EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS PERSONALES DEL **SISTEMA DE INFORMACIÓN DE LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS (S2)**

GLOSARIO DE TÉRMINOS

Para efectos de la presente Evaluación de Impacto de Protección de Datos Personales, se entenderá por:

1. Administrador o Administradores de Ente Público: Unidad administrativa a cargo del área de recursos humanos en los entes públicos del estado de Querétaro y sus municipios, y que será ejercido por el titular de dicha unidad o quien ejerza sus funciones.

2. Contrataciones Públicas: De conformidad con el artículo 29 de la Ley Local de Responsabilidades, en relación con el artículo 43 párrafo primero de la LGRA, así como el artículo 44 de las Bases para el Funcionamiento de la Plataforma Digital Estatal, se refiere a la tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles e inmuebles y dictamen en materia de avalúos;

3. EIPDP: Evaluación de Impacto de Protección de Datos Personales del S2;

4. Ley del Sistema Estatal: Ley del Sistema Estatal Anticorrupción de Querétaro;

5. Ley General de Protección de Datos: Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados;

6. Ley Local de Protección de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Querétaro;

7. Ley Local de Responsabilidades: Ley de Responsabilidades Administrativas del Estado de Querétaro;

8. LGRA: Ley General de Responsabilidades Administrativas;

9. Particulares Inhabilitados: Personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos en la LGRA y en la Ley Local de Responsabilidades;

10. S2: Sistema de Información de los Servidores Públicos que intervengan en Procedimientos de Contrataciones Públicas, mismo que constituye la Plataforma Informática que se pondrá en operación;

11. Servidor Público o Servidores Públicos: Personas físicas que desempeñan un empleo, cargo o comisión en los diversos entes públicos del Estado y sus municipios, conforme a lo dispuesto en el artículo 108 párrafos primero y cuarto de la Constitución Política de los Estados Unidos Mexicanos, en relación con el artículo 37 bis párrafo primero de la Constitución Política del Estado Libre y Soberano de Querétaro;

12. SESEA: Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Querétaro;

13. SESNA: Secretaría Ejecutiva del Sistema Nacional Anticorrupción.

APARTADO I
DESCRIPCIÓN DE LA PLATAFORMA INFORMÁTICA

A. NOMBRE DEL SISTEMA O PLATAFORMA INFORMÁTICA QUE IMPLIQUE UN TRATAMIENTO INTENSIVO DE DATOS PERSONALES.

Sistema de Información de los Servidores Públicos que intervengan en Procedimientos de Contrataciones Públicas (S2).

B. OBJETIVO QUE PERSIGUE LA PLATAFORMA INFORMÁTICA.

El objetivo general del S2, es permitir a los entes públicos del Estado y los municipios, registrar información relacionada con los Servidores Públicos que intervienen en Contrataciones Públicas, en la forma y términos que establece la LGRA y la Ley Local de Responsabilidades, para efectos de prevenir, investigar y sancionar las faltas administrativas y hechos de corrupción conforme a lo previsto en dichas leyes y la normatividad penal correspondiente, así como garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

Asimismo, los objetivos específicos del S2, son:

1. Ayudar a los entes públicos del Estado y sus municipios, a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, a efecto de preservar los principios de transparencia, imparcialidad y honradez.

2. Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

3. Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

4. Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

5. Ayudar a los entes públicos del Estado y sus municipios, a determinar a los Servidores Públicos que deberán cumplir el protocolo de actuación de contrataciones que sea expedido por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme a lo previsto en el artículo 44 párrafos primero y segundo de la LGRA.

6. Permitir al Comité Coordinador del Sistema Estatal Anticorrupción, establecer políticas públicas de combate a la corrupción, metodologías de medición y aprobar los indicadores necesarios para que se puedan evaluar las mismas.

7. La generación de datos estadísticos.

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

El fundamento legal del S2, lo constituyen los artículos 9 fracción XIII, 36 fracción I, 49 fracción II y 51 de la Ley General del Sistema Nacional Anticorrupción; 3 fracción XXII, 43, 44 y 45 de la LGRA; 9, fracciones XII y XVI, 17 párrafo tercero y 34 fracción X, de la Ley del Sistema Estatal; 29, 30 y 31 de la Ley Local de Responsabilidades; 5 fracción II, 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; así como 5 fracción II, 44, 45 y 46 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro.

D. CATEGORÍAS DE LOS TITULARES DE LOS DATOS PERSONALES.

En términos de los artículos 3 fracción XXXI de la Ley General de Protección de Datos, y 3 fracción XXVII de la Ley Local de Protección de Datos, el titular es la persona física a quien corresponden los datos personales.

Por su parte el artículo 134, párrafos primero, tercero, cuarto y sexto de la Constitución Federal, establece que los Servidores Públicos son responsables de cumplir las bases para que la administración de recursos y las Contrataciones Públicas, se apeguen a los principios de eficiencia, eficacia, economía, transparencia, imparcialidad y honradez.

Conforme a los artículos 43 párrafo primero, así como 44 párrafo tercero de la LGRA; 29 de la Ley Local de Responsabilidades; 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; además del 44 párrafo primero y 45 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro, en el S2 de la Plataforma Digital Nacional y de la Plataforma Digital Estatal, se hará énfasis en:

1. Nombres y adscripción de Servidores Públicos que intervengan en procedimientos de Contrataciones Públicas.

2. Relación de Particulares Inhabilitados.

Aunado a lo anterior, en términos de lo señalado en los artículos 43 párrafo segundo de la LGRA, 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional y 45 párrafo primero de las Bases para el Funcionamiento de la Plataforma Digital Estatal, corresponde al Comité Coordinador del Sistema Nacional Anticorrupción, determinar los formatos y mecanismos para registrar la información; y por su parte, el Comité Coordinador del Sistema Estatal Anticorrupción en el artículo 6º de las Bases para el Funcionamiento de la Plataforma Digital Estatal, facultó a al Secretario Técnico, para que emita "*protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones*".

Así, en ejercicio de tal facultad, la SESNA emitió las Especificaciones Técnicas, mismas que son de aplicación obligatoria para los órdenes federal, estatal y municipal, Especificaciones de las que destaca el Diccionario de Datos, del que se advierte que en el S2 también se registrará información sobre los superiores jerárquicos de los Servidores Públicos que intervienen en Contrataciones Públicas.[1]

[1] Las Especificaciones Técnicas emitidas por la SESNA, están disponibles en https://www.plataformadigitalnacional.org/especificaciones/s2 (consultadas el 30 de agosto de 2022)

En virtud de lo anterior, del análisis de las disposiciones constitucionales, legales y administrativas de referencia, serán titulares de los datos, objeto de tratamiento, los siguientes:

1. Los Servidores Públicos que intervengan en procedimientos de Contrataciones Públicas.

2. El Servidor Público que funge como superior inmediato al Servidor Público que intervenga en procedimientos de Contrataciones Públicas.

3. Los Particulares Inhabilitados.

E. LOS DATOS PERSONALES QUE SERÁN OBJETO DE TRATAMIENTO, DISTINGUIENDO LOS DATOS SENSIBLES.

Como se apuntó, conforme a los artículos 43 párrafo primero, así como 44 párrafo tercero de la LGRA; 30 párrafo primero y 31 párrafo tercero de la Ley Local de Responsabilidades; 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; además del 44 párrafo primero y 45 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro; así como en el Diccionario de Datos de las Especificaciones Técnicas emitidas por la SESNA, en ejercicio de la facultad que le otorga el artículo 6º de las citadas Bases para el Funcionamiento de la Plataforma Digital Nacional, en el S2 de la Plataforma Digital Nacional y de la Plataforma Digital Estatal, incluirá la siguiente información y datos personales que serán objeto de tratamiento:[2]

I. Los datos a inscribir en el S2 de los Servidores Públicos que intervengan en procedimientos para Contrataciones Públicas, y que son públicos de conformidad con los artículos 43 párrafo tercero de la LGRA; 29 párrafo segundo de la Ley Local de Responsabilidades; 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro, son:

1. Datos Generales:

1.1. Nombres y apellidos;

2. Datos del empleo, cargo o comisión:

[2] El Diccionario de Datos de las Especificaciones Técnicas, es disponible en https://docs.google.com/spreadsheets/d/1fRhDfHtrBPYyR36zxpenXWind9FP1pLAQJOVS69QwUM/edit#gid=262781770 (consultado el 30 de agosto de 2022).

2.1. Nombre del Ente Público donde labora el Servidor Público y sus siglas;

2.2. Denominación del puesto del Servidor Público;

2.3. Nivel del puesto del Servidor Público;

2.4. Nivel de responsabilidad dentro las contrataciones, que puede ser:

2.4.1. Atención;

2.4.2. Tramitación;

2.4.3. Resolución.

2.5. Tipo de función, que puede ser:

2.5.1. Técnica;

2.5.2. Responsable de la ejecución de los trabajos;

2.5.3. Responsable de la contratación;

2.5.4. Contratante;

2.5.5. Requirente;

2.5.6. Otra.

2.6. Tipos de procedimiento de Contrataciones Públicas en los que puede participar el Servidor Público, que pueden ser:

2.6.1. Adjudicación de contratos, también denominado contrataciones públicas;

2.6.2. Concesiones;

2.6.3. Licencias;

2.6.4. Permisos;

2.6.5. Autorizaciones y prórrogas;

2.6.6. Enajenación de bienes muebles;

2.6.7. Enajenación de bienes inmuebles; y

2.6.8. Asignación y emisión de dictámenes de avalúos.

II. Los datos a inscribir en el S2 del Servidor Público superior inmediato del Servidor Público que intervenga en procedimientos para Contrataciones Públicas, y que son públicos de conformidad con los artículos 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro, son:

1. Datos Generales:

1.1. Nombres y apellidos;

2. Datos del empleo, cargo o comisión:

2.1. Denominación del puesto del Servidor Público;

2.2. Nivel del puesto del Servidor Público.

III. Relación de Particulares Inhabilitados, esto de conformidad con el artículo 44 párrafo tercero de la LGRA y 22 de la Ley Local de Responsabilidades, información que, en términos de los preceptos en cita, en relación con los artículos 43 párrafo tercero de la propia LGRA y 29 párrafo segundo de la Ley Local de Responsabilidades, no se le dará publicidad en el S2, sino sólo acceso a los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2. Los datos que obran en dicha relación son los siguientes:

1. Nombres y apellidos de la persona física, o bien, razón social de la persona moral, que se encuentre inhabilitada para celebrar contratos con entes públicos derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades.

2. Periodo de la inhabilitación.

3. Ente público al que pertenece la autoridad que impuso la inhabilitación.

4. Autoridad que impuso la inhabilitación.

Datos Sensibles.

Los datos sensibles, conforme a los artículos 3 fracción X de la Ley General de Protección de Datos y 3 fracción X de la Ley Local de Protección de Datos, son aquéllos que se refieren a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación, o conlleve un grave riesgo para éste.

Se distinguen como tales los que se recabarán como parte de la relación de personas físicas, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades, los cuales se describen en el numeral III inmediato anterior, esto es así, ya que esa información puede propiciar un trato diferenciado injustificado que conlleve a discriminar al inhabilitado por parte de otros particulares, que al conocer dicha sanción, le nieguen o compliquen su contratación en el ámbito privado; aunado a ello, la publicitación de esa información, también podría provocar una afectación injustificada en los derechos del inhabilitado al generarse materialmente una sanción sin sustento expreso en ley, que tiene características de infamante, situación que trastocaría los mandatos contenidos en los artículos 14 párrafo tercero y 20 párrafo primero de la Constitución Federal.[3]

Las inhabilitaciones en cita, que expresamente la ley señala que son aquellas que derivan de procedimientos administrativos diversos a los previstos en la LGRA y la Ley Local de Responsabilidades, pueden ser, por ejemplo, aquellas impuesta conforme al artículo 76 de la Ley de Obra Pública del Estado de Querétaro, cuyo procedimiento se sujeta a lo previsto en esta Ley, así como a la Ley de Procedimientos Administrativos del Estado de Querétaro.[4]

También son aquellas inhabilitaciones para celebrar contratos con los entes públicos derivado de procedimientos sustanciados conforme a la Ley de Responsabilidades Administrativas del Estado de Querétaro durante su vigencia conforme a lo previsto en el transitorio tercero párrafos primero, segundo y cuarto, del Decreto por el que se expide la Ley General del Sistema Nacional Anticorrupción; la LGRA y la Ley Orgánica del Tribunal Federal de Justicia Administrativa, publicado en el Diario Oficial de la Federación el 18 de julio de 2016.[5]

---

[3] Constitución Federal: Artículos 14 párrafo tercero "*En los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata*".- Artículo 20 párrafo primero: "*Quedan prohibidas las penas de muerte, de mutilación, de infamia, la marca, los azotes, los palos, el tormento de cualquier especie, la multa excesiva, la confiscación de bienes y cualesquiera otras penas inusitadas y trascendentales. Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado*".

[4] Al respecto, véase los artículos 55, 56 Quarter y 76 de la Ley de Obra Pública del Estado de Querétaro.

[5] El primero transitorio y tercero transitorio párrafos primero, segundo y cuarto, del Decreto en cita, establecen lo siguiente: *Primero. El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación, sin perjuicio de lo previsto en los transitorios siguientes.- Tercero. La Ley General de Responsabilidades Administrativas entrará en vigor al año siguiente de la entrada en*

Cabe precisar, que conforme a los artículos 43 párrafo tercero en relación con el 44 párrafo tercero de la LGRA, así como 29 en relación con el 30 de la Ley Local de Responsabilidades, los datos sensibles de referencia no serán publicitados y sólo tendrán acceso a ellos, los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2, para efectos de prevenir, investigar y sancionar las faltas administrativas y hechos de corrupción, así como garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

F. LAS FINALIDADES DEL TRATAMIENTO INTENSIVO DE DATOS PERSONALES.

Los datos personales que recaba la SESEA, a través del S2, podrán ser utilizados para las siguientes finalidades:

1. Integrar el S2 al que refieren los artículos 29 y 30 de la Ley Local de Responsabilidades, así como 9, fracciones XII y XVI, 17 párrafo tercero y 34 fracción X, de la Ley del Sistema Estatal.

2. Recibir e integrar la información pública que los distintos entes públicos del estado de Querétaro y sus municipios, incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas que dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 9, fracciones XII y XVI de la Ley del Sistema Estatal.

3. Ayudar a los entes públicos del Estado y sus municipios, a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, a efecto de preservar los principios de transparencia, imparcialidad y honradez.

4. Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

---

vigor del presente Decreto.- En tanto entra en vigor la Ley a que se refiere el presente Transitorio, continuará aplicándose la legislación en materia de Responsabilidades Administrativas, en el ámbito federal y de las entidades federativas, que se encuentre vigente a la fecha de entrada en vigor del presente Decreto... Los procedimientos administrativos iniciados por las autoridades federales y locales con anterioridad a la entrada en vigor de la Ley General de Responsabilidades Administrativas, serán concluidos conforme a las disposiciones aplicables vigentes a su inicio. En consecuencia, la LGRA inició su vigencia el 19 de julio de 2017.

5. Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

6. Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

7. Ayudar a los entes públicos del Estado y sus municipios, a determinar a los Servidores Públicos que deberán cumplir el protocolo de actuación de contrataciones que sea expedido por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme a lo previsto en el artículo 44 párrafos primero y segundo de la LGRA.

8. Prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, conforme a lo previsto en la LGRA, la Ley Local de Responsabilidades y la normatividad penal aplicable.

9. Permitir al Comité Coordinador del Sistema Estatal Anticorrupción, establecer políticas públicas de combate a la corrupción, metodologías de medición y aprobar los indicadores necesarios para que se puedan evaluar las mismas, conforme a los artículos 9º fracciones III, V, VI y XII, 21 fracción XI, 30 fracción II y 34 fracción IV de la Ley del Sistema Estatal.

10. La generación de datos estadísticos para conocimiento público y como insumo para la obtención de los instrumentos referidos en el numeral anterior.

G. LOS PROCESOS, FASES O ACTIVIDADES OPERATIVAS DE LA PLATAFORMA INFORMÁTICA QUE INVOLUCREN EL TRATAMIENTO DE DATOS PERSONALES, ASÍ COMO SU DESCRIPCIÓN.

Conforme al Catálogo de Perfiles del S2, los perfiles de usuarios a considerar, son los siguientes:

Usuario 1 denominado "*Administrador de la SESEA*", que corresponde a la SESEA y que será ejercido por su Secretario Técnico.

Usuario 2 denominado "*Administrador de Ente Público*", que corresponde a la unidad administrativa a cargo del área de recursos humanos en los entes públicos del estado de Querétaro y sus municipios, y que será ejercido por el titular de dicha unidad o quien ejerza sus funciones.

Usuario 3 denominado "*OIC*", que corresponde a la Secretaría de la Contraloría del Estado o a los órganos internos de control de los entes públicos del estado de Querétaro y sus municipios, el cual será ejercido por el servidor público que autoricen dichas instancias.

Usuario 4 denominado *"Interesado"*, que corresponde a cualquier persona que acceda al S2 con la finalidad de consultar información pública que se refiere a los Servidores Públicos que intervengan en procedimientos para Contrataciones Públicas.

Para mayor entendimiento, en lo subsecuente se hará uso de las denominaciones de usuario apuntadas.

Actividad	Responsable	Descripción
1. Generación de usuarios y contraseñas.	El usuario con perfil de Administrador de la SESEA.	Se generan los usuarios y contraseñas para perfiles de Administrador de Ente Público y de OIC.
2. Captura y validación de datos generales.	Los usuarios con perfil de Administrador de Ente Público.	Se capturan y validan los datos de los Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos.
3. Emisión de reporte sobre captura de servidores públicos.	La SESEA, a través del S2.	Realizada la primera captura correspondiente a todos los Servidores Públicos que intervienen en Contrataciones Públicas y sus superiores inmediatos, el S2 automáticamente emitirá un primer reporte; y después de concluir cada actualización o validación de información quincenal, de la misma manera se emitirán reportes.
4. Consultas públicas.	Cualquier usuario.	Una vez capturada la información de los Servidores Públicos que intervienen en Contrataciones Públicas, la referida a sus nombres, entes

		públicos a los que están adscritos, nivel de responsabilidad y el tipo de procedimiento en la que intervienen, serán de consulta pública.
5. Captura y validación de Particulares Inhabilitados.	Los usuarios con perfil de OIC	Se capturan y validan los datos de los Particulares Inhabilitados.
6. Emisión de reporte sobre Particulares Inhabilitados.	La SESEA, a través del S2.	Realizada la primera captura correspondiente a todos los Particulares Inhabilitados, el S2 automáticamente emitirá un primer reporte; y después de concluir cada actualización de información de la misma manera se emitirán reportes.
7. Eliminación de datos.	La SESEA, a través del S2.	Cuando los datos hayan cumplido con la finalidad para la cual fueron recabados, y que cumplan con las condiciones establecidas en la Ley General de Archivos, podrán ser eliminados del S2.

H. FORMA EN QUE SE RECABARÁN LOS DATOS PERSONALES O, EN SU CASO, LAS FUENTES DE LAS CUALES PROVIENEN.

Fuente	Datos que se recabarán
1. Administrador de Ente Público.	Datos de los Servidores Públicos que intervienen en Contrataciones Públicas y sus superiores inmediatos.
2. OIC	Datos de los Particulares Inhabilitados.
3. S2.	Los usuarios, contraseñas cifradas, así como los reportes correspondientes.

I. LA TRANSFERENCIA DE DATOS PERSONALES QUE, EN SU CASO, PRETENDAN EFECTUARSE CON LA PUESTA EN OPERACIÓN DE LA PLATAFORMA INFORMÁTICA.

Los datos públicos de los Servidores Públicos que intervienen en Contrataciones Públicas y sus superiores inmediatos, una vez registrados en el S2, serán transferidos a la SESNA a través de la Plataforma Digital Nacional, instancia que conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos conforme a lo previsto en la letra F del apartado I de la presente EIPDP.

Asimismo, los datos concernientes a Particulares Inhabilitados, una vez registrados se transferirán a los usuarios con perfil de Administradores de Ente Público y de OIC, instancias que conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos, en este caso, esos fines son específicamente los previstos en la letra F, numerales 4, 5, 6 y 8 del apartado I de la presente EIPDP.

Los datos referidos en el párrafo anterior, también serán transferidos a la SESNA, cuando los requiera, y conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos, en este caso, esos fines son específicamente los previstos en la letra F, numerales 2, 4, 5, 6, 8 y 10 del apartado I de la presente EIPDP.

Las transferencias referidas en los párrafos anteriores, se realizan sin necesidad de recabar el consentimiento de los titulares, ya que se encuentra dentro de los supuestos de excepción previstos en los artículos 70 fracciones I y II de la Ley General de Protección de Datos; 59, 63 y 64 fracciones I y II de la Ley Local de Protección de Datos.

J. DURACIÓN DE LA PLATAFORMA INFORMÁTICA.

La duración del S2, será por tiempo indefinido, ya que hasta la fecha no existe disposición legal, reglamentaria o administrativa, que establezca un plazo de vigencia para el funcionamiento de la Plataforma.

K. LA TECNOLOGÍA QUE SE UTILIZARÁ PARA EFECTUAR EL TRATAMIENTO DE DATOS PERSONALES.

El S2 es el encargado de la captura de datos, del procesamiento de los mismos, generación de reportes y generación de datos, y utiliza la siguiente tecnología para su funcionamiento:

1. Almacenamiento en la nube

2. Sistema operativo *Linux CentOS 7*: Instalado en el servidor de referencia, para manejo del mismo. - 3 GB de Memoria RAM.

3. *Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium.*

4. Base de datos My /PHP.

L. LAS MEDIDAS DE SEGURIDAD DE CARÁCTER ADMINISTRATIVO, FÍSICO Y TECNOLÓGICAS A IMPLEMENTAR.

En la siguiente tabla se presentan las medidas de seguridad de carácter administrativo, físico y tecnológico, que esta Entidad Pública adoptará para garantizar la protección de los datos informáticos objeto del tratamiento en el S2:

Medidas de seguridad	Descripción
Administrativas	Publicación en el Periódico Oficial del Gobierno del Estado "La Sombra de Arteaga", del **Catálogo de Perfiles del S2**, en el cual se distinguen niveles de acceso, gestión y uso de la información del S2 (reglas y privilegios), para cada usuario o grupo de usuarios conforme a sus responsabilidades (determinación de roles y responsabilidades de los operadores del sistema).
	Asistencia a los **talleres de capacitación** sobre el **uso adecuado de los datos personales**, de las personas que la SESEA determine, por las funciones que realizan dentro del S2.
	Identificación del ciclo de vida de los datos personales en función de las finalidades para las que fueron recabados.
	Emisión de guía con recomendaciones para la creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, por ejemplo: Cerrar sesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, entre otros.
	Existencia de trazabilidad y posibilidad de identificar quién tuvo acceso a los datos y los tratamientos realizados.

	Difusión del instructivo de llenado con base al estándar de datos emitido por la SESNA.
	Poner a disposición de los titulares de los datos personales por conducto de los Administradores de Ente y de manera electrónica en el portal de la Plataforma Digital Estatal, el aviso de privacidad del S2.
Físicas/Tec-nológicas	Asignación para cada usuario, de un identificador único en el sistema al cual se le vincularán sus privilegios y acceso.
	Responsabilizar a cada usuario de guardar en secreto las contraseñas y mecanismos correspondientes para su acceso.
	Creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, por ejemplo: Cerrar sesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, entre otros.
	Prohibición del uso en el S2 de software ilegal o no autorizado, para lo cual se cuenta con una bitácora de control de software contra virus y software malicioso.
	Monitorización del tráfico de las actividades en la red de la SESEA para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, entre otras.
	Uso de cifrado con contraseña, certificados digitales, token y autenticación de dos pasos.
	Implementación de reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades (determinación de roles y responsabilidades de los operadores del sistema).
	Uso de **bitácora** de registros de excepciones y eventos relevantes de seguridad en los sistemas y activos que tengan relación con el S2.
	Uso de *Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium*.
	Limitación de acceso al servidor por filtrado de dirección IP.
	Instalación del software de desarrollo en una computadora diferente a la del software de producción.

	Vigilancia constante entre la consistencia del estándar de datos publicado por la Plataforma Digital Nacional y el aplicado en el S2.
	Respaldo mensual de la base de datos.
	Eliminación de fuentes de humedad, cuidado de temperatura interna del *site* y uso de protocolos en caso de desastres naturales; así como correcto aislamiento de cables eléctricos y de datos.
	Cifrado de información interna en el servidor.
	Bloqueo automatizado a los datos de Particulares Inhabilitados, cuando pierdan vigencia las inhabilitaciones impuestas.
	Acceso únicamente para personal autorizado al lugar en que se ubique el *site*, dentro de las instalaciones de la SESEA.
	Limpieza constante de *site* y componentes del S2.

M. EL NOMBRE Y CARGO DE LOS SERVIDORES PÚBLICOS QUE CUENTAN CON LA FACULTAD EXPRESA PARA DECIDIR, APROBAR O AUTORIZAR LA OPERACIÓN DE LA PLATAFORMA INFORMÁTICA.

1. Lic. Jorge Sánchez Martínez, Secretario Técnico de la SESEA, en calidad de administrador de la Plataforma Digital Estatal prevista en la Ley del Sistema Estatal, a la cual pertenece el S2.

2. Lic. José Félix Torres Montero, en calidad de responsable del funcionamiento y operación de la Plataforma Digital Estatal prevista en la Ley del Sistema Estatal, a la cual pertenece el S2.

APARTADO II

LA JUSTIFICACIÓN DE LA NECESIDAD DE IMPLEMENTAR LA PLATAFORMA INFORMÁTICA

Conforme al artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal, los recursos públicos deben administrarse con "*eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a los que estén destinados*"; y en ese sentido, las adquisiciones, arrendamientos y enajenaciones de todo tipo de bienes, prestación de servicios de cualquier naturaleza y la contratación de obra que realice el Estado, por regla general se adjudicarán o llevarán a cabo a través de licitaciones públicas mediante convocatoria pública para que libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de

asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes.

Precisando, además, que cuando el procedimiento de licitación no sea el idóneo, es posible que, para asegurar dichas condiciones, las leyes establezcan las "*bases, procedimientos, reglas, requisitos y demás elementos para acreditar la economía, eficacia, eficiencia, imparcialidad y honradez que aseguren las mejores condiciones para el Estado*".

Sobre lo anterior, es destacable que conforme a los artículos 7.4, 8.4, 9.1 y 12.2 inciso d) de la Convención de las Naciones Unidas contra la Corrupción, los Estados Parte han convenido, entre otros aspectos, que de conformidad con los principios fundamentales de su derecho interno:

1. Procurarán adoptar sistemas destinados a promover la transparencia y a prevenir conflictos de intereses, o a mantener y fortalecer dichos sistemas.

2.- Considerarán la posibilidad de establecer medidas y sistemas para facilitar que los funcionarios públicos denuncien todo acto de corrupción a las autoridades competentes cuando tengan conocimiento de ellos en el ejercicio de sus funciones.

3.- Adoptará las medidas necesarias para establecer sistemas apropiados de contratación pública, basados en la transparencia, la competencia y criterios objetivos de adopción de decisiones, que sean eficaces, entre otras cosas, para prevenir la corrupción. Esos sistemas, en cuya aplicación se podrán tener en cuenta valores mínimos apropiados, deberán abordar, entre otras cosas:

a) La difusión pública de información relativa a procedimientos de contratación pública y contratos;

b) La aplicación de criterios objetivos y predeterminados para la adopción de decisiones sobre contratación pública a fin de facilitar la ulterior verificación de la aplicación correcta de las reglas o procedimientos;

c) Cuando proceda, la adopción de medidas para reglamentar las cuestiones relativas al personal encargado de la contratación pública, en particular declaraciones de interés respecto de determinadas Contrataciones Públicas, procedimientos de preselección y requisitos de capacitación.

4.- Adoptar medidas para "*prevenir la utilización indebida de los procedimientos que regulan a las entidades privadas, incluidos los procedimientos relativos a la concesión de subsidios y licencias por las autoridades públicas para actividades comerciales*".

Adicionalmente, el artículo III.5 de la Convención Interamericana contra la Corrupción, compromete al Estado Mexicano a considerar la aplicabilidad de medidas, dentro de sus propios sistemas institucionales, destinadas a crear, mantener y fortalecer "*sistemas para la contratación de funcionarios públicos y para la adquisición de bienes y servicios por parte del Estado que aseguren la publicidad, equidad y eficiencia de tales sistemas*".

En tal contexto, y atendiendo a los artículos 134 párrafos primero, tercero y cuarto, así como 73 fracciones XXIV y XXIX-V de la Constitución Federal,[6] en relación con los artículos 7.4, 8.4, 9.1 y 12.2 inciso d) de la Convención de las Naciones Unidas contra la Corrupción, así como III.5 de la Convención Interamericana contra la Corrupción, la Ley General del Sistema Nacional Anticorrupción y la LGRA, prevén la existencia de un Sistema de los Servidores Públicos que intervengan en procedimientos de Contrataciones Públicas como parte de la Plataforma Digital Nacional; mientras que la Ley del Sistema Estatal y la Ley Local de Responsabilidades, prevén la existencia del S2, como una herramienta indispensable de la Plataforma Digital Estatal para recibir e integrar información que las autoridades locales incorporen para transmitirse a la citada Plataforma Digital Nacional.

Esa información, conforme a los artículos 29 y 30 de la Ley Local de Responsabilidades, en relación con los artículos 43 párrafo primero y 44 párrafo tercero de la LGRA, sustancialmente la constituyen los nombres y adscripción de los Servidores Públicos que intervienen en procedimientos para Contrataciones Públicas, así como una relación de Particulares Inhabilitados.

Adicionalmente, conforme al Diccionario de Datos de las Especificaciones Técnicas emitidas por la SESNA, lo anterior se complementará con información de Servidores Públicos superiores inmediatos de los Servidores Públicos que intervienen en procedimientos de Contrataciones, tales como sus nombres y apellidos, y los datos de su empleo cargo o comisión, lo cual constituye información pública, en términos de los artículos 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro.

---

[6] Artículo 73 de la Constitución Federal: *El Congreso tiene facultad: XXIV.- Para expedir las leyes que regulen la organización y facultades de la Auditoría Superior de la Federación y las demás que normen la gestión, control y evaluación de los Poderes de la Unión y de los entes públicos federales; así como para expedir la ley general que establezca las bases de coordinación del Sistema Nacional Anticorrupción a que se refiere el artículo 113 de esta Constitución…XXIX-V. Para expedir la ley general que distribuya competencias entre los órdenes de gobierno para establecer las responsabilidades administrativas de los servidores públicos, sus obligaciones, las sanciones aplicables por los actos u omisiones en que éstos incurran y las que correspondan a los particulares vinculados con faltas administrativas graves que al efecto prevea, así como los procedimientos para su aplicación.*

Asimismo, en cumplimiento a lo ordenado por el Comité Coordinador del Sistema Estatal Anticorrupción, en el acuerdo CC/SEA/03/EXTRAORDINARIA/2022 aprobado en Sesión Extraordinaria celebrada el 13 de junio de 2022, y que contiene las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro, publicadas en el Periódico Oficial del Gobierno del Estado "La Sombra de Arteaga" el 24 de junio de 2022, al S2 también se incorporarán los datos referidos en el Apartado I, letra E, fracción I de la presente EIPDP, respecto a Servidores Públicos que intervengan en procedimientos de enajenaciones de bienes inmuebles, esto de conformidad con el artículo 44 de dichas Bases.

Como se aprecia, la información que se incorporará al S2 es relativa a los Servidores Públicos adscritos a los distintos entes públicos del Estado y sus municipios, y que corresponde resguardar a las unidades administrativas a cargo del área de recursos humanos, así como a los órganos internos de control, siendo que éstos últimos además, en términos de lo previsto en el artículo 31 de la Ley Local de Responsabilidades, tendrán a su cargo "*supervisar la ejecución de los procedimientos de contratación pública por parte de los contratantes para garantizar que se lleva a cabo en los términos de las disposiciones en la materia, realizando las verificaciones procedentes si descubren anomalías*".

Así, se justifica plenamente la necesidad de poner en operación el S2, el cual constituye el instrumento indispensable para integrar la información que por Ley, debe obrar en la Plataforma Digital Estatal y en la Plataforma Digital Nacional, en relación a los Servidores Públicos que intervienen en procedimientos de contrataciones, sus superiores inmediatos y sobre aquellos Particulares Inhabilitados; lo anterior, con el propósito de que dicha información sea utilizada por los integrantes del Sistema Estatal Anticorrupción, del Sistema Nacional Anticorrupción y autoridades competentes, en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

Lo anterior, considerando que el tratamiento de datos personales es cualquier operación o conjunto de operaciones relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales,[7] por lo que dicho tratamiento, debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable confiera a quien vaya a realizarlo, lo cual ocurre en la especie conforme a lo expuesto.

Aunado a ello, las medidas de seguridad resultan idóneas para garantizar el derecho a la protección de datos personales de los titulares, en virtud de que la información se encuentra protegida con accesos restringidos a los servidores donde se

[7] Ver artículo 3 fracción XXXIII de la Ley General de Protección de Datos.

resguarda, contraseñas de usuario, cifrado de la información, e incluso monitorización del comportamiento de la Plataforma, sin dejar de mencionar que se tiene previsto realizar capacitaciones que permitan que los usuarios manejen correctamente el S2.

De igual manera se considera que las medidas propuestas son las estrictamente necesarias en el sentido de ser las más moderadas para garantizar el derecho a la protección de datos, ya que a través de su implementación se busca reducir al mínimo nivel los riesgos asociados al tratamiento de los datos personales, considerando que la mayoría de los datos que se registrarán en el S2 serán públicos; así, las medidas administrativas, físicas y tecnológicas previstas, son moderadas pues no restringen a los titulares el uso de sus datos, ni impiden que se les dé la publicidad que por ley corresponde.

Las medidas de seguridad también son las más equilibradas en función al mayor número de beneficios o ventajas que perjuicios en el tratamiento y protección de los datos personales de los titulares, beneficios que se obtendrán al concretar las finalidades descritas en la letra F del apartado I del presente EIPDP; esos **BENEFICIOS** son:

1. Integrar el S2 al que refieren los artículos 29 y 30 de la Ley Local de Responsabilidades, así como 9, fracciones XII y XVI, 17 párrafo tercero y 34 fracción X, párrafo primero de la Ley del Sistema Estatal.

2. Recibir e integrar la información pública que los distintos entes públicos del estado de Querétaro y sus municipios, incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas que dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 4, de la Ley del Sistema Estatal.

3. Ayudar a los entes públicos del Estado y sus municipios, a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, a efecto de preservar los principios de transparencia, imparcialidad y honradez.

4. Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

5. Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

6. Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

7. Ayudar a los entes públicos del Estado y sus municipios, a determinar a los Servidores Públicos que deberán cumplir el protocolo de actuación de contrataciones que sea expedido por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme a lo previsto en el artículo 44 párrafos primero y segundo de la LGRA.

8. Prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, conforme a lo previsto en la LGRA, la Ley Local de Responsabilidades y la normatividad penal aplicable.

9. Permitir al Comité Coordinador del Sistema Estatal Anticorrupción, establecer políticas públicas de combate a la corrupción, metodologías de medición y aprobar los indicadores necesarios para que se puedan evaluar las mismas, conforme a los artículos 9º fracciones III, V, VI y XII, 21 fracción XI, 30 fracción II y 34 fracción IV de la Ley del Sistema Estatal.

10. La generación de datos estadísticos para conocimiento público y como insumo para la obtención de los instrumentos referidos en el inciso anterior.

Así, el S2 con la implementación de las medidas de seguridad previstas en el presente instrumento, refleja un mayor número de beneficios o ventajas que perjuicios para garantizar el derecho a la protección de datos personales de los titulares, debiéndose destacar que la puesta en marcha del S2, **RESULTA**:

a) Idónea, para identificar a los Servidores Públicos que intervienen en los procedimientos de Contrataciones Públicas y a sus superiores inmediatos, y así seguir su desempeño para preservar los principios de transparencia, imparcialidad y honradez, y demás condiciones establecidas en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal, Servidores Públicos que habrán de sujetarse al protocolo de actuación de contrataciones que emita el Comité Coordinador del Sistema Nacional Anticorrupción.

De igual manera, también es idónea para identificar a los particulares que se encuentren inhabilitados para celebrar Contrataciones Públicas derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades, como son las inhabilitaciones impuestas de conformidad con los artículos 76 de la Ley de Obra Pública del Estado de Querétaro, y aquellas derivadas de procedimientos sustanciados conforme a la Ley de Responsabilidades

Administrativas del Estado de Querétaro durante su vigencia y que aún tengan efectos.[8]

Todo lo descrito en el presente inciso, será de utilidad para prevenir, investigar, y sancionar faltas administrativas y hechos de corrupción derivados de procedimientos de Contrataciones Públicas.

b) Necesaria, ya que es el mecanismo más benigno con los derechos fundamentales intervenidos, atento a que solamente se daría difusión a información que es pública, de conformidad con los artículos 43 párrafo tercero de la LGRA; 29 y 30 de la Ley Local de Responsabilidades; 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro.

Mientras que atento a lo previsto en los artículos 43 párrafo tercero en relación con el 44 párrafo tercero de la LGRA, así como 29, 30 y 31 de la Ley Local de Responsabilidades, los datos que obren en la relación de Particulares Inhabilitados, no serán publicitados y sólo tendrán acceso a ellos, los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2, para efectos de prevenir, investigar y sancionar faltas administrativas y hechos de corrupción y garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

De esta manera, se mantendrá la efectiva protección a datos que pudieran generar una mayor afectación a la esfera privada.

c) Proporcional en sentido estricto, ya que guarda una relación adecuada con el significado de los derechos intervenidos, puesto que permite tener escrutinio sobre el desempeño de los Servidores Públicos que intervienen en procedimientos públicos que involucran recursos públicos y que otorgan derechos a terceros, de manera que se vigile que su desarrollo no sea utilizado en beneficio de intereses particulares y, por ende, ajenos a lo que persigue la función pública, generando con ello la posibilidad de realizar jurídica y materialmente, las finalidades constitucionales de prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como la fiscalización y control de recursos públicos.

[8] Será en el Sistema de Información de Servidores Públicos y Particulares Sancionados (S3), en el que se inscribirán las sanciones impuestas a Servidores Públicos y particulares por la comisión de faltas administrativas en términos de la LGRA y hechos de corrupción en términos de la legislación penal, esto en términos de lo señalado en los artículos 52 de la LGRA y 22 de la Ley Local de Responsabilidades.

APARTADO III

LA REPRESENTACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES A TRATAR

En este apartado se describirá y representará cada una de las fases del S2 que implique un tratamiento intensivo o relevante de datos personales.

Se reconocen **CINCO FASES** dentro del ciclo de vida de los datos personales dentro del S2, que son:

Fase I: Obtención de los datos personales.

Fase II: Almacenamiento de los datos.

Fase III: Uso de los datos.

Fase IV: Divulgación de los datos.

Fase V: Cancelación o supresión de los datos.

En el siguiente cuadro se precisan las actividades, los datos que son tratados, las personas que intervienen (donde se especifica las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales) y las tecnologías que se emplean; asimismo, es importante destacar que los plazos de conservación o almacenamiento de los datos personales son referidos expresamente en la fase II, en el apartado de "*datos que son tratados*", mientras que las técnicas para garantizar el borrado seguro de los datos, se pueden apreciar en la fase V:

FASE I				
Formulario	Actividades	Datos que son tratados	Personas que intervienen	Tecnologías que se emplean
Datos de la cuenta del Administrador de Ente Público.	Captura y validación dentro de los datos proporcionados por el Administrador de Ente Público.	(i) Nombre. (ii) Ente Público al que pertenece. (iii) Puesto dentro del Ente Público. (iv) Correo electrónico institucional.	(i) Como facilitador de información, el Administrador de Ente Público. (ii) Capturador de Datos, que serán el Jefe de Departamento de la Plataforma Digital Anticorrupción de	(i) Recabación de información por correo electrónico institucional, medios electrónicos, archivos físicos y/o papelería proporcionados por los responsables de la misma.

			Querétaro, y los Servidores Públicos que se encuentren adscritos a dicho Departamento.	(ii) Captura de información en el módulo de altas de Administradores de Ente Público del S2.
Datos de la cuenta de OIC	Captura y validación dentro de los datos proporcionados por el OIC.	(i) Nombre. (ii) Ente Público al que pertenece. (iii) Puesto dentro del Ente Público. (iv) Correo electrónico institucional.	(i) Como facilitador de información, el OIC. (ii) Capturador de Datos, que serán el Jefe de Departamento de la Plataforma Digital Anticorrupción de Querétaro, y los servidores públicos que se encuentren adscritos a dicho Departamento.	(i) Recabación de información por correo electrónico institucional, medios electrónicos, archivos físicos y/o papelería proporcionados por los responsables de la misma. (ii) Captura de información en el módulo de altas de OIC del S2.
Datos generales del Servidor Público.	(i) Captura de datos de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos. (ii) Generación de reportes.	Del Servidor Público que interviene en procedimientos de Contrataciones Públicas y de sus superiores inmediatos, los datos descritos en el apartado I, letra E fracciones I y II, y que se refieren a los datos generales y datos del empleo cargo o comisión.	(i). Facilitador de información, quien será el Administrador de Ente Público. (ii). Capturador de datos, que será el Administrador de Ente Público.	(i) Recabación de información por correo electrónico institucional, medios electrónicos, archivos físicos o papelería proporcionados por el Administrador de Ente Público. (ii) Captura de información en el módulo de servidores que intervienen en los procesos de Contratación del S2. (iii) Generación de usuario y contraseña,

				mediante el módulo automatizado de generación de contraseñas seguras del S2.
Lista de Particulares Inhabilitados.	(i) Captura de datos de Particulares Inhabilitados; (ii) Generación de reportes.	(i) Nombres y apellidos de la persona física, o bien, razón social de la persona moral, que esté inhabilitada. (ii) Periodo de la inhabilitación. (iii) Ente público al que pertenece la autoridad que impuso la inhabilitación. (iv) Autoridad que impuso la inhabilitación.	Facilitador de información, quien será el OIC de ente público.	(i) Recabación de información por correo electrónico institucional, medios electrónicos, archivos físicos o papelería proporcionados por el OIC. (ii) Captura de información en el módulo de Particulares Inhabilitados del S2. (iii) Generación de usuario y contraseña, mediante el módulo automatizado de generación de contraseñas seguras del S2.
FASE II Almacenamiento de los datos				
Formulario	Actividades	Datos que son tratados	Personas que intervienen	Tecnologías que se emplean
No aplica.	Los datos que son capturados por el Administrador de la SESEA por conducto del Departamento de Sistemas Informáticos y Plataforma Digital, así como por el	Se almacenarán todos los datos descritos en el apartado I, letra E fracciones I y II, y que se refieren a los datos generales y datos del empleo cargo o comisión, referentes a los Servidores	No aplica.	(i) Almacenamiento en la nube (ii) Sistema operativo Linux CentOS 7: Instalado en el servidor de referencia, para manejo del

	Administrador de Ente Público y por el OIC, serán almacenados en los servidores de la SESEA.	Públicos que participan en Procedimientos de Contrataciones Públicas y sus superiores inmediatos; asimismo, la relación de Particulares Inhabilitados, cuyos datos se describen en la fracción III de la letra E en cita. El periodo de conservación de los datos personales será de 7 años a partir de que hayan cumplido con la función para la cual fueron recabados. Para determinar el periodo de almacenamiento, tratándose de los datos de los Servidores Públicos que participan en Contrataciones Públicas y sus superiores inmediatos, se consideran los datos validados quincenalmente por el Administrador de Ente, al validar la información comienzan a correr los 7 años de conservación; y tratándose de la relación de		mismo. - 3 GB de Memoria RAM. (iii) Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium. (iv) Base de datos MySQL/PHP.

		inhabilitados, comenzará a correr a partir de que el OIC hace la inscripción en el S2.		
FASE III Uso de los datos				
Formulario	Actividades	Datos que son tratados	Personas que intervienen	Tecnologías que se emplean
Servidores Públicos que intervienen con contrataciones públicas.	Los datos públicos de los formularios del Servidor Público que interviene en procedimientos de Contrataciones Públicas y de sus superiores inmediatos, se usarán conforme a lo establecido en las finalidades y transferencia de datos precisadas en esta EIPDP.	Los datos públicos de los formularios del Servidor Público que interviene en procedimientos de Contrataciones Públicas y de sus superiores inmediatos.	(i) Administrador de Ente Público. (ii) Interesados. (iii) Administrador de la SESEA. (iv) SESNA.	(i) Acceso con Usuario, contraseña cifrada y validación de consultas mediante token de seguridad y de uso único por usuario. (ii) Módulo de Servidores Públicos que Intervienen en procedimientos de Contrataciones Públicas. (iii) Módulos de Administración del S2, según corresponda el perfil de usuario desempeñado siendo éstos los correspondientes a Administrador de la SESEA, Administrador de Ente Público, e Interesado. (v) Módulo de interoperabilidad con la SESNA.
Formulario de relación de	Los datos del formulario de	(i) Nombres y apellidos de la	(i) Administrador de Ente Público.	(i) Acceso con Usuario,

Particulares Inhabilitados.	Particulares Inhabitados, se usarán conforme a lo establecido en las finalidades y transferencia de datos precisadas en esta EIPDP.	persona física, o bien, razón social de la persona moral que esté inhabilitada (ii) Periodo de la inhabilitación. (iii) Ente público al que pertenece la autoridad que impuso la inhabilitación. (iv) Autoridad que impuso la inhabilitación.	(ii) OIC. (iii) Administrador de la SESEA. (iv) SESNA.	contraseña cifrada y validación de consultas mediante token de seguridad y de uso único por usuario. (ii) Módulo de Particulares Inhabilitados. (iii) Módulos de Administración del S2, según corresponda el perfil de usuario desempeñado siendo éstos los correspondientes a Administrador de la SESEA, Administrador de Ente Público y OIC.
FASE IV Divulgación de los datos				
Formulario	Actividades	Datos que son tratados	Personas que intervienen	Tecnologías que se emplean
No aplica	Los datos que serán objeto de divulgación, serán exclusivamente del Servidor Público que interviene en procedimientos de Contrataciones Públicas, y específicamente los siguientes: su nombre y apellidos, el Ente Público al que está adscrito, denominación de su puesto, nivel	Los datos del Servidor Público que interviene en procedimientos de Contrataciones Públicas, siguientes: su nombre y apellidos, el Ente Público al que está adscrito, denominación de su puesto, nivel de responsabilidad y los tipos de procedimientos de	Personas que tengan perfil de Interesado, que realice la consulta.	(i) Módulo de vista pública del S2.

	de responsabilidad y los tipos de procedimientos de Contrataciones Públicas en que interviene. Dicha Información podrá ser mostrada en un apartado para la consulta del público en general en el S2.	Contrataciones Públicas en que interviene.		
FASE V Cancelación o supresión de los datos				
Formulario	Actividades	Datos que son tratados	Personas que intervienen	Tecnologías que se emplean
No aplica	La eliminación total de los datos almacenados en los servidores de la SESEA, cuando hayan cumplido con las condiciones de cancelación.	Los datos de los formularios de los Servidores Públicos que intervienen en Contrataciones Públicas y de sus superiores inmediatos, así como de Particulares Inhabilitados, precisados en esta EIPDP.	(i) Administrador de Ente Público. (ii) OIC.	(i) Módulo de Servidores que Intervienen en los Procesos de Contratación del S2. (ii) Módulo de relación de Particulares Inhabilitados del S2

En cuanto a los medios y fuentes para recabar los datos personales, estos se especifican en la letra H del apartado I de esta EIPDP, denominada "*forma en que se recabarán los datos personales o, en su caso, las fuentes de las cuales provienen*".

APARTADO IV
IDENTIFICACIÓN, ANÁLISIS Y GESTIÓN DE LOS RIESGOS PARA LA PROTECCIÓN DE DATOS PERSONALES

En este apartado se incluyen la gestión de riesgos, que tiene por objeto identificar y analizar los posibles riesgos y amenazas, así como los datos o consecuencias que pudieran producirse al ponerse en el S2, esto mediante el **Plan General para Gestionar los RIESGOS IDENTIFICADOS**, en el cual:

A. Se identifica y describe de manera específica los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación del S2;

B. Se pondera de forma cuantitativa y cualitativa, la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales; y

C. Se señalan las medidas y controles concretos que se adoptarán para eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales.

El desarrollo del plan de referencia se presenta a continuación:

PLAN GENERAL PARA GESTIONAR LOS RIESGOS IDENTIFICADOS

A. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación de la Plataforma Informática.

Riesgo es la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.[9] El nivel del riesgo se mide según la probabilidad de materializarse y su impacto.

Así, para evaluar un riesgo es necesario prever todos los posibles escenarios en los que se podría actualizar, considerando las amenazas entendiendo éstas como cualquier factor con potencial para provocar un daño o perjuicio a los titulares de los datos sobre los que se realiza el tratamiento.

Para identificar de forma adecuada las amenazas asociadas a las actividades de tratamiento, se debe tener en cuenta el ciclo de vida de los datos en cada operación, desde su inicio hasta el momento en el que finaliza.

B. La ponderación cuantitativa y cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales.

La ponderación de riesgos consiste en valorar y estimar la probabilidad de ocurrencia y el impacto de la materialización del riesgo.

---

[9] Guía Práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetos al RGPD. Agencia Española de Protección de Datos. Página 25. Consultada el 31 de marzo de 2021, disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

La metodología de valoración de la probabilidad de ocurrencia implementada por este Ente Público, se basa en los siguientes cuatro niveles de escala posibles:

Probabilidad de ocurrencia
1.- Muy baja
2.- Limitada (ocasional)
3.- Significativa (alta)
4.- Máxima (muy elevada)

Por su parte, el impacto se determina con base a los posibles daños que se pueden producir si la amenaza se materializa. Por consiguiente, el impacto también se evalúa con la misma escala de cuatro variables:

1. Impacto muy bajo: No genera consecuencias sobre el interesado.

2. Impacto limitado: Sus consecuencias implican un daño menor sin impacto relevante sobre el interesado.

3. Impacto significativo: Sus consecuencias implican un daño elevado con impacto sobre el interesado.

4. Impacto máximo: Consecuencias que implican un daño muy elevado con impacto crítico sobre el interesado.

Tomando como base las escalas de probabilidad e impacto, para poder determinar el riesgo inherente, es necesario asignar valores a cada uno de los niveles de las escalas, los cuales comprenden desde el valor 1, en el caso del muy bajo, hasta el valor 4 en el caso del máximo.

Muy bajo	**1**
Limitado	**2**
Significativo	**3**
Máximo	**4**

El riesgo inherente es el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo

inherente surge de la exposición que se tenga a la operación de tratamiento en lo particular y de la probabilidad de que la amenaza asociada al riesgo se materialice.

El cálculo del riesgo inherente se realiza mediante la siguiente fórmula:

Riesgo= Probabilidad x Impacto

Al aplicar la fórmula anterior a una matriz de riesgo, puede darse el siguiente resultado:

		Impacto			
		Muy bajo	Limitado	Significativo	Máximo
Probabilidad de ocurrencia	Máxima	4	8	12	16
	Significativa	3	6	9	12
	Limitada	2	4	6	8
	Muy Baja	1	2	3	4

Estableciendo valores numéricos a la probabilidad de ocurrencia y otro al impacto, se obtiene una posición en la matriz que corresponde con el riesgo inherente resultado de aplicar la fórmula. El resultado del riesgo inherente se puede considerar en los siguientes niveles en función del valor obtenido:

Bajo	Si el valor se sitúa entre los valores 1 y 2
Medio	Si el valor es mayor de 2 y menor o igual que 6
Alto	Si el valor es mayor que 6 y menor o igual a 9
Muy Alto	Si el valor es mayor que 9

En el siguiente cuadro, en términos de lo expuesto en los apartados A y B de este Plan General para Gestionar los Riesgos Identificados, se presentan los riesgos de carácter administrativo, físicos o tecnológicos que esta Entidad Pública ha detectado y que podrían configurarse con la puesta en operaciones del S2; asimismo, considerando los criterios descritos, se relacionan las amenazas, los riesgos, su probabilidad de ocurrencia, impacto y su riesgo inherente.

<table>
<tr><th colspan="2">Riesgos administrativos</th></tr>
<tr><th colspan="2">Amenaza de pérdida o destrucción no autorizada</th></tr>
<tr><td>Fases del ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención de datos personales.</td><td>Eliminación de datos de los Servidores Públicos de los entes públicos, de manera accidental o intencional.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>3</td><td>6</td></tr>
</table>
Eliminación de datos de los Particulares Inhabilitados, de manera accidental o intencional.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>4</td><td>8</td></tr>
</table>
Acceso al sistema en cualquier tipo de perfil de usuario, por un tercero no facultado y que ponga en riesgo la integridad y veracidad de la información registrada en el S2.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table></td></tr>
<tr><td>Obtención y uso de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table></td></tr>
<tr><th colspan="2">Amenaza de robo, extravío o copia no autorizada</th></tr>
<tr><td>Fases del ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Uso de datos.</td><td>Acceso al sistema en cualquier tipo de perfil de usuario, por un tercero no facultado y que ponga en riesgo la integridad y veracidad de la información registrada en el S2.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table></td></tr>
<tr><td>Almacenamiento y cancelación de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="2">Amenaza de uso, acceso o tratamiento no autorizado</th></tr>
<tr><td>Fases del Ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención de datos personales.</td><td>Captura de información errónea, por una persona distinta al Administrador de Ente Público, de los datos del Servidor Público y de su superior inmediato.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>2</td><td>4</td></tr></table>
Captura de información errónea, por una persona distinta al OIC, de los datos de los Particulares Inhabilitados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><td>Almacenamiento, divulgación y cancelación de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3</td><td>3</td><td>9</td></tr></table></td></tr>
<tr><td>Obtención, uso y divulgación de datos personales.</td><td>Desconocimiento o inaplicación del Catálogo de Perfiles de Usuario del S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3</td><td>3</td><td>9</td></tr></table></td></tr>
<tr><td>Almacenamiento, divulgación, y cancelación de datos Personales.</td><td>Desinformación de usuarios sobre el tratamiento de los datos personales y las consecuencias del incumplimiento de las disposiciones que regulan dicho tratamiento.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>2</td><td>4</td></tr></table></td></tr>
<tr><th colspan="2">Riesgos Físicos/Tecnológicos</th></tr>
<tr><th colspan="2">Amenaza de pérdida o destrucción no autorizada</th></tr>
<tr><td>Fases del ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención, almacenamiento, uso y divulgación de datos personales.</td><td>Eliminación de datos de los Servidores Públicos de la estructura orgánica de entes públicos, de manera intencional, con motivo de un ataque o intrusión al S2 o la base de datos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>Eliminación de datos de los Particulares Inhabilitados, de manera intencional, con motivo de un ataque o intrusión al S2 o la base de datos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>4</td><td>8</td></tr></table></td></tr>
<tr><td>Obtención y uso de datos personales.</td><td>La plataforma no valide el acceso y los privilegios del usuario.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de robo, extravío o copia no autorizada</td></tr>
<tr><td>Fases de ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención y almacenamiento de datos personales.</td><td>Contraseñas extraviadas por pérdida de activos fuera de la Entidad Pública (laptop o cualquier otro dispositivo móvil con acceso al sistema).
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>4</td><td>8</td></tr></table></td></tr>
<tr><td>Almacenamiento de datos personales.</td><td>Base de datos del S2, copiada sin autorización.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>4</td><td>8</td></tr></table></td></tr>
<tr><td>Almacenamiento de datos personales.</td><td>Venta de información personal por un robo de datos del S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><td>Uso y divulgación de datos personales.</td><td>Datos personales disponibles durante las pruebas o desarrollo del S2, que corresponderán únicamente a Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y a sus superiores inmediatos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>2</td><td>4</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de uso, acceso o tratamiento no autorizado</td></tr>
</table>

<table>
<tr><th>Fases de ciclo de vida</th><th>Riesgos</th></tr>
<tr><td>Obtención, almacenamiento, uso y divulgación de datos.</td><td>Existencia de información errónea, de los Servidores Públicos, en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>2</td><td>4</td></tr></table>
Existencia de información errónea, de los Particulares Inhabilitados, en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><td>Uso y divulgación de datos.</td><td>Datos de interoperabilidad erróneos por falta de verificación de la integridad de los datos interoperados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>2</td><td>4</td></tr></table></td></tr>
<tr><td>Almacenamiento, uso y divulgación de datos.</td><td>Eliminación o destrucción de la base de datos que contiene la información de los Servidores Públicos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3</td><td>4</td><td>12</td></tr></table>
Eliminación o destrucción de la base de datos que contiene la información de los Particulares Inhabilitados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3</td><td>5</td><td>15</td></tr></table></td></tr>
<tr><td>Obtención, almacenamiento, uso, divulgación y supresión de datos.</td><td>Ejecución de un código malicioso.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><th colspan="2">Amenaza de daño, la alteración o modificación no autorizada</th></tr>
<tr><td>Fases de ciclo de vida</td><td>Riesgos</td></tr>
</table>

<table>
<tr>
<td>Obtención, almacenamiento, uso, divulgación, así como cancelación y supresión de datos personales.</td>
<td>Que el S2 no esté disponible por daño físico por polvo, corrosión, congelamiento, fuego, agua, contaminación o radiación electromagnética.

<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>3</td><td>3</td><td>9</td></tr>
</table>

Pérdida de información personal, por robo de activos como servidor físico.

<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>3</td><td>6</td></tr>
</table>

Denegación del servicio del S2 por un ataque al sistema.

<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table>

Manipulación del S2 por un ataque informático al sistema.
<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>3</td><td>6</td></tr>
</table>
</td>
</tr>
<tr>
<td>Obtención, uso y almacenamiento de datos personales.</td>
<td>Impedimento de generar reportes de alta y actualización quincenal de la información.

<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table>

Impedimento de generar reportes de alta de la información, de Particulares Inhabilitados.

<table>
<tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr>
<tr><td>2</td><td>2</td><td>4</td></tr>
</table>
</td>
</tr>
</table>

C. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales.

Esta última etapa del proceso de gestión de riesgos, consiste en precisar las medidas de control necesarias para tratar el riesgo y mitigar su nivel de exposición. Las medidas de control tienen como objeto mitigar o minimizar la posibilidad o el impacto asociado al riesgo inherente de una operación de tratamiento.

En virtud de lo anterior, la SESEA adoptará las siguientes **MEDIDAS DE CONTROL**, las cuales, atendiendo a las características del S2 y los riesgos identificados, son encaminadas a mitigar riesgos:

Medidas de control administrativas	
Medidas para mitigar el riesgo	
Riesgo	Descripción de la medida de control
1.- Eliminación de datos de los Servidores Públicos de la estructura orgánica de entes públicos, de manera accidental o intencional. 2.- Eliminación de los datos de los Particulares Inhabilitados, de manera accidental o intencional. 3.- Acceso al sistema en cualquier tipo de perfil de usuario, por un tercero no facultado y que ponga en riesgo la integridad y veracidad de la información registrada en el S2.	Se implementan niveles de acceso, gestión y uso de la información del S2 (reglas y privilegios) para cada perfil de usuario o grupo de usuarios conforme a sus responsabilidades; lo cual se establece en el Catálogo de Perfiles de Usuario del S2. Se emitirá una guía con recomendaciones para la creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender; en dicha guía se explicará, por ejemplo, la forma de cerrar sesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, entre otros aspectos. Valor: -1 en la probabilidad de ocurrencia en cada uno de los riesgos
Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.	Asistencia a los talleres de capacitación sobre el uso adecuado de los datos personales. Valor: -1 en la probabilidad de ocurrencia en el riesgo.
1.- Captura de información errónea, por una persona distinta al Administrador de Ente Público, de la información de los datos del Servidor Público y de su superior inmediato. 2.- Captura de información errónea, por una persona distinta al OIC, de la información de los datos de Particulares Inhabilitados.	Existencia de trazabilidad y posibilidad de identificar quién tuvo acceso a los datos y los tratamientos realizados. Se implementan niveles de acceso, gestión y uso de la información del S2 (reglas y privilegios) para cada perfil de usuario o grupo de usuarios conforme a sus responsabilidades, lo cual se establece en el Catálogo de Perfiles de Usuario del S2. Difusión del instructivo de llenado del S2. Valor: -1 en la probabilidad de ocurrencia del riesgo.
Desconocimiento o inaplicación del Catálogo de Perfiles de Usuario del S2.	Difusión del instructivo de llenado del S2. Difusión del Catálogo de Perfiles de Usuario del S2. Valor: -2 en la probabilidad de ocurrencia del riesgo.

Desinformación de usuarios sobre el tratamiento de los datos personales y las consecuencias del incumplimiento de las disposiciones que regulan dicho tratamiento.	Poner a disposición de los Servidores Públicos, el aviso de privacidad del S2. Valor: -1 en la probabilidad de ocurrencia del riesgo.
Medidas de control físicas/tecnológicas	
Medidas para mitigar el riesgo	
Riesgos	Descripción de la medida de control
1.- Eliminación de datos de los Servidores Públicos de la estructura orgánica de entes públicos, de manera accidental o intencional, con motivo de un ataque o intrusión al S2 o a la base de datos. 2.- Eliminación de datos de Particulares Inhabilitados, de manera accidental o intencional, con motivo de un ataque o intrusión al S2 o a la base de datos. 3.- Contraseñas extraviadas por pérdida de activos fuera de la Entidad Pública (laptop o cualquier otro dispositivo móvil con acceso al sistema). 4.- Existencia de información errónea, de los Servidores Públicos, en el S2. 5.- Existencia de información errónea, de los Particulares inhabilitados, en el S2.	Asignación para cada usuario del S2, de un identificador único al cual se vinculan sus privilegios y acceso. Responsabilizar a cada usuario, sobre la secrecía de sus contraseñas y mecanismos de acceso al S2. Se emitirá una guía con recomendaciones para la creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender; en dicha guía se explicará, por ejemplo, la forma de cerrar sesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, entre otros aspectos. Valor: -1 en la probabilidad de ocurrencia en cada uno de los riesgos.
Denegación del servicio del S2 por un ataque al sistema.	Prohibición de uso de software ilegal o no autorizado. Uso de bitácora de control de software contra virus y software malicioso. Monitorización del tráfico y las actividades en la red de la SESEA, para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, entre otros. Cifrado con contraseña, certificados digitales, token y autenticación de dos pasos. Valor: -1 en la probabilidad de ocurrencia del riesgo.
La plataforma no valide el acceso y los privilegios del usuario.	Se implementan niveles de acceso, gestión y uso de la información del S2 (reglas y privilegios) para cada perfil de usuario o grupo de usuarios conforme a sus responsabilidades, lo cual se establece en el Catálogo de Perfiles de Usuario del S2.

	Se emitirá una guía con recomendaciones para la creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender; en dicha guía se explicará, por ejemplo, la forma de cerrar sesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, entre otros aspectos. Prohibición de uso de software ilegal o no autorizado. Uso de bitácora de control de software contra virus y software malicioso. Valor: -1 en la probabilidad de ocurrencia del riesgo.
1.- Base de datos del S2, copiada sin autorización. 2.- Datos personales disponibles durante las pruebas o desarrollo del S2, que corresponderán únicamente a Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y a sus superiores inmediatos.	Prohibición de uso de software ilegal o no autorizado. Uso de bitácora de control de software contra virus y software malicioso. Monitorización del tráfico y las actividades en la red de la SESEA, para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, entre otros. Uso de Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium. Cifrado con contraseña, certificados digitales, token y autenticación de dos pasos. Limitación de acceso al servidor por filtrado de dirección IP. Valor: -1 en la probabilidad de ocurrencia del riesgo.
1.- Venta de información personal por un robo de datos del S2. 2.- Impedimento de generar reportes de alta y actualización quincenal de la información. 3.- Impedimento de generar reportes de alta de información de Particulares Inhabilitados.	Asistencia a los talleres de capacitación sobre el uso adecuado de los datos personales. Existencia de trazabilidad y posibilidad de identificar quién tuvo acceso a los datos y los tratamientos realizados. Se implementan niveles de acceso, gestión y uso de la información del S2 (reglas y privilegios), para cada usuario o grupo de usuarios conforme a sus responsabilidades, lo cual se establece en el Catálogo de Perfiles de Usuario del S2.

	Bitácora de registros de excepciones y eventos relevantes de seguridad en los sistemas y activos que tengan relación con el S2. Valor: -1 en la probabilidad de ocurrencia en los riesgos.
Datos de interoperabilidad erróneos por falta de verificación de la integridad de los datos interoperados.	Cifrado con contraseña, certificados digitales, token y autenticación de dos pasos. Constante vigilancia entre la consistencia del estándar de datos utilizado por la Plataforma Digital Nacional y el aplicado en el S2. Valor: -1 en la probabilidad de ocurrencia en el riesgo.
1.- Eliminación o destrucción de la base de datos que contiene la información de los Servidores Públicos. 2.- Eliminación o destrucción de la base de datos que contiene la información de Particulares Inhabilitados.	Prohibición de uso de software ilegal o no autorizado. Uso de bitácora de control de software contra virus y software malicioso. Monitorización del tráfico y las actividades en la red de la SESEA, para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, entre otros. Uso de Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium. Cifrado con contraseña, certificados digitales, token y autenticación de dos pasos. Respaldo constante de la base de datos. Valor: -2 en la probabilidad de ocurrencia en el riesgo.
1.- Ejecución de un código malicioso. 2.- Manipulación del S2 por un ataque informático al sistema.	Prohibición de uso de software ilegal o no autorizado. Uso de bitácora de control de software contra virus y software malicioso. Monitorización del tráfico y las actividades en la red de la SESEA, para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, entre otros. Uso de Seguridad SSL, Protección DDOS, Directorios Protegidos, VPS Premium. Cifrado con contraseña, certificados digitales, token y autenticación de dos pasos.

	Valor: -1 en la probabilidad de ocurrencia en el riesgo.
Que el S2 no esté disponible por daño físico por polvo, corrosión, congelamiento, fuego, agua, contaminación o radiación electromagnética.	Limpieza constante de site y componentes. Eliminación de fuentes de humedad, cuidado de temperatura interna del site y uso de protocolos en caso de desastres naturales. Correcto aislamiento de cables eléctricos y de cables de datos. Valor: -2 en la probabilidad de ocurrencia en los riesgos.
Pérdida de información personal, por robo de activos como servidor físico.	Cifrado de información interna en el servidor. Valor: -1 en la probabilidad de ocurrencia en el riesgo.

Una vez que se encuentran descritas las medidas de control adoptadas, para reflejar sus efectos deben confrontarse nuevamente con la probabilidad de ocurrencia y el impacto, siguiendo la misma fórmula, y la escala de valores que se usaron para determinar el **RIESGO INHERENTE**.

De esta manera se obtiene el llamado riesgo residual, que se podría definir como el riesgo de cada actividad una vez que se aplican las medidas de control para mitigar su nivel de riesgo.

La siguiente tabla, refleja los resultados obtenidos en la aplicación de las medidas de control, y en las cuales se puede observar que, en todos los casos, las medidas de control han reducido los riesgos al mínimo aceptable, garantizando con ello, la protección de los datos personales de los titulares.

<table>
<tr><th colspan="2">Riesgos administrativos</th></tr>
<tr><th colspan="2">Amenaza de pérdida o destrucción no autorizada</th></tr>
<tr><td>Fases del ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención de datos personales.</td><td>Eliminación de datos de los Servidores Públicos de los entes públicos, de manera accidental o intencional.

<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>Eliminación de datos de los Particulares Inhabilitados de manera accidental o intencional.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>4</td><td>4</td></tr></table>
Acceso al sistema en cualquier tipo de perfil de usuario, por un tercero no facultado y que ponga en riesgo la integridad y veracidad de la información registrada en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td>Obtención y uso de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de robo, extravío o copia no autorizada</td></tr>
<tr><td>Fases del ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Uso de datos.</td><td>Acceso al sistema en cualquier tipo de perfil de usuario, por un tercero no facultado y que ponga en riesgo la integridad y veracidad de la información registrada en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td>Almacenamiento y cancelación de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de uso, acceso o tratamiento no autorizado</td></tr>
<tr><td>Fases del Ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención de datos personales.</td><td>Captura de información errónea, por una persona distinta al Administrador de Ente Público, de los datos del Servidor Público y de su superior inmediato.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>Captura de información errónea, por una persona distinta al OIC de los datos de los Particulares Inhabilitados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td>Almacenamiento, divulgación y cancelación de datos personales.</td><td>Permitir el manejo a personal no capacitado con respecto al uso adecuado de los datos personales.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3-1=3</td><td>3</td><td>6</td></tr></table></td></tr>
<tr><td>Obtención, uso y divulgación de datos personales.</td><td>Desconocimiento o inaplicación del Catálogo de Perfiles de Usuario del S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3-2=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td>Almacenamiento, divulgación, y cancelación de datos Personales.</td><td>Desinformación de usuarios sobre el tratamiento de los datos personales y las consecuencias del incumplimiento de las disposiciones que regulan dicho tratamiento.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
</table>

Amenaza de pérdida o destrucción no autorizada	
Fases del ciclo de vida	Riesgos

<table>
<tr><td>Obtención, almacenamiento, uso y divulgación de datos personales.</td><td>Eliminación de datos de los Servidores Públicos de la estructura orgánica de entes públicos, de manera intencional, con motivo de un ataque o intrusión al S2 o la base de datos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table>
Eliminación de datos de los Particulares Inhabilitados de manera intencional, con motivo de un ataque o intrusión al S2 o la base de datos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>4</td><td>4</td></tr></table></td></tr>
<tr><td>Obtención y uso de datos personales.</td><td>La plataforma no valide el acceso y los privilegios del usuario.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de robo, extravío o copia no autorizada</td></tr>
<tr><td>Fases de ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención y almacenamiento de datos personales.</td><td>Contraseñas extraviadas por pérdida de activos fuera de la Entidad Pública (laptop o cualquier otro dispositivo móvil con acceso al sistema).
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>4</td><td>4</td></tr></table></td></tr>
<tr><td>Almacenamiento de datos personales.</td><td>Base de datos del S2, copiada sin autorización.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>4</td><td>4</td></tr></table></td></tr>
<tr><td>Almacenamiento de datos personales.</td><td>Venta de información personal por un robo de datos del S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><td>Uso y divulgación de datos personales.</td><td>Datos personales disponibles durante las pruebas o desarrollo del S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de uso, acceso o tratamiento no autorizado</td></tr>
<tr><td>Fases de ciclo de vida</td><td>Riesgos</td></tr>
<tr><td>Obtención, almacenamiento, uso y divulgación de datos.</td><td>Existencia de información errónea, de los Servidores Públicos, en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table>
Existencia de información errónea, de los Particulares Inhabilitados en el S2.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td>Uso y divulgación de datos.</td><td>Datos de interoperabilidad erróneos por falta de verificación de la integridad de los datos interoperados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
<tr><td>Almacenamiento, uso y divulgación de datos.</td><td>Eliminación o destrucción de la base de datos que contiene la información de los Servidores Públicos.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3-2=1</td><td>4</td><td>4</td></tr></table>
Eliminación o destrucción de la base de datos que contiene la información de los Particulares Inhabilitados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3-2=1</td><td>5</td><td>5</td></tr></table></td></tr>
<tr><td>Obtención, almacenamiento, uso, divulgación y supresión de datos.</td><td>Ejecución de un código malicioso.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td colspan="2">Amenaza de daño, la alteración o modificación no autorizada</td></tr>
</table>

<table>
<tr><th>Fases de ciclo de vida</th><th>Riesgos</th></tr>
<tr><td>Obtención, almacenamiento, uso, divulgación, así como cancelación y supresión de datos personales.</td><td>Que el S2 no esté disponible por daño físico por polvo, corrosión, congelamiento, fuego, agua, contaminación o radiación electromagnética.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>3-2=1</td><td>3</td><td>3</td></tr></table>
Pérdida de información personal, por robo de activos como servidor físico.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table>
Denegación del servicio del S2 por un ataque al sistema.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table>
Manipulación del S2 por un ataque informático al sistema.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>3</td><td>3</td></tr></table></td></tr>
<tr><td>Obtención, uso y almacenamiento de datos personales.</td><td>Impedimento de generar reportes de alta y actualización quincenal de la información.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table>
Impedimento de generar reportes de alta de la información, de Particulares Inhabilitados.
<table><tr><th>Probabilidad de ocurrencia</th><th>Impacto</th><th>Riesgo inherente</th></tr><tr><td>2-1=1</td><td>2</td><td>2</td></tr></table></td></tr>
</table>

Como se puede apreciar, cuando aplicamos los valores de las medidas de control a los valores de riesgo, éste se reduce a niveles clasificados como bajo y medio, por lo que dichas medidas de control adoptadas por la SESEA, son pertinentes para procurar una adecuada protección de los datos personales que serán registrados en el S2.

APARTADO V
ANÁLISIS DE CUMPLIMIENTO NORMATIVO

En este apartado se señalan los mecanismos o procedimientos que adoptará el S2, para cumplir por defecto y diseño con los principios, deberes, derechos y demás obligaciones previstas en la Ley General de Protección de Datos, la Ley Local de Protección de Datos y demás disposiciones aplicables, lo cual se expone a continuación:

A. Principios:

1.- Licitud.

a) Descripción: Se encuentra previsto en los artículos 17 de la referida Ley General de Protección de Datos, y 11 de la Ley Local de Protección de Datos, preceptos que señalan que el tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, ya que el ejercicio de las facultades y atribuciones a cargo de la SESEA en su calidad de administradora del S2, se ajusta a lo previsto en los artículos 9 fracción XIII, 36 fracción I, 49 fracción II y 51 párrafo primero de la Ley General del Sistema Nacional Anticorrupción; 3 fracción XXII, 43, 44 y 45 de la LGRA; 4, 9, fracción XII y XVI y 34 fracción X y XI de la Ley del Sistema Estatal; 2, fracción XX, 20, 30 y 31 de la Ley Local de Responsabilidades; 5 fracción II, 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; así como 5 fracción II, 44, 45 y 46 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro.

El cumplimiento del principio de licitud, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1 Mecanismos de regulación y supervisión que ejerce el Comité Coordinador del Sistema Estatal Anticorrupción, conforme a los artículos 8 y 9, fracciones XII y XVI de la Ley del Sistema Estatal, así como 14, 16 y 36 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro, según los cuales dicho Comité establece dichas Bases y se le debe dar cuenta sobre el correcto funcionamiento de la Plataforma Digital Estatal, instrumento tecnológico al cual pertenece el S2, además de que se le debe informar semestralmente sobre su funcionamiento, recomendaciones para mejorarlo, y sobre las fallas que ésta o cualquiera de sus componentes presenten, así como las medidas tomadas para solucionarlas.

b.2. Este principio se garantiza, mediante los procedimientos previstos en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

2.- Finalidad.

a) Descripción: Se encuentra previsto en los artículos 18 de la Ley General de Protección de Datos y 12 de la Ley Local de Protección de Datos, preceptos que señalan que todo tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable confiera al responsable del tratamiento.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, ya que las finalidades en efecto son concretas (atienden a la consecuencia de fines específicos o determinados), explícitas (se expresan y dan a conocer de manera clara en el aviso de privacidad) así como lícitas y legítimas (las finalidades son acordes con las atribuciones expresas del responsable); esas finalidades son las que se refieren en el apartado I letra F de la presente EIPDP, y que para mayor claridad a continuación se reproducen:

b.1. Integrar el S2 al que refieren los artículos 29 y 30 de la Ley Local de Responsabilidades, así como 4, 9 fracciones XII y XVI, y 34 fracción X de la Ley del Sistema Estatal.

b.2. Recibir e integrar la información pública que los distintos entes públicos del estado de Querétaro y sus municipios, incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas que dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 34, fracción X de la Ley del Sistema Estatal.

b.3. Ayudar a los entes públicos del Estado y sus municipios, a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, a efecto de preservar los principios de transparencia, imparcialidad y honradez.

b.4. Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

b.5. Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

b.6. Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

b.7. Ayudar a los entes públicos del Estado y sus municipios, a determinar a los Servidores Públicos que deberán cumplir el protocolo de actuación de contrataciones que sea expedido por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme a lo previsto en el artículo 44 párrafos primero y segundo de la LGRA.

b.8. Prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, conforme a lo previsto en la LGRA, la Ley Local de Responsabilidades y la normatividad penal aplicable.

b.9. Permitir al Comité Coordinador del Sistema Estatal Anticorrupción, establecer políticas públicas de combate a la corrupción, metodologías de medición y aprobar los indicadores necesarios para que se puedan evaluar las mismas, conforme a los artículos 9º fracciones III, V, VI y XII, 21 fracción XI, 30 fracción II y 34 fracción IV de la Ley del Sistema Estatal.

b.10. La generación de datos estadísticos para conocimiento público y como insumo para la obtención de los instrumentos referidos en el inciso anterior.

El cumplimiento del principio de finalidad, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Construir y poner a disposición de los titulares de datos personales, el aviso de privacidad del S2, de conformidad con lo previsto en los artículos 3 fracción II, 20 fracción III, 21 párrafo segundo, 26, 28 y 69 de la Ley General de Protección de Datos y los artículos 3 fracción II, 12, 14, 15, 20, 21, 22, 53, 61 y 63 de la Ley Local de Protección de Datos.

b.2. Procedimiento previsto en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

3.- Lealtad.

a) Descripción: Se encuentra previsto en los artículos 19 de la Ley General de Protección de Datos y 13 de la Ley Local de Protección de Datos, preceptos que señalan que no se deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, entendiendo ésta como la confianza que deposita el titular en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en las leyes.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, ya que los datos se obtienen directamente de quienes tienen perfil de usuario de Administrador de Ente Público (los relacionados con datos de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos) y de OIC (tratándose de la relación de Particulares Inhabilitados).

El cumplimiento del principio de lealtad, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Mecanismos de seguridad, otorgando usuarios y claves específicas a los Administradores de Entes Públicos y OIC, a fin de que registren la información que corresponde, esto de conformidad con lo previsto en los artículos 18 y 19 de las Bases para el Funcionamiento de la Plataforma Digital Estatal.

b.2. Construir y poner a disposición de los titulares de datos personales, el aviso de privacidad del S2, de conformidad con lo previsto en los artículos 3 fracción II, 20 fracción III, 21 párrafo segundo, 26, 28 y 69 de la Ley General de Protección de Datos y los artículos 3 fracción II, 12, 14, 15, 20, 21, 22, 53, 61 y 63 de la Ley Local de Protección de Datos.

b.3. Procedimiento previsto en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

4.- Consentimiento.

a) Descripción: Se encuentra previsto en los artículos 20 a 22 y 65 de la Ley General de Protección de Datos, así como 7, 12, 14, 15, 21, 51 y 59 de la Ley Local de Protección de Datos, preceptos que señalan que el titular de los datos personales debe autorizar el tratamiento o transferencia de manera libre, específica, e informada, salvo que se actualice alguna de las hipótesis previstas en los artículos 22 y 70 de la Ley General en cita, así como 16, 60 y 64 de la Ley Local de referencia.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, ya que se actualizan las hipótesis previstas en los artículos 22 fracciones I y II, y 70 fracciones I y II de la Ley General de Protección de Datos; 16, 60 y 64 de la Ley Local de Protección de Datos, por lo que la SESEA a través del S2, no está obligada a recabar el consentimiento del titular de los datos personales de los Servidores Públicos que intervengan en los procedimientos de Contrataciones Públicas, para su tratamiento y transferencia, en virtud que se realiza en ejercicio de las facultades conferidas en los artículos 9 fracción XIII, 36 fracción I, 49 fracción II y 51 párrafo primero de la Ley General del Sistema Nacional Anticorrupción; 3 fracción XXII, 43, 44 y 45 de la LGRA; 9 fracciones III, V, VI y XII, 21 fracción XI, 30 fracción II y 34 fracción IV de la Ley del Sistema Estatal; 2 fracción XX, 29, 30 y 31 de la Ley Local de Responsabilidades; 5 fracción II, 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; así como 5 fracción II, 44, 45 y 46 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro.

El cumplimiento del principio de consentimiento, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Informar a los titulares de los datos personales, mediante el aviso de privacidad correspondiente, que se actualizan las hipótesis previstas en los artículos 22 fracciones I y II, y 70 fracciones I y II de la Ley General de Protección de Datos; 16 fracción V y 64 fracciones I y II de la Ley Local de Protección de Datos, por lo que no se requiere su autorización para dar tratamiento y realizar las transferencias respectivas.

b.2. Procedimiento previsto en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

5.- Calidad.

a) Descripción: Se encuentra previsto en los artículos 23 y 24 de la Ley General de Protección de Datos, así como 17 a 18 de la Ley Local de Protección de Datos, preceptos que señalan que el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos; que se presume que se cumple con la calidad en los datos personales, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario; además de que los datos personales que hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad, deberán ser

suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, pues como ya se señaló, los datos se obtienen de quienes tienen perfil de usuario de Administrador de Ente Público (los relacionados con datos de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos) y de OIC (tratándose de la relación de Particulares Inhabilitados); siendo que a los primeros les son proporcionados directamente de los titulares y los segundos, son las autoridades competentes para imponer las inhabilitaciones en mención, actualizándose con ello la presunción de calidad en los datos personales.

El cumplimiento del principio de calidad, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Obtención de datos, de quienes tienen perfil de usuario de Administrador de Ente Público (los relacionados con datos de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos) y de OIC (tratándose de la relación de Particulares Inhabilitados); siendo que a los primeros les son proporcionados directamente de los titulares y los segundos, son las autoridades competentes para imponer las inhabilitaciones en mención; lo anterior, utilizando mecanismos de seguridad, otorgando usuarios y claves específicas a dichos Administradores de Ente Público y OIC, esto de conformidad con lo previsto en los artículos 18 y 19 de las Bases para el Funcionamiento de la Plataforma Digital Estatal.

b.2. Construir y poner a disposición de los titulares de datos personales, el aviso de privacidad del S2, de conformidad con lo previsto en los artículos 3 fracción II, 20 fracción III, 21 párrafo segundo, 26, 28 y 69 de la Ley General de Protección de Datos y los artículos 3 fracción II, 12, 14, 15, 20, 21, 22, 53, 61 y 63 de la Ley Local de Protección de Datos de la Ley Local de Protección de Datos.

b.3. Cumplimiento de la fase V del ciclo de vida descrito en el apartado III de la presente EIPDP, correspondientes a "*cancelación o supresión de los datos*", respectivamente, sujetando la eliminación de datos, al cumplimiento de las condiciones establecidas en la Ley General de Archivos.

b.4. Procedimiento previsto en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

6.- Proporcionalidad.

a) Descripción: Se encuentra previsto en los artículos 25 de la Ley General de Protección de Datos, así como 19 de la Ley Local de Protección de Datos, preceptos que señalan que sólo se deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, pues como ya se apuntó en el apartado II de la presente EIPDP, el tratamiento de datos personales en el S2, guarda una relación adecuada con el significado de los derechos intervenidos, puesto que permite tener escrutinio sobre el desempeño de los Servidores Públicos que intervienen en procedimientos públicos que involucran recursos públicos y que otorgan derechos a terceros, de manera que se vigile que su desarrollo no sea utilizado en beneficio de intereses particulares y, por ende, ajenos a lo que persigue la función pública, generando con ello la posibilidad de realizar jurídica y materialmente, las finalidades constitucionales de prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como la fiscalización y control de recursos públicos.

El cumplimiento del principio de proporcionalidad, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Procedimiento previsto en la Ley General de Protección de Datos y la Ley Local de Protección de Datos, para que los titulares de datos personales soliciten Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de los mismos.

b.2. Restricciones en el tratamiento de los datos que obren en la relación de Particulares Inhabilitados; dichos datos no serán publicitados y a los mismos sólo tendrán acceso los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2, para efectos de prevenir, investigar y sancionar faltas administrativas y hechos de corrupción y garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

7.- Información.

a) Descripción: Se encuentra previsto en los artículos 26 de la Ley General de Protección de Datos, así como 20 de la Ley Local de Protección de Datos, preceptos que señalan que se deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

b) Mecanismos o procedimientos para su cumplimiento: Se cumple, pues se contará y se pondrá a disposición de los Servidores Públicos y de los entes públicos a los que se transferirá, el aviso de privacidad correspondiente al S2.

El cumplimiento del principio de información, se garantiza mediante los siguientes mecanismos o procedimientos:

b.1. Construir y poner a disposición de los titulares de datos personales, por conducto de los Administradores de Ente y de manera electrónica en el portal de la Plataforma Digital Estatal, el aviso de privacidad del S2, de conformidad con lo previsto en los artículos 3 fracción II, 20 fracción III, 21 párrafo segundo, 26, 28 y 69 de la Ley General de Protección de Datos y los artículos 3 fracción II, 12, 14, 15, 20, 21, 22, 53, 61 y 63 de la Ley Local de Protección de Datos.

b.2. Difundir, por medios electrónicos y físicos, el aviso de privacidad del S2.

8.- Responsabilidad en el tratamiento de datos personales (cumplimiento de principios deberes y obligaciones).

a) Descripción: Conforme a los artículos 29 de la Ley General de Protección de Datos, así como 23 de la Ley Local de Protección de Datos, se deben implementar los mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dichos ordenamientos y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a la Comisión de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Querétaro, según corresponda, debiendo observar la Constitución Federal, los Tratados Internacionales en los que el Estado mexicano sea parte; pudiéndose valer de estándares o mejores prácticas nacionales o internacionales, en lo que no contravenga la normativa mexicana.

b) Mecanismos o procedimientos para su cumplimiento: Los mecanismos a adoptar para cumplir con el principio de responsabilidad y con ello, los deberes y obligaciones derivadas de la normativa de protección de datos personales, se precisan en los artículos 30 de la Ley General de Protección de Datos, así como 24 de la Ley Local de Protección de Datos.

Mecanismos para el cumplimiento de principios, deberes y obligaciones	Medidas para implementarlos
1. Destinar recursos autorizados para tal fin, para la instrumentación de programas y políticas de protección de datos personales;	La SESEA, dentro de su gasto corriente, tiene un monto estimado de **$200,000.00 (DOSCIENTOS MIL PESOS 00/100 M.N.)** en el ejercicio fiscal 2023 para el funcionamiento del Área denominada **"Plataforma Digital del Estado de Querétaro"**, adscrita a la Secretaría Técnica de la SESEA; monto que será destinado a la atención del funcionamiento ordinario y solución de eventualidades relacionadas con el acceso a la información y protección de datos personales, del sistema S2
2. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;	Las políticas que la SESEA implementará sobre la protección de datos personales, se contendrán en **cinco Avisos de Privacidad** construidos de conformidad con los artículos 3 fracción II, 20 fracción III, 21 párrafo segundo, 26, 28, y 69 de la Ley General de Protección de Datos y los artículos 3 fracción II, 12, 14, 15, 20, 21, 22, 53, 61 y 63 de la Ley Local de Protección de Datos. Esos Avisos de Privacidad son: a) El correspondiente a la SESEA, como organismo público descentralizado, y que se dirige a la ciudadanía en general. b) Correspondiente al expediente personal de los trabajadores de la SESEA. c) El correspondiente a contratistas y proveedores de la SESEA. d) El correspondiente al Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancia de Presentación de Declaración Fiscal de la Plataforma Digital Estatal de Querétaro (S1).

	e) El correspondiente al S2.
3. Poner en práctica un programa continuo de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;	Se desarrollará el **Programa Anual de Capacitación 2023** en materia de Transparencia y Protección de Datos Personales, aprobado por el Comité de Transparencia de la SESEA, dentro del cual se impartirán temas sobre Protección de Datos Personales.
4. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;	**Por conducto de la Unidad de Transparencia de la Secretaría Ejecutiva**, revisión anual de las políticas contenidas en los avisos de privacidad referidos en el numeral 2 del presente cuadro. **Por conducto del Comité de Transparencia de la Secretaría Ejecutiva**, revisión y emisión del Programa Anual de Capacitación en materia de Transparencia y Protección de Datos Personales.
5. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;	**Por conducto de la Unidad de Transparencia de la Secretaría Ejecutiva**, verificar permanentemente que el S2 ponga a disposición de los usuarios su aviso de privacidad. **Por conducto del titular de auditoría o su similar del Órgano Interno de Control de la SESEA**, revisión del cumplimiento de las disposiciones aplicables en materia de protección de datos personales, tal actividad se incluye en su Programa de Trabajo y de Auditorías del año 2022. **Por conducto de la SESEA a través del Área denominada "Plataforma Digital del Estado de Querétaro"**: a) Revisión anual sobre la existencia de bitácora de control de software contra virus y software malicioso

	b) Revisión y actualización semestral de equipos de cómputo propiedad de la SESEA, a fin de verificar que cuenten con contraseñas de seguridad; c) Revisión semestral del software instalado en los equipos de la SESEA, para verificar que no existe software ilegal o no autorizado por la propia SESEA; d) Vigilancia permanente sobre la existencia y funcionamiento de los equipos instalados en el site de la Plataforma Digital Estatal; y e) Vigilancia permanente del cumplimiento de las medidas de seguridad descritas en la presente EIPDP.
6. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;	**La SESEA a través de su Unidad de Transparencia**, podrá orientar a los ciudadanos en caso de tener dudas respecto del ejercicio de sus derechos, y en caso de quejas contra algún funcionario público de la Entidad, se cuenta con un Órgano Interno de Control, instancia que, conforme a lo previsto en la LGRA, es competente para atender quejas o denuncias. Asimismo, en el portal de Internet de la SESEA, están disponibles los teléfonos y correo electrónico por el que se puede hacer contacto, así como un formulario simplificado, para remitir mensajes por medio del mismo portal, los cuales se pueden referir a quejas.
7. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley	Se deberá contar con las siguientes políticas, programas, servicios, sistemas y plataformas informáticas, relacionadas con el tratamiento de datos personales, de conformidad con la normatividad vigente en materia de protección de datos personales:

General de Protección de Datos y demás disposiciones aplicables en la materia, garantizando que cumplan por defecto con las obligaciones previstas en dicha normativa.	a) Las políticas en cuanto al tratamiento y transferencia de datos personales, contenidas en los avisos de privacidad emitidos por la SESEA, que son: El correspondiente a la SESEA, como organismo público descentralizado, dirigido a la ciudadanía en general; el correspondiente al expediente personal de los trabajadores de la SESEA; el correspondiente a contratistas y proveedores de la SESEA; el correspondiente al Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancia de Presentación de Declaración Fiscal de la Plataforma Digital Estatal de Querétaro (S1); y el correspondiente al S2. b) El Programa Anual de Capacitación 2022 en materia de Transparencia y Protección de Datos Personales. c) El Programa de Trabajo y de Auditorías 2022, del titular de auditoría del OIC de la SESEA, que prevé la revisión del cumplimiento conciso de las obligaciones comunes en materia de transparencia, tanto en la página del Sistema Nacional de Transparencia como en la de la propia SESEA, además de la revisión del cumplimiento de las disposiciones aplicables en materia de protección de datos personales. d) El Portal de Internet de la SESEA, disponible en: https://wp.seaqueretaro.org/ e) El S2.

APARTADO VI
OPINIÓN TÉCNICA DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Conforme al artículo 3º fracción XVI de la Ley General de Protección de Datos, EIPDP es el documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados.

Es el caso, que conforme a lo dispuesto en los artículos 9 fracción XIII, 36 fracción I 49 fracción II y 51 de la Ley General del Sistema Nacional Anticorrupción; 3 fracción XXII, 43, 44 y 45 de la LGRA; 9, fracciones XII y XVI, 17 párrafo tercero y 34 fracción X, de la Ley del Sistema Estatal; 29, 30 y 31 de la Ley Local de Responsabilidades; 5 fracción II, 46 y 47 de las Bases para el Funcionamiento de la Plataforma Digital Nacional; así como 5 fracción II, 44, 45 y 46 de las Bases para el Funcionamiento de la Plataforma Digital Estatal de Querétaro, el S2 constituye una plataforma informática que implica un tratamiento intensivo de datos personales, la cual debe ser administrada por la SESEA, por conducto de su Secretario Técnico, plataforma que está próxima a operar con datos reales.

El objetivo general del S2, es permitir a los entes públicos del Estado y los municipios, registrar información relacionada con los Servidores Públicos que intervienen en Contrataciones Públicas, en la forma y términos que establece la LGRA y la Ley Local de Responsabilidades, para efectos de prevenir, investigar y sancionar las faltas administrativas y hechos de corrupción conforme a lo previsto en dichas leyes y la normatividad penal correspondiente, así como garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

Así, la SESEA al tener a su cargo la administración del S2, dará tratamiento, por ser inscritos en dicha plataforma, a los siguientes datos:

I. Los datos a inscribir en el S2 de los Servidores Públicos que intervengan en procedimientos para Contrataciones Públicas, y que son públicos de conformidad con los artículos 43 párrafo tercero de la LGRA; 29 párrafo segundo de la Ley Local de Responsabilidades; 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro:

1. Datos Generales:

1.1. Nombres y apellidos;

2. Datos del empleo, cargo o comisión:

2.1. Nombre del Ente Público donde labora el Servidor Público y sus siglas;

2.2. Denominación del puesto del Servidor Público;

2.3. Nivel del puesto del Servidor Público;

2.4. Nivel de responsabilidad dentro las contrataciones, que puede ser:

2.4.1. Atención;

2.4.2. Tramitación;

2.4.3. Resolución.

2.5. Tipo de función, que puede ser:

2.5.1. Técnica;

2.5.2. Responsable de la ejecución de los trabajos;

2.5.3. Responsable de la contratación;

2.5.4. Contratante;

2.5.5. Requirente;

2.5.6. Otra.

2.6. Tipos de procedimiento de Contrataciones Públicas en los que puede participar el Servidor Público, que pueden ser:

2.6.1. Adjudicación de contratos, también denominado contrataciones públicas;

2.6.2. Concesiones;

2.6.3. Licencias;

2.6.4. Permisos;

2.6.5. Autorizaciones y prórrogas;

2.6.6. Enajenación de bienes muebles;

2.6.7. Enajenación de bienes inmuebles; y

2.6.8. Asignación y emisión de dictámenes de avalúos.

II. Los datos a inscribir en el S2 del Servidor Público superior inmediato del Servidor Público que intervenga en procedimientos para Contrataciones Públicas, y que son públicos de conformidad con los artículos 70 fracciones II y VII de la Ley General de Transparencia y Acceso a la Información Pública; así como 66 fracciones II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro:

1. Datos Generales:

1.1. Nombres y apellidos;

2. Datos del empleo, cargo o comisión:

2.1. Denominación del puesto del Servidor Público;

2.2. Nivel del puesto del Servidor Público.

III. Relación de Particulares Inhabilitados, esto de conformidad con el artículo 44 párrafo tercero de la LGRA y 22 de la Ley Local de Responsabilidades, información que, en términos de los preceptos en cita, en relación con los artículos 43 párrafo tercero de la propia LGRA y 29 párrafo segundo de la Ley Local de Responsabilidades, no se le dará publicidad en el S2, sino sólo acceso a los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2. Los datos que obran en dicha relación son los siguientes:

1. Nombres y apellidos de la persona física, o bien, razón social de la persona moral, que se encuentre inhabilitada para celebrar contratos con entes públicos derivado de procedimientos administrativas *diversos* a los previstos por la LGRA y la Ley Local de Responsabilidades.

2. Periodo de la inhabilitación.

3. Ente público al que pertenece la autoridad que impuso la inhabilitación.

4. Autoridad que impuso la inhabilitación.

Ahora bien, los datos personales que recabará la SESEA, a través del S2, podrán ser utilizados para las siguientes **FINALIDADES**:

1. Integrar el S2 al que refieren la Ley Local de Responsabilidades, así como la Ley del Sistema Estatal.

2. Recibir e integrar la información pública que los distintos entes públicos del estado de Querétaro y sus municipios, incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas que dicte el Comité Coordinador del Sistema Nacional Anticorrupción.

3. Ayudar a los entes públicos del Estado y sus municipios, a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, a efecto de preservar los principios de transparencia, imparcialidad y honradez.

4. Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

5. Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

6. Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

7. Ayudar a los entes públicos del Estado y sus municipios, a determinar a los Servidores Públicos que deberán cumplir el protocolo de actuación de contrataciones que sea expedido por el Comité Coordinador del Sistema Nacional Anticorrupción.

8. Prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, conforme a lo previsto en la LGRA, la Ley Local de Responsabilidades y la normatividad penal aplicable.

9. Permitir al Comité Coordinador del Sistema Estatal Anticorrupción, establecer políticas públicas de combate a la corrupción, metodologías de medición y aprobar los indicadores necesarios para que se puedan evaluar las mismas.

10. La generación de datos estadísticos para conocimiento público y como insumo para la obtención de los instrumentos referidos en el numeral anterior.

De esta manera, es imprescindible que la SESEA ponga en operación el S2, que como ya se explicó, constituye el instrumento indispensable para que los entes públicos del estado de Querétaro y sus municipios, registren los datos de los Servidores Públicos que intervienen en los procedimientos de Contrataciones Públicas, los del superior inmediato de dichos Servidores Públicos, así como la relación de Particulares Inhabilitados, y así hacer uso efectivo del instrumento que para el efecto prevén la Ley General del Sistema Nacional Anticorrupción, la Ley del Sistema Estatal así como la propia LGRA y la Ley Local de Responsabilidades.

Ahora bien, conforme al artículo 75 de la Ley General de Protección de Datos, se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

1.- Existan riesgos inherentes a los datos personales a tratar;

2.- Se traten datos personales sensibles, y

3.- Se efectúen o pretendan efectuar transferencias de datos personales.

Al respecto el artículo 69 de la Ley Local de Protección de Datos, establece que se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales, considerando los siguientes factores:

1.- Existan riesgos inherentes a los datos personales a tratar;

2.- Se traten datos personales sensibles, y

3.- Se efectúen o pretendan efectuar transferencias de datos personales.

Conforme a los artículos 14 fracción XX y 74 párrafo segundo de la Ley General de Protección de Datos, el contenido de las EIPDP debe determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales el cual, además, tiene como función expedir las disposiciones administrativas necesarias para la valoración del contenido de ese instrumento.

Adicionalmente, el propio artículo 14 en su fracción XIX de la Ley General de Protección de Datos, faculta al Sistema Nacional en cita, para que expida "*criterios adicionales para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales*".

En ese contexto, y en uso de las atribuciones de referencia, el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emitió el "*Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*", publicado en el Diario Oficial de la Federación el 23 de enero de 2018, acuerdo que conforme a las propias disposiciones que facultan al Sistema Nacional para emitirlo, y además conforme a su artículo 3º, es de aplicación obligatoria para la SESEA.[10]

Asimismo, en términos del artículo 8º del Acuerdo en cita, se está en presencia de un tratamiento intensivo o relevante, cuando concurre alguna (y no todas) de las condiciones previstas en el artículo 75 de la Ley General de Protección de Datos, siendo que en opinión del Oficial de Protección de Datos Personales de la SESEA, en la especie se actualizan las referidas en sus tres fracciones, que consisten en lo siguiente:

1.- Existen riesgos inherentes a los datos personales a tratar: Esto conforme al Acuerdo en cita, es entendido como el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales a tratar para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos, las categorías de titulares, el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.

Lo anterior se actualiza, pues en el S2 se registrarán datos de todos los Servidores Públicos que intervienen en procedimientos de contrataciones en el estado de Querétaro y sus municipios, así como de sus superiores inmediatos, además de la lista de Particulares Inhabilitados, lo que representa un gran volumen de datos a tratar y una intensidad o frecuencia importante, pues habrá de actualizarse por mandato de ley, de manera quincenal, reportando las bajas, sustituciones o nuevos ingresos a los mencionados cargos, y cada vez que exista alguna inhabilitación firme, esto de conformidad con lo ordenado en los artículos 43 párrafo primero y 44 párrafo tercero de la LGRA, así como 29 y 30 de la Ley Local de Responsabilidades.

---

[10] Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales: "*Artículo 3. Son sujetos obligados a cumplir con las presentes Disposiciones administrativas cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos, del orden federal, estatal y municipal, así como partidos políticos que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General o las legislaciones estatales en la materia y las presentes Disposiciones administrativas, impliquen un tratamiento intensivo o relevante de datos personales*".

Además, conforme a los artículos 3 fracción VIII y 23 de las Bases para el Funcionamiento de la Plataforma Digital Estatal,[11] la información que se conecte e integre al S2 deberá ser interoperable con los otros cinco sistemas que conforman la Plataforma Digital Estatal,[12] lo cual podrá llevar a la realización de cruces de datos personales entre múltiples sistemas o plataformas informáticas.

De lo anterior también destaca, que el manejo de la información de personas físicas inhabilitadas para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos en la LGRA y en la Ley Local de Responsabilidades, guardan cierta sensibilidad tal como se explica en el siguiente numeral.

2.- Se trate de datos personales sensibles: Dichos datos conforme a los artículos 3 fracción X de la Ley General de Protección de Datos y 3 fracción X de la Ley Local de Protección de Datos, son aquéllos que se refieren a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación, o conlleve un grave riesgo para éste.

También se actualiza, pues de los datos a los que serán tratados en el S2, puede distinguirse como sensibles los que se recabarán como parte de la relación de personas físicas, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades, los cuales se describen en el numeral III de la letra E de la presente EIPDP, esto es así, ya que esa información puede propiciar un trato diferenciado injustificado que conlleve a discriminar al inhabilitado por parte de otros particulares, que al conocer dicha sanción, le nieguen o compliquen su contratación en el ámbito privado; aunado a ello, la publicitación de esa información, también podría provocar una afectación injustificada en los derechos del inhabilitado al generarse materialmente una sanción sin sustento expreso en ley, que tiene características de infamante, situación que trastocaría los mandatos contenidos en los artículos 14 párrafo tercero y 20 párrafo primero de la Constitución Federal.

---

[11] Las Bases para el Funcionamiento de la Plataforma Digital Estatal se publicaron en el Periódico Oficial del Estado "La Sombra de Arteaga" en fecha 24 de junio de 2022.

[12] Conforme al artículo 49 de la Ley General del Sistema Nacional Anticorrupción, la Plataforma Digital Nacional del Sistema Nacional estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los siguientes sistemas electrónicos: I. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal; II. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas; III. Sistema nacional de Servidores públicos y particulares sancionados; IV. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización; V. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y VI. Sistema de Información Pública de Contrataciones.

Las inhabilitaciones en cita, que expresamente la ley señala que son aquellas que derivan de procedimientos administrativos diversos a los previstos en la LGRA y la Ley Local de Responsabilidades, podrán ser, por ejemplo, aquellas impuestas conforme al artículo 76 de la Ley de Obra Pública del Estado de Querétaro, cuyo procedimiento se sujeta a lo previsto en esta Ley, así como a la Ley de Procedimientos Administrativos del Estado de Querétaro; también aquellas inhabilitaciones para celebrar contratos con los entes públicos derivado de procedimientos sustanciados conforme a la Ley de Responsabilidades Administrativas del Estado de Querétaro, durante su vigencia conforme a lo previsto en el transitorio tercero párrafos primero, segundo y cuarto, del Decreto por el que se expide la Ley General del Sistema Nacional Anticorrupción; la LGRA y la Ley Orgánica del Tribunal Federal de Justicia Administrativa, publicado en el Diario Oficial de la Federación el 18 de julio de 2016.

Es importante destacar, que conforme a los artículos 43 párrafo tercero en relación con el 44 párrafo tercero de la LGRA, así como 29 y 30 de la Ley Local de Responsabilidades, los datos sensibles de referencia no serán publicitados y sólo tendrán acceso a ellos, los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2, para efectos de prevenir, investigar y sancionar las faltas administrativas y hechos de corrupción, así como garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

3.- Se efectúen o pretendan efectuar transferencias de datos personales, entendidas como cualquier comunicación de datos personales, realizada a persona distinta del titular, responsable o encargado, siendo que los datos públicos que se registren en el S2, podrán ser transferidos a la SESNA a través de la Plataforma Digital Nacional; y además los datos concernientes a Particulares Inhabilitados, una vez registrados se transferirán a los usuarios con perfil de Administradores de Ente Público y de OIC, instancias que conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos, en este caso, esos fines son específicamente los previstos en la letra F, numerales 4, 5, 6 y 8 del apartado I de la presente EIPDP, y que para mayor claridad, a continuación se reproducen:

Numeral 4 de la letra F, apartado I: Ayudar a los órganos internos de control de los entes públicos del Estado y sus municipios, para detectar riesgos de corrupción en procedimientos de Contrataciones Públicas.

Numeral 5 de la letra F, apartado I: Ayudar a los entes públicos del Estado y sus municipios, a verificar que los particulares, personas físicas o morales, con quienes se vayan a celebrar Contrataciones Públicas, no se encuentren inhabilitados para celebrarlos.

Numeral 6 de la letra F, apartado I: Ayudar a la Secretaría de la Contraloría del Estado y a los órganos internos de control de los entes públicos del Estado y sus municipios, a supervisar la ejecución de los procedimientos de Contrataciones Públicas, así como a llevar a cabo las verificaciones procedentes si descubren anomalías.

Numeral 8 de la letra F, apartado I: Prevenir, investigar y sancionar faltas administrativas y hechos de corrupción, conforme a lo previsto en la LGRA, la Ley Local de Responsabilidades y la normatividad penal aplicable.

Los referidos datos de Particulares Inhabilitados, también serán transferidos a la SESNA, cuando los requiera, y conforme a lo previsto en el artículo 67 de la Ley General de Protección de Datos, se obligan a utilizarlos exclusivamente para los fines que fueron transferidos, en este caso, esos fines son específicamente los previstos en la letra F, numerales 2, 4, 5, 6, 8 y 10 del apartado I de la presente EIPDP. A continuación se describen, para mayor claridad, los referidos en los numerales 2 y 10, ya que el resto se transcribieron en líneas inmediatas anteriores:

Numeral 2 de la letra F, apartado I: Recibir e integrar la información pública que los distintos entes públicos del estado de Querétaro y sus municipios, incorporen para su transmisión e integración a la Plataforma Digital Nacional, conforme a los lineamientos, estándares y políticas que dicte el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo previsto en el artículo 51, párrafo segundo, de la Ley del Sistema Estatal.

Numeral 10 de la letra F, apartado I: La generación de datos estadísticos para conocimiento público y como insumo para la obtención de los instrumentos referidos en el numeral 9 de esa misma letra y apartado, que son: Políticas públicas de combate a la corrupción, metodologías de medición e indicadores necesarios para que se puedan evaluar las mismas.

Es de destacar, que las transferencias descritas, se realizarán sin necesidad de recabar el consentimiento de los titulares, ya que se encuentran dentro de los supuestos de excepción previstos en los artículos 70 fracciones I y II de la Ley General de Protección de Datos; 59, 63 y 64 fracciones I y II de la Ley Local de Protección de Datos.

Aunado a lo anterior, con la puesta en operación del S2, en Opinión del propio Oficial de Protección de Datos Personales de la SESEA, también se actualizan las hipótesis señaladas en el artículo 9 fracciones II, IV, VI, VIII, XI, XII y XIII del multicitado Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que refieren que se estará en

presencia de un tratamiento intensivo o relevante de datos personales, cuando se pretenda:

1.- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares;

2.- Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos;

3.- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas; o

4.- Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiéndolos o poniéndolos a su disposición en cualquier forma.

Al respecto, se debe señalar que únicamente se recabarán y por tanto se dará dicho acceso, sobre datos públicos de los Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas y de sus superiores inmediatos; y los datos que obren en la lista de Particulares Inhabilitados, no serán publicitados y sólo tendrán acceso a ellos, los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2.

5.- Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos, lo cual se realizará, como ya se explicó, tratándose de los datos de personas físicas, que obren en la lista de Particulares Inhabilitados, información que puede propiciar un trato diferenciado injustificado que conlleve a discriminar al inhabilitado por parte de otros particulares, aunado a que también podría provocar una afectación injustificada en los derechos del inhabilitado al generarse materialmente una sanción sin sustento expreso en ley, que tiene características de infamante.

Por ello, sobre la actualización de esta hipótesis, en opinión del Oficial de Protección de Datos Personales de la SESEA, para mantener la efectiva protección de datos que pudieran generar una mayor afectación a la esfera privada, es adecuado que

atento a lo previsto en los artículos 43 párrafo tercero en relación con el 44 párrafo tercero de la LGRA, así como 29 y 30 de la Ley Local de Responsabilidades, los datos que obren en la relación de Particulares Inhabilitados, no sean publicitados y sólo tengan acceso a ellos, los Servidores Públicos autorizados conforme al Catálogo de Perfiles del S2, para efectos de prevenir, investigar y sancionar faltas administrativas y hechos de corrupción y garantizar el cumplimiento de las condiciones y principios establecidos en el artículo 134 párrafos primero, tercero y cuarto de la Constitución Federal.

6.- Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar, lo cual se actualiza, pues una de las finalidades del S2 será ayudar a establecer un registro y clasificación de Servidores Públicos que intervienen en procedimientos de Contrataciones Públicas, precisando su cargo y nivel de participación en dichos procedimientos, conforme a lo previsto en el artículo 43 párrafo primero y 30 de la LGRA y 29 de la Ley Local de Responsabilidades, así como establecer un registro de Particulares Inhabilitados, esto de conformidad con el artículo 44 párrafo tercero de la propia LGRA.

Lo anterior permitirá a los Servidores Públicos competentes, tomar decisiones relacionadas con la celebración de Contrataciones Públicas, al poder verificar si los particulares se encuentran inhabilitados para celebrarlas, y en general, detectar riesgos de corrupción, constituyendo una herramienta útil para supervisar la ejecución de los procedimientos respectivos para verificar la posible existencia de anomalías.

7.- Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales, lo cual se actualizará una vez que se cuente con un registro significativo de personas físicas inhabilitadas para celebrar contratos con entes públicos derivado de procedimientos administrativos diversos a los previstos por la LGRA y la Ley Local de Responsabilidades, inhabilitaciones que si bien no derivarán de condenas e infracciones penales, sí constituirán datos personales sensibles.

Como se advierte, conforme a lo establecido por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, instancia competente para determinar el contenido de las EIPDP, emitir disposiciones administrativas para valorar su contenido así como criterios para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales, el S2 cae en los supuestos para considerar que se está ante un tratamiento intensivo o relevante de datos personales, en atención a los criterios que dicho Consejo también ha definido y que ya se describieron, contenidos en el "*Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general*

para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales", instrumento que potencia la protección de datos personales mediante la construcción de EIPDP, pues clarifica que los supuestos que obligan su emisión, deben ser entendidos de forma disyuntiva y no conjuntiva, así como de manera enunciativa y no limitativa, Acuerdo que debe prevalecer sobre cualquier otro instrumento que pretenda entender restrictivamente esos supuestos.

En consecuencia, en esta opinión se concluye que en la especie se configura el tratamiento intensivo o relevante de datos personales, y que en atención al mismo, **es acertado el contenido de la EIPDP del S2 pues cumple con los parámetros exigidos en la Ley General de Protección de Datos**, **la Ley local de Protección de Datos** y en el "*Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*", desarrollando todos los apartados exigidos en el Capítulo III de dicho Acuerdo.