COMISION ESTATAL DE
DERECHOS HUMANOS
VERACRUZ

GUÍA PARA LA ELIMINACIÓN DE INFORMACIÓN

QUE CONTIENE DATOS PERSONALES Y DOCUMENTOS DE ARCHIVO ELECTRÓNICOS

Presentación

La destrucción y borrado a través de un proceso seguro, es un tema de vital importancia para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular para garantizar el derecho a la protección de los datos personales de las personas usuarias. La Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz (en adelante Ley 316) desarrolla una serie de principios y deberes que establecen obligaciones concretas para quienes sean responsables del tratamiento de datos personales, a fin de crear condiciones para su protección, evitar manejos indebidos, y permitir que las personas ejerzan su derecho a la autodeterminación informativa.

Entre estos principios, destaca el de *calidad*, el cual establece que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, completos, pertinentes, actualizados y correctos. Asimismo, señala que cuando los datos personales hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron, deben ser eliminados de oficio, con independencia de que la persona titular de los datos personales ejerza su derecho de cancelación.

Por otra parte, los deberes de *confidencialidad y seguridad* establecen la obligación de implementar las medidas de seguridad físicas, técnicas y administrativas necesarias para garantizar la confidencialidad de dicha información y protegerla de cualquier uso o acceso no autorizado, durante todo su ciclo de vida, incluyendo la supresión de estos. Bajo estas premisas, los sujetos obligados tienen el deber de analizar los medios más eficaces que conviene implementar para llevar a cabo procesos de borrado seguro de la información que ya cumplió sus plazos de conservación documental.

En cumplimiento a estas obligaciones y de conformidad con las políticas para el tratamiento y protección de los datos personales que forman parte del Sistema de Gestión de Seguridad, así como los Instrumentos de Archivo vigentes en esta Comisión, se emite la presente guía que tiene por objeto armonizar el procedimiento que las áreas administrativas que conforman la Comisión Estatal de Derechos Humanos (en adelante la CEDHV) deben seguir para garantizar el ciclo de vida de los datos personales, especialmente en lo que concierne a la etapa de supresión, así como la eliminación de documentos de archivo electrónicos que ya cumplieron con su finalidad y los plazos de conservación documental.

Marco Jurídico

El ciclo de vida de los datos personales es el periodo durante el cual el responsable hace uso de ellos, que va desde su recopilación, uso, hasta su supresión. De acuerdo con el artículo 3 fracción XXX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el término *supresión*, se refiere a la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas.

El artículo 26 de la Ley 316, señala que los responsables deberán establecer y documentar los procedimientos que lleven a cabo para la conservación y, en su caso, bloqueo y supresión de los datos personales, considerando los periodos de conservación, así como implementar mecanismos que les permitan cumplirlos y realizar revisiones periódicas sobre la necesidad de conservar algunos de ellos con fines estadísticos.

En ese sentido, la etapa de supresión de la información que contiene datos personales debe estar armonizada a los periodos de conservación establecidos en el Catálogo de Disposición Documental (CADIDO), conforme a las series que le correspondan a cada sistema de datos personales, puesto que están vinculados al ejercicio de las funciones, atribuciones o competencias que le corresponden a cada área.

La misma Ley 316, dice que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable, a través del área encargada de la información, deberá crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales; es decir, desde su obtención hasta su supresión.

Asimismo, el punto 7 de las Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de los Datos Personales en la CEDHV menciona que la supresión de datos personales o baja de los mismos atenderá a los procesos establecidos por la Unidad de Archivos de conformidad con la normatividad que le resulte aplicable.

Al respecto, es preciso mencionar que, si bien históricamente los archivos han sido asociados a documentos físicos, el artículo 4 fracción III de la Ley General de Archivos, define a estos como el conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones, con independencia del tipo de soporte, espacio o lugar en el que se encuentren, comprendiendo entre ellos a los archivos físicos y electrónicos. En el entendido de que los documentos electrónicos también contienen evidencia del ejercicio de sus atribuciones, por lo que forman parte de su actuación institucional.

En concordancia, el CADIDO de los Instrumentos de Archivo de la CEDHV, señala que los plazos que se establecen en él se aplican a todos los expedientes integrados por este Organismo, sin importar el soporte en que se encuentren y que su valoración se realizará con plena equivalencia a los expedientes de las series documentales, que le correspondan.

Por ello, los procesos de baja documental comprenden la destrucción de archivos tanto en su formato físico, como automatizado (electrónicos, sonoros, gráficos, etc.) incluyendo a la información que

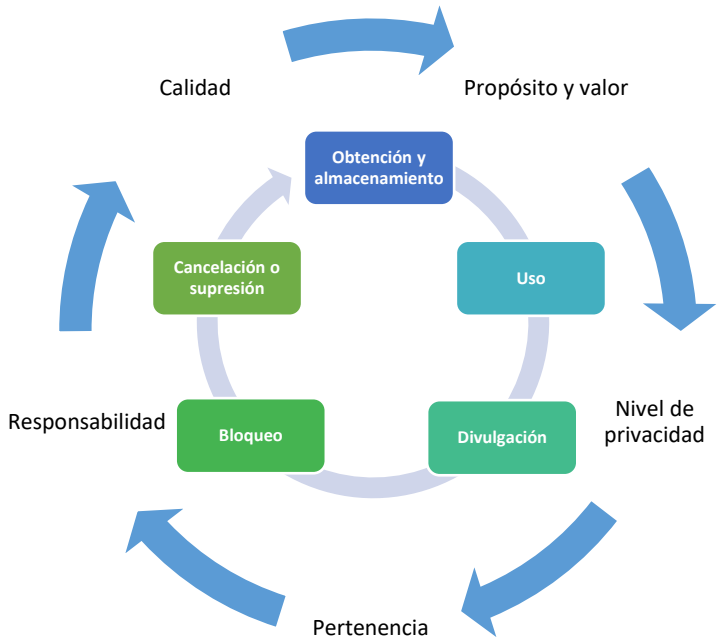
contiene datos personales. Dichos procesos deben realizarse de conformidad con el procedimiento establecido en los Instrumentos de Archivo vigentes en la Comisión Estatal.

I. Aspectos para tomar en cuenta

1. El Ciclo de vida de los datos personales

El Sistema de Gestión de Seguridad para la protección de los datos personales, debe contemplar una política de gestión de datos personales que fije los lineamientos de los medios a través de los cuales se recaban los datos, que identifique los procesos de la organización que los utilizan, con quién se comparten y en qué momento y por qué medios se deben suprimir.

Los datos personales poseen un ciclo de vida, y asociado a este, se les reconocen propiedades que van cambiando a lo largo del ciclo, entre las principales se encuentran las siguientes:



Fuente: Elaboración propia

2. Categoría de datos

Según su riesgo inherente, existen tres categorías de sistemas de datos personales que deben considerarse para llevar a cabo un proceso de destrucción, los cuales nos guiarán para determinar el tipo de borrado que se debe aplicar:

- Nivel Estándar: Considera información general concerniente a una persona, por ejemplo, datos de identificación y contacto, datos laborales y académicos, estado civil.
- Nivel Sensible: Esta categoría contempla los datos que permiten conocer la ubicación física de una persona, tales como la dirección física e información relativa al tránsito de las

personas dentro y fuera del país. También aquellos que permitan inferir el patrimonio de una persona, los datos de autentificación (contraseñas, huellas, información biométrica, etc.); datos jurídicos como antecedentes penales y datos sensibles que afecten la esfera más íntima de su titular.

- Nivel Especial: Considera a datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización pueden causar daño directo a sus titulares; ejemplo, códigos de seguridad o información adicional de tarjetas bancarias.

3. Medios de almacenamiento o soportes

Para definir los métodos de borrado, es necesario establecer la naturaleza de los activos[1] y los documentos de archivo que los integran; es decir, si los datos personales y/o información se encuentran en un medio de almacenamiento físico o un medio de almacenamiento electrónico o automatizado.

- Medios de almacenamiento físicos: Son todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo, los expedientes almacenados en un archivero.
- Medios de almacenamiento electrónico o automatizado: Son todo recurso al que se puede acceder sólo mediante el uso de un equipo de cómputo que procese su contenido para examinar, modificar o almacenar información o los datos personales. Podemos considerar entre estos medios tanto los propios del equipo de cómputo como los portátiles, también podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea. Por ejemplo: memorias USB, CD, almacenamiento en la nube, disco duro, equipos de cómputo.

4. Características de un borrado seguro

Existen técnicas de borrado seguro, que buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos. De acuerdo a estándares internacionales en la materia, las características que deben cumplir un borrado o destrucción segura son:

- Irreversibilidad: Se debe garantizar que no existe un proceso que permita recuperar la información.
- Seguridad y confidencialidad: Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.
- Favorable al medio ambiente: El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente.

[1] Activos: Las bases de datos, sistemas o expedientes que contengan datos personales, recabados o en posesión de la CEDHV con motivo de sus atribuciones.

5. ¿Cuáles son los beneficios de un borrado seguro?

- ✓ Eliminar adecuadamente los medios de almacenamiento en desuso representa una medida de seguridad efectiva para minimizar las fugas o el mal uso de los datos personales y/o información por parte de una persona mal intencionada, o no autorizada.
- ✓ Se optimizan los espacios y los procesos, en particular con la eliminación periódica de los archivos que ya cumplieron su vigencia documental.
- ✓ Se previenen las afectaciones económicas y de imagen debido a multas, compensación de daños y pérdida de información de titulares.

6. Métodos de borrado seguro

A continuación, se muestran opciones de borrado seguro:

<table>
<tr><th colspan="4">Métodos para el Borrado Seguro de los Datos Personales</th></tr>
<tr><th colspan="2">Métodos físicos</th><th colspan="2">Métodos Lógicos</th></tr>
<tr><td colspan="2">Se basan en la destrucción de los medios de almacenamiento</td><td colspan="2">Se basan en la limpieza de los datos almacenamos</td></tr>
<tr><td>Destrucción de los medios del almacenamiento físicos
Trituración
Incineración
Químicos</td><td>Destrucción de los medios de almacenamiento electrónico
Desintegración
Trituración
Abrasión
Fundición</td><td>Desmagnetización: Exposición de los dispositivos de almacenamiento a un campo magnético.</td><td>Sobre escritura: Escribir información nueva en la superficie de almacenamiento. Tiene como ventaja la reutilización de las herramientas.</td></tr>
</table>

7. Documentos de archivo electrónicos

Los documentos de archivo son el registro material que da testimonio de la actividad del Sujeto Obligado en el ejercicio de sus facultades, competencias o funciones, con independencia de su soporte.

Para llevar un control de los documentos de archivo electrónicos, se deberán considerar, qué documentos o bases de datos de formato electrónico se consideran documentos de archivo. Éstos, deberán relacionarse en el inventario general y deberán seguir la lógica de identificación, clasificación, organización y conservación archivística que el resto de los documentos de formato físico.

El Diccionario de Archivos emitido por el INAI retoma la definición de documento de archivo electrónico que la Ley Federal de Archivos abrogada, señalaba en su artículo 4 fracción XXI; un documento electrónico es aquel que almacena información en un medio que precisa de un dispositivo electrónico para su lectura. Por otra parte, los lineamientos derivados de esta Ley definían al documento de archivo electrónico como: Al que registra un acto administrativo, jurídico, fiscal o contable, creado, recibido, manejado y usado en el ejercicio de las facultades y actividades de la

dependencia o entidad de la Administración Pública Federal que precisa de un dispositivo electrónico para su registro, almacenamiento, acceso, lectura, impresión, transmisión, respaldo y preservación.

Según lo anterior, se puede entender que un documento de archivo electrónico es aquel que requiere de dispositivos para su lectura o visualización; es decir, una pantalla y equipos de audio o video. Pueden estar registrados en cintas magnéticas, discos ópticos, o casetes de video. Pero también puede estar elaborado digitalmente mediante un leguaje binario que requiere de un equipo, así como un software de arranque y un software para su acceso.

Los documentos de archivo electrónicos pueden ser analógicos o digitales, pero un documento de archivo digital no puede ser equivalente a un documento de archivo electrónico.

Una aproximación a una definición de documento de archivo digital es aquel que es representado por secuencias de valores numéricos diferenciados llamados bits, que conforme a un código o convención preestablecido pueden representar datos, precisa de software y hardware para su elaboración, visualización y representación.

Asimismo, una aproximación a la definición de documento de archivo electrónico en formato analógico: es aquel documento de archivo cuya información es expresada mediante señales electrónicas continuas semejantes o análogas y transportada mediante un conductor eléctrico que requiere de un equipo electrónico para su inteligibilidad.

Con base en lo anterior, un documento de archivo digital se distingue por la codificación, la descodificación de bits o cadenas de bits. Algunos ejemplos de documentos de archivo digital son: los que cuentan con firma electrónica, CFDI, facturas, trámites o gestiones de las personas realizados mediante plataformas de internet, o aquellos que se encuentran digitalizados, (como las copias de respaldo de las solicitudes de intervención que se almacenan en el Sistema de Control de Gestión).

En el caso de los documentos electrónicos generados por las áreas para el cumplimiento de las funciones asignadas que no poseen firmas o sellos de autenticación, como son archivos de Word (tarjetas informativas, reportes de expedientes, listas, etc.), archivos de Excel, etc., que se guardan como borradores; éstos se considerarán documentos de comprobación administrativa inmediata, y seguirán el proceso de baja documental que establezca la Coordinación de Archivos.

No obstante, cuando se trate de documentos que forman parte de un expediente en trámite, se sugiere conservarlos hasta la conclusión de este o su turno a otra área administrativa, a fin de mantener un respaldo de las actuaciones que lo conforman en tanto no se digitalice en el Sistema de Control de Gestión.

II. Recomendaciones para la conservación, bloqueo y supresión de datos personales

Como se mencionó con anterioridad, la etapa de supresión de datos personales debe considerar previamente el cumplimiento de otras dos, que son la conservación y el bloqueo.

Conservación. El momento indicado para eliminar los datos personales depende del plazo de conservación, el cual se fija a partir de las disposiciones legales aplicables en la materia de que se

trate; los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y el periodo de bloqueo, por lo que forzosamente debe coincidir con los plazos establecidos en el CADIDO que corresponda.

El plazo de conservación de los datos personales atenderá a lo siguiente:

1. El tiempo requerido para llevar a cabo las finalidades del tratamiento (fijado en el sistema de datos correspondiente), por lo que puede corresponder con el periodo de trámite.
2. El periodo de bloqueo (supone plazo adicional al necesario para el cumplimiento de las finalidades, su duración se establece tomando en cuenta el tiempo que sea necesario conservarlos para deslindar posibles responsabilidades derivadas de la relación entre responsables y titulares), puede ser coincidente con el periodo de concentración, o de acuerdo con la procedencia del ejercicio del derecho de Cancelación.
3. Los plazos legales, administrativos, contables, fiscales, jurídicos o históricos aplicables, (establecidos en los instrumentos de archivo), pueden ser coincidentes con el periodo total de conservación.

Para la conservación de la información que contiene datos personales ya sea que se encuentre en formato físico o automatizado, se deberán seguir los lineamientos que establezca la Coordinación de Archivos para el manejo de archivo de trámite y/o concentración conforme les sea aplicable.

Bloqueo. El bloqueo es la etapa intermedia antes de llegar a la supresión de datos personales. Implica la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de la relación establecida entre el responsable y la persona titular de los datos personales.

No obstante, puede variar en los casos en que sea procedente una solicitud para el ejercicio del derecho de Cancelación. En este caso, la cancelación da lugar al bloqueo de los datos personales, el cual iniciará a partir de que éste se declare procedente en términos de la ley aplicable. Por lo anterior, el bloqueo de datos personales puede obedecer a dos procedimientos:

a) Por la procedencia de una solicitud de Acceso, Rectificación, Cancelación u Oposición (ARCO), en la que se ejercite el derecho de cancelación.
b) Porque los datos cumplieron la finalidad para la cual fueron recabados.

Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación o supresión en términos de la normatividad.

Supresión. La supresión consiste en la eliminación, borrado o cancelación de los datos personales. Procede cuando de conformidad con el Sistema de Datos del que forman parte y los instrumentos de control archivístico, éstos hayan cumplido con el plazo de conservación otorgado. Es decir, transcurrido este tiempo, se considera que los datos han cumplido la finalidad o finalidades para las cuales fueron recabadas y por tanto se puede proceder a su supresión de conformidad con el procedimiento de borrado seguro que se sugiera.

La etapa de supresión debe ser coincidente con el cumplimiento del plazo de conservación que se establezca en el CADIDO.

III. Directrices para la conservación, supresión (cancelación, eliminación o borrado) de datos personales y baja de documentos de archivo electrónicos.

Los documentos de archivos electrónicos producidos o recibidos por las áreas, se consideran parte del archivo, ya sea que contengan o no datos personales, por lo que se encuentran sujetos a los procesos de conservación y resguardo establecidos en los Instrumentos de Archivo de la Comisión Estatal. El artículo 20 de la Ley General de Archivos establece que todos los documentos de archivo en posesión del Sujeto Obligado forman parte del Sistema Institucional.

El plazo de conservación es la suma del tiempo que deben resguardarse los documentos de archivo tanto en archivo de trámite como en concentración, para posteriormente pasar a su destino final, ya sea de baja documental o de conservación en archivo histórico.

Una vez que la información ha cumplido con este plazo (si no cuenta con valores históricos), procede su baja documental y tratándose de aquella que contiene datos personales, procede la supresión. Lo que se traduce en la destrucción de los documentos de archivo tanto de soportes físicos como automatizados.

Para llegar a la baja documental y/o supresión de datos personales, se deben considerar las etapas siguientes:

1. Etapa de Conservación. La conservación de la información se realizará conforme las disposiciones que establezcan los Instrumentos de Archivo de la CEDHV, con independencia del tipo de soporte en que se encuentren (físico o automatizado) y que contenga o no, datos personales. Puede corresponder al periodo de archivo de trámite y concentración.

a) Archivo de trámite

Hace referencia a la unidad responsable de administración de documentos de uso cotidiano y necesario para el ejercicio de las atribuciones de una unidad administrativa. Documentos de archivo que permanecen en el área hasta su transferencia primaria.

b) Archivo de concentración

Se refiere a la unidad responsable de administración de documentos cuya consulta es esporádica y que permanecen en ella hasta su transferencia secundaria o baja documental.

Documentos que, al concluir su etapa de trámite son transferidos de manera primaria al archivo para ser resguardados. Permanecen en conservación hasta su transferencia secundaria o baja documental.

2. **Etapa de bloqueo.** (Solo aplicable a la información que contiene datos personales). Los responsables establecerán el periodo que conformará la etapa de bloqueo, dependiendo de sus plazos de conservación y la legislación aplicable. Puede coincidir con el periodo de archivo de trámite y/o concentración.

a) Disociación: Tratándose de archivos que contienen datos personales, coincidente con el periodo de bloqueo, el responsable deberá identificar si los datos aun cuando hayan cumplido sus finalidades y su plazo de conservación, son susceptibles de conservarse con fines estadísticos. De ser así, deberá llevar a cabo un procedimiento de disociación.

Disociación, se refiere al procedimiento de separación de los nombres o datos de identificación de las personas a las que hacen referencia, de forma tal que no sea posible identificar a su titular, es decir, a quien pertenecen, ni permitir por su estructura, contenido o grado de segregación, identificarlo.

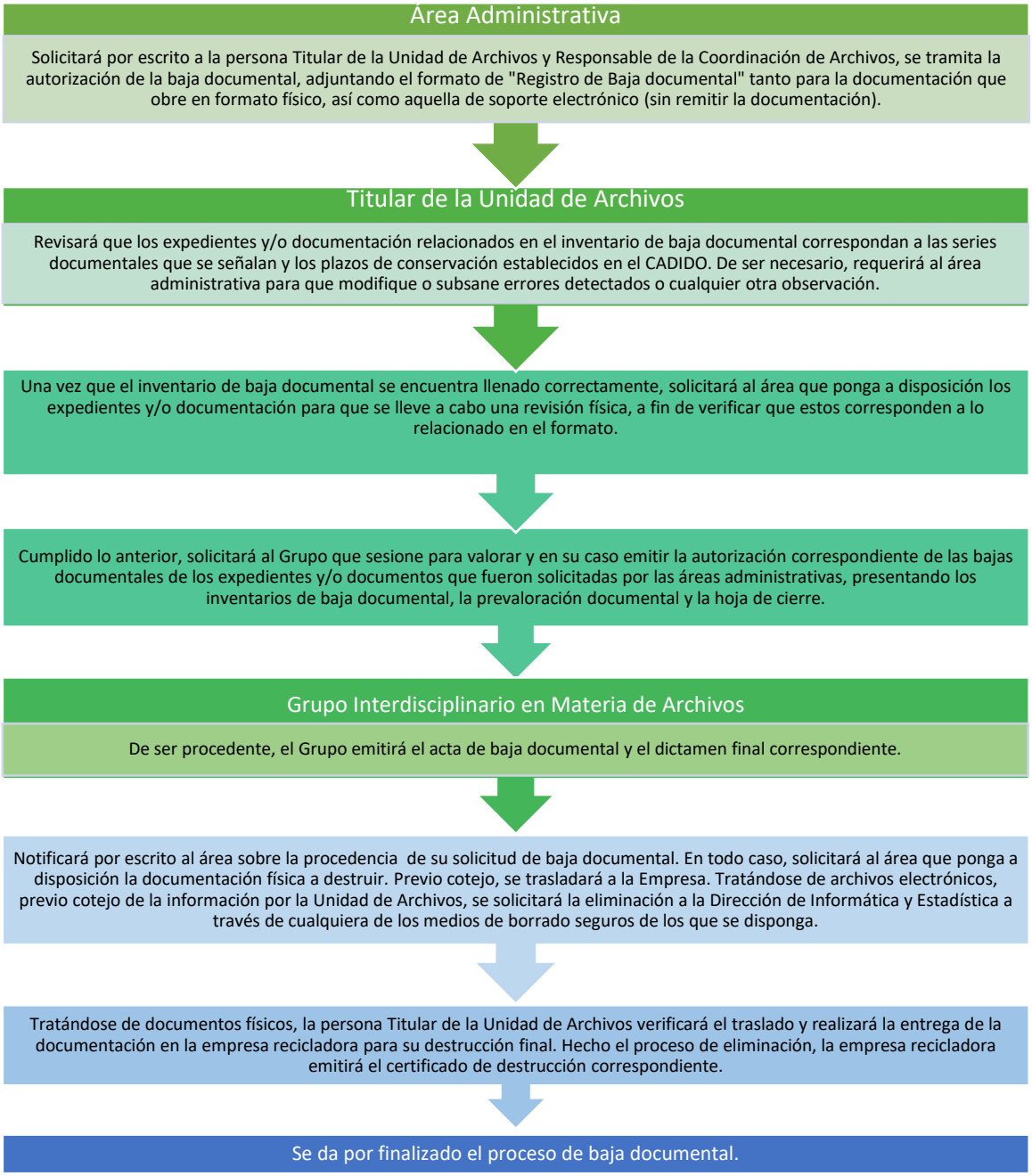
3. **Etapa de Baja documental o Supresión**. Los documentos de archivo que ya cumplieron sus periodos de trámite y concentración, pueden ser objeto de transferencias secundarias; es decir, pasar al archivo histórico si es que poseen valores históricos. En caso de que no sea así, procede entonces su baja documental.

   Tratándose de datos personales, la supresión, cancelación o eliminación de datos, procede una vez que se han agotado las etapas previas del procedimiento. Es decir, que se han cumplido los tiempos de conservación y bloqueo y, en su caso, llevado a cabo el proceso de disociación de los datos para su conservación con fines estadísticos.

   Es importante señalar que la etapa de supresión de datos deberá estar armonizada con el procedimiento de baja documental que el área administrativa en coordinación con la Unidad de Archivos debe realizar. No obstante, es necesario aclarar que ambos procedimientos son distintos.

a) La baja documental hace referencia al procedimiento mediante el cual se autoriza la destrucción de series documentales que han cumplido los tiempos de conservación establecidos en el CADIDO, con independencia de que contengan datos personales. Comprende todos los documentos de archivo con independencia del tipo de soporte, aunque generalmente se enfoca en archivos físicos.

Para llevar a cabo un procedimiento de baja documental, el área administrativa deberá seguir las indicaciones de la Coordinación de Archivos, en términos generales, el procedimiento para llevar a cabo una baja documental es el siguiente:



b) La supresión o cancelación, si bien obedece igualmente a los tiempos de conservación de los instrumentos de archivo, va más allá de una destrucción física de documentos, ya que abarca también la eliminación de la información que contiene datos personales en cualquier otro medio de almacenamiento (bases de datos, dispositivos, etc.), con independencia de que se consideren documentos de archivo, generalmente enfocada en medios automatizados.

Por ello, la supresión de datos personales puede llevarse a cabo en el mismo momento en que se autorice una baja documental, por lo que el procedimiento será el mismo que se lleve a cabo para la autorización de bajas documentales. Se entiende entonces que, al autorizarse una baja documental,

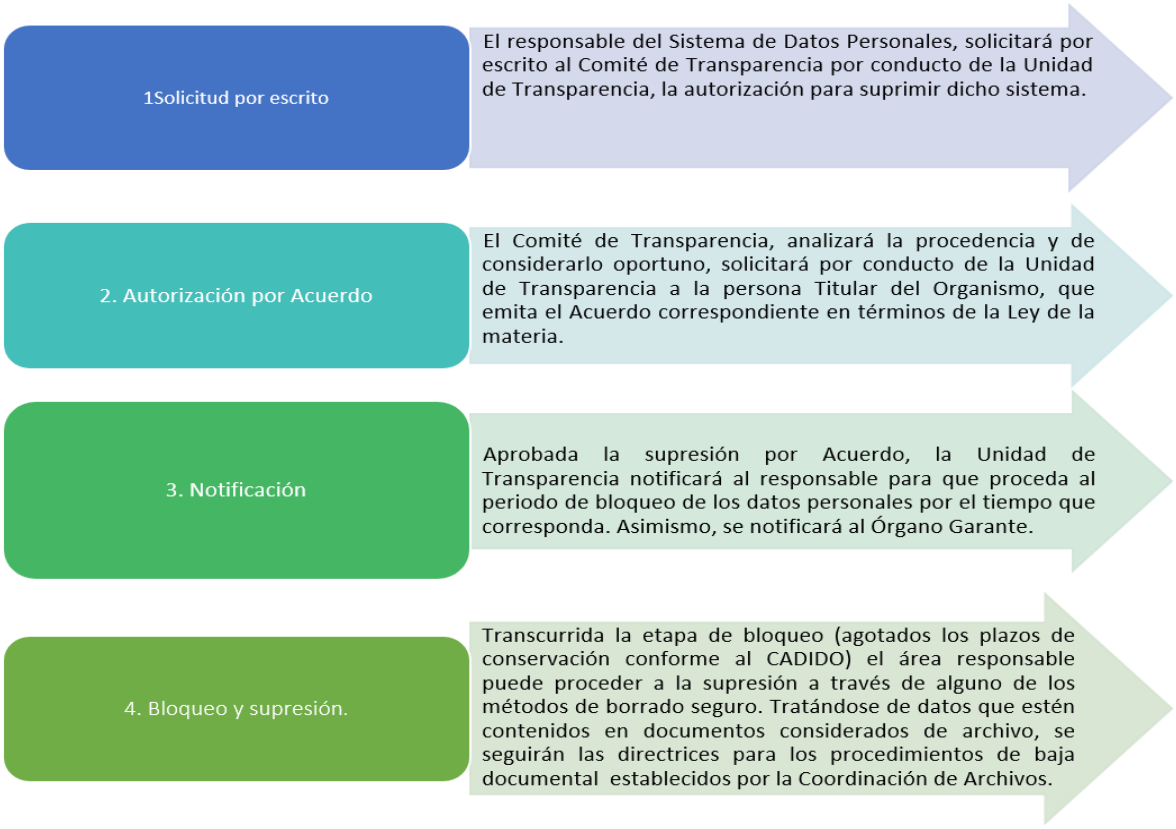
se estará autorizando también la destrucción de la información que contiene datos personales tanto en medios físicos como automatizados que se contengan en dichos documentos de archivo.

En casos excepcionales en los que deba realizarse una supresión de datos personales que no se haya considerado dentro de un proceso de baja documental, la autorización deberá solicitarse por escrito al Comité de Transparencia, por conducto de la Unidad de Transparencia. En todo caso, el proceso de borrado seguro será solicitado de la misma manera a la Dirección de Informática y Estadística. Para el borrado seguro de información que se encuentre en formato automatizado, se recomienda utilizar el método lógico de sobreescritura a fin de poder reutilizar los medios de almacenamiento. Tratándose de dispositivos electrónicos que ya no tienen vida útil, éstos se pondrán a disposición de la Unidad de Archivos para su destrucción como corresponde.

IV. Supresión de un Sistema de Datos Personales

Un sistema de Datos Personales puede suprimirse (eliminarse) en su totalidad cuando derivado de las actividades que realiza el responsable ya no sea necesario el tratamiento de determinados datos personales, porque el Sujeto Obligado ya no tenga facultades para recabar y dar tratamiento a la información que contiene datos personales. Por ejemplo, cuando derivado de la modificación de una norma, se limiten las facultades para el tratamiento de datos del responsable.

En ese caso, el procedimiento para la supresión considerará lo siguiente:



El Acuerdo mediante el cual se apruebe la supresión de un sistema de datos, deberá señalar lo siguiente:

- Indicar el nombre del Sistema o los Sistemas que se suprimen.
- Establecer el destino que tendrán los datos personales contenidos en el Sistema y, en su caso, las previsiones adoptadas para su destrucción de acuerdo con la Ley General de Archivos o su equivalente en el Estado de Veracruz.
- Ordenar el cumplimiento del periodo de bloqueo y especificar si en la destrucción de datos personales se excluirán datos para fines estadísticos o históricos, previo procedimiento de disociación conforme a la valoración documental para el archivo histórico del Sujeto Obligado.
- Suprimir el Registro Electrónico del Sistema o los Sistemas ante el Órgano Garante.
- Ordenar la notificación al Órgano Garante de la supresión de los Sistemas dentro del plazo establecido por la normatividad multicitada

Una vez cumplido los plazos correspondientes, se procede a un Borrado Seguro (extinción y/o baja documental de los archivos que componen el Sistema en los medios físicos y electrónicos).

Hecho lo anterior, se seguirá el procedimiento de borrado seguro establecido. Es decir, para la correcta supresión de los Sistemas de Datos Personales correspondientes, el área responsable del Sistema deberá ejecutar el Procedimiento para conservación, bloqueo y supresión de los datos personales antes descrito.

Fuentes de consulta

Instituto Nacional de Transparencia, A. a. (2021). *Diccionario de Archivos.* México: INAI. Obtenido de https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIOARCHIVOS_digital.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (Junio de 2015). Metodología de Análisis de Riesgo BAA. Obtenido de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2016). *Guía para el Borrado Seguro de Datos Personales* (Primera ed.). D.F., México: INAI. Obtenido de http://transparencia.inaes.gob.mx/doctos/pdf/transparencia/Guias/Gu%EDa_Borrado_Seguro_DatosPersonales.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2019). *Diccionario de Protección de Datos Personales. Conceptos fundamentales* (Primera ed.). México: INAI. Obtenido de https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

Suprema Corte de Justicia de la Nación. (Septiembre de 2021). Guía para la conservación y eliminación de documentos y expedientes que contienen datos personales. Obtenido de https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Gu%C3%ADa_conservaci%C3%B3n_eliminaci%C3%B3n_dp_v290921.pdf