AI-ADV-10-2026

GERENCIA GENERAL
ADMINISTRACIÓN Y PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

1.1 Origen

La presente Advertencia se origina en cumplimiento del Plan Anual de Trabajo de la Auditoría Interna.

1.2 Objetivo

Advertir sobre las posibles consecuencias de determinadas conductas o decisiones a los órganos pasivos que fiscaliza el PTIC, con el fin de brindar un servicio preventivo y oportuno a la administración activa de la institución

2. DESARROLLO DE LA ADVERTENCIA

Como parte de los servicios preventivos que debe brindar la Auditoría Interna, y en el marco de cumplimiento de sus obligaciones y competencias establecidas en el artículo 22 de la Ley General de Control Interno, 8292, especialmente el inciso d); donde se dispone: ***"d) Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento";*** así como, lo establecido, en igual sentido, por las *Normas para el Ejercicio de la Auditoría Interna en el Sector Público*, aprobadas por la Contraloría General de la República mediante resolución R-DC-064-2014 del 11 de agosto de dos mil catorce; se presenta la siguiente información referente a algunos temas que se consideran de relevancia, por las implicaciones que tienen en el cumplimiento de objetivos institucionales y las que pudieran derivarse en adelante y que se detallan seguidamente.

En cuanto a la revisión documental disponible sobre el cumplimiento de la Ley N° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, vigente desde el 5 de setiembre de 2011, se identificaron actuaciones institucionales en materia de protección de datos personales desde el año 2020, mediante gestiones orientadas a la elaboración del protocolo de protección de datos y seguridad de la información. En febrero de 2021, la Presidencia Ejecutiva dispuso la conformación de una comisión temporal para atender dicho encargo. Posteriormente, entre 2023 y 2025, se desarrollaron acciones relacionadas con capacitación, elaboración y seguimiento del Plan Institucional de Protección de Datos Personales 2024-2027 y designación de personas representantes de distintas dependencias.

Los principales hechos identificados se resumen en la siguiente tabla. El detalle de los documentos, fechas y actuaciones revisadas se incorpora en el **Anexo 1**, denominado "Cronología documental de la gestión institucional en materia de protección de datos personales".

Periodo	Hecho relevante	Situación identificada
2020-2021	En noviembre de 2020 se solicita la conformación de un equipo de trabajo. En febrero de 2021, la Presidencia Ejecutiva ordena formalmente a la Asesoría Legal la creación de una comisión temporal para elaborar un protocolo mínimo de actuación.	Se reconoce formalmente la obligación institucional; sin embargo, la instancia se constituye para un encargo específico y temporal, sin definición de rectoría permanente.
2022	La PRODHAB comunica al sector público la necesidad de reforzar capacidades frente a vulneraciones de seguridad y tratamiento adecuado de datos personales.	El antecedente externo refuerza la necesidad de fortalecer controles técnicos, normativos y organizativos en la materia.
2023	Se autoriza la participación de personas funcionarias en capacitación de la PRODHAB y se atienden gestiones asociadas al consentimiento informado en formularios institucionales.	Se inicia una fase más activa de atención técnica y jurídica, aunque todavía concentrada en gestiones puntuales y preparatorias.
2024	Se remite a la PRODHAB el Plan Institucional de Protección de Datos Personales 2024-2027. Se atienden consultas sobre transferencia de datos, se aplica un cuestionario diagnóstico y se incorporan términos de uso y políticas de privacidad en los sistemas institucionales.	Se establece una hoja de ruta institucional, pero persiste la ausencia de trámites críticos: protocolo mínimo de actuación, inscripción de bases de datos, análisis de riesgos y fortalecimiento de medidas de seguridad.
2025	La Presidencia Ejecutiva instruye la designación de representantes del Comité y solicita colaboración para la clasificación de datos personales. La entrevista de Auditoría confirma la ausencia de rectoría formal, la falta de dedicación exclusiva y la inexistencia de una figura especializada en seguridad de la información.	Se avanza en la organización del seguimiento del Plan, pero persisten debilidades estructurales: falta de estandarización en la clasificación de datos, insuficiencia de recursos y ausencia de una instancia con capacidad operativa y atribuciones definidas.

De la revisión documental efectuada se confirma que la instancia actualmente denominada "Comité de Protección de Datos" fue concebida originalmente como una comisión temporal, sin que se haya identificado un acto administrativo posterior que defina de manera integral su naturaleza, denominación, autoridad, responsabilidades permanentes y condiciones operativas, pese a que en la práctica se utiliza la denominación de comité.

Asimismo, la entrevista realizada a la Subcoordinadora permitió corroborar la ausencia de formalidad constitutiva del comité y que, además, esta instancia funciona como un mecanismo de seguimiento del Plan Institucional y que sus actividades son atendidas por personas funcionarias que tienen otras funciones asignadas, sin que exista una asignación de tiempo completo para esta labor. Adicionalmente, señaló la persona funcionaria que la clasificación de los datos personales recolectados y almacenados mediante formularios, bases de datos y sistemas institucionales no se encuentra estandarizada, evidenciándose deficiencias en el diseño de los instrumentos de recolección y en la categorización de la información, lo cual ha generado duplicidades y contradicciones que dificultan el análisis integral de riesgos y la toma de decisiones informadas.

En el marco de la ejecución del Plan, la Asesoría Legal institucional ha asumido un rol central en la coordinación y atención de los asuntos vinculados al tratamiento de datos personales. Como parte de ese rol activo, la Asesoría Legal mediante oficio ALEA-1163-2024 del 18 de diciembre de 2024, remitió a la Presidencia Ejecutiva del INA el primer informe referente al estado del Plan Institucional para la Protección de Datos Personales del INA 2024-2027 (PE-756-2024), en el cual se destaca lo siguiente:

1. El Plan surge por un requerimiento formal de PRODHAB.
2. Se cumplió formalmente con las actividades programadas para 2024.
3. Se identificaron al menos 65 bases de datos institucionales.
4. Existe un nivel importante de desconocimiento institucional sobre protección de datos personales.

    - 83% indicó no estar capacitado.
    - 75% desconoce la normativa.
    - 75% desconoce si existe transferencia de datos.

5. La muestra del cuestionario no alcanzó el nivel esperado de participación (61,96%).
6. Varias acciones críticas para el cumplimiento efectivo aún se encuentran pendientes para 2025-2026.
7. No existe una figura institucional designada de Oficial de Seguridad de la Información ni Oficial de Protección de Datos.
8. Persisten necesidades de fortalecimiento normativo, procedimental y tecnológico.

Para más detalle sobre las conclusiones y recomendaciones plasmadas en el informe. **Ver anexo 3**. Conclusiones y Recomendaciones (INFORME ESTADO – AVANCE: Plan Institucional para la Protección de Datos Personales del INA 2024-2027).

Se evidencia por medio de este informe presentado a Presidencia lo siguiente:

- La necesidad de valorar el establecimiento de procedimientos específicos para la implementación de medidas físicas y organizativas.

- Los resultados del "Cuestionario diagnóstico sobre la aplicación de la protección de datos personales en el INA", revelaron que existe un volumen considerable de bases de datos que requieren la creación o actualización de procedimientos en materia de protección de datos personales.

- Crear una categoría específica para reportar incidentes de datos personales y enviarlos al encargado de seguridad o al Oficial de Datos (*figura que actualmente en el INA, no existe, y que fue mencionado en el informe AI-ICI-08-2024 Gestión de Seguridad de la Información, por esta Auditoría Interna*). Sin embargo, esto no es operativo actualmente porque el software ARANDA no cuenta con soporte.

- La revisión de los términos de uso de los sistemas y las políticas de privacidad, la cual permitió identificar casos de recolección de datos personales sin respaldo explícito en dichos instrumentos. Como medida inicial, mediante el oficio SGT-519-2024 del 7 de noviembre de 2024, se procedió a la incorporación de los términos de uso y las políticas de privacidad en todos los sistemas del INA.

- Se plantea la necesidad de la integración de diferentes mecanismos de recolección de datos personales y su cumplimiento de los términos de uso y políticas de privacidad supra mencionados.

De conformidad con lo expuesto en la Ley N° 8968 Protección de la persona frente al tratamiento de sus datos personales, se establece

> "***ARTÍCULO 6.- Principio de calidad de la información***
> *Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.*
>
> *1. Actualidad*
> *Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular.*

2. Veracidad
Los datos de carácter personal deberán ser veraces.
La persona responsable de la base de datos está obligado a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita.

3.- Exactitud
Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.
Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección.

4.-Adecuación al fin
Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.
No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley.
Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública. (…)

ARTÍCULO 10.- Seguridad de los datos
El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.
Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.
No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.
Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos. (…)

ARTÍCULO 12.- Protocolos de actuación
Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.
Para que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.

La manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, "iuris tantum", el cumplimiento de las disposiciones contenidas en esta ley, para los efectos de autorizar la cesión de los datos contenidos en una base. (…)

ARTÍCULO 21.- Registro de archivos y bases de datos
Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasbase o la transferencia de los datos.
Deberá inscribir cualesquiera otras informaciones que las normas de rango legal le impongan y los protocolos de actuación a que hacen referencia el artículo 12 y el inciso c) del artículo 16 de esta ley."

La Ley N° 8220 Protección al ciudadano del exceso de requisitos y trámites administrativos, establece:

*"**Artículo 2º-Presentación única de documentos**. La información que presenta un administrado ante una entidad, órgano o funcionario de la Administración Pública, no podrá ser requerida de nuevo por estos, para ese mismo trámite u otro en esa misma entidad u órgano. De igual manera, ninguna entidad, órgano o funcionario público, podrá solicitar al administrado, información que una o varias de sus mismas oficinas emitan o posean.*
Para que una entidad, órgano o funcionario de la Administración Pública pueda remitir información del administrado a otra entidad, órgano o funcionario, la primera deberá contar con el consentimiento del administrado.
Quedan exceptuadas de la aplicación de este artículo las personerías jurídicas."

De conformidad con lo expuesto en la Ley N° 7975 Información no divulgada, se indica:

*"**ARTÍCULO 4.- Información excluida de protección.** Esta ley no protegerá la información que:*
a) Sea del dominio público.
b) Resulte evidente para un técnico versado en la materia con base en información disponible de previo.
c) Deba ser divulgada por disposición legal u orden judicial. No se considerará que entra al dominio público la información confidencial que cumpla los requisitos del primer párrafo del artículo 2 de esta ley y haya sido proporcionada a cualquier autoridad por quien la posea, cuando la haya revelado para obtener licencias, permisos, autorizaciones, registros o cualquier otro acto de autoridad, por constituir un requisito formal. En todo caso, las autoridades o entidades correspondientes deberán guardar confidencialidad."

A partir de la cronología documentada, se concluye que el Instituto Nacional de Aprendizaje (INA) inició formalmente en noviembre de 2020 un proceso para establecer un sistema de protección de datos personales, en respuesta al mandato de la Ley N° 8968. Este proceso ha sido reactivo, gradual y sujeto a plazos extensos, transitando desde una fase inicial de reconocimiento de la obligación legal (2020-2021) hacia la construcción de un modelo de cumplimiento (comité, planes) a partir de 2023, acelerada por requerimientos y recordatorios de la PRODHAB.

A inicios de 2025, se consolida una gobernanza formal con un Comité de Protección de Datos designado; sin embargo, persisten debilidades que limitan el avance efectivo: no existe claridad sobre la naturaleza de esta instancia, si es un equipo, comité o comisión, carece de una denominación estandarizada y no se han establecido mecanismos formales de seguimiento que permitan monitorear el cumplimiento de los cronogramas del Plan. A pesar de contar con el Plan Institucional, no se ha logrado concretar la transferencia de datos en el marco de convenios interinstitucionales, debido a la ausencia del protocolo mínimo de actuación y de la inscripción de bases de datos ante la PRODHAB, lo que mantiene a la institución en un periodo de vulnerabilidad.

El inicio tardío del proceso, once años después de la promulgación de la Ley N° 8968, evidencia una respuesta reactiva que ha condicionado el avance institucional en esta materia. En consecuencia, el principal riesgo transversal es que, pese a los avances documentados, la brecha entre la normativa y su implementación efectiva permita la materialización de riesgos con impactos tanto institucionales como personales, para quienes ostentan responsabilidades formales. Dentro de los riesgos con posible materialización se identifican los siguientes:

Tipo	Riesgo	Posible materialización
Operativos	R024 - Capacidad de Respuesta	Ausencia de una figura especializada permanente, insuficiencias en la planificación del tiempo y recurso humano requerido para atender oportunamente las actividades. Así mismo, actividades rezagadas por carga de trabajo, una dedicación limitada del personal al Plan y la necesidad de laborar fuera de jornada.
	R029 – Normativa Interna Inadecuada	La ausencia o insuficiencia de protocolos, procedimientos y/o lineamientos específicos para regular la gestión de protección de datos podría generar actuaciones no estandarizadas, inconsistencias en su aplicación y dificultades para asegurar el adecuado cumplimiento de las responsabilidades institucionales.
	R031 - Satisfacción de la Clientela	Solicitudes relacionadas con los derechos sobre datos personales no atendidos oportunamente.
	R060 - Coordinación	Falta de coordinación y seguimiento entre las dependencias responsables generando atrasos, omisiones o incumplimientos en la ejecución del Plan Institucional de Protección de Datos Personales.
Sistemas de Información	R066 - Confidencialidad	Tratamiento inadecuado, acceso, utilización, transferencia o divulgación no autorizada de datos personales, especialmente cuando las medidas de seguridad, clasificación y protocolos no se encuentren implementados.
Estratégicos	R006 - Dirección y liderazgo	Ausencia de una instancia formalmente constituida y de una figura especializada con autoridad y responsabilidades definidas para dirigir la gestión de protección de datos, situación que puede generar vacíos operativos y limitar la toma oportuna de decisiones.
Recursos Humanos	R016 - Competencias	Errores u omisiones en el tratamiento de datos personales derivados del desconocimiento de la normativa, responsabilidades y controles aplicables por parte de las personas funcionarias.

Tipo	Riesgo	Posible materialización
Integridad	R033 - Cumplimiento de la normativa jurídica y técnica	Incumplimiento de la Ley N° 8968, su Reglamento y disposiciones de la PRODHAB, por falta o atraso en la implementación de protocolos, procedimientos, análisis de riesgos y demás medidas requeridas para la protección de datos personales.

3. RESUMEN DE LO ADVERTIDO

Con fundamento en los hechos verificados y antecedentes analizados, la Auditoría Interna advierte a la Gerencia General, sobre la necesidad de instruir y liderar el fortalecimiento del modelo de protección de datos personales del Instituto Nacional de Aprendizaje, a fin de asegurar el cumplimiento integral, oportuno y sostenible de la Ley N° 8968 y su normativa conexa. Para ello, se sugiere:

1. **Diseñar, formalizar e implementar una estructura institucional específica en materia de protección de datos personales**, dotada de atribuciones claramente definidas, autoridad para la toma de decisiones y capacidad operativa, que permita la gestión integral y coordinada de todos los aspectos relacionados con esta materia. Dicha estructura deberá contar con roles, responsabilidades, recursos y mecanismos de articulación interinstitucional, así como una denominación única y estandarizada que refleje formalmente su naturaleza y alcance, a fin de fortalecer la gobernanza, asegurar el cumplimiento de la Ley N° 8968 y reducir los riesgos asociados al tratamiento inadecuado de datos personales.

2. **Fortalecer la ejecución del Plan Institucional de Protección y Tratamiento de Datos Personales**, mediante la incorporación de cronogramas formales y detallados para cada actividad programada, que incluyan plazos definidos, responsables asignados, hitos de cumplimiento e indicadores de seguimiento. Asimismo, establecer un mecanismo periódico de monitoreo y reporte de avances que permita a la Administración Superior verificar el grado de cumplimiento, detectar desviaciones oportunamente y adoptar acciones correctivas, con el fin de asegurar la ejecución efectiva y oportuna del Plan.

3. **Avanzar en la elaboración del protocolo mínimo de actuación**, que permita la inscripción de las bases de datos del INA ante la PRODHAB y, de forma independiente, regule y habilite la transferencia de datos personales en el marco de los convenios interinstitucionales vigentes, en estricto apego a la normativa.

La atención de estos aspectos contribuirá a fortalecer el cumplimiento normativo, la gestión de los riesgos vinculados con el tratamiento de datos personales y la capacidad institucional para responder oportunamente ante requerimientos regulatorios, incidentes de seguridad y consultas de las personas titulares de datos.

4. OBSERVACIONES

4.1. Responsabilidad del Control Interno

Desde la competencia de esta Auditoría Interna, es deber recordar a la administración, lo establecido en la Ley General de Control Interno, Nº 8292, artículos 39 y 41, los numerales 38, inciso d), y 39 de la Ley Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, N° 8422, y demás normativa aplicable, en cuanto a que, todos los funcionarios públicos (titulares subordinados) que debiliten con sus acciones el sistema de control interno, u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable, o que incumplan injustificadamente con sus deberes y funciones en materia de control interno; incurrirán en responsabilidad administrativa y civil según corresponda.

4.2. Plazo para informar sobre las acciones llevadas a cabo

En el ejercicio de las competencias conferidas legalmente a las Auditorías Internas, que van desde la prevención hasta el seguimiento de las decisiones y acciones que la administración deba tomar o ejecutar, se solicita, de manera respetuosa, que, en un plazo no mayor a diez días hábiles, contados a partir de la recepción de esta advertencia, se comunique por escrito a este Órgano de Fiscalización las acciones que se aplicarán en relación con lo indicado.

4.3. Responsables de la advertencia

La advertencia fue realizada por las personas funcionarias de esta Auditoría: Albertina Cruz Casco, Silvia Elena Carranza Marín, María Pilar Corrales Vargas, Teresa Sáenz Ávila bajo la supervisión de Didier Chavarría Chaves, Encargado del Proceso de Fiscalización Tecnologías de la Información y Comunicación.

Firmado digitalmente
Albertina Cruz Casco
Auditora encargada de la Advertencia

Firmado digitalmente
Silvia Elena Carranza Marín
María Pilar Corrales Vargas
Teresa Sáenz Ávila
Auditoras colaboradoras de la Advertencia

Firmado digitalmente
Didier Chavarría Chaves
Encargado de Proceso

Firmado digitalmente
Alfredo Hasbum Camacho
Auditor General

Anexo 1
Cronología documental de antecedentes sobre protección de datos personales

Fecha	Oficio	Remitente / Destinatario	Resumen del contenido
nov 2020	UPE-306-2020	Unidad de Planificación Estratégica / Presidencia Ejecutiva	Solicita conformar un equipo encargado de elaborar lineamientos en protección de datos personales y seguridad de la información, en cumplimiento de la Ley N° 8968.
feb 2021	PE-223-2021	Presidencia Ejecutiva / Asesoría Legal	Solicita formalmente a la Asesoría Legal la elaboración de un protocolo mínimo de actuación, mediante la conformación de una comisión temporal con participación de diversas instancias institucionales. Instruye mantener informada a la Presidencia Ejecutiva de los avances de manera mensual.
abr 2022	Comunicado 02-2022	PRODHAB / Sector público	Comunicado dirigido al sector público sobre vulneraciones de seguridad y al tratamiento adecuado de datos personales, evidenciando la necesidad de reforzar capacidades técnicas y normativas.
oct 2023	APD-117-10-2023	PRODHAB / Sector público	Invitación a todo el sector público para participar en una capacitación sobre Protección de Datos Personales y la implementación de protocolos mínimos de actuación, de carácter obligatorio desde 2011.
nov 2023	ALEA-970-2023	Asesoría Legal / Presidencia Ejecutiva	Remite fechas de capacitación y lista de funcionarios propuestos para participar en la capacitación de PRODHAB.
nov 2023	PE-2720-2023	Presidencia Ejecutiva / Asesoría Legal	Autoriza formalmente la participación de los funcionarios propuestos en la capacitación de PRODHAB.
nov 2023	SGT-1075-2023	Subgerencia Técnica / Asesoría Legal	Solicita la elaboración de un consentimiento informado para los formularios FR-GR-188 y FR-GR-01, aprobados por Presidencia Ejecutiva mediante oficio PE-2676-2023.
nov 2023	PE-2676-2023	Presidencia Ejecutiva / Subgerencia Técnica	Aprueba los formularios FR-GR-188 y FR-GR-01 para recolección de información no divulgada.
dic 2023	ALEA-1098-2023	Asesoría Legal / Subgerencia Técnica	Emite el consentimiento informado solicitado para los formularios de recolección de información.
ene 2024	APD-008-01-2024	PRODHAB / Sector público	Recuerda a las instituciones públicas la fecha límite del 15 de abril de 2024 para la entrega del plan de trabajo aprobado por el jerarca para la implementación de los protocolos mínimos de actuación.

Fecha	Oficio	Remitente / Destinatario	Resumen del contenido
abr 2024	ALEA-260-2024	Asesoría Legal / Presidencia Ejecutiva	Remite el Plan Institucional para la Protección de Datos Personales del INA 2024-2027 para su revisión y aprobación. Ver **anexo 2**
abr 2024	PE-756-2024	Presidencia Ejecutiva / PRODHAB	Remite oficialmente el Plan Institucional para la Protección de Datos Personales del INA 2024-2027 a la PRODHAB. Ver **anexo 2**
ago 2024	ALEA-650-2024	Asesoría Legal / PRODHAB	Consulta formal sobre la transferencia de datos personales desde las bases de datos SEMS y SIFA al Ministerio de Salud para la emisión del carné digital de manipulación de alimentos. Precedido por ALEA-170-2024, ALEA-416-2024 y ALEA-534-2024.
ago 2024	PE-1657-2024	Presidencia Ejecutiva / PRODHAB	Comunica a la PRODHAB que el Presidente Ejecutivo es el responsable de las bases de datos del INA.
set 2024	ALEA-796-2024	Asesoría Legal / Subgerencia Técnica	Responde a la solicitud SGT-194-2024 y redacta los términos de uso, condiciones y política de seguridad para la Ventanilla Única, en cumplimiento de la normativa de protección de datos personales, los cuales deben ser observados y acatados a lo interno de la institución.
set 2024	GG-CI-28-2024	Gerencia General / Todos los funcionarios	Instruye de forma obligatoria la atención de un cuestionario diagnóstico sobre protección de datos personales, con fecha límite el 20 de octubre de 2024.
oct 2024	Respuesta de PRODHAB a ALEA-650-2024	PRODHAB / Asesoría Legal	Indica que el INA está facultado para suscribir convenios con el Ministerio de Salud siempre que se cumplan los principios de la Ley N.° 8968. Destaca que el INA aún no tiene bases de datos inscritas.
oct 2024	ALEA-916-2024	Asesoría Legal / Presidencia Ejecutiva	Informa sobre los trámites obligatorios posteriores a la firma del convenio con el MS: 1) inscripción del Protocolo Mínimo de Transferencia, 2) publicación de Términos de Uso y Política de Privacidad, y 3) inscripción de bases de datos SEMS y SIFA. Designa al Presidente Ejecutivo como responsable de la base de datos y a los administradores de sistemas como "Responsable" para efectos del protocolo.
nov 2024	SGT-514-2024	Subgerencia Técnica / Asesoría Legal	Remite los términos de uso, aviso y política de privacidad para el tratamiento de datos personales para revisión legal y posterior aprobación.
nov 2024	ALEA-995-2024	Asesoría Legal / Subgerencia Técnica	Comunica las modificaciones legales requeridas a los términos de uso y política de privacidad.

Fecha	Oficio	Remitente / Destinatario	Resumen del contenido
nov 2024	SGT-519-2024	Subgerencia Técnica / Áreas correspondientes	Solicita la publicación de los términos de uso y políticas de privacidad en el sitio web institucional. Comunica formalmente a administradores de sistemas y jefaturas de GTIC los días 11 y 20 de noviembre mediante GG-1834-2024 y USIT-371-2024.
dic 2024	ALEA-1163-2024	Asesoría Legal / Presidencia Ejecutiva	Primer informe del estado del Plan Institucional 2024-2027. Detalla acciones realizadas en 2024 (capacitación, inventario, cuestionario, revisión de términos de uso) y acciones programadas para 2025 (curso, campañas, análisis de riesgos, procedimientos). Incluye conclusiones del cuestionario diagnóstico: 83% no capacitado, 75% desconoce normativa, 48% conoce medidas de seguridad.
ene 2025	PE-252-2025	Presidencia Ejecutiva / Comité de Protección de Datos Personales	Instruye a las dependencias que integran el Comité a designar representantes propietarios y suplentes. Designa a la Sra. Ansuette Esquivel Zayas-Bazan como coordinadora y a la Sra. Nancy Granados Peraza como subcoordinadora.
jun 2025	PE-1698-2025	Presidencia Ejecutiva / Unidades organizativas	Solicita colaboración para definir líneas estratégicas clave en el marco del Plan Institucional.
ago 2025	PE-2552-2025	Presidencia Ejecutiva / Unidades organizativas	Complementa la solicitud de colaboración para la aplicación de la tabla de clasificación de datos personales acorde a su ciclo de vida.
dic 2025	Entrevista de Auditoría Interna	Auditoría Interna / Subcoordinadora del Comité de Protección de Datos	Se confirma que el Comité no fue concebido como órgano rector ni unidad ejecutora, sino como mecanismo de seguimiento del Plan. Las actividades se atienden sin dedicación exclusiva (15%-25% del tiempo laboral), requiriendo atención fuera del horario ordinario. Se evidencia falta de estandarización en la clasificación de datos y la inexistencia de un Oficial de Seguridad de la Información.

Anexo 2
Plan Institucional Protección de Datos Personales

LÍNEA ESTRATÉGICA	ACTIVIDADES	RESPONSABLES	OTRAS INSTANCIAS INVOLUCRADAS	PLAZOS DE EJECUCIÓN	INSUMOS / RECURSOS	META
1. Capacitación en el tema de protección y tratamiento de datos personales	1.1 Crear una campaña informativa en materia de protección y tratamiento de datos personales (utilizar Campaña de PRODHAB 2021 coordinar con Comunicación) (oficio relanzando la Campaña) o posteriores	Comisión Institucional	Asesoría de Comunicación/PRODHAB	2024	Recurso humano, material de PRODHAB	Una campaña informativa
	1.2 Desarrollar un curso de autoaprendizaje en materia de protección y tratamiento de datos personales.	Comisión Institucional	UIPE/USEVI	I semestre del 2025	Recurso humano, plataformas digitales	Un curso de autoaprendizaje
	1.3 Capacitar a la población institucional en materia de protección y tratamiento de datos personales, por medio de un curso de autoaprendizaje.	Comisión Institucional	Asesoría de Comunicación/USEVI/Desarrollo de Recursos Humanos	2025 y en adelante	Plataforma digital	100 % de la población funcionaria capacitada
	1.4 Desarrollar una campaña de concientización sobre los delitos informáticos.	Comisión Institucional	Asesoría de Comunicación	I semestre del 2025	Cápsulas	Una campaña socializada con la población funcionaria
	1.5 Capacitar, actualizar, concientizar de manera permanente a la población funcionaria en diversas temáticas asociadas a la protección y tratamiento de datos personales.	Comisión Institucional	Desarrollo de Recursos Humanos	I semestre de los años 2025, 2026	Charlas, cursos formativos, webinar	Recursos diversos para la capacitación, actualización y concientización a la población funcionaria
2. Inventario institucional para identificar cómo se aplica el tratamiento y protección de los datos personales de las personas usuarias y funcionarias del INA.	2.1 Elaborar un cuestionario para identificar cómo se aplica la protección de los datos personales que se encuentran en medios físicos, digitales (papel, fotos, entre otros) y para valorar el conocimiento del personal funcionario en el tema.	Comisión Institucional	NA	Junio del 2024	Recurso humano/Forms	Un cuestionario institucional
	2.2 Aplicar un cuestionario como herramienta diagnóstica que permita valorar cómo se realiza el tratamiento de datos personales a nivel institucional.	Todas las Unidades Organizativas (Grupos focales)	Comisión Institucional, Asesoría de Comunicación	Junio a julio del 2024	Recurso Humano, cuestionario, plantilla	Un cuestionario institucional
	2.3 Realizar un levantamiento de información de todas las bases de datos existentes que estén en soporte físico o digital y determinar si deben o no atender lo dispuesto por la Ley N° 8968 y su Reglamento.	Todas las Unidades Organizativas (Grupos focales)	NA	II semestre del 2024	Plantilla	Inventario institucional

LÍNEA ESTRATÉGICA	ACTIVIDADES	RESPONSABLES	OTRAS INSTANCIAS INVOLUCRADAS	PLAZOS DE EJECUCIÓN	INSUMOS / RECURSOS	META
3. Análisis de los datos recolectados en el cuestionario institucional	3.1 Aplicar una tabla de clasificación de datos personales de acuerdo a la normativa existente, de acuerdo a las etapas del ciclo de vida del tratamiento de datos personales.	Todas las Unidades Organizativas	NA	I semestre del 2025	Plantilla de clasificación / Recurso Humano	Tabla de clasificación
	3.2 Realizar un análisis de riesgos de acuerdo a la clasificación de los datos personales identificados a nivel institucional.	Todas las Unidades Organizativas	NA	II semestre del 2025	Plantilla de clasificación / Recurso Humano	Tabla de clasificación
	3.3 Establecer un inventario institucional de medidas de seguridad por departamento en materia de protección de datos personales.	Todas las Unidades Organizativas	NA	II semestre del 2025	Plantilla de clasificación / Recurso Humano	Tabla de clasificación
	3.4 Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva.	Todas las Unidades Organizativas	NA	II semestre del 2025	Plantilla de clasificación / Recurso Humano	Medidas de seguridad definidas y en aplicación
4. Implementación de acciones para el adecuado tratamiento de los datos de las personas usuarias y funcionarias a través de mecanismos de seguridad.	4.1. Implementar las medidas de seguridad necesarias para el tratamiento de datos personales de conformidad con el análisis de riesgos.	Todas las Unidades Organizativas	NA	I trimestre del 2026	Recurso Humano/Sistemas cuando corresponda	Medidas de seguridad definidas y en aplicación
	4.2. Revisión de instructivos y procedimientos técnicos en el uso y tratamiento de los datos personales (historial del tratamiento, dudas y quejas de titulares y ejercicio de derechos).	Todas las Unidades Organizativas	NA	I trimestre del 2026	Recurso humano, instructivos, procedimientos	Instructivos y procedimientos revisados y actualizados
	4.3. Crear medidas y procedimientos técnicos que permitan tener un historial de los datos personales durante su tratamiento a fin de cumplir con los protocolos mínimos de actuación.	Todas las Unidades Organizativas	NA	I trimestre del 2026	Recurso humano, instructivos, procedimientos	Medidas y procedimientos definidos e implementados
	4.4. Preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión como parte de la gestión de riesgos. (Art. 35 de la Ley 8968).	Todas las Unidades Organizativas	NA	I trimestre del 2026	Recurso humano, instructivos, procedimientos	Mecanismos de monitoreo implementados
	4.5. Revisar los contratos y convenios suscritos en los Procesos y Unidades.	Todas las Unidades Organizativas	Asesoría Legal	I trimestre del 2026	Recurso humano/Sistemas/Contratos y convenios	100 % de los contratos y convenios revisados y actualizados
	4.6. Revisar la asignación de mecanismos físicos y lógicos aplicados a la información en los sistemas e implementar acciones preventivas	Todas las Unidades Organizativas	NA	De manera trimestral a partir de junio del 2024.	Reportes de sistemas/Recurso humano	Controles de acceso implementados

LÍNEA ESTRATÉGICA	ACTIVIDADES	RESPONSABLES	OTRAS INSTANCIAS INVOLUCRADAS	PLAZOS DE EJECUCIÓN	INSUMOS / RECURSOS	META
	para la protección y tratamiento de los datos de las personas.			*En los casos de renuncias, despido, jubilación, rotación de personal, traslados o permutas, licencias, incapacidades extendidas: se debe realizar de inmediato la restricción o actualización del acceso a sistemas.*		
	4.7. Crear una categoría específica dentro del Service Desk para la gestión de las incidencias asociadas al tratamiento de datos personales.	GTIC y USST	NA	I semestre del 2024	Sistemas institucionales/ Recurso humano	Categoría implementada en Service Desk
	4.8. Revisar la aplicación de la Política de ciberseguridad 2023 y 2027 para vincular las acciones al tratamiento adecuado de los datos personales.	GTIC	NA	I semestre del 2025	Recurso Humano	Política de ciberseguridad implementada al 100 % en las acciones
	4.9. Continuar a nivel institucional con tratamiento a la información en cada una de las áreas a fin de cumplir con la triada de la seguridad de la información: disponibilidad, confidencialidad e integridad, en atención a lo dispuesto en las Normas Técnicas de Gestión y Control de la Tecnología de la Información (NTGCTI) del Micitt.	Todas las Unidades Organizativas	GTIC	2024	GTIC	INA el enfoque de protección y tratamiento de datos personales. Dentro de: Campaña anual de correo de concientización. Reunión de inducción de personas funcionarias de primer ingreso. Revisión de los documentos del SGSI (Sistema de Gestión de Seguridad de la Información): Política, Marco normativo y (*sic*).
	4.10. Realizar el procedimiento para el tratamiento de los datos personales por encargo y velar por el cumplimiento de las reglas relacionadas con el uso de la figura del encargo de datos.	Unidades que manejan datos por encargo	Asesoría Legal	II semestre del 2024	Recurso humano	Procedimientos creados y socializados

LÍNEA ESTRATÉGICA	ACTIVIDADES	RESPONSABLES	OTRAS INSTANCIAS INVOLUCRADAS	PLAZOS DE EJECUCIÓN	INSUMOS / RECURSOS	META
	4.11. Establecer procedimientos para el ejercicio de los derechos de las personas usuarias y funcionarias en materia de protección de datos personales. (revocación, etc.)	Unidad de Servicio al Usuario y Recursos Humanos	Proceso de Servicio al Usuario y staff de Recursos Humanos en cada Unidad Regional	I semestre del 2024	Recurso humano	Procedimientos creados y socializados
	4.12. Revisión de los términos de uso de sistemas y políticas de privacidad (SIL).	Todas las Unidades Organizativas	NA	I semestre del 2024	Recurso Humano	Políticas de seguridad implementadas
	4.13. Creación de procedimientos para la atención de solicitudes de datos personales al INA por entes externos (valorar la vía de excepción).	Todas las Unidades Organizativas	Asesoría Legal	I semestre del 2025	Recurso Humano	Procedimientos creados y socializados
	4.14. Establecer las reglas generales para la protección de los archivos físicos y digitales (tablas de datos, listas, formas, etc.) que contengan datos personales. (SSS–anonimizar–desasociar–minimización) (Ver formato de PRODHOAB).	Comisión Institucional/Archivo Institucional	Unidades Organizativas	I semestre del 2024	Recurso humano	Lineamientos definidos y socializados
5. Política de protección de datos	5.1. Creación de un reglamento institucional para la protección de datos personales (pautas generales en los temas de menores de edad, transferencia de datos (de datos que vienen por Encargo Interno o Externo, referencias de personas con discapacidad (figura garante y/o CONAPDIS), datos biométricos, entre otros)	Comisión Institucional	Asesoría Legal y PROHAB	I trimestre del 2026	Recurso humano	Reglamento institucional
	5.2. Establecer un procedimiento de Control Interno para el cumplimiento del derecho a la privacidad de los datos personales.	Control Interno	Comisión Institucional	I semestre del 2025	Recurso humano / Herramienta de autoevaluación	Procedimiento incluido en la herramienta de autoevaluación
	5.3. Valorar la creación de una persona con el rol de Oficial de Datos Personales.	Gerencia General	Asesoría Legal	I semestre del 2026	Oficio de solicitud	Nombramiento de una persona Oficial de Datos Personales.

Fuente: Oficio N°. ALEA-260-2024

Anexo 3
Conclusiones y Recomendaciones (INFORME ESTADO - AVANCE Plan Institucional para la Protección de Datos Personales del INA 2024-2027)

Conclusiones

En atención a las actividades definidas en el "Plan de acción para la protección y tratamiento de datos personales en el INA 2024-2027", se logró el cumplimiento de la totalidad de las actividades planificadas para el año 2024.

Sin entrar en detalles y por mencionar algunos resultados del "Cuestionario diagnóstico sobre la aplicación de la protección de datos personales en el INA", el cual será utilizado como herramienta de trabajo en el año 2025 para definir las líneas de trabajo prioritarias a nivel institucional, se enuncian algunos de sus resultados:

- Se refleja un alto porcentaje de desconocimiento de la población funcionaria de lo relativo a la materia de protección de datos personales y su cumplimiento, ya que un 83% dice no estar capacitada; un 75% desconoce si se hace transferencia de datos a otras instituciones y un 75% desconoce la normativa.
- En cuanto a tratamiento de datos personales, se detectó el 46% sí realiza tratamiento de datos personales.
- A nivel digital en base de datos estructuradas que se manejan a nivel de red, se tiene infraestructura y procedimientos que aseguran el acceso autorizado; al respecto las personas el 48% indicó que si se cuentan con medidas de seguridad y conocen cuales son, pero un 24% no las conoce y otro 24% indican que, si existen, pero no saben cuáles son.
- Existe un volumen base de datos personales y sistemas, así como la necesidad de actualizar y establecer procedimientos en materia de protección de datos personales, acorde con el cumplimiento de los derechos, principios y medidas de seguridad establecidos en la Ley N°8968 y su reglamento, siendo de especial relevancia cumplir con la definición de los protocolos mínimos de actuación, cuando ello proceda.

Lo indicado anteriormente evidencia la necesidad que existe en la institución de continuar trabajando en el tema, con el fin de acatar lo definido en la normativa nacional y evitar caer a un incumplimiento del plan presentado a la PRODHAB.

En relación a las personas funcionarias que integra el Comité, se concluye lo siguiente:

- Es de agradecer la participación activa de los miembros actuales del Comité, quienes a pesar de las cargas de trabajo, lograron cumplir con las acciones propuestas para este año.
- Se determinó que para el caso de la Asesoría de Desarrollo Social (ADS), se considera que su participación en estas sesiones ya no serían necesaria, a reserva que les sea solicitada información o se les asigne una acción relativa a la protección de datos personales.

- Se informa que la compañera Nancy Granados Peraza, Encargada de la Unidad de Archivo Central Institucional (UACI), estará apoyando al Comité, como subcoordinadora.
- Se detallan las acciones a cumplir en el 2025; sin embargo, podrían ser redireccionadas debido al análisis de las respuestas del cuestionario aplicado a nivel institucional que realizará la UPE, lo cual se solicitará mediante oficio, ya que podrían reflejar acciones prioritarias a cumplir en materia de protección de datos personales.

LINEA ESTRATÉGICA	ACTIVIDADES	PLAZOS DE EJECUCIÓN
1. Capacitación en el tema de protección y tratamiento de datos personales	1.2. Desarrollar un curso de autoaprendizaje en materia de protección y tratamiento de datos personales.	I semestre del 2025
	1.3. Capacitar a la población institucional en materia de protección y tratamiento de datos personales, por medio de un curso de autoaprendizaje.	2025 y en adelante
	1.4. Desarrollar una campaña de concientización sobre los delitos informáticos.	I semestre del 2025
	1.5. Capacitar, actualizar, concientizar de manera permanente a la población funcionaria en diversas temáticas asociadas a la protección y tratamiento de datos personales.	I semestre de los años 2025, 2026
3. Análisis de los datos recolectados en el cuestionario institucional	3.1. Aplicar una tabla de clasificación de datos personales de acuerdo a la normativa existente de acuerdo a las etapas del ciclo de vida del tratamiento de datos personales.	I semestre del 2025
	3.2. Realizar un análisis de riesgos de acuerdo a la clasificación de los datos personales identificados a nivel institucional.	II semestre del 2025
	3.3. Establecer un inventario institucional de medidas de seguridad por departamentos en materia de protección de datos personales.	II semestre del 2025
	3.4. Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva.	II semestre del 2025
4. Implementación de acciones para el adecuado tratamiento de los datos de las personas usuarias y funcionarias a través de mecanismos de seguridad.	4.8. Revisar la aplicación de la Política de ciberseguridad 2023 y 2027 para vincular las acciones al tratamiento adecuado de los datos personales.	II semestre del 2025
	4.13. Creación de procedimientos para la atención de solicitudes de datos personales al INA por entes externos (valorar la vía de excepción)	I semestre del 2025
5. Política de protección de datos	5.2. Establecer un procedimiento de Control Interno para el cumplimiento del derecho a la privacidad de los datos personales.	I semestre del 2025

Adicionalmente, es indispensable continuar con las campañas de información acerca del tema de protección de datos personales, en cumplimiento al inciso b del artículo 32 del Reglamento a la Ley 8968, así como definir un manual de capacitación, actualización y concientización, donde por medio de coordinación con el Proceso de Desarrollo de Recursos Humanos y la Asesoría de Comunicación se realicen charlas, conversatorios con panelistas expertos en la materia, entre otros, a fin de que la población institucional tenga un mayor acercamiento a la temática, siendo de especial relevancia, el conocimiento de las personas funcionarias sobre las obligaciones en materia de derecho de protección de datos personales.

Recomendaciones para la Presidencia Ejecutiva

1- Resulta de vital relevancia, para el cumplimiento de las acciones del plan institucionales correspondientes al 2025, contar con la participación activa de todos y cada uno de los miembros del Comité, a fin de poder coordinar la atención de las diferentes acciones en las dependencias que lo conforman, de manera que se pueda cumplir lo definido en materia de protección de datos personales y que podamos en forma sinérgica cumplir con el plan propuesto.

   A fin de poder contar con una mejor asistencia para el año 2025, se solicita el apoyo de la Presidencia, para que interponga sus buenos oficios de manera que las distintas jefaturas de las dependencias que integran este Comité nombren antes del 17 de enero del 2025, a una persona propietaria y otra suplente, que puede representarle y dar continuidad a las labores asignadas.

2- Solicitar apoyo a la Gerencia General para la publicación de los procedimientos indicados en los puntos 4.10 y 4.11, así como para aquellos documentos normativos que se produzcan posteriormente, producto del trabajo de este Comité.

3- Se requiere que la institución nombre al menos a la figura de Oficial de Seguridad de la Información (mencionado en el punto 4.9 de este documento), así solicitado por la Auditoría Interna en el informe AI-ICI-08-2024 Gestión de Seguridad de la Información, quien podría integrar además el Comité de Protección de Datos, a efecto de coordinar lo relativo a la protección de datos.