# Lineamientos

## para fiscalizar responsables o usuarios de bases de datos

## VERIFICACIONES JURÍDICAS

Este documento contiene los lineamientos generales a tener en cuenta por los inspectores para la fiscalización de las actividades de tratamiento de datos personales. Contiene las bases de fiscalización, constituido por las verificaciones jurídicas y las verificaciones técnicas, que se llevan a cabo al momento de la visita al responsable o usuario de las bases de datos.

| 1. LICITUD DEL TRATAMIENTO - CATEGORÍAS ESPECIALES | | |
|---|---|---|
| Obtiene consentimiento del titular para tratar sus datos personales. | | |
| Los datos se obtienen de fuentes de acceso público irrestricto. | | |
| Los datos se recogen en virtud de funciones propias de poderes del Estado. | | |
| Los datos se recogen en virtud de una obligación legal. | | |
| Los datos recogidos son necesarios para el desarrollo o cumplimiento de una relación científica, profesional o contractual entre el titular de datos y el responsable de tratamiento. | | |
| Los datos son recogidos por entidades financieras y se relacionan con sus operaciones y clientes (Art. 39 de la Ley N° 21.126). | | |
| Los datos recogidos se organizan en un listado de datos básicos autorizados por la ley. | | |
| **LICITUD DEL TRATAMIENTO EN CASO DE DATOS SENSIBLES** | | |
| Datos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. | | |
| Norma que autoriza, si la hubiere, el tratamiento de los datos recogidos. | | |
| **TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES** | | |
| Efectúa tratamiento de datos relativos a antecedentes penales o contravencionales. | | |
| 2. CALIDAD DE LOS DATOS | | |
| Recogen los datos personales con fines determinados. | | |
| Recogen los datos personales con fines explícitos. | | |
| Recogen los datos de manera proporcional con la finalidad del tratamiento. | | |
| Tratan los datos ulteriormente, con finalidad distinta a la de recolección. | | |
| Los datos personales se mantienen exactos y actualizados. | | |
| Establece plazo de guarda y procedimiento de destrucción. | | |
| Suprimen los datos personales inexactos respecto de la finalidad. | | |
| Los datos se mantienen durante más tiempo del necesario respecto de la finalidad. | | |
| Los datos personales están disociados. | | |

| 3. CONSENTIMIENTO |
| --- |
| Obtiene el consentimiento por escrito del afectado para el tratamiento de sus datos personales. |
| Solicita el consentimiento de forma clara e independiente de los demás asuntos. |
| Solicita el consentimiento usando lenguaje claro y sencillo. |
| Informa la finalidad con carácter previo a recabar el consentimiento. |
| Permite y establece mecanismos para retirar el consentimiento. |
| CONSENTIMIENTO DE NIÑOS |
| Recaba el consentimiento de menores con la autorización de sus padres y/o tutores. |
| Recaba el consentimiento teniendo en cuenta la capacidad progresiva del menor. |
| **4. INFORMACIÓN** |
| Facilita al interesado toda la información relativa al tratamiento. |
| La información que se brinda es concisa, transparente e inteligible. |
| La información se facilita en lenguaje claro y sencillo. |
| Facilita información por escrito o por otros medios, incluidos los electrónicos. |
| La facilita verbalmente, previa acreditación de identidad del solicitante. |
| **5. SEGURIDAD Y CONFIDENCIALIDAD** |
| Implementa medidas técnicas de seguridad para evitar el tratamiento no autorizado o ilícito de los datos. |
| Implementa medidas de seguridad para evitar la pérdida, destrucción o daño accidental. |
| Implementa medidas organizativas de seguridad. |
| Designa responsable para la aplicación de la normativa en la organización. |
| Suscribe convenios de confidencialidad con las personas que intervienen en cualquier fase de tratamiento de datos personales. |
| El deber de confidencialidad subsiste aun después de finalizada la relación con el titular de la base de datos. |
| En la organización se encuentra designado un responsable o delegado de protección de datos. |
| Realizan evaluaciones de impacto en materia de datos personales para identificar y gestionar los riesgos de los proyectos y prácticas de la organización. |
| Implementa un sistema de notificaciones ante los titulares de datos y la Agencia de Acceso a la Información Pública en caso de incidentes de seguridad. |
| Se implementan medidas de privacidad por defecto. |
| Se implementan medidas de privacidad por diseño. |
| **6. CESION DE DATOS** |
| Verifica el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario. |
| Los datos personales son cedidos con el consentimiento previo del titular de los datos. |
| El responsable le informa al titular que su consentimiento es revocable y toma medidas para hacer efectiva la opción de revocación. |

| |
|---|
| La cesión está autorizada por una ley. Especificar cuál. |
| La cesión se realiza entre dependencias del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias. |
| El cesionario recibe los datos de fuentes de acceso público irrestricto. |
| El cesionario es un organismo público que recibe los datos para el ejercicio de funciones propias de los poderes del Estado. |
| El cesionario recibe los datos en virtud de una obligación legal. |
| El cesionario recibe los datos con motivo de una relación contractual, científica o profesional, y la cesión es necesaria para el cumplimiento de dicha relación. |
| El cesionario es una entidad crediticia que recibe informaciones de sus clientes conforme al Art. 39 de la Ley N° 21.526. |
| **7. TRANSFERENCIA INTERNACIONAL DE DATOS** |
| Realiza transferencias a países u organizaciones internacionales declarados de nivel adecuado por la Agencia de Acceso a la Información Pública. |
| La transferencia se realiza amparada en la existencia de un contrato que incorpora garantías de protección de los datos personales. |
| La transferencia se realiza amparada en la existencia de normas corporativas vinculantes que incorporan garantías de protección de los datos personales. |
| La transferencia se realiza en el marco de la colaboración judicial internacional. |
| La transferencia se realiza en el marco de un tratado o convenio internacional que incorpora garantías de protección de los datos personales. |
| La transferencia se realiza en el marco de la cooperación entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. |
| Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los titulares. |
| Se dispone del consentimiento explícito del titular de datos y se le ha informado de los posibles riesgos de la transferencia. |
| **8. PRESTACIÓN DE SERVICIOS DE INFORMACIÓN CREDITICIA** |
| Evalúa la solvencia económico-financiera de los afectados con respeto de los plazos (5 años, que se reducirá a 2 años cuando el deudor cancele o de otro modo extinga la obligación, haciendo constar dicha circunstancia). |
| **9. PUBLICIDAD** |
| Establece perfiles determinados con fines promocionales, comerciales o publicitarios. |
| Otorga el retiro o bloqueo a solicitud del titular. |
| **10. DERECHOS DEL TITULAR DE DATOS** |
| Facilita al interesado el ejercicio de sus derechos -acceso, actualización, rectificación, supresión- por distintos medios. |

| |
|---|
| Facilita gratuitamente el ejercicio de derechos. |
| Responde a los reclamos de acceso en plazo (10 días corridos desde la notificación fehaciente). |
| Responde a los reclamos de actualización, rectificación y supresión (5 días hábiles desde la notificación fehaciente). |
| Informa al titular acerca del derecho de presentar reclamo ante la Autoridad de Control. |

# LINEAMIENTOS PARA LAS VERIFICACIONES TÉCNICAS

| 1. RECOLECCIÓN DE DATOS |
|---|
| Permite el ingreso completo de los datos requeridos (validación de formato). |
| Indica en forma clara y concreta el tipo de información a ingresar y el formato de la misma. |
| Verifica la exactitud del dato ingresado (en caso de que el tipo de registro lo permita). |
| Cifra la comunicación cliente-servidor durante la recolección (https). |
| Utiliza certificados digitales seguros y validados por entidades autorizadas (CA). |
| Cifra la comunicación durante el traslado desde el servidor de aplicación hacia la base de datos. |
| **2. CONTROL DE ACCESO** |
| Dispone de un inventario de activos informáticos actualizado, define propietarios y los notifica. |
| Identifica inequívocamente a cada usuario, registra accesos y actividad. |
| Establece una política de contraseñas seguras. |
| Limita el acceso de los usuarios a los datos personales o establece un seguimiento de su actividad. |
| Evita el uso de usuarios genéricos. |
| Realiza control de acceso físico al centro de datos. |
| **3. CONTROL DE CAMBIOS** |
| Verifica los cambios a realizar en entornos productivos. |
| Dispone de un registro de las verificaciones y/o pruebas realizadas. |
| Dispone de un procedimiento de control de cambios en entornos productivos. |
| **4. RESPALDO Y RECUPERACIÓN** |
| Dispone de un plan de contingencia, detallando el procedimiento de resguardo de información y recuperación. |
| Registra pruebas de recuperación realizadas. |
| Dispone de un inventario que identifique las copias de seguridad, su ubicación y el medio en el que se almacenan. |
| Cifra las copias de resguardo utilizando herramientas seguras. |
| Elimina en forma segura la información recuperada durante las pruebas. |
| Dispone de medidas de protección contra incendios o inundaciones en el sitio de almacenamiento de los medios físicos que contienen las copias de resguardo. |
| Almacena las copias de resguardo en una locación física diferente a la del sistema productivo. |

| 5. GESTIÓN DE VULNERABILIDADES |
| --- |
| Documenta las medidas de seguridad adoptadas para los sistemas de información. |
| Aplica segmentación de roles y perfiles, gestión de mensajes de error. |
| Implementa reglas y controles de seguridad en los servidores conectados a una red externa. |
| Implementa controles para la prevención de virus informáticos en los servidores. |
| Actualiza en forma periódica el software de los servidores. |
| Establece una persona responsable del cumplimiento de las medidas de seguridad. |
| Dispone de un registro que permita realizar un seguimiento ante eventos o acciones de un posible incidente (sistema de logs). |
| Sincroniza los servidores con un servidor de horario público. |
| Dispone de un sistema de gestión de incidentes. |
| Aplica filtros de inyección de código en bases de datos y aplicaciones. |
| Implementa controles para la detección de intrusiones. |
| Realiza auditorías externas a fin de evaluar la seguridad de los sistemas internos. |
| **6. DESTRUCCIÓN DE LA INFORMACIÓN** |
| Dispone de un procedimiento de destrucción de datos. |
| Implementa un proceso de destrucción físico o lógico de la información que asegure el borrado total. |
| Establece una persona autorizada para la destrucción y documenta su autorización. |
| **7. GESTIÓN DE INCIDENTES** |
| Elabora un procedimiento de gestión ante incidentes de seguridad. |
| Establece una persona responsable de la comunicación. |

República Argentina - Poder Ejecutivo Nacional
2020 - Año del General Manuel Belgrano

**Hoja Adicional de Firmas**
**Informe gráfico**

**Número:** IF-2020-91223642-APN-DNPDP#AAIP

CIUDAD DE BUENOS AIRES
Martes 29 de Diciembre de 2020

**Referencia:** ANEXO II Lineamientos para fiscalizar responsables o usuarios de bases de datos

---

El documento fue importado por el sistema GEDO con un total de 6 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2020.12.29 13:50:17 -03:00

Eduardo Hernán Cimato
Director Nacional
Dirección Nacional de Protección de Datos Personales
Agencia de Acceso a la Información Pública

Digitally signed by Gestion Documental Electronica
Date: 2020.12.29 13:50:18 -03:00