



Documento de Seguridad



GOBIERNO DE
MÉXICO



CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES
CIENCIAS Y TECNOLOGÍAS



ÍNDICE

I.	Introducción	3
II.	Objetivo	5
III.	Marco normativo	5
IV.	Inventario de datos personales y de los sistemas de tratamiento	5
IV.1	Adjudicación en materia de adquisiciones, Servicios y Obra pública	5
IV.2	Selección, Contratación e Identificación de Personal	8
IV.3	Recepción y evaluación de documentos de aspirantes en convocatorias para puestos académicos del INECOL	11
IV.4	Ingreso al Posgrado y registro de trámites de personal académico y estudiantil ..	12
V.	Funciones y obligaciones de las personas que traten datos personales	16
VI.	Análisis de riesgos	16
VII.	Análisis de brecha	17
VIII.	Plan de trabajo	19
IX.	Mecanismos de monitoreo y revisión de las medidas de seguridad	20
X.	Programa general de capacitación	21

I. INTRODUCCIÓN

El 26 de enero de 2017, se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), mediante la cual se establecen las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de sujetos obligados de los tres órdenes de gobierno; se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO) mediante procedimientos sencillos y expeditos; asimismo, se establece la protección de los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento.

Para desarrollar las disposiciones previstas en la LGPDPPSO en lo relativo al ámbito federal se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), los cuales establecen en su artículo 3, párrafo segundo que *"...Los fideicomisos y fondos públicos del orden federal considerados como entidades paraestatales, de conformidad con la legislación aplicable, deberán dar cumplimiento por sí mismos a las obligaciones previstas en la Ley General y los lineamientos Generales de Protección de Datos Personales..."*.

El Instituto de Ecología, A.C. (INECOL), es una entidad paraestatal de conformidad con los artículos 2 y 3 de la Ley de Entidades Paraestatales y el artículo 46 de la Ley Orgánica de la Administración Pública Federal. Es un Centro Público de Investigación de acuerdo con lo establecido en el artículo 82 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación. Conforme a su acta constitutiva, el INECOL, está facultado para celebrar contratos, realizar trabajos de investigación o divulgación con cualquier entidad u organismo del sector público federal, con los gobiernos de los Estados o con otras instituciones nacionales o internacionales. Por lo anterior se considera como sujeto obligado en materia de protección de datos personales y por ende responsable de los datos personales que trata para el ejercicio de sus atribuciones.

Entre los elementos que se deben cumplir de la LGPDPPSO se encuentra el Documento de Seguridad (DS), que de acuerdo con su artículo 3, fracción 14 se define como *"...Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee..."*.

De ahí que el presente DS tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior del INECOL por las diversas Unidades Administrativas que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de estos, en términos de lo previsto en los artículos 35 y 36 de la LGPDPPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, este Centro Público de Investigación ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de estos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo con sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un Sistema Interno para la Gestión y Tratamiento de los Datos Personales en Posesión de este Instituto, pues tal y como lo dispone el artículo 34 de la LGPDPPSO, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Es así, que el INECOL comprometido con la tutela de los datos personales que trata y, acorde a la recomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integridad de los mismos, así como su seguimiento y supervisión continuos.

Dicho lo anterior, el presente documento se integra a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para el INECOL la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO, como en los LGPDPPSP por parte de todos los involucrados; además de avanzar en un proceso de sensibilización permanente respecto de la relevancia que tiene para la institución adoptar medidas correctivas y preventivas. En ese tenor, y en cumplimiento del artículo 35 de la LGPDPPSO se elaboró el presente DS.



II. OBJETIVO

Establecer e implementar controles administrativos, físicos y técnicos en el INECOL para garantizar la protección de datos personales en posesión de sus Unidades Administrativas, así como garantizar su confidencialidad e integridad.

III. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Archivos.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Manual de Organización del Instituto de Ecología, A.C.
- Código de Conducta y Código de Ética de las y los Servidores Públicos del Instituto de Ecología, A.C. (INECOL).

IV. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

El INECOL, integra el presente DS con base en la información generada por las Unidades Administrativas en apego de sus funciones y de conformidad con las disposiciones que le son aplicables. La información analizada se centrará en 4 sistemas donde se manejan datos personales, los cuales son Adjudicación en materia de adquisiciones, servicios y obra pública, selección, contratación e identificación de personal, Recepción y evaluación de documentos de aspirantes en convocatorias para puestos académicos del INECOL e Ingreso al posgrado y registro de trámites de personal académico y estudiantil, en cada sistema se evalúa la información recabada y se determinarán su tratamiento.

IV.1 ADJUDICACIÓN EN MATERIA DE ADQUISICIONES, SERVICIOS Y OBRA PÚBLICA

Unidad Administrativa: Subdirección de Bienes y Servicios

Fundamento jurídico que habilita el tratamiento: Artículo 70 fracciones XXVIII apartado A-B y XXXII de la Ley General de Transparencia y Acceso a la Información Pública, Artículo 45 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.



Cuadro 1. Inventario de datos para la adjudicación en materia de adquisiciones, servicios y obra pública.

Actividad	Descripción
Datos recabados	- Nombre - Firma y rubrica - Identificación oficial de la persona física, apoderado legal o de quien comparece en su representación a los eventos para la sustanciación de los procedimientos de adjudicación. - Registro federal de contribuyentes (RFC) - Acta de nacimiento - CURP - Domicilio fiscal - Teléfono y correo electrónico de contacto - constancia de situación fiscal - Opinión de cumplimiento de SAT - Opinión de cumplimiento del INFONAVIT - Opinión de cumplimiento de IMSS - Carta de datos bancarios - Comprobante de domicilio.
Finalidad del tratamiento	- Creación de Expedientes para órdenes de compra, pedidos o contratos - Contacto con el proveedor para trámites de compra - Para captura de datos en Transparencia y Contratos Específicos - Para Contratos y Cotizaciones - Sustanciar procedimientos de licitación pública, invitación a cuando menos tres proveedores o contratistas

Actividad	Descripción
	- o Formalización de diversas contrataciones al amparo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y Ley de Obras Públicas y Servicios Relacionados con las Mismas (LOPSRM), - o Trámites de pago y/o Convenios celebrados con el INECOL, - o Dar cumplimiento a las obligaciones de Transparencia comunes de conformidad a lo establecido en el artículo 70 fracciones XXVIII incisos A) y B); y XXXII de la Ley General de Transparencia y Acceso a la Información Pública.
Formato de la base de datos	Físico y electrónico
Descripción general de la ubicación Física y/o electrónica	Archiveros de la Unidad Administrativa y equipos de cómputo. Los expedientes electrónicos se almacenan en los equipos de cómputo de los servidores públicos que se encuentran autorizados para recibir la documentación, así como en el Servidor de la Institución.
Cargo del servidor público responsable	- o Subdirector de Bienes y Servicios - o Jefe del Departamento de Adquisiciones - o Jefe del Departamento de Servicios
Servidores públicos que tienen acceso a los sistemas de tratamiento	- o Personal del Departamento de Tesorería - o Personal del Departamento de Contabilidad - o Encargado de Compras Especiales - o Encargado de Almacén General - o Coordinador de Servicios - o Coordinador Parque Vehicular
Ciclo de vida de la información	De acuerdo con la serie documental que le corresponde en el CADIDO del INECOL.

IV.2 SELECCIÓN, CONTRATACIÓN E IDENTIFICACIÓN DE PERSONAL**Unidad Administrativa:** Subdirección de Desarrollo Institucional

Fundamento jurídico que habilita el tratamiento: Art. 25 LFT, Ley General del Servicio Militar Nacional, LSS Art. 99 Frac. III, LISR Art. 39, 40 y 41 ACUERDO por el que se emiten las Disposiciones en las materias de Recursos Humanos y del Servicio Profesional de Carrera, así como el Manual Administrativo de Aplicación General en materia de Recursos Humanos y Organización y el Manual del Servicio Profesional de Carrera.

Cuadro 2. Inventario de datos para la selección, contratación e identificación de personal.

Actividad	Descripción
Datos recabados	- o Nombre completo - o Domicilio particular - o Teléfono particular - o Teléfono celular - o Estado civil - o Firma - o RFC - o CURP - o Sexo - o Cédula migratoria - o Fecha de nacimiento - o Lugar de nacimiento - o Fotografía - o Edad - o Cartilla del servicio militar - o Número de licencia de manejo - o Número de pasaporte

Actividad	Descripción
	○ Número de seguridad social ○ Credencial para votar ○ Correo electrónico Datos académicos ○ Títulos ○ Certificados ○ Constancias ○ Cédula profesional ○ Datos laborales ○ Documentos de reclutamiento y selección ○ Referencias personales y laborales ○ Datos bancarios ○ Estado de cuenta de Afore ○ Seguros ○ Constancia de situación fiscal ○ Descuentos por orden judicial ○ Créditos ○ Ingresos ○ Exámenes psicométricos ○ Nombre de familiares, dependientes y beneficiarios ○ Datos de salud ○ Información señalada en la solicitud de empleo ○ Registro biométrico facial
Finalidad del tratamiento	○ Realizar los trámites de contratación e identificación de personal. ○ Administrar y dispersar la nómina.

[Handwritten signature and initials]



Actividad	Descripción
	- o Integración del expediente personal físico y/o electrónico. - o Cumplir con las obligaciones patronales. - o Pago de remuneraciones, otorgamiento de prestaciones y movimientos de personal. - o Elaborar constancias, efectuar cotejos y expedir todo tipo de documentos relacionados con la administración de personal. - o Generar controles estadísticos y administrativos, actividades de seguimiento de la relación laboral que sostiene o sostuvo con el INECOL. - o Cumplir con las obligaciones de transparencia comunes establecidas en la Ley. - o General de Transparencia y Acceso a la Información Pública. - o Dar cumplimiento con la NOM-035-STPS-2018. - o Registrar asistencia electrónica. - o Transferencia a terceros en cumplimiento a atribuciones legales.
Formato de la base de datos	Físico y electrónico.
Descripción general de la ubicación Física y/o electrónica	Los expedientes de personal se almacenan en el archivo del Departamento de Recursos Humanos. Los expedientes electrónicos se almacenan en los equipos de cómputo de los servidores públicos que se encuentran autorizados para recibir la documentación, así como en el Servidor de la Institución.
Cargo del servidor público responsable	Jefa de Departamento de Recursos Humanos.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Auxiliar de Otras Prestaciones.



Actividad	Descripción
	Responsable de Impuestos y Aportaciones al Seguro Social. Técnico en seguridad social Técnico de Nóminas Técnico financiero
Ciclo de vida de la información	De acuerdo con la serie documental que le corresponde en el CADIDO del INECOL.

IV.3 RECEPCIÓN Y EVALUACIÓN DE DOCUMENTOS DE ASPIRANTES EN CONVOCATORIAS PARA PUESTOS ACADÉMICOS DEL INECOL

Unidad Administrativa: Secretaría Académica

Fundamento jurídico que habilita el tratamiento: El fundamento legal para el tratamiento de los datos personales son los artículos 103, de la Ley Federal de Transparencia y Acceso a la Información Pública, artículo 106 de la Ley General de Transparencia y Acceso a la Información Pública y artículos 17, 18, 26, 27, 28 y 31 de la LGPDPPSO, y 1, 3, 4, 7, 8, 9, 27, 28, 29, 30, 31, 32 y 34 de los LGPDPPSP.

Cuadro 3. Inventario de datos personales para la recepción y evaluación de documentos de aspirantes en convocatorias para puestos académicos del INECOL.

Actividad	Descripción
Datos recabados	- Nombre - Datos de contacto, teléfono, domicilio, correo electrónico - Curriculum Vitae. - C.V.U. - Correo electrónico. - Datos académicos, tales como formación académica, complementaria y tecnológica. - Datos laborales, tales como experiencia laboral.

Actividad	Descripción
	○ Aquellos que deriven de las manifestaciones o documentación que aporten los aspirantes
Finalidad del tratamiento	Para documentar e integrar el registro de participantes en las convocatorias emitidas por el INECOL, de tal forma que permita llevar a cabo el procedimiento de evaluación y contratación de ser seleccionados para ocupar un puesto académico en el Instituto de Ecología A.C.
Formato de la base de datos	Físico y Electrónico.
Descripción general de la ubicación Física y/o electrónica	Los expedientes electrónicos se almacenan en los equipos de cómputo de los servidores públicos que se encuentran autorizados para recibir la documentación, así como en el Servidor de la Institución.
Cargo del servidor público responsable	Secretario Académico
Servidores públicos que tienen acceso a los sistemas de tratamiento	○ Investigadores de las Redes Académicas ○ Integrantes del Consejo Interno ○ Integrantes de la Comisión Evaluadora Interna ○ Asistente de la Secretaría Académica
Ciclo de vida de la información	De acuerdo con la serie documental que le corresponde en el CADIDO del INECOL.

IV.4 INGRESO AL POSGRADO Y REGISTRO DE TRÁMITES DE PERSONAL ACADÉMICO Y ESTUDIANTIL

Unidad Administrativa: Secretaría de Posgrado

Fundamento jurídico que habilita el tratamiento: El tratamiento de sus datos personales se realiza con fundamento en los artículos 61, fracciones II, III, IV, V y VIII, 113, 122, 123, 124, 130, 134 y 147 de la Ley Federal de Transparencia y Acceso a la Información Pública; artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública; 16, 17, 18, 19, 22, 26, 27, 28, 31, 52, 85, fracciones I, II, III y IV, 94 y 103 de la LGPDPSO, y 1, 3, 4, 7, 8, 9, 27, 28, 29, 30, 31, 32 y 34 de los LGPDPS.

Cuadro 4. Inventario de datos para el ingreso al posgrado y registro de trámites de personal académico y estudiantil

Actividad	Descripción
Datos recabados	○ Nombre completo ○ Domicilio particular ○ Teléfono particular ○ Teléfono celular ○ Estado civil ○ Firma ○ RFC ○ CURP ○ Género ○ Visa ○ Fecha de nacimiento ○ Lugar de nacimiento ○ Fotografía ○ Edad ○ Pasaporte ○ Credencial para votar ○ Número de CVU ○ Correo electrónico ○ ORCID ○ URL oficial ○ Títulos ○ Certificados ○ Constancias ○ Cédula profesional

Actividad	Descripción
	○ Datos de estudios anteriores necesarios para la emisión del título físico y electrónico. ○ Exámenes ○ Calificaciones ○ Resultados de entrevistas ○ Encuestas ○ Información señalada en la solicitud de ingreso al posgrado ○ Nombre de familiares, dependientes y beneficiarios ○ Datos de salud
Finalidad del tratamiento	○ Realizar los trámites de ingreso para realizar estudios de posgrado como estudiante o estudiante-visitante. ○ Realizar los trámites de identificación estudiantil ○ Generar informes estadísticos y administrativos. ○ Elaborar constancias y expedir documentos relacionados con sus estudios hasta la obtención del grado y su registro en las instancias correspondientes. ○ Registrar solicitudes de trámites en otras instancias gubernamentales ○ Integración del expediente personal físico y/o electrónico. ○ Cumplir con las obligaciones establecidas en los convenios y convocatorias aplicables en la materia. ○ Efectuar cotejos de la documentación proporcionada. ○ Realizar actividades de seguimiento de los estudios o de la impartición de cursos. ○ Cumplir con las obligaciones de transparencia comunes establecidas en la

Actividad	Descripción
	Ley General de Transparencia y Acceso a la Información Pública. ○ Dar cumplimiento a la normatividad aplicable. ○ Recabar información de encuestas o cuestionarios previamente autorizados y previa notificación del motivo de estas. ○ Transferencia a terceros en cumplimiento a atribuciones legales.
Formato de la base de datos	Físico y electrónico. Sistema de Control Escolar y el Subsistema de Aspirantes
Descripción general de la ubicación Física y/o electrónica	Los expedientes de personal se almacenan en el archivo del Departamento de Recursos Humanos, mientras que el de los alumnos en el archivo de la Secretaría de Posgrado. Los expedientes electrónicos se almacenan en los equipos de cómputo de los servidores públicos que se encuentran autorizados para recibir la documentación, así como en el Servidor de la Institución.
Cargo del servidor público responsable	Secretario de Posgrado
Servidores públicos que tienen acceso a los sistemas de tratamiento	○ Coordinadora de Servicios Escolares ○ Asistente del Secretario de Posgrado ○ Asistente de Ventanilla ○ Asistente de Archivo ○ Asistente de Cursos ○ Asistente Operativo ○ Apoyo en Informática
Ciclo de vida de la información	De acuerdo con la serie documental que le corresponde en el CADIDO del INECOL.



V. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

De conformidad con el artículo 33, fracción II de la LGPDPPSO y 57 de los LGPD PSP, los servidores públicos del INECOL que manejen datos personales en el ejercicio de sus funciones y de las atribuciones de la Unidad Administrativa a la que se encuentran adscritos observarán, al menos, las siguientes funciones y obligaciones:

Funciones:

- Mantener actualizado los inventarios de datos personales cuando les aplique.
- Resguardar los datos personales en apego a las políticas y procedimientos emitidos por la Unidad de Transparencia del INECOL.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de estos, a los que tienen acceso, se encuentren actualizados.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de estos, informar dicho incidente a la Unidad de Transparencia del INECOL y llevar el registro de los hechos.

Obligaciones:

- Aceptar las condiciones de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos que el INECOL establezca.
- Cuando lo solicite la Unidad de Transparencia, participar en la actualización del DS generando los insumos necesarios para el tratamiento de los datos personales que maneja.
- Implementar y apegarse constantemente a las medidas de seguridad diseñadas en las políticas internas para la gestión y tratamiento de los datos personales en posesión del INECOL.
- Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

VI. ANÁLISIS DE RIESGOS

Este apartado del DS se deriva del artículo 33 fracción IV de la LGPDPPSO, donde se establece que el responsable deberá realizar "... un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;..." por lo que se analizará cada activo (datos personales y elementos físicos e infraestructura que soportan a los datos personales) identificado en el inventario de datos



personales. El resultado de este análisis se podrá consultar en el anexo técnico de este documento.

VII. ANÁLISIS DE BRECHA

De acuerdo con las Políticas Internas para la Gestión y el Tratamiento de los Datos Personales en Posesión del INECOL, se definen las medidas de seguridad de los datos personales en la siguiente clasificación:

a) Físicas

Las personas servidoras públicas INECOL, deberán:

- Resguardar los expedientes en archiveros y gavetas bajo llave.
- No reciclar documentos que contengan datos personales, así como verificar que no se utilicen hojas que puedan contener datos personales y/o información confidencial de la organización, ya que pudieran ser divulgados o expuestos y utilizados para finalidades distintas a las legítimas establecidas en el aviso de privacidad correspondiente.
- No tirar documentos con datos personales sin triturar o destruir.
- No dejar documentos con datos personales en las fotocopadoras, scanners e impresoras.
- Mantener los escritorios limpios, cualquier documento o expediente debe estar resguardado, fuera de la vista, cuando no se esté utilizando.
- Proteger el acceso físico al lugar en el que se encuentra el medio de almacenamiento.
- Bloquear los datos personales una vez agotado el periodo de conservación.
- Para el caso de las contrataciones de servicios en las que haya tratamiento de datos personales, atendiendo a la normatividad aplicable, la Unidad Administrativa deberá gestionar la entrega de evidencia de la supresión de los datos personales, conforme a lo acordado en el contrato correspondiente.

b) Administrativas

- Cada Unidad Administrativa deberá integrar un Inventario de datos personales que considere la totalidad de los procesos que, en el ejercicio de sus atribuciones, competencias y funciones implique el tratamiento de datos personales.
- Cada Unidad Administrativa deberá identificar en los procesos en los cuales realice el tratamiento de datos personales, los riesgos y su valoración en relación con su impacto y probabilidad de ocurrencia.

- La Unidad de Transparencia, proporcionará los procedimientos, formatos o guías (emitidas por el INAI) mediante los cuales se facilite a las Unidades Administrativas la elaboración de los inventarios de datos personales.
- La Unidad de Transparencia, integrará y administrará el Inventario Institucional de datos personales.
- Los inventarios de cada Unidad Administrativa se actualizarán periódicamente atendiendo a los cambios o mejoras, y deberán informarse para que se realice la actualización del Inventario Institucional de Datos Personales. La Unidad de Transparencia promoverá juntamente con las Unidades Administrativas, y el área de tecnologías de la información, la implementación de medidas de seguridad para la protección de datos personales.
- Las Unidades Administrativas que recaben los datos personales, así como la Unidad de Transparencia y tecnologías de la información en el ámbito de sus competencias, determinarán, los términos específicos para la transferencia de datos personales, así como las medidas de seguridad pertinentes.
- El Comité de Transparencia aprobará el formato de clausulado que, en su caso, será incluido en los contratos o instrumentos jurídicos que celebre el INECOL, con la finalidad de formalizar la transferencia de datos personales y la relación con terceros encargados de tratarlos.
- Los plazos de conservación de los documentos que contengan datos personales, establecidos en el inventario no deberán exceder aquéllos señalados en el Catálogo de disposición documental vigente del INECOL.
- Todo el personal que obtenga maneje, trate, transfiera o reciba datos personales deberá firmar la carta de consentimiento, así como la suscripción de la carta compromiso del código de ética de la Administración Pública Federal y del código de conducta de las y los servidores públicos del INECOL, donde se establecen las conductas a seguir en materia de transparencia y confidencialidad, que son:
 - No filtrar información o esparcir rumores o comentarios que dañen la reputación de las compañeras y los compañeros de trabajo y en general de la institución o de la administración para la cual se labora.
 - Proporcionar información a la sociedad de manera equitativa, sin criterios discrecionales, excepto cuando se justifique la confidencialidad y utilizando los procedimientos establecidos para ello.
 - Actuar con imparcialidad, cuidado y dedicación en la elaboración y preparación de la información interna.
 - Cuidar la información a su cargo, impidiendo la sustracción, la destrucción, el ocultamiento o la utilización indebida de la misma.
 - Entregar la información a su cargo, impidiendo la sustracción, la destrucción, el ocultamiento o la utilización indebida de la misma.

- Entregar la información requerida en los tiempos y formas estipulados con claridad y calidad.
- c) Técnicas
 - El área de TIC's realizará monitoreos y establecerá una cadena de avisos en caso de vulnerabilidad a la seguridad de la información; asimismo, se harán eventualmente pruebas de intrusión.
 - Se revisará de manera periódica la administración y asignación de contraseñas con el fin de apoyar a los administradores y usuarios de servicios de tecnología a reducir los impactos de los riesgos generados por el manejo y resguardo de la información.
 - El personal como usuario de los equipos informáticos, deberá tener un identificador único en el sistema al cuál se vincularán sus privilegios y accesos.
 - Asimismo, cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso.
 - En un ambiente multiusuario no se deberán compartir datos personales, excepto que se establezca por escrito la protección de datos personales con el fin de conceder privilegios en función de los roles y responsabilidades para el cumplimiento de sus deberes, sin que se exponga al acceso, eliminación, copia o alteración no autorizados de la información.
 - Ningún usuario, está autorizado a llevar consigo o sacar del Instituto discos ópticos, discos compactos, memorias o cualquier otro medio electrónico con aplicaciones o información propiedad del INECOL, a no ser que esta sustracción y portabilidad de información y documentación sea para fines laborales específicos.
 - Ningún usuario está autorizado a instalar/ desinstalar o borrar parcialmente datos, información, bases de datos, paquetería o aplicaciones en los bienes informáticos y de telecomunicaciones propiedad del Instituto, ya sea equipo bajo su resguardo o de algún otro usuario.

En general la evaluación del análisis de riesgos y el análisis de brecha permite mostrar un panorama en el que los controles actuales necesitan optimizarse de manera que contribuyan a disminuir los riesgos detectados. El resultado de este análisis se podrá consultar en el anexo técnico de este documento.

VIII. PLAN DE TRABAJO

En cumplimiento al artículo 33, fracción VI de la LGPDPPSO, el responsable debe elaborar un plan de trabajo para las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales. Este plan de trabajo será elaborado en apego a los resultados obtenidos por el análisis de riesgos y de brecha, con la finalidad de identificar cuáles son las áreas de oportunidad o vulnerabilidades del tratamiento de datos personales a los que se enfrenta actualmente el INECOL. Las actividades generales que se pretenden implementar son las siguientes:

- Realizar reuniones con las Unidades Administrativas que tienen bajo su cargo datos personales con la finalidad de identificar soluciones administrativas, físicas y técnicas que permitan mejorar la evaluación del análisis de riesgos.
- Implementar mecanismos o elementos de control desde la Unidad de Transparencia que permitan garantizar la implementación de las políticas generales de seguridad del INECOL y verificar que se estén implementando.

La estructura del plan de trabajo podrá ser consultado en el anexo técnico de este documento.

IX. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

El monitoreo y revisión de las medidas de seguridad descritas en el presente documento dan cumplimiento al artículo 63 de los LGPDPS y al artículo 33, fracción VII de la LGPDPSO. Entre los elementos que se monitorearán se encuentran los siguientes:

- I. Los nuevos activos que se incluyan en la gestión de riesgos;
- II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
- III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo; y
- VII. Los incidentes y vulneraciones de seguridad ocurridas.

El artículo 36 de la LGPDPSO únicamente considera los casos en los que será necesario realizar una actualización al DS:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales, que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; o

- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Los mecanismos de monitoreo y revisión de las medidas de seguridad que el INECOL adoptará se realizará de la siguiente manera:

- Analizar los resultados del análisis de riesgos de cada sistema con la finalidad de identificar cambios en cuanto a las amenazas, vulnerabilidades, impacto y la probabilidad de ocurrencia de alguno de estos eventos.
- Para garantizar un correcto manejo de vulneraciones en materia de seguridad de datos personales, la Unidad de Transparencia coordinará con apoyo de la Dirección de administración, la elaboración de procedimientos para implementar acciones que permitan el manejo de vulneraciones.
- La adopción del ciclo de mejora continua es primordial, por lo que será necesario que los resultados obtenidos del análisis de riesgos de cada sistema y los resultados de las vulneraciones sean considerados para el establecimiento de acciones correctivas y preventivas, lo que derivará en mejoras para el DS.

X. PROGRAMA GENERAL DE CAPACITACIÓN

El programa de capacitación tiene fundamento en el artículo 30 fracción III, de la LGPDPPSO y establece que, para el cumplimiento del principio de responsabilidad, se debe *"...poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales..."*, por lo que, para dar cumplimiento a esta disposición, la Unidad de Transparencia del INECOL, considerará en su programa anual de capacitación temas referentes al manejo de Datos Personales y específicamente para este rubro considerará como mínimo lo siguiente:

- Asegurarse que el personal en apego de sus funciones y responsabilidades reciba capacitación especializada cuando opere algún software que incluya datos personales.
- Capacitación en general al personal que tenga bajo su resguardo datos personales.
- Coordinar con el departamento de recursos humanos la implementación de una detección de necesidades de capacitación o en su caso considerar los mecanismos propuestos por el INAI.
- Establecer los criterios de evaluación que permitan identificar que los participantes en las capacitaciones adquirieron y entendieron los conocimientos necesarios para asegurar que las medidas de seguridad adoptadas en este documento se cumplan.



Anexo Técnico del Documento de Seguridad del INECOL



GOBIERNO DE
MÉXICO



CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES
CIENCIAS Y TECNOLOGÍAS



INECOL
INSTITUTO DE ECOLOGÍA, A.C.

I. ANÁLISIS DE RIESGOS

Este apartado del DS se deriva del artículo 33 fracción IV de la LGPDPSO, donde se establece que el responsable deberá realizar "...un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;..." por lo que se analizará cada activo (datos personales y elementos físicos e infraestructura que soportan a los datos personales) identificado en el inventario de datos personales. Debido a que los datos personales en cada sistema son repetitivos se realizará un análisis integral.

La evaluación de los riesgos se elaboró en apego a la metodología y formato propuesto por la Guía de Apoyo publicada en el portal del INAI. Los Datos o activos analizados corresponde a los 4 sistemas en los que se identificó el uso de datos personales que son los siguientes:

- Adjudicación en materia de adquisiciones, servicios y obra pública
- Selección, contratación e identificación de personal
- Recepción y evaluación de documentos de aspirantes en convocatorias para puestos académicos del INECOL
- Ingreso al posgrado y registro de trámites de personal académico y estudiantil

Para facilitar el manejo de la evaluación, los datos personales se clasificaron de la siguiente manera:

- **Datos identificativos:** El nombre, domicilio, teléfono particular, teléfono celular, firma, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, y demás análogos;
- **Datos electrónicos:** Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;
- **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, y demás análogos;
- **Datos patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, y demás análogos;

- **Datos sobre procedimientos administrativos:** La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio, y demás análogos;
- **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, y demás análogos;
- **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria, y demás análogos;
- **Datos sobre la salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona, y demás análogos;
- **Datos biométricos:** Huellas dactilares, ADN, geometría de la mano, características de iris y retina, y demás análogos;
- **Datos especialmente protegidos (sensibles):** En algunos casos los datos biométricos arriba señalados, origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; y demás análogos.

En el Cuadro 1 se presenta la clasificación de datos personales por Unidad Administrativa en función del tipo de dato en posesión del INECOL, con la finalidad de establecer los niveles de riesgos a los que se enfrenta cada grupo de datos personales.

Cuadro 1. Clasificación de datos personales a cargo del INECOL en sus 4 sistemas.

Clasificación	Unidad Administrativa			
	Subdirección de Bienes y Servicios	Subdirección de Desarrollo Institucional	Secretaría Académica	Secretaría de Posgrado
Datos Identificativos	Nombre completo de la persona física	Nombre completo	Nombre completo	Nombre completo
	Firma y rúbrica	Domicilio particular	Domicilio particular	Domicilio particular
	Identificación oficial de la persona física, apoderado legal o de quien comparece en su representación a los eventos para la sustanciación de los procedimientos de adjudicación.	Teléfono particular	Teléfono particular	Teléfono particular
	RFC	Estado civil		Teléfono celular
	Acta de nacimiento	Firma		Estado civil
	CURP	RFC		Firma
	-	CURP		RFC
	-	Sexo		CURP

Clasificación	Unidad Administrativa			
	Subdirección de Bienes y Servicios	Subdirección de Desarrollo Institucional	Secretaría Académica	Secretaría de Posgrado
	Comprobante de domicilio	Fecha y lugar de nacimiento		Género
		Fotografía		Visa
		Edad		Fecha de nacimiento
		Cartilla del servicio militar		Lugar de nacimiento
		Número de licencia de manejo		Fotografía
		Número de pasaporte		Edad
		Número de seguridad social		Pasaporte
		Credencial para votar		Credencial para votar
		-		Nombre de familiares, dependientes y beneficiarios
		Datos electrónicos		Correo electrónico
-	-		Correo electrónico	
-	-		ORCID	
-	-		URL oficial	
Datos laborales	-	Referencias personales y laborales	Experiencia laboral	-
		Datos bancarios		
		Estado de cuenta de Afore		
		Seguros		
		Exámenes psicométricos		
Datos patrimoniales	Constancia de situación fiscal	Constancia de situación fiscal	-	-
	Opinión de cumplimiento de SAT	Créditos		
	Domicilio fiscal	Ingresos		
	Opinión de cumplimiento del INFONAVIT	-		
	Opinión de cumplimiento de IMSS	-		
	Carta de datos bancarios	-		
Datos sobre procedimientos administrativos	-	Descuentos por orden judicial	-	-
Datos académicos	-	Títulos	Curriculum vitae	Títulos
		Certificados	Formación académica, complementaria y tecnológica	Certificados
		Constancias	-	Constancias
		Cédula profesional		Cédula profesional
		Datos laborales		Datos de estudios anteriores necesarios para la emisión del título físico y electrónico.

Clasificación	Unidad Administrativa			
	Subdirección de Bienes y Servicios	Subdirección de Desarrollo Institucional	Secretaría Académica	Secretaría de Posgrado
		Curriculum vitae		Exámenes
				Calificaciones
				Resultados de entrevistas
				Encuestas
				Información señalada en la solicitud de ingreso al posgrado
Datos de tránsito y movimiento migratorio	-	Cédula migratoria	-	-
Datos sobre la salud	-	Datos de salud	-	Datos de salud
Datos biométricos:	-	Registro biométrico facial	-	-
Datos especialmente protegidos (sensibles)	-	-	-	-

Con el resultado de la clasificación de datos del Cuadro 1, se analizarán los riesgos de manera integral, abarcando 9 clasificaciones de información y los 4 sistemas que se están analizando. El resultado de la evaluación de riesgos se puede apreciar en el Cuadro 2.




ST

Cuadro 2. Análisis de riesgos para los 4 sistemas que manejan datos personales en el INECOL.

Clasificación de datos por activos	Amenaza	Vulnerabilidad	C	I	D	Impacto	Probabilidad	Riesgo
Datos identificativos	SE ELIMINAN: Veintitrés filas, correspondientes a las columnas denominadas: Amenaza, Vulnerabilidad, Confidencialidad (C), Integridad (I), Disponibilidad (D), Impacto, Probabilidad y Riesgo del Cuadro 2. Análisis de riesgo. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el <i>Anexo 8. Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales</i>, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.							
Datos electrónicos								
Datos laborales								
Datos patrimoniales								
Datos sobre procedimientos administrativos								
Datos académicos								

Clasificación de datos por activos	Amenaza	Vulnerabilidad	C	I	D	Impacto	Probabilidad	Riesgo
	SE ELIMINAN: Dieciocho filas, correspondientes a las columnas denominadas: Amenaza, Vulnerabilidad, Confidencialidad (C), Integridad (I), Disponibilidad (D), Impacto, Probabilidad y Riesgo del Cuadro 2. Análisis de riesgo. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales, Variable y formato 2.1 Deber de seguridad.</i> Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.							
Datos de tránsito y movilidad migratoria								
Datos sobre la salud								
Datos biométricos								
Análisis de impacto para los titulares								

Clasificación de datos por activos	Amenaza	Vulnerabilidad	C	I	D	Impacto	Probabilidad	Riesgo
SE ELIMINAN: Veintidós renglones, correspondientes al Análisis de impacto para los titulares. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales</i>, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.								
C, I, D: Corresponde a Confidencialidad, Integridad y Disponibilidad. Estos rubros integran el impacto en una clasificación cuantitativa del 1 al 5.								

ayef



II. ANÁLISIS DE BRECHA

De acuerdo con las Políticas Internas para el Tratamiento de Datos Personales en el INECOL, se definen las medidas de seguridad de los datos personales en la siguiente clasificación:

a) Físicas

Las personas servidoras públicas INECOL, deberán:

- Resguardar los expedientes en archiveros y gavetas bajo llave.
- Evitar reciclar documentos que contengan datos personales, así como verificar que no se utilicen hojas que puedan contener datos personales y/o información confidencial de la organización, ya que pudieran ser divulgados o expuestos y utilizados para finalidades distintas a las legítimas establecidas en el aviso de privacidad correspondiente.
- Evitar tirar documentos con datos personales sin triturar o destruir.
- No dejar documentos con datos personales en las fotocopadoras, scanners e impresoras.
- Mantener los escritorios limpios, cualquier documento o expediente debe estar resguardado, fuera de la vista, cuando no se esté utilizando.
- Proteger el acceso físico al lugar en el que se encuentra el medio de almacenamiento.
- Bloquear los datos personales una vez agotado el periodo de conservación.
- Para el caso de las contrataciones de servicios en las que haya tratamiento de datos personales, atendiendo a la normatividad aplicable, la Unidad Administrativa deberá gestionar la entrega de evidencia de la supresión de los datos personales, conforme a lo acordado en el contrato correspondiente.

b) Administrativas

- Cada Unidad Administrativa deberá integrar un Inventario de datos personales que considere la totalidad de los procesos que, en el ejercicio de sus atribuciones, competencias y funciones implique el tratamiento de datos personales.
- Cada Unidad Administrativa deberá identificar en los procesos en los cuales realice el tratamiento de datos personales, los riesgos y su valoración en relación con su impacto y probabilidad de ocurrencia.
- La Unidad de Transparencia, proporcionará los procedimientos, formatos o guías (emitidas por el INAI) mediante los cuales se facilite a las Unidades Administrativas la elaboración de los inventarios de datos personales.



- La Unidad de Transparencia, integrará y administrará el Inventario Institucional de datos personales.
- Los inventarios de cada Unidad Administrativa se actualizarán periódicamente atendiendo a los cambios o mejoras, y deberán informarse para que se realice la actualización del Inventario Institucional de Datos Personales. La Unidad de Transparencia promoverá en coordinación con las Unidades Administrativas, y el área de tecnologías de la información, la implementación de medidas de seguridad para la protección de datos personales.
- Las Unidades Administrativas que recaben los datos personales, así como la Unidad de Transparencia y tecnologías de la información en el ámbito de sus competencias, determinarán, los términos específicos para la transferencia de datos personales, así como las medidas de seguridad pertinentes.
- El Comité de Transparencia aprobará el formato de clausulado que, en su caso, será incluido en los contratos o instrumentos jurídicos que celebre el INECOL, con la finalidad de formalizar la transferencia de datos personales y la relación con terceros encargados de tratarlos.
- Los plazos de conservación de los documentos que contengan datos personales, establecidos en el inventario no deberán exceder aquéllos señalados en el Catálogo de disposición documental vigente del INECOL.
- El personal de nuevo ingreso firmará la carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales, así como el código de conducta y código de ética de las y los servidores públicos del INECOL, donde se establecen las conductas a seguir en materia de transparencia y confidencialidad, que son:
 - Evitar filtrar información o esparcir rumores o comentarios que dañen la reputación de las compañeras y los compañeros de trabajo y en general de la institución o de la administración para la cual se labora.
 - Proporcionar información a la sociedad de manera equitativa, sin criterios discrecionales, excepto cuando se justifique la confidencialidad y utilizando los procedimientos establecidos para ello.
 - Actuar con imparcialidad, cuidado y dedicación en la elaboración y preparación de la información interna.
 - Cuidar la información a su cargo, impidiendo la sustracción, la destrucción, el ocultamiento o la utilización indebida de la misma.
 - Entregar la información a su cargo, impidiendo la sustracción, la destrucción, el ocultamiento o la utilización indebida de la misma.
 - Entregar la información requerida en los tiempos y formas estipulados con claridad y calidad.

c) Técnicas



- El área de TIC's realizará monitoreos y establecerá una cadena de avisos en caso de vulnerabilidad a la seguridad de la información; asimismo, se harán eventualmente pruebas de intrusión.
- Se revisará de manera periódica la administración y asignación de contraseñas con el fin de apoyar a los administradores y usuarios de servicios de tecnología a reducir los impactos de los riesgos generados por el manejo y resguardo de la información.
- El personal como usuario de los equipos informáticos, deberá tener un identificador único en el sistema al cuál se vincularán sus privilegios y accesos.
- Asimismo, cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso.
- En un ambiente multiusuario no se deberán compartir datos personales, excepto que se establezca por escrito la protección de datos personales con el fin de conceder privilegios en función de los roles y responsabilidades para el cumplimiento de sus deberes, sin que se exponga al acceso, eliminación, copia o alteración no autorizados de la información.
- Ningún usuario, está autorizado a llevar consigo o sacar del Instituto cintas discos ópticos, discos compactos, memorias o cualquier otro medio electrónico con aplicaciones o información propiedad del INECOL, a no ser que esta sustracción y porte de información y documentación sea para fines laborales específicos.
- Ningún usuario está autorizado a instalar, desinstalar o borrar parcialmente datos, información, bases de datos, paquetería o aplicaciones en los bienes informáticos y de telecomunicaciones propiedad del Instituto, ya sea equipo bajo su resguardo o de algún otro usuario.

Con respecto a las acciones implementadas para cada clasificación de datos, en el Cuadro 3 se presenta el análisis de brecha de cada grupo de datos.



Cuadro 3. Análisis de brecha con respecto a las medidas propuestas en las políticas Internas para el tratamiento de datos personales.

Clasificación de datos por activos	Amenaza	Riesgo inherente					Controles de seguridad implantados	Evidencia	Responsable	Nivel de madurez
		C	I	D	Im	Pr				
Nueve Clasificaciones aplicables (Cuadro 1)	SE ELIMINA: La información de las columnas denominadas Amenaza, Riesgo inherente, Controles de seguridad implantados, Evidencia, Responsable y Nivel de madurez del Cuadro 3. Análisis de brecha. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales</i> , Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.									

Clasificación de datos por activos	Amenaza	Riesgo inherente					Controles de seguridad implantados	Evidencia	Responsable	Nivel madurez	de
		C	I	D	Im	Pr					
	SE ELIMINA: La información de las columnas denominadas Amenaza, Riesgo inherente, Controles de seguridad implantados, Evidencia, Responsable y Nivel de madurez del Cuadro 3. Análisis de brecha. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales</i>, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.										

Clasificación de datos por activos	Amenaza	Riesgo inherente					Controles de seguridad implantados	Evidencia	Responsable	Nivel madurez	de
		C	I	D	Im	Pr					
	SE ELIMINA: La información de las columnas denominadas Amenaza, Riesgo inherente, Controles de seguridad implantados, Evidencia, Responsable y Nivel de madurez del Cuadro 3. Análisis de brecha. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales</i>, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.										

Anexo Técnico del Documento de Seguridad

Clasificación de datos por activos	Amenaza	Riesgo inherente					Controles de seguridad implantados	Evidencia	Responsable	Nivel de madurez
		C	I	D	Im	Pr				
		SE ELIMINA: La información de las columnas denominadas Amenaza, Riesgo inherente, Controles de seguridad implantados, Evidencia, Responsable y Nivel de madurez del Cuadro 3. Análisis de brecha. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años.								

C, I, D, Im, Pr: Corresponde a Confidencialidad, Integridad, Disponibilidad, Impacto y Probabilidad respectivamente.

C, I, D, Im, Pr: Corresponde a Confidencialidad, Integridad, Disponibilidad, Impacto y Probabilidad respectivamente.



De las 9 clasificaciones de datos analizados y de los 12 controles de seguridad implantados a través de las Políticas Internas para la Gestión y el Tratamiento de los Datos Personales en Posesión del INECOL, se puede observar que solo 4 cuentan con un nivel de madurez "L2", lo que indica que los controles son repetitivos pero intuitivos y se traduce en que se realizan de forma preventiva y constante, pero que no está documentado. Para el nivel de madurez "L1", son 7 los controles que se encuentran en esta clasificación y se traduce en acciones que se implementan cuando surge un problema, es decir se actúa en consecuencia de algún evento que pueda vulnerar la protección de datos personales. Finalmente, el rubro sobre la orografía de la zona en la que se encuentra las instalaciones, que evitan que se inunde las zonas en las que se tiene resguardados los documentos físicos que contienen datos personales bajo la responsabilidad del INECOL.

En general la evaluación del análisis de riesgos y del análisis de brecha permite mostrar un panorama en el que los controles actuales necesitan optimizarse de manera que contribuyan a disminuir el riesgo de cada clasificación de datos.

III. PLAN DE TRABAJO

En cumplimiento al artículo 33, fracción VI de la LGPDPPSO, el responsable debe elaborar un plan de trabajo para las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales. Este plan de trabajo será elaborado en apego a los resultados obtenidos por el análisis de riesgos y de brecha, con la finalidad de identificar cuáles son las áreas de oportunidad o vulnerabilidades del tratamiento de datos personales a los que se enfrenta actualmente el INECOL. Las actividades generales que se pretenden implementar son las siguientes:

- Realizar reuniones con las unidades administrativas que tienen bajo su cargo datos personales con la finalidad de identificar soluciones administrativas, físicas y técnicas que permitan mejorar la evaluación del análisis de riesgos.
- Implementar mecanismos o elementos de control desde la Unidad de Transparencia que permitan garantizar la implementación de las políticas generales de seguridad del INECOL y verificar que se estén implementando.

Adicionalmente, a través de la Unidad de Transparencia se realizará el seguimiento del plan de trabajo (Cuadro 4) y se establecerá como base para asegurar que las acciones descritas en el presente DS se cumplan.

Cuadro 4. Plan de trabajo del DS del INECOL.

Riesgo	Nivel	Medidas preventivas y de control	Tipo de recursos necesarios	Fecha de inicio	Fecha de revisión
SE ELIMINA: La información correspondiente al Riesgo, Nivel, Medidas preventivas y de control, Tipos de recursos necesarios, Fecha de inicio y Fecha de revisión del Cuadro 4. Plan de Trabajo del Documento de Seguridad. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales, Variable y formato 2.1 Deber de seguridad. Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años					



Riesgo	Nivel	Medidas preventivas y de control	Tipo de recursos necesarios	Fecha de inicio	Fecha de revisión
SE ELIMINA: La información correspondiente al Riesgo, Nivel, Medidas preventivas y de control, Tipos de recursos necesarios, Fecha de inicio y Fecha de revisión del Cuadro 4. Plan de Trabajo del Documento de Seguridad. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales, Variable y formato 2.1 Deber de seguridad.</i> Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años					



Riesgo	Nivel	Medidas preventivas y de control	Tipo de recursos necesarios	Fecha de inicio	Fecha de revisión
SE ELIMINA: La información correspondiente al Riesgo, Nivel, Medidas preventivas y de control, Tipos de recursos necesarios, Fecha de inicio y Fecha de revisión del Cuadro 4. Plan de Trabajo del Documento de Seguridad. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA), y en cumplimiento a lo establecido en el Anexo 8. <i>Formatos obligatorios para la publicación de medios de verificación documentales dentro del apartado virtual Protección de Datos Personales, Variable y formato 2.1 Deber de seguridad.</i> Fecha de clasificación: veintidós de junio de dos mil veintitrés, Séptima Sesión Extraordinaria del Comité de Transparencia. Área que propuso la clasificación: Unidad de Transparencia. Periodo de reserva: 5 años					

Este plan de trabajo se analizará posterior a la autorización del presente documento por el Comité de Transparencia del INECOL y se definirán los plazos a corto, mediano y largo plazo en los que se monitorearán las medidas preventivas y de control que se adoptarán para garantizar que se implementen. Este plan de trabajo se actualizará en caso de que el tratamiento de los datos personales sea modificado previa consideración del comité de transparencia del INECOL.

