, rol, área de adscripción, correo electrónico institucional, teléfono institucional, domicilio oficial del ente público y demás datos de contacto institucionales de personas servidoras públicas, cuando se encuentre vinculada con el ejercicio de atribuciones públicas, procedimientos de contratación, uso de recursos públicos, transparencia, rendición de cuentas o datos abiertos, tendrá naturaleza de información pública o institucional, sin que deba equipararse automáticamente a información confidencial o privada.

Lo anterior no impide que el S6 pueda involucrar datos personales protegidos cuando la información se refiera a personas físicas en su esfera privada o no institucional, particularmente personas físicas proveedoras o contratistas, licitantes, oferentes, representantes legales, puntos de contacto particulares, beneficiarios finales o propietarios reales, así como domicilios particulares, correos electrónicos personales, teléfonos personales, identificadores no públicos, datos sensibles o información privada contenida indebidamente en campos abiertos, documentos, hitos o anexos del sistema.

En cumplimiento de sus obligaciones como responsable, la SESEA-NL desarrolla la presente Evaluación de Impacto como una herramienta preventiva que permite

valorar la licitud, proporcionalidad, necesidad, seguridad y responsabilidad del tratamiento de datos personales en el S6, estableciendo medidas técnicas, administrativas y organizativas orientadas a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y calidad de la información, así como la protección de los derechos de las personas titulares.

MARCO NORMATIVO

La presente evaluación se sustenta en un conjunto de disposiciones constitucionales, legales, administrativas y técnicas que rigen el tratamiento de datos personales en posesión de sujetos obligados, el funcionamiento del Sistema Estatal Anticorrupción, la interoperabilidad con la Plataforma Digital Nacional y la operación de los sistemas que integran el Sistema Estatal de Información.

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado Libre y Soberano de Nuevo León.
- 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 General del Sistema Nacional Anticorrupción.
- Ley del Sistema Estatal Anticorrupción para el Estado de Nuevo León.
- Ley General de Responsabilidades Administrativas.
- Ley de Responsabilidades Administrativas del Estado de Nuevo León.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.
- Ley General de Archivos y Ley de Archivos para el Estado de Nuevo León.
- Bases para el Funcionamiento de la Plataforma Digital Nacional.

- Bases para el Funcionamiento del Sistema Estatal de Información.
- Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León.
- Lineamientos, criterios y disposiciones aplicables emitidos por el órgano garante local en materia de protección de datos personales.
- Especificaciones Técnicas aplicables al Sistema de Información Pública de Contrataciones (S6).

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 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 las disposiciones administrativas aplicables para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, se proporciona la siguiente información.

A. Denominación del sujeto obligado responsable del tratamiento

Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León (SESEA-NL).

B. Nombre del proyecto



Sistema de Información Pública de Contrataciones (S6) del Sistema Estatal de Información (SEI).

C. Objetivos generales y específicos que persigue el sistema

Objetivo general

El objetivo general del Sistema de Información Pública de Contrataciones (S6) es permitir el registro, actualización, sistematización, consulta, publicación e interoperabilidad de la información pública relacionada con los procedimientos de contratación pública de los entes públicos del Estado de Nuevo León y sus municipios, conforme a las disposiciones aplicables del Sistema Nacional Anticorrupción, el Sistema Estatal Anticorrupción, la Plataforma Digital Nacional y el Sistema Estatal de Información.

El S6 opera como un subsistema interoperable del Sistema Estatal de Información, mediante el cual se incorporan datos de los procedimientos de contratación pública en sus distintas etapas, incluyendo actores involucrados, planeación, contratación pública, adjudicación, contrato y ejecución contractual, con el propósito de fortalecer la transparencia, la integridad, la rendición de cuentas, la trazabilidad del gasto público y la prevención de riesgos de corrupción.

Objetivos específicos

1. Registrar y sistematizar la información de los procedimientos de contratación pública conforme a los formatos, catálogos, lineamientos y especificaciones técnicas aplicables al S6.
2. Permitir la consulta pública de información sobre contrataciones, contratos, adjudicaciones, proveedores, contratistas, actores involucrados, montos,

documentos, hitos, modificaciones y ejecución contractual, en términos de la normatividad aplicable.

3. Garantizar la interoperabilidad del S6 con la Plataforma Digital Nacional y con los demás componentes del Sistema Estatal de Información, mediante mecanismos técnicos que permitan la consulta, actualización y disponibilidad de datos conforme a los estándares aplicables.
4. Fortalecer la transparencia y la rendición de cuentas en los procedimientos de contratación pública, favoreciendo la trazabilidad de las decisiones administrativas y de los recursos públicos ejercidos.
5. Prevenir riesgos de corrupción, conflictos de interés, simulación, opacidad o discrecionalidad indebida en los procedimientos de contratación pública, mediante la publicación ordenada y estructurada de información relevante.
6. Garantizar que el tratamiento de datos personales que resulte necesario para la operación del S6 se realice conforme a los principios de licitud, finalidad, proporcionalidad, minimización, calidad, seguridad y responsabilidad.
7. Generar insumos para reportes, estadísticas, análisis institucionales, evaluaciones de integridad pública y políticas públicas orientadas a mejorar los procesos de contratación y adquisiciones públicas.

D. Fundamento legal de la plataforma informática que implica tratamiento relevante de datos personales

El fundamento legal del Sistema de Información Pública de Contrataciones (S6) se integra, entre otras disposiciones, por los artículos 113 de la Constitución Política de los Estados Unidos Mexicanos; 201 de la Constitución Política del Estado Libre y Soberano de Nuevo León; 49, fracción VI, y 51, párrafo segundo, de la Ley General del Sistema Nacional Anticorrupción; 44 y 45 de la Ley General de Responsabilidades Administrativas; 42, fracción X, y 49 de la Ley del Sistema Estatal Anticorrupción del Estado de Nuevo León; 44 y 45 de la Ley de

sl

Responsabilidades Administrativas del Estado de Nuevo León; 63 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; 24, fracción XVIII, del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Nuevo León; así como los artículos 5, fracción VI, 16, 17, 18, 19, 20, 22, 23, 24, 25, 50, 51 y 52 de las Bases para el Funcionamiento del Sistema Estatal de Información.

Este marco jurídico reconoce al Sistema de Información Pública de Contrataciones como un componente de la Plataforma Digital Nacional y del Sistema Estatal de Información, orientado a integrar, sistematizar, publicar e interoperar información relativa a contrataciones públicas, conforme a los principios de transparencia, máxima publicidad, datos abiertos, integridad, eficiencia, rendición de cuentas y protección de datos personales.

Asimismo, este fundamento faculta a la SESEA-NL para coordinar, administrar y supervisar el funcionamiento del Sistema Estatal de Información, así como para establecer los instrumentos técnicos, administrativos y operativos necesarios para la implementación de los sistemas que lo integran, incluyendo el S6, sin perjuicio de las obligaciones que correspondan a los entes públicos en la carga, actualización, verificación y conservación de la información que generen en el ejercicio de sus atribuciones.

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

En el marco del funcionamiento del S6, la información principal corresponde a procedimientos de contratación pública, presupuestos, documentos, montos, métodos de contratación, etapas, hitos, modificaciones, adjudicaciones, contratos y ejecución contractual. Para efectos de esta evaluación, deberá distinguirse entre la

información pública o institucional vinculada con personas servidoras públicas y los datos personales protegidos de personas físicas en su esfera privada o no institucional.

La información relativa al nombre, cargo, función, rol, área de adscripción, correo electrónico institucional, teléfono institucional, domicilio oficial del ente público y demás datos de contacto institucionales de personas servidoras públicas, cuando se encuentre vinculada con el ejercicio de atribuciones públicas, procedimientos de contratación, decisiones administrativas, uso de recursos públicos, transparencia, rendición de cuentas o datos abiertos, tendrá naturaleza de información pública o institucional, sin que deba equipararse automáticamente a información confidencial o privada. Lo anterior no impide que se adopten medidas de seguridad y calidad respecto de dicha información, ni que se protejan datos privados, sensibles, excesivos o no necesarios que pudieran incorporarse indebidamente en documentos, campos abiertos o anexos del sistema.

El tratamiento de datos personales en el S6 se limita a información necesaria, adecuada y proporcional para cumplir las finalidades legales y operativas del sistema, sin que se autorice la captura de datos personales sensibles, datos privados, información confidencial o información no necesaria para las finalidades del S6. Esta regla deberá aplicarse de manera compatible con los principios de transparencia, máxima publicidad, rendición de cuentas y datos abiertos, evitando tanto la divulgación indebida de información confidencial como la clasificación injustificada de información pública o institucional.

a) Categorías de titulares o personas relacionadas con la información tratada

1. Personas servidoras públicas que intervienen en procedimientos de contratación pública, tales como personal de áreas contratantes, requirentes,

técnicas, responsables de ejecución, asistentes a juntas de aclaraciones, auditoras, emisoras de pago, receptoras de pago o responsables de funciones vinculadas al procedimiento. La información relativa a su nombre, cargo, función, rol, área de adscripción, correo electrónico institucional, teléfono institucional y domicilio oficial del ente público será tratada como información pública o institucional cuando esté relacionada con el ejercicio de atribuciones públicas, procedimientos de contratación, transparencia, rendición de cuentas, uso de recursos públicos o datos abiertos.

2. Personas físicas proveedoras, contratistas, licitantes, invitadas a cotizar, oferentes, solicitantes de aclaraciones o participantes en investigaciones de mercado.
3. Representantes legales, personas autorizadas, puntos de contacto institucionales o particulares vinculados con personas físicas o morales participantes en procedimientos de contratación. Tratándose de puntos de contacto de entes públicos, se privilegiará el uso de datos institucionales; tratándose de particulares, se aplicarán las medidas de protección de datos personales que correspondan.
4. Beneficiarios finales o propietarios reales, cuando dicho dato resulte procedente y aplicable conforme a las especificaciones técnicas y a la normatividad vigente.
5. Personas de contacto de entes públicos, instituciones garantes, entidades compradoras, entidades contratantes o instituciones que expiden garantías, cuando su identificación resulte necesaria para fines de comunicación, trazabilidad o verificación del procedimiento. Cuando se trate de personas servidoras públicas, deberán utilizarse preferentemente datos de contacto institucionales.

6. Personas físicas que aparezcan en documentos, hitos, registros, transacciones, garantías, pagos, adjudicaciones, modificaciones contractuales o procesos relacionados, siempre que el registro resulte necesario y proporcional para las finalidades del S6.

b) Datos personales objeto de tratamiento

Los datos personales que podrán tratarse en el S6 se desprenden de los apartados de información de contrataciones a registrar, particularmente del artículo 7 del Catálogo de Perfiles de Usuario del S6. Para efectos de esta evaluación, se identifican como datos personales aquellos que puedan referirse a personas físicas identificadas o identificables y que no tengan naturaleza pública o institucional en razón de su vínculo con el ejercicio de funciones públicas, sin que toda la información de contratación constituya dato personal protegido o información confidencial.

Categoría de información	Datos o campos que pueden implicar tratamiento de datos personales o información pública/institucional vinculada con personas físicas	Titulares o personas relacionadas
Actores involucrados	Función o rol en el procedimiento; identificador único del actor; nombre comercial; denominación o razón social, o nombre completo tratándose de personas físicas; nombre, apellido paterno y apellido materno; cargo o posición; personalidad jurídica; RFC cuando resulte aplicable; identificadores adicionales; domicilio; URL de registro; página web; pertenencia o membresía a una organización o grupo, únicamente cuando sea necesario y procedente. Tratándose de personas servidoras públicas, el nombre, cargo, función, rol, área, correo electrónico institucional, teléfono institucional, domicilio oficial y RFC institucional del ente público, cuando resulte aplicable, se considerarán información pública o institucional vinculada con el ejercicio de atribuciones públicas.	Personas servidoras públicas, personas físicas proveedoras o contratistas, licitantes, oferentes, invitadas a cotizar, solicitantes de aclaraciones, representantes o personas vinculadas con entes públicos o particulares, distinguiendo entre información institucional y datos personales protegidos.

SL

Puntos de contacto	Nombre de la persona de contacto; nombre, apellido paterno y apellido materno; correo electrónico institucional o de contacto; número telefónico institucional o de contacto; número de fax; URL de contacto; idiomas disponibles para la atención. Tratándose de entes públicos, deberán privilegiarse datos institucionales.	Personas de contacto de entes públicos, instituciones, proveedores, contratistas o participantes en el procedimiento. La información institucional de personas servidoras públicas tendrá naturaleza pública o institucional cuando se relacione con sus funciones.
Beneficiarios finales o propietarios reales	Nombre completo; identificador en registros oficiales; nacionalidades; correo electrónico; teléfono; fax; domicilio, únicamente cuando proceda conforme a las especificaciones técnicas y a la normatividad aplicable, observando criterios de minimización, necesidad y proporcionalidad.	Beneficiarios finales o propietarios reales de personas morales o estructuras jurídicas, cuando proceda conforme a las especificaciones técnicas y normas aplicables.
Planeación e investigación de mercado	Proveedores invitados; proveedor oferente; datos de cotizaciones recibidas; identificadores y nombres vinculados con solicitudes, cotizaciones, bienes, servicios y unidades involucradas. Tratándose de unidades públicas, la información institucional de personas servidoras públicas se tratará conforme a los principios de transparencia y máxima publicidad.	Personas físicas proveedoras, contratistas, oferentes o invitadas a cotizar, así como personas servidoras públicas vinculadas con unidades solicitantes, responsables o contratantes.
Contratación pública	Entidad contratante; método de contratación; juntas de aclaraciones; personas servidoras públicas asistentes; licitantes asistentes; licitantes participantes; documentos del procedimiento, cuando contengan datos identificativos. La información institucional de personas servidoras públicas vinculada con su asistencia o intervención en el procedimiento tendrá naturaleza pública o institucional.	Personas servidoras públicas, licitantes, personas físicas proveedoras, contratistas o representantes relacionados con el procedimiento.
Adjudicación	Identificador de adjudicación; proveedor o contratista adjudicado; documentos, modificaciones, fecha de adjudicación y datos de identificación asociados.	Personas físicas proveedoras o contratistas adjudicadas, representantes o personas vinculadas con el procedimiento adjudicado.
Contrato y ejecución	Identificador del contrato; fecha de firma; garantías; garante; transacciones; pagador; receptor del pago; documentos de ejecución; hitos y modificaciones contractuales, distinguiendo entre información pública contractual, información institucional de personas servidoras públicas y datos personales protegidos de particulares.	Personas físicas proveedoras, contratistas, garantes, receptoras de pago, personas servidoras públicas o representantes vinculados con el contrato o su ejecución.

bl

c) Información de contrataciones que no necesariamente constituye dato personal

También se registrará información que, por sí misma, no constituye dato personal, aunque puede vincularse a personas físicas identificadas o identificables dentro del expediente electrónico del procedimiento. Entre dicha información se encuentran identificadores del procedimiento, títulos, descripciones, estatus, métodos de contratación, criterios de adjudicación, valores máximos y mínimos, montos, moneda, periodos, fechas, documentos, hitos, modificaciones, garantías, transacciones, bienes o servicios licitados o contratados, clasificación de bienes o servicios, fuentes de financiamiento y procesos relacionados.

De igual forma, la información de identificación institucional de personas servidoras públicas que permita conocer su intervención en procedimientos de contratación pública, tales como nombre, cargo, función, rol, área, correo electrónico institucional, teléfono institucional, domicilio oficial y demás datos de contacto institucionales, deberá tratarse como información pública o institucional cuando se relacione con el ejercicio de atribuciones públicas, la trazabilidad de decisiones administrativas, el uso de recursos públicos, la transparencia, la rendición de cuentas o los datos abiertos.

d) Datos personales sensibles

El S6 no tiene por finalidad tratar datos personales sensibles. En consecuencia, las personas usuarias deberán abstenerse de registrar datos relativos al origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas o morales, opiniones políticas, afiliación sindical, preferencia sexual o cualquier otra categoría de información que pueda afectar la esfera más íntima de la persona titular

o dar lugar a discriminación, salvo que exista una base jurídica expresa, estrictamente necesaria y compatible con las finalidades del sistema.

Cuando un campo técnico permita capturar información como nacionalidades, pertenencia o membresía a organizaciones o grupos, dicha captura deberá realizarse con criterios de necesidad, proporcionalidad y minimización, evitando registrar información que revele datos sensibles, afiliaciones políticas, sindicales, religiosas o cualquier otra información confidencial que no resulte necesaria para el cumplimiento de las finalidades del S6.

F. Finalidades del tratamiento de los datos personales

1. Finalidades primarias

- Registrar, actualizar, sistematizar, consultar, publicar e interoperar la información pública relacionada con procedimientos de contratación pública de los entes públicos estatales y municipales.
- Identificar a los actores que intervienen en las distintas etapas del procedimiento de contratación, incluyendo personas servidoras públicas, proveedores, contratistas, licitantes, puntos de contacto, representantes, beneficiarios finales o propietarios reales, cuando resulte aplicable.
- Distinguir, para efectos de publicidad, consulta, protección y minimización, entre información pública o institucional de personas servidoras públicas vinculada con el ejercicio de funciones públicas y datos personales protegidos de particulares o información privada que exceda dicho ámbito.
- Dar cumplimiento a las obligaciones derivadas del Sistema Nacional Anticorrupción, del Sistema Estatal Anticorrupción, de la Plataforma Digital Nacional y del Sistema Estatal de Información.

SL

- Garantizar la trazabilidad, integridad, disponibilidad y verificabilidad de la información de contratación pública, conforme a los principios de transparencia, máxima publicidad, datos abiertos y rendición de cuentas.
- Permitir la interoperabilidad del S6 con la Plataforma Digital Nacional y, en su caso, con otros sistemas o componentes del Sistema Estatal de Información.
- Prevenir riesgos de corrupción, opacidad, conflictos de interés o irregularidades en los procedimientos de contratación pública.
- Atender requerimientos institucionales derivados de auditorías, revisiones, investigaciones, solicitudes de información, acciones de control interno, procedimientos administrativos o legales, en términos de las disposiciones aplicables.

2. Finalidades secundarias

- Generar estadísticas, reportes, visualizaciones, indicadores y productos analíticos sobre contrataciones públicas, siempre que ello sea compatible con las finalidades primarias y se respeten los principios de proporcionalidad y minimización.
- Elaborar insumos para el diseño, seguimiento y evaluación de políticas públicas de integridad, contrataciones abiertas, eficiencia administrativa, prevención de corrupción y mejora regulatoria.
- Desarrollar análisis institucionales que permitan identificar patrones, riesgos o áreas críticas en los procesos de contratación pública, preferentemente mediante datos disociados, agregados o anonimizados cuando no sea necesario identificar a una persona física.

G. Sujetos responsables del tratamiento de los datos personales

1. Responsable del tratamiento

La SESEA-NL será la responsable del tratamiento de los datos personales en el S6, en virtud de que administra y coordina el funcionamiento del sistema como parte del Sistema Estatal de Información, determina los fines y medios del tratamiento dentro del ámbito de sus atribuciones, supervisa la correcta operación del sistema y define las medidas técnicas, administrativas y organizativas que deberán observarse para la protección de los datos personales.

2. Entes públicos participantes

Los entes públicos estatales y municipales que registren información en el S6 serán responsables de la calidad, veracidad, integridad, actualización, oportunidad y pertinencia de la información que generen y carguen en el sistema, así como de observar las obligaciones que les correspondan conforme a sus atribuciones y a la normatividad en materia de contrataciones públicas, transparencia, archivos, responsabilidades administrativas y protección de datos personales.

3. Encargados del tratamiento

Se considerarán encargados del tratamiento las personas físicas o morales, unidades técnicas, proveedores de servicios tecnológicos u operadores que, en su caso, traten datos personales por cuenta y bajo las instrucciones de la SESEA-NL, mediante contrato, convenio, instrumento jurídico o designación correspondiente, para actividades relacionadas con desarrollo, mantenimiento, alojamiento, soporte, seguridad, interoperabilidad o infraestructura del S6.



H. Transferencias y remisiones de datos personales

Las transferencias y remisiones de datos personales en el S6 se realizarán únicamente cuando resulten necesarias, pertinentes y proporcionales para cumplir las finalidades legales del sistema, garantizar su interoperabilidad, atender obligaciones de transparencia, fiscalización, control, auditoría, investigación o cumplimiento normativo, o cuando exista una disposición legal que así lo autorice.

1. Transferencias

Podrán realizarse transferencias a autoridades competentes, órganos garantes, autoridades fiscalizadoras, órganos internos de control, autoridades jurisdiccionales o administrativas, y demás sujetos que cuenten con atribuciones legales para requerir o consultar información relacionada con contrataciones públicas, responsabilidades administrativas, transparencia, acceso a la información o protección de datos personales.

2. Remisiones

Podrán existir remisiones a encargados del tratamiento que brinden servicios tecnológicos, de desarrollo, mantenimiento, alojamiento, soporte, interoperabilidad, seguridad o infraestructura del S6. Dichas remisiones deberán documentarse mediante los instrumentos jurídicos correspondientes, incluyendo cláusulas de confidencialidad, seguridad, no reutilización, devolución, supresión y atención de incidentes.

3. Interoperabilidad con la Plataforma Digital Nacional

La comunicación de información hacia la Plataforma Digital Nacional se realizará conforme a las Bases para el Funcionamiento de la Plataforma Digital Nacional, las Especificaciones Técnicas aplicables al S6 y las Bases para el Funcionamiento del

Sistema Estatal de Información, observando los principios de minimización, seguridad, calidad, integridad y proporcionalidad del tratamiento.

I. Derechos ARCO y procedimientos para su ejercicio

Las personas titulares de los datos personales tratados en el S6 podrán ejercer sus derechos de acceso, rectificación, cancelación y oposición, así como los demás derechos que resulten aplicables conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

El derecho de acceso permite a la persona titular conocer los datos personales que obran en posesión del responsable, así como las condiciones generales de su tratamiento. El derecho de rectificación permite solicitar la corrección de datos inexactos, incompletos o desactualizados. El derecho de cancelación permite solicitar la supresión de datos cuando hayan dejado de ser necesarios para las finalidades del tratamiento o se traten en contravención a la normativa aplicable. El derecho de oposición permite solicitar que se cese el tratamiento de datos personales cuando existan motivos legítimos y jurídicamente procedentes.

Las solicitudes podrán presentarse ante la Unidad de Transparencia de la SESEA-NL, de forma presencial, por los medios institucionales habilitados o a través de la Plataforma Nacional de Transparencia. La solicitud deberá contener, cuando menos, el nombre de la persona titular y domicilio o medio para recibir notificaciones; documentos que acrediten su identidad y, en su caso, la personalidad e identidad de su representante; descripción clara y precisa de los datos personales respecto de los cuales se busca ejercer el derecho; derecho que se pretende ejercer o lo que solicita la persona titular; y cualquier otro elemento que facilite la localización de los datos.

El ejercicio de derechos ARCO se atenderá conforme a los plazos, requisitos, causales de procedencia o improcedencia y procedimientos previstos en la legislación aplicable. Cuando la información se encuentre bajo control de un ente público generador o cargador de datos, la SESEA-NL podrá realizar las gestiones de coordinación necesarias para localizar, verificar o actualizar la información, sin perjuicio de las obligaciones que correspondan al ente público de origen.

El ejercicio de los derechos ARCO se analizará conforme a la naturaleza de la información y a las finalidades legales del S6. Cuando se trate de información pública o institucional de personas servidoras públicas vinculada con el ejercicio de atribuciones, procedimientos de contratación, uso de recursos públicos, transparencia, rendición de cuentas o datos abiertos, los derechos de cancelación u oposición no podrán ejercerse para suprimir o impedir la publicación de información que deba mantenerse disponible por mandato legal o por interés público. Lo anterior no limita el derecho de rectificación cuando la información sea inexacta, incompleta o desactualizada, ni la protección de datos privados, sensibles, excesivos o no necesarios que pudieran haberse incorporado indebidamente.

J. Conservación y plazos de retención de datos

Los datos personales tratados en el S6 serán conservados únicamente durante el tiempo necesario para cumplir con las finalidades legales, administrativas, archivísticas, de transparencia, fiscalización, rendición de cuentas e interoperabilidad que justifican su tratamiento. Los plazos específicos deberán determinarse conforme a la normativa aplicable en materia de archivos, contrataciones públicas, responsabilidades administrativas, fiscalización, transparencia y protección de datos personales, así como conforme al Catálogo de Disposición Documental que resulte aplicable a la SESEA-NL y, en su caso, a los entes públicos generadores de la información.

Mientras los procedimientos de contratación se encuentren en curso, la información permanecerá activa para fines de registro, actualización, seguimiento y consulta. Una vez concluidos los procedimientos y cumplidos los plazos de conservación administrativa, legal, fiscalizadora o archivística aplicables, la información podrá ser objeto de baja, depuración, bloqueo, supresión, anonimización o conservación histórica, según corresponda a su valor documental, legal, administrativo o público.

La SESEA-NL y los entes públicos deberán evitar conservar datos personales por un plazo mayor al necesario, salvo que exista obligación legal, interés público, procedimiento pendiente, auditoría, investigación, responsabilidad administrativa, requerimiento de autoridad o disposición archivística que justifique su conservación.

K. Evaluación de riesgos y medidas de mitigación

La evaluación de riesgos del S6 considera la naturaleza de los datos tratados, el volumen potencial de registros, la interoperabilidad con la Plataforma Digital Nacional, la participación de múltiples entes públicos, la consulta pública de información, el uso de perfiles diferenciados y la posible existencia de datos personales protegidos de personas físicas proveedoras, contratistas, representantes, beneficiarias finales, puntos de contacto particulares, así como información pública o institucional de personas servidoras públicas vinculada con procedimientos de contratación pública.

Riesgo	Descripción	Impacto potencial	Probabilidad	Nivel
Acceso no autorizado	Ingreso al S6 por personas no autorizadas o uso indebido de credenciales.	Divulgación de información, pérdida de confidencialidad, afectación a derechos de titulares y responsabilidad administrativa.	Media	Alto
Publicación o captura excesiva de	Captura o publicación de datos personales	Exposición indebida de datos personales	Media	Alto

datos privados, sensibles o confidenciales	privados, datos sensibles, domicilios particulares, correos personales, teléfonos personales, identificadores no públicos, información patrimonial no procedente, datos de beneficiarios finales o propietarios reales fuera de los supuestos aplicables, o información contenida en documentos anexos que exceda las finalidades del S6.	protegidos, incumplimiento de principios de minimización y proporcionalidad, afectación a derechos de titulares y posibles responsabilidades.		
Datos inexactos o desactualizados	Carga incorrecta, incompleta o no actualizada por parte de entes públicos.	Afectación a la calidad de la información, errores en consulta pública, riesgos reputacionales o jurídicos.	Media	Medio-Alto
Modificación no autorizada	Alteración o manipulación de registros de contratación sin autorización.	Afectación a la integridad, trazabilidad y confiabilidad del sistema.	Media	Alto
Pérdida o destrucción accidental	Fallas técnicas, errores humanos, fallos de infraestructura o incidentes que provoquen pérdida de información.	Interrupción del servicio, pérdida de disponibilidad y afectación a la continuidad operativa.	Baja	Medio
Interoperabilidad insegura	Fallas en APIs, credenciales, transmisión o validación de datos hacia sistemas externos.	Exposición de datos, inconsistencias, indisponibilidad o rechazo de registros.	Media	Alto
Tratamiento indebido por encargados	Uso de datos por proveedores o terceros sin apego a instrucciones o cláusulas contractuales.	Vulneración de derechos, sanciones, incumplimiento contractual y daño institucional.	Baja	Medio-Alto
Captura de datos sensibles no requeridos	Registro de información sensible en campos abiertos o documentos asociados.	Afectación significativa a titulares, posible discriminación o incumplimiento grave.	Baja	Alto
Clasificación indebida de información pública o institucional como confidencial	Aplicación excesiva de criterios de protección de datos personales respecto de información institucional de personas servidoras públicas vinculada con contrataciones públicas.	Restricción injustificada del acceso a información pública, afectación al principio de máxima publicidad, debilitamiento de la trazabilidad y de la rendición de cuentas del S6.	Media	Medio-Alto

sl

Medidas de mitigación

Para mitigar los riesgos identificados, la SESEA-NL implementará medidas administrativas, técnicas, físicas y contractuales, bajo un enfoque de responsabilidad proactiva y mejora continua.

1. Medidas administrativas

- Definición de perfiles de usuario, niveles de acceso, facultades, obligaciones y responsabilidades mediante el Catálogo de Perfiles de Usuario del S6.
- Capacitación y acompañamiento a las personas usuarias responsables de la carga, validación, actualización y consulta de información.
- Emisión de criterios técnicos, guías, formatos, instructivos y comunicaciones oficiales para prevenir errores de captura o publicación excesiva.
- Incorporación de criterios para distinguir entre información pública o institucional de personas servidoras públicas y datos personales protegidos de particulares o información privada, a fin de evitar tanto la publicación excesiva de datos confidenciales como la clasificación indebida de información pública relacionada con contrataciones públicas.
- Procedimientos para altas, bajas, modificación de usuarios, restablecimiento de credenciales, gestión de incidentes y soporte técnico.
- Revisión periódica de cumplimiento normativo en materia de protección de datos personales, transparencia, archivos y contrataciones públicas.

2. Medidas técnicas

- Control de acceso basado en roles y privilegios mínimos, conforme a los perfiles definidos.

- Autenticación segura de las personas usuarias y mecanismos de gestión de sesiones.
- Cifrado de información en tránsito y, cuando resulte aplicable, en reposo.
- Bitácoras de acceso, modificación, consulta, carga, actualización y eliminación de registros, conforme a las capacidades técnicas y los mecanismos habilitados por la SESEA-NL.
- RespalDOS periódicos, mecanismos de recuperación ante fallas y controles de continuidad operativa, conforme a los procedimientos de respaldo que establezca la SESEA-NL para la infraestructura del S6.
- Validación de campos obligatorios, reglas de consistencia, controles de integridad y mecanismos de prevención de captura excesiva.
- Monitoreo de seguridad, pruebas de vulnerabilidad, actualización de componentes y atención de incidentes, conforme a la disponibilidad técnica y presupuestal de la SESEA-NL.

3. Medidas físicas

- Control de acceso físico a instalaciones, equipos, medios de respaldo y áreas técnicas relacionadas con la operación del sistema.
- Resguardo seguro de documentación física o medios electrónicos que contengan información relacionada con el S6.
- Procedimientos de disposición segura, destrucción o baja de soportes físicos o electrónicos, cuando proceda.

4. Medidas contractuales

- Cláusulas de confidencialidad, seguridad, no divulgación, no reutilización y tratamiento bajo instrucciones en contratos o convenios con encargados.

- Obligación de reportar incidentes, vulneraciones o accesos no autorizados de forma inmediata.
- Supervisión del cumplimiento de obligaciones por parte de proveedores o terceros que intervengan en soporte, desarrollo, alojamiento o mantenimiento del sistema.

L. Medidas de seguridad

Las medidas de seguridad del S6 se orientan a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de la información, de conformidad con el análisis de riesgos, el ciclo de vida de los datos, las finalidades del tratamiento y el volumen de información registrada. Estas medidas deberán actualizarse conforme evolucionen los riesgos tecnológicos, la operación del sistema, la normatividad aplicable y las mejores prácticas en materia de seguridad de la información.

Tipo de medida	Descripción
Administrativas	Aviso de privacidad; Evaluación de Impacto; Catálogo de Perfiles; designación de responsables; capacitación; procedimientos de atención de incidentes; controles de alta y baja de usuarios; lineamientos de operación.
Técnicas	Control de acceso por roles; autenticación; cifrado; bitácoras; respaldos; monitoreo; validaciones de campos; controles de interoperabilidad; pruebas de seguridad y actualización de componentes.
Físicas	Control de acceso a instalaciones; resguardo de equipos y medios de almacenamiento; custodia de documentación; destrucción segura de soportes y restricción de acceso a áreas técnicas.
Contractuales	Cláusulas con encargados; confidencialidad; obligaciones de seguridad; limitación de finalidades; devolución o supresión de datos; reporte de incidentes; auditoría o supervisión.

M. Responsabilidades y roles

a) Responsable del tratamiento

La SESEA-NL determina las finalidades y medios del tratamiento dentro del S6, administra la operación del sistema, define criterios técnicos y de seguridad, supervisa el funcionamiento del Sistema Estatal de Información y atiende las obligaciones que correspondan en materia de protección de datos personales.

b) Administrador de la SESEA-NL

Corresponde al perfil institucional asignado a la persona servidora pública que determine la SESEA-NL para administrar, coordinar y supervisar la operación del S6, gestionar accesos, parámetros, interoperabilidad, funcionamiento técnico-operativo, incidencias y medidas de seguridad del sistema.

c) Administrador del Ente Público

Corresponde a la persona servidora pública o unidad administrativa designada por cada ente público para registrar, capturar, actualizar, verificar y dar seguimiento a la información de contrataciones de su propio ente público, conforme a las especificaciones técnicas y a la normatividad aplicable.

d) Interesado o persona usuaria de consulta pública

Corresponde a cualquier persona que consulte la información pública disponible en el S6 a través de los canales habilitados, sin facultades de carga, modificación o eliminación de información.

e) Responsable o enlace de protección de datos personales

Coadyuva en la supervisión del cumplimiento de las obligaciones en materia de protección de datos personales, atención de derechos ARCO, análisis de riesgos,

actualización de avisos de privacidad, gestión de incidentes y mejora continua del programa institucional de protección de datos personales.

N. Nombre y cargo de las personas servidoras públicas 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 responsable institucional de la operación del Sistema Estatal de Información y de los instrumentos que permiten la implementación del S6.
2. Ing. Luis Antonio López García, Coordinador de Tecnologías de la Información, en calidad de responsable técnico del funcionamiento, operación, soporte e interoperabilidad del Sistema Estatal de Información y del S6, conforme al ámbito de sus atribuciones.

2. JUSTIFICACIÓN DE LA NECESIDAD DE IMPLEMENTACIÓN DEL SISTEMA DE INFORMACIÓN PÚBLICA DE CONTRATACIONES (S6)

La implementación del S6 se justifica en la necesidad de fortalecer la transparencia, integridad, trazabilidad, eficiencia, rendición de cuentas y prevención de riesgos de corrupción en los procedimientos de contratación pública. Este sistema constituye un componente estratégico del Sistema Estatal de Información y permite alinear la información estatal y municipal con los estándares de la Plataforma Digital Nacional en materia de contrataciones públicas.

1. Fortalece la transparencia de las contrataciones públicas mediante la publicación estructurada de información sobre planeación, procedimientos, adjudicaciones, contratos, ejecución, documentos, hitos, modificaciones y transacciones.

2. Permite la trazabilidad de decisiones, actores, etapas, montos y documentos vinculados con los procedimientos de contratación pública.
3. Facilita la detección de riesgos de corrupción, conflictos de interés, concentración de proveedores, modificaciones recurrentes, adjudicaciones directas, fragmentación de procedimientos u otros patrones relevantes.
4. Contribuye al cumplimiento de obligaciones del Sistema Nacional Anticorrupción, el Sistema Estatal Anticorrupción y la Plataforma Digital Nacional.
5. Favorece el derecho de acceso a la información pública y el principio de máxima publicidad mediante datos abiertos y reutilizables.
6. Proporciona insumos para auditoría, fiscalización, control interno, evaluación de políticas públicas y mejora de procesos de contratación.
7. Promueve la estandarización de datos y la interoperabilidad entre sistemas, reduciendo duplicidades, inconsistencias y barreras de acceso a la información.
8. Permite que el tratamiento de datos personales asociado a las contrataciones se realice bajo criterios documentados de licitud, proporcionalidad, minimización, seguridad y responsabilidad.

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 y en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, los responsables del tratamiento deben identificar de manera clara y precisa las fases en que los datos personales serán obtenidos, registrados, utilizados, consultados, publicados, conservados, actualizados y, en su caso, suprimidos. Este mapeo del ciclo de vida de los datos personales permite acreditar el cumplimiento del principio de responsabilidad y facilita la adopción de medidas de seguridad proporcionales a la naturaleza, alcance, contexto y finalidades del tratamiento.



En el caso del Sistema de Información Pública de Contrataciones (S6) del Sistema Estatal de Información (SEI), el tratamiento de datos personales se genera en el contexto del registro, captura, validación, actualización, consulta, publicación e interoperabilidad de información relacionada con los procedimientos de contratación pública. Dicho tratamiento puede comprender datos personales protegidos de personas físicas proveedoras o contratistas, licitantes, representantes legales, personas de contacto particulares, beneficiarios finales o propietarios reales, así como información pública o institucional de personas servidoras públicas que intervengan en las etapas de planeación, contratación pública, adjudicación, formalización, ejecución, modificación y cierre contractual.

En consecuencia, durante todo el ciclo de vida de la información deberá distinguirse entre datos personales protegidos y datos institucionales de publicidad procedente. Esta distinción es necesaria para evitar, por un lado, la incorporación o difusión de datos privados, sensibles, excesivos o no necesarios y, por otro, la restricción injustificada de información pública vinculada con contrataciones públicas, uso de recursos públicos, transparencia, rendición de cuentas y datos abiertos.

El tratamiento de datos personales en el S6 deberá realizarse únicamente respecto de la información necesaria, adecuada y proporcional para cumplir las finalidades legales del sistema, observando en todo momento los principios de licitud, finalidad, lealtad, proporcionalidad, calidad, información, seguridad y responsabilidad, así como los criterios de minimización aplicables. En consecuencia, deberá evitarse el registro de datos personales excesivos, datos personales sensibles o información confidencial que no resulte indispensable para las finalidades del S6, sin clasificar indebidamente como confidencial la información pública o institucional de personas servidoras públicas relacionada con el ejercicio de sus funciones.



a) Fases del ciclo de vida de los datos personales

1. Obtención

Los datos personales y la información pública o institucional que se integren en el Sistema de Información Pública de Contrataciones (S6) serán obtenidos a partir de fuentes documentales, electrónicas o digitales generadas por los entes públicos estatales y municipales que lleven a cabo procedimientos de contratación pública. La información podrá derivar de registros administrativos, expedientes de contratación, procesos de planeación, investigaciones de mercado, solicitudes de cotización, juntas de aclaraciones, actos de adjudicación, contratos, garantías, pagos, documentos de ejecución, modificaciones contractuales, hitos del procedimiento y demás constancias institucionales relacionadas con el ciclo de contratación pública.

La información será recabada por las unidades administrativas responsables de los procedimientos de contratación, áreas requirentes, áreas técnicas, áreas contratantes, áreas responsables de la ejecución, unidades administrativas de pago, órganos internos de control u otras áreas designadas por los entes públicos conforme a sus atribuciones. Asimismo, podrá provenir de sistemas institucionales, registros oficiales, padrones públicos, bases de datos abiertas, mecanismos de interoperabilidad o documentos generados por licitantes, proveedores, contratistas, representantes legales o personas de contacto, siempre que dicha información resulte necesaria para las finalidades del S6.

Cuando exista conexión con la Plataforma Digital Nacional (PDN), la integración de la información deberá realizarse mediante mecanismos de transferencia segura, autenticada y conforme a las especificaciones técnicas aplicables, observando las Bases para el Funcionamiento del Sistema Estatal de Información, las Bases para

el Funcionamiento de la Plataforma Digital Nacional y los criterios técnicos que emita la SESEA-NL.

2. Registro e ingreso al sistema

La información se registrará en el S6 mediante los módulos, formularios, campos y estructuras habilitados para la captura de los apartados de Actores Involucrados, Planeación, Contratación Pública, Adjudicación, Contrato, Ejecución, Garantías, Transacciones, Documentos, Hitos, Modificaciones y Procesos Relacionados, conforme a las especificaciones técnicas aplicables y al Catálogo de Perfiles de Usuario del S6.

La persona usuaria con perfil de Administrador del Ente Público será responsable de capturar, actualizar y validar la información correspondiente a su ente público, mientras que la SESEA-NL, por conducto del perfil de Administrador de la SESEA-NL y de las áreas técnicas competentes, podrá supervisar la operación, disponibilidad, integridad, consistencia e interoperabilidad del sistema. En los supuestos en que la herramienta requiera la captura directa de información contenida en documentos, deberá evitarse incorporar datos personales adicionales, excesivos o no previstos en los campos correspondientes.

3. Almacenamiento y conservación

Los datos personales registrados en el S6 se alojarán en bases de datos, repositorios o infraestructura tecnológica administrada o supervisada por la SESEA-NL, conforme a las medidas de seguridad técnicas, administrativas y físicas que resulten aplicables. El almacenamiento deberá garantizar la integridad, disponibilidad y confidencialidad de la información, así como la trazabilidad de

accesos, modificaciones, actualizaciones, consultas y demás operaciones realizadas por las personas usuarias autorizadas.

La conservación de la información deberá atender a las finalidades legales del S6, a la naturaleza pública de los procedimientos de contratación, a la normatividad aplicable en materia de archivos, transparencia, responsabilidades administrativas, fiscalización, contrataciones públicas y protección de datos personales, así como al Catálogo de Disposición Documental y demás instrumentos de gestión documental que resulten aplicables.

4. Uso y tratamiento

Los datos personales integrados en el S6 serán tratados para registrar, validar, actualizar, sistematizar, consultar, publicar e interoperar información pública relacionada con los procedimientos de contratación pública en el ámbito estatal y municipal. El uso de la información deberá limitarse al cumplimiento de las finalidades institucionales del sistema y a las atribuciones de las personas usuarias conforme a su perfil de acceso.

El tratamiento de datos personales en el S6 se limitará a:

- Dar cumplimiento a las obligaciones legales en materia de contrataciones públicas, transparencia, datos abiertos, integridad, rendición de cuentas, responsabilidades administrativas y fiscalización;
- Permitir la trazabilidad de los procedimientos de contratación pública, desde la planeación hasta la ejecución contractual;
- Registrar y consultar información relativa a actores involucrados, licitantes, proveedores, contratistas, personas servidoras públicas, puntos de contacto,



beneficiarios finales o propietarios reales, garantías, pagos, adjudicaciones, contratos, modificaciones y ejecución contractual;

- Facilitar la interoperabilidad con la Plataforma Digital Nacional y con otros componentes del Sistema Estatal de Información;
- Fortalecer los mecanismos de control, vigilancia, auditoría, fiscalización, prevención de riesgos de corrupción y seguimiento del ejercicio del gasto público;
- Generar reportes, estadísticas, análisis, visualizaciones y productos institucionales que contribuyan al seguimiento de los procedimientos de contratación pública, siempre que se observen los principios de proporcionalidad, minimización y protección de datos personales.

El tratamiento se llevará a cabo conforme a los perfiles de usuario autorizados, las finalidades descritas en el aviso de privacidad correspondiente, la Evaluación de Impacto en la Protección de Datos Personales del S6, las especificaciones técnicas aplicables y las disposiciones legales en materia de protección de datos personales.

5. Difusión y acceso público

La información registrada en el S6 podrá ser puesta a disposición pública a través de los canales que habilite la SESEA-NL y, en su caso, mediante su interoperabilidad con la Plataforma Digital Nacional, conforme a la normatividad aplicable en materia de transparencia, acceso a la información pública, datos abiertos, responsabilidades administrativas, contrataciones públicas y protección de datos personales.

La difusión de información deberá limitarse a los datos que tengan carácter público conforme a la legislación aplicable y a las finalidades del sistema. En caso de que la información contenga datos personales confidenciales, datos personales

sensibles, información reservada o datos cuya publicación no resulte necesaria para las finalidades del S6, deberán aplicarse las medidas correspondientes de clasificación, testado, disociación, anonimización o restricción de acceso, según corresponda.

La clasificación, testado, disociación, anonimización o restricción de acceso no deberá aplicarse de manera automática respecto de la información institucional de personas servidoras públicas vinculada con el ejercicio de sus atribuciones, procedimientos de contratación pública, uso de recursos públicos, transparencia, rendición de cuentas o datos abiertos. En consecuencia, no deberán considerarse confidenciales, por ese solo hecho, el nombre, cargo, función, rol, área de adscripción, correo electrónico institucional, teléfono institucional o domicilio oficial del ente público, salvo que exista una causa legal específica y debidamente fundada que justifique una restricción excepcional.

6. Actualización y rectificación

Los datos registrados en el S6 podrán ser actualizados, modificados o corregidos por las personas usuarias autorizadas conforme a sus perfiles de acceso, cuando resulte necesario para garantizar la calidad, exactitud, integridad, vigencia y congruencia de la información. La actualización podrá derivar de correcciones internas, requerimientos de subsanación, observaciones de la SESEA-NL, solicitudes del ente público correspondiente, ejercicio de derechos ARCO, determinaciones de autoridad competente o modificaciones propias del procedimiento de contratación pública, distinguiendo siempre entre datos personales protegidos e información pública o institucional.

La rectificación de datos personales deberá realizarse conforme a los procedimientos previstos en la normatividad aplicable, asegurando que toda

modificación sea trazable, documentada y consistente con las fuentes oficiales que sustentan la información registrada.

7. Supresión, baja, anonimización o conservación restringida

Una vez cumplidas las finalidades del tratamiento y agotados los plazos de conservación aplicables, los datos personales protegidos deberán ser suprimidos, anonimizados, disociados o conservados bajo acceso restringido, conforme a la normatividad en materia de archivos, transparencia, responsabilidades administrativas, fiscalización, contrataciones públicas y protección de datos personales. La información pública o institucional podrá conservarse y difundirse en los términos de la normativa aplicable, cuando subsistan obligaciones de transparencia, rendición de cuentas, fiscalización, datos abiertos, archivo o interés público.

En caso de que subsista un procedimiento legal, administrativo, jurisdiccional, de auditoría, fiscalización, investigación o responsabilidad administrativa vinculado con la contratación correspondiente, la conservación de los datos podrá extenderse hasta que se resuelva de manera definitiva la situación jurídica o administrativa que justifique su permanencia.

b) Fuentes internas y/o externas

- Registros administrativos internos de los entes públicos estatales y municipales relacionados con la planeación, tramitación, adjudicación, formalización, ejecución, modificación, pago y cierre de procedimientos de contratación pública.

- Expedientes, sistemas o plataformas institucionales de contrataciones, adquisiciones, obra pública, servicios, almacenes, presupuesto, contabilidad, pagos, garantías, investigación de mercado y seguimiento contractual.
- Documentos y registros generados por áreas contratantes, áreas requirentes, áreas técnicas, áreas responsables de la ejecución, unidades de pago, órganos internos de control, contralorías, unidades jurídicas y demás áreas competentes.
- Información proporcionada por licitantes, proveedores, contratistas, personas físicas o morales que soliciten aclaraciones, personas que envíen cotizaciones derivadas de investigaciones de mercado, representantes legales, puntos de contacto, beneficiarios finales o propietarios reales, cuando resulte necesaria para la finalidad del S6.
- Padrones, bases de datos abiertas, registros oficiales, fuentes públicas, sistemas interoperables, Plataforma Digital Nacional y otros componentes del Sistema Estatal de Información, conforme a las especificaciones técnicas y disposiciones aplicables.

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

- Captura de información por parte de los entes públicos obligados mediante formularios electrónicos, módulos o campos habilitados en el S6, conforme a las estructuras y especificaciones técnicas aplicables.
- Integración o actualización automatizada mediante interfaces de programación de aplicaciones, mecanismos de interoperabilidad o conexión segura con sistemas institucionales, cuando se encuentren disponibles y autorizados.
- Captura directa de información contenida en documentos de contratación pública, tales como planeaciones, solicitudes de cotización, investigaciones de mercado, convocatorias, bases, actas, adjudicaciones, contratos, garantías,

27

pagos, hitos, modificaciones, documentos de ejecución y demás constancias relacionadas con el procedimiento.

- Remisión oficial de información por medios electrónicos institucionales o comunicaciones formales de los entes públicos, validada por las áreas responsables conforme a sus atribuciones.
- Consulta e incorporación de datos provenientes de fuentes públicas, padrones o registros oficiales, siempre que su utilización sea compatible con las finalidades del S6 y se respeten los principios de licitud, finalidad, proporcionalidad y calidad.

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

- Las unidades administrativas responsables de contrataciones públicas en los entes obligados, incluyendo áreas contratantes, áreas requirentes, áreas técnicas y áreas responsables de la ejecución, encargadas de registrar, cargar, validar o actualizar la información del procedimiento de contratación.
- Las unidades administrativas de presupuesto, contabilidad, tesorería, pagos, almacenes, servicios generales, obra pública o áreas equivalentes, cuando intervengan en la generación o validación de información relacionada con presupuestos, transacciones, garantías, ejecución contractual o pagos.
- Los órganos internos de control, contralorías, unidades jurídicas, áreas de auditoría y entes fiscalizadores, en el ámbito de sus atribuciones, para efectos de revisión, control, fiscalización, investigación, prevención de riesgos de corrupción o seguimiento de responsabilidades administrativas.
- Las unidades de tecnologías de la información de los entes públicos, responsables del soporte técnico, seguridad informática, interoperabilidad y operación de los sistemas institucionales vinculados con el S6.

- La SESEA-NL, por conducto de las áreas responsables del Sistema Estatal de Información, tecnologías de la información, protección de datos personales, transparencia y demás áreas competentes, en su carácter de responsable del tratamiento, administración, coordinación, supervisión, resguardo e interoperabilidad del S6.
- Las personas usuarias con perfiles de Administrador de la SESEA-NL, Administrador del Ente Público e Interesado, en los términos y con los alcances previstos en el Catálogo de Perfiles de Usuario del S6.

e) Plazos de conservación o eliminación de los datos personales

- Los datos personales tratados en el S6 serán conservados únicamente durante el tiempo necesario para cumplir las finalidades del sistema, atendiendo a la Ley General de Archivos, la Ley de Archivos para el Estado de Nuevo León, el Catálogo de Disposición Documental aplicable, la normatividad en materia de contrataciones públicas, transparencia, responsabilidades administrativas, fiscalización y protección de datos personales.
- La información vinculada con procedimientos de contratación en curso permanecerá activa mientras subsistan las etapas de planeación, contratación pública, adjudicación, formalización, ejecución, modificación, pago, cierre, fiscalización o revisión correspondiente.
- En caso de que exista un procedimiento legal, administrativo, jurisdiccional, de auditoría, fiscalización, investigación o responsabilidad administrativa relacionado con la contratación, la conservación se extenderá hasta que concluya de manera definitiva el procedimiento que justifique su permanencia.
- Una vez cumplidas las finalidades y plazos aplicables, y siempre que no exista causa legal que justifique su conservación, los datos personales serán suprimidos, anonimizados, disociados o conservados bajo acceso restringido conforme a procedimientos institucionales seguros.

52

- La eliminación, anonimización o disociación deberá documentarse mediante registros, bitácoras o constancias que permitan acreditar la trazabilidad de la acción realizada y el cumplimiento del marco normativo aplicable.

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

- Control de accesos basado en roles y perfiles de usuario, conforme al Catálogo de Perfiles de Usuario del S6.
- Autenticación segura de personas usuarias y administración controlada de credenciales de acceso.
- Cifrado de información en tránsito y, cuando resulte técnicamente aplicable, cifrado de información en reposo.
- Bitácoras de acceso, modificación, consulta, actualización y operaciones relevantes dentro del sistema, conforme a las capacidades técnicas y los mecanismos habilitados por la SESEA-NL.
- Respallos periódicos, mecanismos de recuperación ante incidentes y políticas de continuidad operativa, conforme a los procedimientos de respaldo que establezca la SESEA-NL para la infraestructura del S6.
- Monitoreo, pruebas de vulnerabilidad, actualización de componentes tecnológicos y aplicación de parches de seguridad, conforme a la disponibilidad técnica y presupuestal de la SESEA-NL.
- Medidas de minimización, clasificación, testado, disociación o anonimización respecto de información que sea objeto de consulta pública.
- Protocolos de transferencia segura e interoperabilidad con la Plataforma Digital Nacional y con otros sistemas autorizados.

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

- Borrado lógico seguro mediante herramientas o procedimientos que impidan la recuperación ordinaria de la información.
- Destrucción física o disposición segura de medios de almacenamiento que contengan datos personales, cuando resulte aplicable.
- Cifrado previo de la información y destrucción controlada de claves criptográficas, cuando sea técnicamente procedente.
- Anonimización o disociación irreversible de datos personales cuando la conservación de información estadística, histórica, técnica o de datos abiertos sea necesaria sin identificar a las personas titulares.
- Registro documental de las acciones de supresión, anonimización, disociación o destrucción, con indicación de fecha, persona responsable, medio utilizado y justificación normativa.
- Revisión periódica de bases de datos, respaldos, repositorios y registros auxiliares para verificar que la eliminación o anonimización se aplique de manera integral y consistente.
- Capacitación del personal responsable sobre gestión documental, conservación, supresión segura y protección de datos personales.

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 de Información Pública de Contrataciones (S6) del Sistema Estatal de Información, considerando la posibilidad de que se comprometa la confidencialidad, integridad, disponibilidad, trazabilidad, exactitud o proporcionalidad de los datos personales tratados, ya sea por vulnerabilidades técnicas, errores humanos, accesos indebidos, registros excesivos, configuraciones inadecuadas, fugas de información, fallas de interoperabilidad o actos maliciosos.

El tratamiento de datos personales en el S6 implica la recopilación, registro, validación, sistematización, actualización, consulta, publicación e interoperabilidad de información relacionada con procedimientos de contratación pública, incluyendo datos personales protegidos de personas físicas proveedoras o contratistas, licitantes, personas que solicitan aclaraciones o presentan cotizaciones, representantes legales, puntos de contacto particulares, beneficiarios finales o propietarios reales, instituciones que expiden garantías, pagadores, receptores de pago y demás actores involucrados. Asimismo, comprende información pública o institucional de personas servidoras públicas vinculada con las etapas de planeación, contratación pública, adjudicación, contrato y ejecución contractual.

Si bien el S6 no tiene por finalidad recabar datos personales sensibles, por la amplitud de los campos de captura, la existencia de apartados descriptivos, hitos, modificaciones, documentos, datos de contacto y registros vinculados con beneficiarios finales o propietarios reales, resulta necesario prever riesgos asociados a la incorporación de información excesiva, confidencial, inexacta o no necesaria para las finalidades del sistema. De igual manera, debe prevenirse el riesgo de clasificar indebidamente como confidencial información pública o institucional de personas servidoras públicas vinculada con contrataciones públicas, lo que podría afectar la máxima publicidad, la trazabilidad y la rendición de cuentas.

sl

1.1 Riesgos administrativos identificados:

- Asignación incorrecta de perfiles de usuario o privilegios superiores a los necesarios para la operación del S6.
- Registro de información excesiva, confidencial, privada o no necesaria en campos descriptivos, apartados de contacto, documentos, hitos, modificaciones o justificaciones vinculadas con procedimientos de contratación pública.
- Publicación o consulta de datos personales privados, sensibles, confidenciales o no necesarios que debieron ser minimizados, testados, disociados o restringidos conforme a la normatividad aplicable.
- Clasificación o testado indebido de información pública o institucional de personas servidoras públicas vinculada con procedimientos de contratación pública, uso de recursos públicos, transparencia, rendición de cuentas o datos abiertos.
- Uso indebido de la información por parte de personas usuarias autorizadas, para fines distintos a los previstos en el S6.
- Falta de capacitación periódica del personal de los entes públicos y de la SESEA-NL sobre protección de datos personales, seguridad de la información, minimización y proporcionalidad en la captura de datos.
- Deficiencias en la validación de la calidad, exactitud, integridad y actualización de la información registrada por los entes públicos.
- Ausencia o insuficiencia de documentación que acredite las actividades de tratamiento, controles de acceso, atención de incidentes, auditorías, capacitaciones o revisiones de cumplimiento.
- Inadecuada coordinación entre las unidades administrativas responsables de contrataciones públicas, áreas de tecnologías de la información, órganos internos de control y la SESEA-NL para atender correcciones, bajas, actualizaciones o incidencias.

1.2 Riesgos físicos identificados:

- Acceso físico no controlado a instalaciones, equipos, servidores, respaldos o medios de almacenamiento vinculados con la operación del S6.
- Robo, extravío o destrucción accidental de dispositivos de almacenamiento, equipos portátiles, respaldos o documentación física que contenga datos personales asociados a procedimientos de contratación pública.
- Falta de controles físicos adecuados para el resguardo de documentación o medios electrónicos utilizados en la carga, validación o soporte del S6.
- Riesgos derivados de siniestros, fallas eléctricas, incendio, inundación u otros eventos que puedan afectar la disponibilidad de la infraestructura tecnológica o de los respaldos de información.
- Disposición inadecuada de documentos físicos, medios electrónicos obsoletos o respaldos que contengan datos personales relacionados con el S6.

1.3 Riesgos tecnológicos identificados:

- Acceso no autorizado a la plataforma, bases de datos, módulos de administración, módulos de carga o interfaces de consulta pública del S6.
- Vulnerabilidades en la aplicación web o en sus componentes, tales como inyección SQL o NoSQL (Operadores MongoDB), XSS, CSRF, fallas de autenticación, errores de configuración o exposición indebida de servicios.
- Deficiente cifrado de datos personales en tránsito o en reposo, particularmente en procesos de carga, consulta, respaldo, interoperabilidad o intercambio de información.
- Fallas en el control de sesiones, autenticación de usuarios, administración de contraseñas, revocación de accesos o baja de perfiles de usuario.
- Interoperabilidad con la Plataforma Digital Nacional o con otros sistemas sin mecanismos suficientes de autenticación, trazabilidad, validación, cifrado o control de integridad.

- Publicación accidental de datos personales privados, sensibles, confidenciales o no previstos para consulta pública por errores de configuración, sincronización, interoperabilidad o parametrización de niveles de acceso.
- Pérdida, alteración o corrupción de información derivada de fallas técnicas, ausencia de respaldos, errores de carga, errores de actualización o incidentes de ciberseguridad.
- Extracción masiva, uso automatizado abusivo o consulta no controlada de información pública disponible en el S6, que pueda generar riesgos de reutilización indebida, perfilamiento o afectación a titulares cuando se combine con datos personales protegidos o fuentes externas.
- Uso de software obsoleto, librerías sin actualización, componentes vulnerables o falta de pruebas periódicas de seguridad.
- Insuficiencia de bitácoras, monitoreo, alertas, registros de actividad o mecanismos de auditoría que permitan detectar accesos indebidos, modificaciones no autorizadas o patrones anómalos.

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 ocurrencia de cada riesgo identificado y el impacto que tendría sobre los derechos y libertades de las personas titulares si dicho riesgo se materializara. La ponderación considera la naturaleza de los datos tratados, el volumen de información, los perfiles de acceso, el carácter público o restringido de los registros, la interoperabilidad con la Plataforma Digital Nacional, la participación de entes públicos y la posibilidad de afectaciones reputacionales, patrimoniales, comerciales, administrativas o jurídicas para las personas titulares.

2.1 Metodología empleada para la valoración

Se utiliza una matriz de riesgos en la que 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, número de personas usuarias, controles existentes, complejidad operativa e interoperabilidad.
Nivel de impacto	Bajo, Medio, Alto	En función del daño posible a la persona titular, el volumen de datos afectados, el tipo de dato, la publicidad o restricción de la información, consecuencias legales, reputacionales, comerciales o patrimoniales.

El resultado de la ponderación determina el nivel de riesgo residual y sirve de base para seleccionar medidas de mitigación proporcionales, razonables y adecuadas a la naturaleza del tratamiento realizado en el S6.

2.2 Criterios específicos de análisis

- Probabilidad Alta: El riesgo es inminente o probable a corto plazo si no se implementan medidas adicionales, o deriva de una exposición amplia por número de usuarios, interoperabilidad, consulta pública o complejidad técnica.
- Probabilidad Media: El riesgo puede ocurrir bajo determinadas condiciones, por errores de configuración, falta de capacitación, fallas de validación o controles parcialmente implementados.
- Probabilidad Baja: El riesgo es excepcional o remoto bajo un entorno de control maduro, con medidas de seguridad, capacitación, supervisión y trazabilidad adecuadas.
- Impacto Alto: Puede comprometer datos personales protegidos, información confidencial, beneficiarios finales, datos de contacto no institucionales, RFC de personas físicas cuando resulte aplicable, domicilios particulares, registros de proveedores o contratistas, o generar consecuencias legales, reputacionales, patrimoniales o comerciales relevantes.

- Impacto Medio: Puede afectar derechos de algunas personas titulares, generar inconsistencias, reclamos, correcciones, requerimientos institucionales o sanciones menores.
- Impacto Bajo: Afecta datos no sensibles, información institucional o supuestos en los que el impacto puede contenerse fácilmente con las medidas implementadas, sin perjuicio de que deba preservarse la calidad, integridad y máxima publicidad de la información pública.

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
Registro o publicación de datos personales privados, sensibles, excesivos o confidenciales en campos descriptivos, documentos, hitos o justificaciones, sin que ello comprenda la información pública o institucional de personas servidoras públicas vinculada con el ejercicio de funciones públicas.	Media	Alto	Alto
Acceso no autorizado por personal interno o personas usuarias con privilegios superiores a los necesarios.	Media	Alto	Alto
Modificación, alteración o eliminación no autorizada de información de procedimientos de contratación pública.	Media	Alto	Alto
Inexactitud, desactualización o inconsistencia de información registrada por los entes públicos.	Media	Medio/Alto	Alto
Exposición indebida de datos de contacto no institucionales, RFC de personas físicas cuando resulte aplicable, domicilios particulares, representantes legales o beneficiarios finales.	Media	Alto	Alto
Fallas de interoperabilidad, autenticación o configuración en interfaces con la Plataforma Digital Nacional u otros sistemas.	Media	Alto	Alto
Extracción masiva o reutilización indebida de información disponible para consulta pública.	Media	Medio	Medio

Pérdida de disponibilidad del S6 por fallas técnicas, ataques o ausencia de respaldos probados.	Baja/Media	Medio/Alto	Medio/Alto
Robo, extravío o destrucción accidental de equipos, respaldos o medios físicos con datos personales.	Baja	Medio	Medio
Incumplimiento de obligaciones en materia de transparencia, protección de datos personales, atención de derechos ARCO o deber de seguridad.	Baja/Media	Alto	Alto
Clasificación indebida de información pública o institucional de personas servidoras públicas como confidencial.	Media	Medio/Alto	Medio-Alto

Esta clasificación permite establecer prioridades en la implementación de controles y dar cumplimiento al principio de responsabilidad proactiva, asegurando que las medidas adoptadas sean proporcionales a los riesgos identificados y al tipo de tratamiento realizado en el S6.

2.4 Conclusión de la ponderación

- Existen riesgos altos que deben ser mitigados de forma prioritaria, especialmente los relacionados con accesos indebidos, registro excesivo de datos privados o confidenciales, publicación de información no necesaria, fallas de interoperabilidad, vulnerabilidades tecnológicas y deficiencias en la validación de información por los entes públicos. También deberá atenderse el riesgo de clasificar indebidamente información pública o institucional vinculada con personas servidoras públicas y contrataciones públicas.
- La mayoría de los riesgos identificados pueden reducirse a un nivel aceptable mediante la implementación o fortalecimiento de medidas administrativas, físicas y tecnológicas, así como mediante capacitación, controles de acceso, validación de datos, bitácoras, cifrado, monitoreo y revisión periódica.
- Se recomienda actualizar la matriz de riesgos de manera periódica, especialmente cuando se modifiquen las funcionalidades del S6, las especificaciones técnicas de la Plataforma Digital Nacional, los perfiles de usuario,



los campos de captura, los mecanismos de consulta pública o los procedimientos de interoperabilidad.

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

Una vez identificados y valorados los riesgos, la SESEA-NL deberá documentar y aplicar controles organizacionales, físicos y técnicos que reduzcan la probabilidad de ocurrencia o el impacto en caso de materialización. Las acciones deberán ser proporcionales y adecuadas a la naturaleza del S6, a las categorías de datos tratados, a los perfiles de acceso, a la disponibilidad técnica del sistema y a las obligaciones de transparencia, datos abiertos, contrataciones públicas y protección de datos personales.

3.1 Tipología de medidas aplicadas por tipo de riesgo

A. Riesgos tecnológicos y de ciberseguridad

Estos riesgos representan una de las principales áreas de exposición del S6 y se mitigan mediante controles técnicos de seguridad, autenticación, cifrado, validación, monitoreo e interoperabilidad segura:

Riesgo	Medidas técnicas de mitigación
Acceso no autorizado por terceros o personal interno.	Implementación de control de acceso basado en roles, autenticación robusta, contraseñas seguras, baja oportuna de perfiles, bitácoras de acceso y revisión periódica de privilegios.
Registro, publicación o exposición de datos personales privados, sensibles, excesivos o confidenciales.	Validaciones en campos de captura, controles de obligatoriedad, criterios de minimización, alertas sobre datos sensibles, revisión de campos descriptivos, reglas de publicación conforme a perfiles de acceso y distinción entre información institucional de personas servidoras públicas y datos personales protegidos de particulares.
Vulnerabilidades en la aplicación o en sus componentes.	Validación estricta de entradas, uso de consultas seguras, sanitización de datos, pruebas de vulnerabilidad, actualización de componentes, parches de seguridad y monitoreo de eventos.

Fallas de interoperabilidad o transmisión insegura de datos.	Uso de APIs seguras, cifrado en tránsito, autenticación entre sistemas, registros de intercambio, validación de integridad, control de errores y mecanismos de recuperación.
Pérdida de disponibilidad o integridad de la información.	Respallos automáticos, almacenamiento seguro, pruebas periódicas de restauración, planes de continuidad, redundancia y monitoreo de disponibilidad.
Extracción masiva o consulta abusiva de información pública.	Mecanismos de control de tráfico, límites de consulta, monitoreo de patrones anómalos, protección contra automatización abusiva y revisión de logs.
Uso de contraseñas débiles o credenciales compartidas.	Políticas robustas de contraseñas, bloqueo por intentos fallidos, prohibición de compartir credenciales, capacitación y responsabilidades documentadas para las personas usuarias. En tanto el sistema de autenticación OAuth del S6 no cuente con validación automatizada de políticas de contraseñas, dichas medidas se gestionarán mediante procedimientos administrativos, controles de usuario y acciones de supervisión.

B. Riesgos organizacionales y administrativos

Estos riesgos se controlan mediante políticas, procedimientos, capacitación, responsabilidades documentadas y supervisión institucional:

Riesgo	Medidas administrativas de mitigación
Falta de políticas institucionales o criterios operativos.	Desarrollo, difusión y actualización de políticas de privacidad, seguridad de la información, perfiles de usuario, conservación, minimización, clasificación, publicidad, testado y publicación de información, incluyendo criterios para distinguir información pública o institucional de personas servidoras públicas y datos personales protegidos.
Capacitación insuficiente del personal.	Programas periódicos de capacitación para personas administradoras de la SESEA-NL, administradoras de entes públicos, personal técnico y áreas responsables de contrataciones públicas, incluyendo criterios de máxima publicidad, clasificación y protección de datos personales.
Carga de información inexacta, incompleta o desactualizada.	Controles de validación, requerimientos de subsanación, revisión por el ente público, lineamientos de captura, seguimiento de observaciones y responsabilidad del Usuario 2 sobre la información registrada.
Tratamiento para finalidades distintas al S6.	Avisos de privacidad, reglas de uso, responsabilidades documentadas, perfiles de acceso, auditorías internas y sanciones administrativas o contractuales en caso de incumplimiento.
Gestión deficiente de incidentes.	Protocolo de detección, registro, análisis, contención, mitigación, documentación y notificación de incidentes conforme a la normatividad aplicable.
Falta de control sobre encargados o terceros.	Contratos, convenios o cláusulas específicas de confidencialidad, seguridad, no reutilización, devolución o supresión de datos, auditoría y responsabilidad en materia de protección de datos personales.

C. Riesgos físicos y de infraestructura

Estos riesgos se mitigan mediante controles físicos, operativos y de continuidad:

Riesgo	Medidas físicas de mitigación
Accesos no autorizados a instalaciones, equipos o respaldos.	Control de acceso físico a áreas restringidas, resguardo de equipos, registros de ingreso, vigilancia y medidas de seguridad en espacios donde se administre o soporte el S6.
Robo, extravío o destrucción de dispositivos o medios físicos.	Inventario de equipos, resguardo seguro, cifrado de dispositivos, políticas de uso de medios externos, borrado seguro y documentación de movimientos.
Daños por siniestros o fallas de infraestructura.	Plan de continuidad de operaciones, respaldo de información, protección contra incendios, control de temperatura, revisión de infraestructura crítica y procedimientos de recuperación.
Disposición inadecuada de documentos o medios obsoletos.	Protocolos de destrucción segura, borrado lógico o físico, destrucción de soportes, registros de disposición y validación de irreversibilidad.

3.2 Tratamiento de riesgos residuales: aceptar, transferir o eliminar

Algunos riesgos no pueden eliminarse completamente; por ello, se aplican criterios de gestión residual conforme a la naturaleza del tratamiento y a las capacidades técnicas, administrativas y jurídicas de la SESEA-NL:

- Eliminar el riesgo: En los casos en que el tratamiento de ciertos datos no resulte indispensable para las finalidades del S6, se aplicará el principio de minimización, suprimiendo su recolección, captura, publicación o conservación.
- Mitigar el riesgo: Se implementarán controles adicionales o redundantes que reduzcan la probabilidad de ocurrencia o el impacto del riesgo, tales como controles de acceso, validaciones, cifrado, monitoreo, capacitación, bitácoras y auditorías.
- Transferir el riesgo: Cuando participen encargados, proveedores tecnológicos o terceros, se podrán establecer obligaciones contractuales específicas, cláusulas de confidencialidad, responsabilidades de seguridad, auditoría y, en su caso, mecanismos de cobertura o aseguramiento aplicables.
- Aceptar el riesgo: Únicamente procederá cuando el nivel residual sea bajo, existan controles suficientes y se cuente con evidencia documental que justifique la aceptación, manteniendo vigilancia continua y revisión periódica.



3.3 Instrumentación, seguimiento y evidencia documental

Para garantizar la trazabilidad, los controles implementados deberán documentarse, verificarse y actualizarse de manera periódica. En particular, deberán:

- Integrarse en los instrumentos institucionales de seguridad de la información y protección de datos personales aplicables al S6.
- Ser verificados mediante auditorías internas, revisiones técnicas, controles de cumplimiento y seguimiento de incidencias.
- Contar con evidencia documental para su validación ante el INFONL u otras autoridades competentes, incluyendo bitácoras, políticas, reportes de revisión, constancias de capacitación, registros de incidentes, controles de acceso y documentación técnica.
- Ser revisados y actualizados cuando existan modificaciones en las funcionalidades del S6, en las Especificaciones Técnicas de la Plataforma Digital Nacional, en los perfiles de usuario, en los datos registrados o en la normatividad aplicable.
- Permitir la mejora continua de los controles implementados, atendiendo a los resultados de auditorías, incidentes, vulnerabilidades detectadas, cambios tecnológicos y criterios emitidos por autoridades competentes.

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

El Sistema de Información Pública de Contrataciones (S6) del Sistema Estatal de Información adopta los siguientes mecanismos y procedimientos para asegurar que el tratamiento masivo o relevante de datos personales cumpla con el marco

normativo aplicable en materia de protección de datos personales, transparencia, acceso a la información pública, datos abiertos, responsabilidades administrativas, contrataciones públicas y seguridad de la información:

1. Designación del Responsable de Protección de Datos Personales del Sistema.

Designar a la persona responsable de protección de datos personales, con autonomía técnica y operativa, encargada de coordinar, supervisar y verificar el cumplimiento de la normativa en materia de protección de datos personales en los procesos relacionados con la operación, administración, carga, actualización, consulta, publicación, interoperabilidad y resguardo de la información contenida en el Sistema de Información Pública de Contrataciones (S6).

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

Contar con políticas institucionales, protocolos y procedimientos internos que regulen el manejo, captura, almacenamiento, actualización, consulta, publicación, interoperabilidad y resguardo de los datos personales tratados en el S6, asegurando la aplicación de medidas técnicas, administrativas y organizativas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información, así como a evitar el registro de datos excesivos, sensibles o confidenciales que no resulten necesarios para las finalidades del sistema. Dichas políticas deberán incorporar criterios específicos para distinguir entre información pública o institucional de personas servidoras públicas y datos personales protegidos de particulares o información privada, a fin de evitar tanto la publicación excesiva de datos confidenciales como la clasificación indebida de información pública relacionada con contrataciones públicas.

3. Evaluación de Impacto en la Protección de Datos Personales aplicada al Sistema.

Realizar una Evaluación de Impacto en la Protección de Datos Personales que identifique los riesgos inherentes al tratamiento de datos personales en el S6, considerando la información relativa a actores involucrados, personas físicas proveedoras o contratistas, representantes legales, personas de contacto particulares, beneficiarios finales o propietarios reales, licitantes, garantías, transacciones, adjudicaciones, contratos y demás datos vinculados con los procedimientos de contratación pública, así como la información pública o institucional de personas servidoras públicas que intervengan en dichos procedimientos. Dicha evaluación deberá valorar la probabilidad e impacto de los riesgos detectados y definir las medidas preventivas, correctivas y de mitigación necesarias, conforme a la normatividad aplicable y a los criterios emitidos por el INFONL.

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

Implementar programas de capacitación y sensibilización dirigidos a las personas servidoras públicas que participen en la administración, operación, carga, validación, actualización, consulta o supervisión del S6, con la finalidad de fortalecer la cultura de protección de datos personales, la seguridad de la información, la observancia de los principios de licitud, finalidad, proporcionalidad, calidad, seguridad y responsabilidad, así como el cumplimiento de las obligaciones legales aplicables al tratamiento de información en materia de contrataciones públicas. La capacitación deberá incluir criterios de clasificación, testado, publicidad, máxima publicidad y protección de datos personales, con énfasis en la distinción entre datos institucionales de personas servidoras públicas y datos personales protegidos de



particulares, proveedores, contratistas, licitantes, representantes, beneficiarios finales o propietarios reales.

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 las personas titulares puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición respecto de los datos personales tratados en el S6, conforme a los requisitos, plazos y modalidades previstos 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 demás disposiciones aplicables. Lo anterior, sin perjuicio de las limitaciones que, en su caso, deriven de obligaciones legales de conservación, publicidad, transparencia, fiscalización, responsabilidades administrativas, archivo o interés público, especialmente cuando se trate de información pública o institucional de personas servidoras públicas vinculada con procedimientos de contratación pública.

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

Efectuar revisiones periódicas, auditorías internas y controles de cumplimiento para verificar que la información registrada en el S6 se trate conforme a las finalidades autorizadas, los perfiles de acceso, las especificaciones técnicas aplicables, los avisos de privacidad correspondientes y las medidas de seguridad implementadas. Estos mecanismos deberán permitir la detección y corrección oportuna de inconsistencias, accesos indebidos, registros excesivos, errores de captura, vulnerabilidades técnicas, incumplimientos normativos o restricciones injustificadas a información pública o institucional que deba permanecer disponible conforme a los principios de transparencia y máxima publicidad.



7. Gestión de incidentes y vulneraciones de seguridad en el Sistema.

Disponer de protocolos para la detección, registro, análisis, contención, atención, documentación y notificación de incidentes o vulneraciones de seguridad que puedan afectar los datos personales tratados en el S6. Dichos protocolos deberán prever la comunicación interna inmediata, la evaluación del impacto sobre los derechos de las personas titulares, la implementación de medidas correctivas, la documentación de las acciones realizadas y, cuando resulte procedente, la notificación al órgano garante competente y a las personas titulares afectadas, conforme a la legislación aplicable.

8. Actualización normativa y mejora continua del Sistema.

Mantener un proceso permanente de revisión y actualización de las políticas, procedimientos, criterios operativos, medidas de seguridad y mecanismos de interoperabilidad aplicables al S6, atendiendo a los cambios normativos, avances tecnológicos, criterios emitidos por autoridades competentes, modificaciones en las especificaciones técnicas de la Plataforma Digital Nacional y mejores prácticas en materia de protección de datos personales, transparencia, datos abiertos y seguridad de la información.

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

Asegurar la generación, conservación y disponibilidad de la documentación que acredite el cumplimiento de las obligaciones en materia de protección de datos personales, incluyendo avisos de privacidad, bitácoras de acceso, registros de usuarios, constancias de capacitación, evaluaciones de impacto, reportes de auditoría, evidencias de atención a incidentes, controles de seguridad,

comunicaciones con entes públicos y demás documentos que permitan demostrar el cumplimiento normativo ante el INFONL u otras autoridades competentes.

10. Cumplimiento normativo y opinión del Responsable de Protección de Datos Personales.

La SESEA-NL deberá asegurar que todo tratamiento de datos personales realizado en el S6 observe los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad previstos en la normatividad aplicable. Asimismo, deberá garantizar el ejercicio de los derechos ARCO de las personas titulares y contar con la opinión del Responsable de Protección de Datos Personales, quien deberá pronunciarse sobre la viabilidad del tratamiento, la suficiencia de las medidas de seguridad, la proporcionalidad de los datos tratados, la mitigación de riesgos y la correcta distinción entre información pública o institucional de personas servidoras públicas y datos personales protegidos de particulares o información privada.

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

Al momento de elaboración de esta Evaluación de Impacto, no se cuenta con consultas externas específicas adicionales a las actividades de revisión institucional, técnica y jurídica realizadas para la implementación del S6. En caso de que se lleven a cabo consultas con entes públicos, áreas técnicas, órganos garantes, especialistas o instancias vinculadas con la Plataforma Digital Nacional, sus resultados deberán incorporarse al expediente de implementación y, en su caso, actualizar la presente evaluación.



7. OPINIÓN DEL RESPONSABLE DE PROTECCIÓN DE DATOS PERSONALES

Como Responsable de Protección de Datos Personales del Sistema de Información Pública de Contrataciones (S6) 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.

He examinado los documentos normativos, operativos y técnicos que sustentan el tratamiento relevante de datos personales en el marco del funcionamiento del Sistema S6, incluyendo el Catálogo de Perfiles de Usuario, las funcionalidades del sistema, las Especificaciones Técnicas aplicables, las medidas de seguridad implementadas, los controles de interoperabilidad con la Plataforma Digital Nacional, los avisos de privacidad y los registros de cumplimiento normativo. Asimismo, revisé que la evaluación distinga entre información pública o institucional de personas servidoras públicas vinculada con el ejercicio de atribuciones públicas y datos personales protegidos de particulares o información privada que exceda dicho ámbito.

Con base en esta revisión, confirmo que:

- Se han identificado de forma clara y precisa los riesgos inherentes al tratamiento de datos personales que se realiza a través del Sistema S6, así como los riesgos asociados a la publicación excesiva de información privada y a la clasificación indebida de información pública o institucional vinculada con contrataciones públicas.
- Se han establecido medidas técnicas, administrativas y organizativas adecuadas para mitigar dichos riesgos, conforme a los principios y deberes previstos 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 demás disposiciones aplicables.

- El tratamiento de datos personales previsto para el S6 se encuentra vinculado con finalidades determinadas, explícitas, legítimas y proporcionales, relacionadas con el registro, sistematización, consulta, publicación e interoperabilidad de información pública de contrataciones, distinguiendo entre información institucional de personas servidoras públicas y datos personales protegidos de particulares, proveedores, contratistas, licitantes, representantes, beneficiarios finales o propietarios reales.
- Se han previsto medidas para evitar el tratamiento de datos personales excesivos, sensibles o confidenciales que no resulten necesarios para las finalidades del sistema, particularmente en los campos descriptivos, puntos de contacto particulares, documentos, hitos, modificaciones, datos de beneficiarios finales o propietarios reales y demás apartados susceptibles de incorporar información privada no necesaria.
- Se ha integrado un esquema de mejora continua que contempla la revisión periódica de los procedimientos, la actualización de medidas de seguridad, la capacitación del personal involucrado, la atención de incidentes de seguridad y el fortalecimiento de los controles aplicables al tratamiento de datos personales.

Adicionalmente, se recomienda mantener y fortalecer las estrategias de capacitación continua dirigidas a las personas servidoras públicas que participen en la operación del S6; revisar periódicamente los criterios de minimización, publicidad, clasificación, testado, disociación y protección de datos personales; y verificar que la información pública o institucional de personas servidoras públicas vinculada con contrataciones públicas no sea clasificada indebidamente como confidencial, sin

la información pública o institucional de personas servidoras públicas vinculada con contrataciones públicas no sea clasificada indebidamente como confidencial, sin perjuicio de proteger datos privados, sensibles, excesivos o no necesarios que pudieran incorporarse al sistema.

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 de Información Pública de Contrataciones (S6) del Sistema Estatal de Información.

Fecha: 03 de junio de 2026

Nombre y firma:

Mtro. Bernardo Sierra Gómez

Coordinador Ejecutivo



SECRETARÍA
EJECUTIVA DEL
SISTEMA ESTATAL
ANTICORRUPCIÓN
NUEVO LEÓN

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

8. INFORMACIÓN Y DOCUMENTOS COMPLEMENTARIOS

Para la integración del expediente administrativo, técnico y jurídico del S6, se recomienda conservar, entre otros documentos, los siguientes:

- Catálogo de Perfiles de Usuario del Sistema de Información Pública de Contrataciones (S6).
- Declaratoria de inicio de funciones y operación del S6.
- Aviso de Privacidad simplificado e integral del S6.

- Formatos de designación de Administrador del Ente Público, altas de usuario y responsivas de credenciales.
- Bitácoras de pruebas técnicas, incidencias, soporte, interoperabilidad y respaldo de información.
- Evidencia de capacitación, acompañamiento y comunicación oficial a entes públicos.
- Plan de trabajo para la implementación del Sistema Estatal de Información y acuerdos institucionales relacionados.
- Documentación de medidas de seguridad, análisis de riesgos, controles técnicos y procedimientos de atención a incidentes.

Monterrey, Nuevo León, a 03 de junio de 2026.

Atentamente



Mtro. Bernardo Sierra Gómez



SECRETARÍA
EJECUTIVA DEL
SISTEMA ESTATAL
ANTICORRUPCIÓN

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