ACUERDO MEDIANTE EL CUAL SE APRUEBAN LAS POLÍTICAS, MÉTODOS Y TÉCNICAS ORIENTADAS A LA SUPRESIÓN DEFINITIVA DE DATOS PERSONALES QUE OBREN EN EL COMITÉ EJECUTIVO NACIONAL DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL.

CONSIDERANDOS

1. Que el Congreso de la Unión, en cumplimiento al transitorio Segundo del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), publicada el veintiséis de enero de dos mil diecisiete en el Diario Oficial de la Federación (DOF), entrando en vigor al día siguiente de su publicación de acuerdo a lo previsto en el Artículo Primero Transitorio de la referida Ley General.

2. Que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición al uso de su información personal, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos personales, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

3. Que con fecha veintiséis de enero de dos mil diecisiete se publicó en el DOF el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual, de conformidad con su Artículo Primero Transitorio, entró en vigor el día siguiente de su publicación.

4. Que tras la publicación en el DOF, y entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por medio de la cual se incluyeron como sujetos obligados a proteger los datos personales que obren en su poder a los Partidos Políticos, de conformidad con lo dispuesto en el artículo 1 de la referida Ley.

5. Que en materia de supresión de datos personales la normativa establece losiguiente:

a) En la LGPDPPSO en el artículo 3, se establece:

> **Artículo 3.** Para los efectos de la presente Ley se entenderá por:
> …

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

> **XXX. Supresión:** 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 previamenteestablecidas por el responsable;

Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Artículo 24. El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódicasobre la necesidad de conservar los datos personales.

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, lassiguientes actividades interrelacionadas:

> I. 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 devida de los datos personales, es decir, su obtención, uso y posterior supresión;
> …

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

Artículo 83. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

El Comité de Transparencia será la autoridad máxima en materia de protecciónde datos personales.

Artículo 84. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

> I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
> …
>
> IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
>
> V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas enel documento de seguridad;"

b) Lineamientos Generales de Protección de Datos Personales para el Sector Público

(Lineamientos Generales):

Supresión de los datos personales

Artículo 23. En la supresión de los datos personales a que se refiere el artículo 23, párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los quese encuentren los datos personales:

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

I. **Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales;

II. **Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y

III. **Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

1) Que con base en lo establecido en el artículo 23 de la Ley General y artículo 23 de los Lineamientos Generales cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos; para lo cual se deberán establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

2) Que en el establecimiento de las políticas, métodos y técnicas referidas se deberán considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos, y/o electrónicos en los que se encuentren los datos personales: irreversibilidad, seguridad y confidencialidad, así como, que sea favorable al medio ambiente.

3) Que el Partido Revolucionario Institucional es una entidad de interés pública, con personalidad jurídica y patrimonio propio que goza de facultades para regular su vida interna y determinar su organización interior y los procedimientos correspondientes, de conformidad con los artículos 3 y 23, numeral 1 inciso c de la Ley General de Partidos Políticos.

4) Que el derecho a la protección de los datos personales es un derecho humano que debe ser garantizado por los sujetos obligados.

5) Que de los Estatuto Generales del Partido Revolucionario Institucional establecen que el Comité Nacional de Transparencia será el órgano responsable de garantizar los mecanismos para la protección de los datos personales que obren en su posesión, a través de su acceso, rectificación, cancelación y oposición en los términos previstos en la legislación aplicable, así como, de establecer lineamientos y manuales que permitan hacer eficientes los procedimientos de solicitudes de acceso a la información y de protección de datos personales.

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

6) Que los lineamientos que emite el Comité Nacional de Transparencia del Partido Revolucionario Institucional, para regular aspectos técnicos y operativos en las materias de su competencia, se encuentra establecida en sus Estatutos Generales, los cuales disponen la facultad de establecer lineamientos y manuales que permitan hacer eficientes los procedimientos de solicitudes de acceso a la información y de protección de datos personales; establecer, instruir, coordinar y supervisar, políticas, acciones y lineamientos para facilitar la obtención de información y el ejercicio de los derechos de acceso a la información y protección de datos personales; así como, establecer las medidas de seguridad y los mecanismos para la protección de los datos personales, incluyendo su acceso, rectificación cancelación y oposición en los términos previstos en estos estatutos, reglamentos y la legislación aplicable.

7) Que, con base en lo anterior, y de conformidad con lo dispuesto en el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales en Posesión del Partido Revolucionario Institucional (Reglamento de Transparencia), en su artículo 16, el Comité Nacional de Transparencia, tiene facultades para: establecer las medidas de seguridad y los mecanismos para la protección de los datos personales, incluyendo su acceso, rectificación, cancelación y oposición en los términos previstos en la legislación aplicable; supervisar, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad; y, coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el Partido.

8) Que la Unidad de Transparencia, Acceso a la Información y Protección de Datos Personales (Unidad de Transparencia) de conformidad con lo establecido en los Estatutos Generales y en el artículo 34 Reglamento de Transparencia tiene entre sus facultades la de auxiliar al Comité en sus funciones, realizar los trámites internos necesarios para la protección de los datos personales; desarrollas o adoptar esquemas de mejores prácticas, con el objeto de elevar el nivel de protección de datos personales, facilitar el ejercicio de los derechos ARCO por parte de los titulares; y complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales.

9) Que la Unidad de Transparencia, propone al Comité Nacional de Transparencia del Partido Revolucionario Institucional el proyecto de Acuerdo mediante el cual se aprueban las políticas, métodos y técnicas orientadas a la supresión definitiva de datos personales.

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

Por lo expuesto en las consideraciones de hecho y de derecho, y con fundamento en lo dispuesto en los artículos 6o., apartado A, fracción I y II, y 16 de la Constitución Política de los Estados Unidos Mexicanos; 3, 23, 24, 33, 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 3 y 23, numeral 1 inciso c de la Ley General de Partidos Políticos; de los Estatutos Generales del Partido Revolucionario Institucional; 23 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; 16 y 34 del Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales en Posesión del Partido Revolucionario Institucional, el Comité Nacional de Transparencia del Partido Revolucionario Institucional emite el siguiente:

ACUERDO

PRIMERO. Se aprueban las políticas, métodos y técnicas orientadas a la supresión definitiva de datos personales que obren en el Comité Ejecutivo Nacional del Partido Revolucionario Institucional conforme al documento anexo que forma parte integral del presente Acuerdo.

SEGUNDO. Se instruye a la Unidad de Transparencia del Partido Revolucionario Institucional, realice las gestiones necesarias a efecto de que el presente Acuerdo y su anexo se publiquen en la página oficial del partido.

TERCERO. Este Acuerdo y su anexo entrarán en vigor al día siguiente de su aprobación.

Así lo acordó, por unanimidad el Comité Nacional de Transparencia del Partido Revolucionario Institucional, en sesión ordinaria celebrada el treinta de mayo de dos mil veinticuatro.

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

POLÍTICAS, MÉTODOS Y TÉCNICAS ORIENTADAS A LA SUPRESIÓN DEFINITIVA DE DATOS PERSONALES QUE OBREN EN EL COMITÉ EJECUTIVO NACIONAL DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL.

Sección I
Disposiciones generales

Primero. Las presentes políticas, métodos y técnicas orientadas a la supresión definitiva de datos personales tienen por objeto ser una guía para los responsablesde las unidades administrativas al interior del Partido, para la supresión de datos personales, cuando estos hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, previo bloqueo en su caso, yuna vez que concluya el plazo de conservación de los mismos.

Segundo. Las disposiciones establecidas en estas políticas, métodos y técnicas son de observancia obligatoria para el Partido Revolucionario Institucional.

Tercero. Para los efectos de las presentes políticas, métodos y técnicas, se entenderá por:

I. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo deprescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá asu cancelación en la base de datos que corresponda;

II. **Borrado seguro:** el borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datospersonales, de modo que la probabilidad de recuperarlos sea mínima.

III. **Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

IV. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

V. **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima desu titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

VI. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

VII. **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

VIII. **Equipo de cómputo** se entiende cualquier dispositivo electrónico que permita el procesamiento de información, por ejemplo, computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, entre otros.

IX. **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

X. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XI. **Medios de almacenamiento electrónico:** Los medios de almacenamiento electrónico, 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 almacenarlos datos personales. Podemos considerar entre estos medios, por ejemplo, a los discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o SD, CD-ROM, DVD-R, CD-RW, DVD-RW, Blu- rays, cintas magnéticas, Disco UDO, entre otros. También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamientoen línea y/o en la nube.

XII. **Medios de almacenamiento físico:** Los medios de almacenamiento físico sontodo 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 oalmacenar datos personales, de forma enunciativa más no limitativa, se encuentran,los archiveros, gavetas/cajones, bodegas, estantes, oficinas, carpetas y documentos físicos.

XIII. **Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la LGPDPPSO que deciden sobre el tratamiento de datos personales;

XIV. **Sujeto obligado:** Partido Revolucionario Institucional (Partido)

XV. **Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucciónde los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

XVI. **Titular:** La persona física a quien corresponden los datos personales;

XVII. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento,posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales,

XVIII. **Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

Sección II
Políticas

Cuarto. El borrado seguro de los datos personales es un tema de cumplimiento legal, por lo que cuando los datos personales hayan dejado de ser necesarios paralas finalidades para las cuales se obtuvieron (mismas que se establecen en el avisode privacidad), deben ser eliminados, tomando en cuenta las disposiciones legalesaplicables para los plazos de conservación.

Quinto. El responsable del tratamiento está obligado a eliminar, de oficio, los datospersonales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron, con independencia de que el titular de los datos personales ejerza su derecho de cancelación.

Sexto. Para la eliminación de los datos personales se deberá tomar en cuenta el plazo de conservación de los mismos, el cual se fija a partir de las disposiciones legales aplicables en la materia de que se trate; por ejemplo: los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información y el periodo de bloqueo.

Séptimo. El plazo de conservación es igual al tiempo requerido para llevar a cabo las finalidades del tratamiento, más, los plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables, más el periodo de bloqueo. Pueden existircasos en que los tres tiempos o plazos coincidan.

Octavo. El responsable debe de implementar y mantener medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Así, con motivo del principio de calidad y del deber de seguridad, los datos personales deben eliminarse cuando ya no se requieren para la finalidad parala cual se obtuvieron, y su eliminación debe ser segura, de forma que se evite un uso indebido de los mismos.

Noveno. Para mitigar los riesgos de que una persona utilice técnicas de recuperación de información, para obtener datos personales de los medios de almacenamiento desechados o reutilizados por el partido, se deberán implementartécnicas de borrado seguro.

Décimo. El borrado seguro deberá estar estrechamente ligada al ciclo de vida de los activos, y principalmente, a la protección de los datos personales en los sistemasde tratamiento.

Décimo primero. Se deberán documentar las operaciones de borrado realizadas, por lo que, al seleccionar una herramienta de borrado, se deberá elegir aquélla quepermita la creación de un documento que identifique claramente que el proceso deborrado se ha realizado, detallando cuándo y cómo ha sido realizado.

Comité Ejecutivo Nacional
Av. Insurgentes Norte No. 59, Col. Buenavista, C.P. 06350, Alcaldía Cuauhtémoc, Ciudad de México.
T. (55) 5729.9600
www.pri.org.mx
REVOLUCIONARIOS

En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosacon el medio ambiente.

Décimo segundo. Para poder definir los métodos de borrado, es necesario establecer la naturaleza de los activos, es decir, si los datos personales se almacenan en un medio de almacenamiento físico o un medio de almacenamiento electrónico.

Décimo tercero. Para un borrado seguro de la información o la destrucción de los medios de almacenamiento, se deberá evitar:

I. PARA MEDIOS DE ALMACENAMIENTO FÍSICO:

a) **La destrucción manual:** Romper archivos y documentos a mano, contijeras o rasgarlos con un cutter es un método inseguro para desechareste tipo de activos. Este método permite que una persona malintencionada pueda recuperar los fragmentos de la basura y los ensamble a modo de rompecabezas para extraer informaciónimportante.

b) **Tirar documentos de forma íntegra a la basura:** Arrojar a la basura documentos con información valiosa o utilizarlos como papel de reciclaje es una conducta aún más riesgosa que la anterior.

II. PARA MEDIOS DE ALMACENAMIENTO ELECTRÓNICO:

a) **Los comandos de borrado por defecto de los sistemas operativos:** Cuando se utiliza un comando como “borrar” o “eliminar”, lo único que se está quitando de esa tabla es la referencia al archivo,pero la información permanece en el medio de almacenamiento, hasta que se reutilice este espacio con un nuevo archivo. Así que, con la simple utilización de algún software (en ocasiones gratuito), se podrían recuperar todos los archivos “borrados”.

b) **“Formatear”:** Cuando se formatea un medio de almacenamiento, seeliminan las tablas o listas de archivos mencionadas anteriormente, pero igual que en el caso anterior, la información sigue en el dispositivo y puede recuperarse con el uso de software.

Décimo cuarto. El responsable de los datos personales al interior de las unidades administrativas del Partido, deberá analizar los medios más eficaces que convengaimplementar para evitar que se pueda recuperar la información que ya no requieren,tomando en consideración que no sea posible recuperar la información tanto físicacomo electrónica y evitar que personas no autorizadas puedan tener acceso a esos datos, para lo cual se deberá de tomar en consideración las siguientes características:

a) **Irreversibilidad.** Se debe garantizar que no existe un proceso que permita recuperar la información.

b) **Seguridad y confidencialidad.** Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenidodurante su existencia.

c) **Favorable al medio ambiente.** El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Décimo quinto. Para el borrado seguro de los datos personales se deberá contemplar el riesgo inherente de los datos personales en los sistemas de tratamiento, es decir, el valor significativo tanto para los titulares y responsables, como para cualquier persona no autorizada que pudiera beneficiarse de ellos.

Décimo sexto. Para elegir el método de borrado seguro más adecuado se deberán contemplar diferentes factores, como, el volumen y tipo de datos personales que semanejan y el presupuesto con el que se cuenta para llevar a cabo el procedimiento.

Sección III
Métodos y Técnicas

Décimo séptimo. Los métodos para el Borrado Seguro de los Datos Personales, con métodos físicos, se basan en la destrucción de los medios de almacenamiento,es decir, en la destrucción de los medios de almacenamiento físico; y la destrucciónde los medios de almacenamiento electrónicos. Mientras que, los métodos para el Borrado Seguro de los Datos Personales, con métodos lógicos, se basan en la limpieza de los datos almacenados, como puede ser, la des magnetización y el sobre-escritura.

Décimo octavo. Métodos físicos de borrado, son aquellos que implican un daño irreversible a la destrucción total de los medios de almacenamiento, tanto físico como electrónico.

Así, dentro de las técnicas de destrucción para los medios de almacenamiento físico se encuentran los siguientes:

1. **Trituración.** Este método es uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivos. Para ello, se deberá considerar el tipo de corte, pues existen dos tiposprincipales de trituradoras:

- **En línea recta o tiras:** Cortan el documento en tiras delgadas. Se recomienda usar el corte en tiras de 2 mm de ancho o menos, a fin de evitar que la información pueda ser recuperada rearmando losfragmentos.

- **En corte cruzado o en partículas:** Corta el documento de forma verticaly horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.

2. **Incineración.** La incineración de medios de almacenamiento físico consisteen su destrucción a través del uso del fuego. Actualmente la práctica de la incineración no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente, sin embargo, es una opción segura para la destrucción de los datos personales, **siempre y cuando se valide que el activo se redujo a cenizas.**

3. **Químicos.** En algunos casos también es posible destruir documentos por medio de químicos, sin embargo, esta opción tampoco es muy recomendablepor temas ecológicos.

   Para la destrucción de los medios de almacenamiento electrónicos se utilizarán técnicas tales como:

   a) **Desintegración.** Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

   b) **Trituración o Pulverización.** Procedimiento mediante el cual un cuerposólido se convierte en pequeñas partículas.

   c) **Abrasión.** Acción de arrancar, desgastar o pulir algo por rozamiento ofricción.

   d) **Fundición o Fusión.** Paso de un cuerpo del estado sólido al líquido porla acción del calor.

Décimo noveno. Para la destrucción de medios de almacenamiento electrónico, sepodrá llevar a cabo una subcontratación del servicio, que además de la eliminacióndefinitiva del activo podrá contemplar con opciones de tratamiento de desperdiciosy de reciclaje para hacer que el proceso sea más amigable con el ambiente.

Vigésimo. Métodos lógicos de borrado; son aquellos que implican la sobre-escriturao modificación del contenido del medio de almacenamiento electrónico. Así, dentrode las técnicas de destrucción se encentran los siguientes:

1. **Desmagnetización.** Este método expone a los dispositivos dealmacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador. Debido a las fuerzas

físicas del proceso, es posible que el hardware donde se encuentra la información se vuelva inoperable, por lo que se recomienda aplicar este método si no se volverá autilizar el medio de almacenamiento.

La desmagnetización se considera más segura que algunos procesos de destrucción física, ya que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo.

La potencia requerida para borrar el dispositivo depende de su tamaño y forma, y para hacer efectivo el borrado, se requiere de una configuración particular para cada medio de almacenamiento. Por la naturaleza del equiponecesario para este proceso, podrá realizarse bajo un esquema de contratación del servicio.

2. **Sobre-escritura.** Consiste en sobrescribir todas las ubicaciones dealmacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software. El método más simple consiste en realizar una sola sobre-escritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobre escrituras o "pasadas" con variaciones en los caracteres grabados al medio de almacenamiento.

   Una ventaja particular del sobre-escritura es que las herramientas se pueden utilizar para borrar un archivo o carpeta específica, sin necesidad dealterar o detener la operación de todo un medio de almacenamiento o equipode cómputo.

3. **Cifrado de medios.** Cuando un archivo electrónico o medio de almacenamiento se encuentra cifrado, es posible aplicar el denominado "borrado criptográfico" (*Cryptographic Erase o CE*), para borrar únicamente las claves que se utilizaron para cifrar el medio de almacenamiento o archivo.Esto deja únicamente datos en un formato tal que es imposible obtener información de ellos sin dichas claves.

La efectividad de esta técnica depende:

a) Del tipo de cifrado utilizado en el medio de almacenamiento o archivo.

b) Del nivel de seguridad del método de borrado aplicado a las claves.

Vigésimo primero. Los medios de almacenamiento y sus respectivos métodos de borrado que pondrán ser utilizados por los responsables de las unidades administrativas que den tratamiento a datos personales al interior del Partido se muestran a continuación:

Medio de almacenamiento	Tipo de medio	Método de borrado seguro
Medio de almacenamiento físico	• Archiveros • Gavetas • Bodegas • Estantes • Oficinas	• Trituración • Incineración • Uso de químicos
Magnético	• Disco duro • Disco duro externo o portátil • Cintas magnéticas	• Sobre-escritura • Desmagnetización • Destrucción física
Óptico (dispositivos re-grabables)	• CD-RW / DVD-RW • Blu-Ray re-gradable (BD- RE)	• Sobre-escritura
Magneto-óptico	• Disco magneto-óptico • MiniDisc • HI-MD	• Sobre-escritura • Destrucción física
Estado sólido	• Pendrive / USB • Tarjetas de memoria (Flash drive) • Dispositivo de estado sólido	• Sobre-escritura • Destrucción física

Vigésimo segundo. En los casos en los que se opte por realizar una subcontratación para realizar el borrado seguro de la información se tiene que considerar lo siguiente:

a) **Si el borrado seguro se realiza en las instalaciones de un tercero**, esto implica posibles gastos de transporte, así como la necesidad de establecer medidas para el resguardo, registro y vigilancia de los medios de almacenamiento. Por lo que se debe ser cuidadoso con este proceso a fin deque no existan fugas de información o pérdidas de activos.

b) **Se requiere establecer un contrato donde se defina de forma detallada el servicio que prestará el tercero**, así como las responsabilidades de ambas partes.

c) Se debe verificar si el proveedor cuenta con credenciales, certificaciones, o cualquier prueba de que el borrado seguro se realizaen un ambiente controlado.

d) **Es importante atestiguar el borrado y solicitar al prestador de servicio un certificado o acta del proceso de borrado realizado.**

Sin importar si el borrado seguro se hace dentro de la organización, o bien a través de una subcontratación, se debe administrar la generación de evidencia de dicho proceso, por ejemplo, con certificados, actas, fotografías y/o bitácoras de la destrucción, a fin de que, ante un procedimiento del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se

puedademostrar el cumplimiento de esta medida de seguridad y/o ante autoridad competente.

Vigésimo tercero. Es recomendable validar la ejecución del borrado seguro, con elobjetivo de confirmar que los datos personales en el medio de almacenamiento fueron eliminados de forma eficiente. Éste proceso puede encargarse a personal que no haya estado involucrado en la ejecución del borrado seguro.

En particular, para medios electrónicos, se puede aplicar algún mecanismo para revisar o auditar el proceso de borrado seguro.

Vigésimo cuarto. Como parte fundamental de la evidencia del proceso de borrado seguro es conveniente contar con un registro de los medios a los cuales se les aplicóla eliminación de datos personales, para los medios de almacenamiento de tipo magnético, óptico, magneto-óptico o de estado sólido, es posible consolidar un reporte con la siguiente información:

- Fabricante del dispositivo
- Modelo
- Número de serie (si es posible)
- Tipo de medio
- Método de borrado seguro aplicado
- Herramienta utilizada (si es el caso)
- Método de revisión (si es el caso)
- Personas involucradas en el proceso de borrado seguro
- Personas involucradas en el proceso de revisión (si es el caso)
- Fecha de ejecución

Vigésimo quinto. A falta de disposición expresa en estas políticas, métodos y técnicas, se aplicarán de manera supletoria y en el siguiente orden de prelación, lasdisposiciones de la Ley General de Protección de Datos Personales en Posesión deSujetos Obligados, los Lineamientos Generales de Protección de Datos Personalespara el Sector Público[1] y la Guía para el Borrado Seguro de Datos Personales

Emitida por el Instituto Nacional de Transparencia, Acceso a la Información yProtección de Datos Personales.

Transitorios

Único. Estas políticas, métodos y técnicas orientadas a la supresión definitiva dedatos personales entrarán en vigor al día siguiente de su aprobación.

[1] Aprobados por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante el Acuerdo ACT-PUB/19/12/2017.10 o bien el acuerdo que lo reforme.