ECIJA
MÉXICO

Política de Protección de Datos Personales

Descripción de la metodología

ETAPA 1
Inventario de datos personales y sistemas de tratamientos

Con el objeto de revisar los procesos de tratamientos de datos, **ECIJA** procede a la identificación del ciclo de vida de éstos. Para ello, **ECIJA** revisa y evalúa las acciones y tareas habituales llevadas a cabo en los distintos procesos de las áreas, departamento o unidades de negocio del cliente. Esta identificación se realiza a través de la revisión documental existente, así como la aplicación de cuestionarios y entrevistas al personal designado o responsables de las áreas, departamentos o unidades de negocio correspondientes.

Con la información anterior, se procede a la elaboración de un mapa de tratamientos y dependencias, que permita la identificación de la siguiente información:

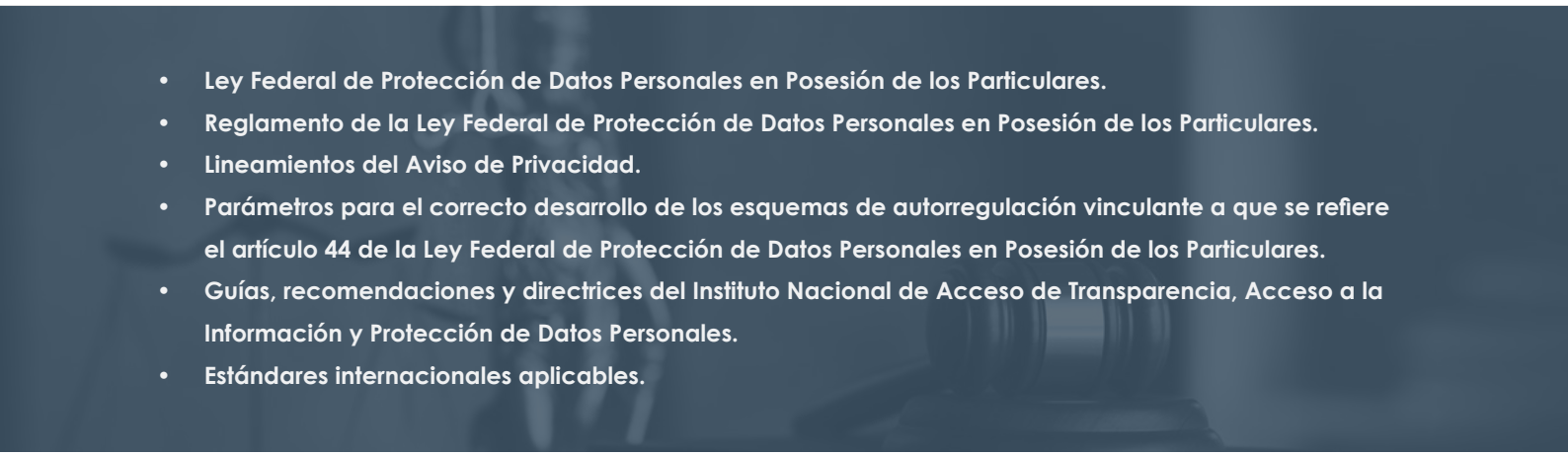
- Categorías de titulares.
- Categorías de datos personales.
- Fines del tratamiento.
- Transferencias o remisiones de datos personales.
- Uso de tecnologías para la obtención automática de datos personales.
- Sistemas o medios de almacenamiento y medidas de seguridad aplicadas.
- Plazos y procesos para el bloqueo y supresión de los datos personales.
- Personal, áreas, departamentos, unidades de negocio y/o proveedores involucrados en el procesamiento de los datos personales.

ETAPA 2
Diagnóstico de cumplimiento y nivel de riesgo

La fase indicada se aborda llevando a cabo el análisis de todos los aspectos necesarios para garantizar el cumplimiento de la normatividad aplicable, tanto desde el punto de vista jurídico, organizacional y en relación con la adopción de las medidas de seguridad necesarias.

2.1
Evaluación de aspectos jurídicos

En primer lugar, se procede a la identificación de las obligaciones legales aplicables en materia de tratamiento de datos personales, lo que permitirá la definición del marco normativo que servirá de base para el correcto desarrollo del proyecto, teniéndose en cuenta principalmente:



- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares.**
- **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.**
- **Lineamientos del Aviso de Privacidad.**
- **Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.**
- **Guías, recomendaciones y directrices del Instituto Nacional de Acceso de Transparencia, Acceso a la Información y Protección de Datos Personales.**
- **Estándares internacionales aplicables.**

Igualmente, se procede a la identificación de las mejores prácticas en el sector de la industria que esté involucrado en el tratamiento de los datos personales y el establecimiento de controles encaminados a garantizar el cumplimiento de la normativa, reduciendo los riesgos asociados con su tratamiento.

2.2
Evaluación de aspectos organizacionales

En segundo lugar, se procede con la identificación de los mecanismos requeridos para dar cumplimiento a las obligaciones legales en materia de protección de datos personales durante todos los procesos que componen el ciclo de vida de los datos personales. Principalmente, se analiza el cumplimiento de los siguientes principios:

Licitud	Confirmar que el tratamiento de los datos personales que se llevaba a cabo de encuentre legalmente permitido.

Información	Puesta a disposición de un aviso de privacidad previo a la obtención de los datos personales, teniendo en cuenta los canales de obtención de los datos personales y contacto con los titulares (ej.: formato físico, electrónico, sonoro, visual, etc.
Consentimiento	Obtención del consentimiento del titular para el tratamiento de sus datos personales conforme a los términos del aviso de privacidad, mediante casillas de marcado en formas físicos o electrónicos, firma autógrafa o electrónico, grabaciones, etc.
Finalidad	Implementación de mecanismos que permitan al titular negar el tratamiento de sus datos para finalidades secundarias, a través de casillas de marcado o el establecimiento de plazos de espera.
Proporcionalidad	Verificar la necesidad, idoneidad y relevancia de los datos recabados, así como el período de su tratamiento y conservación, contando con procesos de bloqueo y supresión de los datos personales.
Calidad	Establecimiento de procesos que permitan garantizar la exactitud de los datos personales recabados y su actualización.
Lealtad	Tratar los datos para fines legalmente permitidos, sin incurrir en prácticas engañosas o fraudulentas para su obtención y garantizar la confidencialidad de los datos.
Responsabilidad	Implementación de medidas para garantizar el uso adecuado de los datos personales al interior de la organización, mediante la implementación de políticas internas, protocolos de actuación, catálogos de funciones, etc.

2.3 Evaluación de aspectos seguridad

En tercer lugar, y en caso de ser requerido por el cliente, se procede con la identificación de los riesgos asociados a los datos personales, así como al resto de activos involucrados en su tratamiento (ej.: personal, hardware, software, redes, telecomunicaciones, etc.), para con base en ello determinar los controles de seguridad que pueden mitigar los incidentes.

En este sentido, **ECIJA** procede a identificar de manera individualizada y específica los siguientes aspectos:

- Nivel de riesgo a los que están sujetos los datos personales.
- Amenazas y vulnerabilidades de seguridad.
- Escenarios de vulneración y sus consecuencias.

Una vez identificados los activos y procesos relacionados a los datos personales, así como las amenazas, vulnerabilidades y escenarios de incidentes relacionados, se puede proceder al análisis de brecha de las medidas de seguridad, el cual consiste en identificar las medidas existentes, las implementadas correctamente, las faltantes y si existen nuevas medidas que puedan remplazar a las ya existentes e implementadas.

2.4
Reporte de hallazgos relevantes

Con base en el resultado de las evaluaciones anteriores, **ECIJA** emite un reporte con los hallazgos y riesgos detectados, así como las acciones recomendadas a seguir para garantizar el pleno cumplimiento a la normatividad aplicable, tanto desde el punto de vista jurídico y organizacional, como desde el punto de vista de seguridad de la información.

ETAPA 3
Diseño de la Política de Protección de Datos Personales

En esta fase se procede al diseño o adaptación de la Política, según la medidas correctivas y propuestas de mejora identificadas en el reporte de hallazgos relevantes, como:

- Avisos de privacidad, política de cookies.
- Mecanismos de obtención del consentimiento integrando requisitos legales en el diseño de la infraestructura atendiendo al criterio de privacy by design.
- Cláusulas o acuerdos de protección de datos personales con empleados, clientes, proveedores y terceros.
- Catálogo de funciones y obligaciones del personal, área, departamento o unidad de negocio que trata los datos personales.
- Políticas internas para garantizar el uso adecuado y legítimo de los datos personales.
- Esquemas de autorregulación vinculante.
- Designación, nombramiento y funcionamiento del delegado, departamento y/o comité de datos personales.
- Procedimiento para la atención de solicitudes de derechos de los titulares.
- Procedimiento para el bloqueo y supresión de los datos.
- Procedimiento Privacy by Design.
- Programa de auditoría interna y externa.
- Programa de concientización y capacitación al personal.
- Sistema de Gestión de Seguridad de Datos Personales

ETAPA 4
Implementación de la Política de Protección de Datos Personales

Con el objetivo facilitar y fomentar la implantación efectiva de las recomendaciones propuestas, **ECIJA** elaborará una hoja de ruta en la que se recogerá de cada recomendación y acción correctiva lo siguiente:

- Nivel de dificultad y plazo para llevarla a cabo
- Departamento afectado por esa recomendación
- Riesgos asociados a la no adopción de las medidas propuestas

Para garantizar la adecuada instrumentación y cumplimiento de la Política, resulta necesario llevar a cabo acciones de concientización y capacitación del personal involucrado en el tratamiento de los datos personales, con apartados especializados para el delegado, departamento y/o comité de datos personales, y en su caso, del comité de seguridad. La Política establecerá los lineamientos del programa de concientización y capacitación de la empresa.

ETAPA 5
Revisiones y auditorías

Es necesario evaluar y medir los resultados de la Política, a fin de verificar su cumplimiento, la eficacia y eficiencia del mismo. Esto se logra a través del monitoreo cotidiano a nivel interno y la realización de auditorías internas. Asimismo, se recomienda realizar una auditoría externa por parte de **ECIJA** con el fin de revisar los resultados de estos monitoreos y auditorías para identificar circunstancias que requieran de especial atención o cualquier desviación significativa sobre la Política. El procedimiento a seguir y la periodicidad con la cual deben llevarse a cabo estas acciones se detalla en la Política.

ETAPA 6
Actualización y mejora continua

En esta fase, se adoptan las medidas correctivas y preventivas en función de los resultados de las revisiones y verificaciones efectuadas, para lograr la mejora continua de la Política. Por ejemplo, en caso de identificarse cualquier cambio en el contexto de su operación u organización que impacte en el tratamiento de los datos personales, se deberá llevar a cabo la actualización de los mecanismos, lineamientos, procesos y procedimientos que integran la Política.

ECIJA

ECIJA

MÉXICO

Torre Mural, Av. Insurgentes Sur 1605 piso 27, Col. San José Insurgentes, C.P. 03900. Ciudad de México, México Tel: (+52) 55 5662 6840 www.ecija.mx