Procedimientos y plazos de conservación para el bloqueo en su caso y supresión de los datos personales que obran en posesión del Instituto Nacional Electoral

(Anexo Único del Acuerdo INE-CT-ACG-PDP-003-2018)

CONTENIDO

1 Glosario 3
2 Objetivo 6
3 Alcance de los Procedimientos 7
4 Alcance del principio de calidad 7
5 Introducción 8
6 Roles y responsabilidades 9
7 Supresión de los datos personales 10
7.1 Consideraciones generales 10
7.2 Consideraciones para la eliminación en medios digitales 10
7.3 Procedimiento de supresión en medios electrónicos 11
7.4 Técnicas de eliminación de datos personales 12
7.4.1 En medios Digitales. 12
7.4.2 En medios físicos 12
7.5 Métodos de verificación 13
7.6 Documentación 13
7.7 Selección del método de eliminación basado en el nivel de riesgo 14
8 Bloqueo de los datos personales 15
8.1 Consideraciones generales 15
8.2 Procedimiento de bloqueo en medio digitales 16
9 Revisiones periódicas para la conservación de los datos personales 17
10 Anexos 17
10.1 Anexo I. Categorización delos datos personales y valor de riesgo asociado 17
10.1.1 Clasificación por tipo de dato personal 17
10.1.2 Identificación del nivel de riesgo 19
10.2 Anexo II. Técnica de eliminación por tipo de medio 20

10.2.1 Medios físicos 20
10.2.2 Medios digitales 20
10.3 Anexo III. Certificado de eliminación de datos 26
11 Referencias 27

1 GLOSARIO

Para efectos del presente documento se entenderá por:

i. **Archivo de Concentración:** Unidad del Archivo Institucional responsable de la administración de documentos cuya consulta es esporádica por parte de los Órganos del Instituto, dichos documentos permanecerán en él hasta su destino final.
ii. **Archivo de Trámite:** Unidad responsable, dentro de cada uno de los Órganos del Instituto, de la administración de documentos de uso cotidiano y necesario para el ejercicio de sus atribuciones.
iii. **ATA (Advanced Technologies Attachment).** Interfaz de conexión para medios magnéticos.
iv. **Baja documental.** Eliminación de aquella documentación que haya prescrito en sus valores administrativos, legales, fiscales o contables y que no contenga valores históricos.
v. **Bases de datos.** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
vi. **BD.** Disco Blue-ray.
vii. **Bloqueo.** 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 éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.
viii. **Borrado Criptográfico.** Método de eliminación en el cual, la Llave de Cifrado del Medio (Media Encryption Key – MEK) utilizada para el cifrado de los datos (Key Encryption Key – KEK) es eliminada, haciendo que los datos cifrados con esa llave no puedan ser recuperados.
ix. **Catálogo de Disposición Documental**: Registro general y sistemático que establece el plazo de conservación de las series documentales, tanto en archivos de trámite como en el archivo de concentración.
x. **CD.** Disco Compacto.
xi. **CD-RW**. Disco Compacto de Lectura/Escritura. Puede aplicarse método de eliminación por purga y reescritura.

xii. **CD**-**R**. Disco Compacto que permite la multisesión. Cada sesión creada se queda grabada en el disco.

xiii. **Custodio**: Área responsable de la administración diaria de la seguridad en los sistemas de información.

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

xv. **Destrucción**. Aplicación de técnicas que hacen imposible la recuperación de datos utilizando técnicas de laboratorio de avanzadas (osciloscopios, estaciones de soldadura, cámaras limpias, por mencionar algunas); incapacita el uso posterior de los medios para el almacenamiento de datos.

xvi. **Desintegración**. Método de destrucción física para la eliminación de datos en un medio. Corresponde al acto de separar al medio en las partes que lo componen.

xvii. **Desmagnetizar**. Proceso de exponer los medios magnéticos a un fuerte campo magnético.

xviii. **Destrucción física**. Medio de eliminación segura de datos para un medio.

xix. ***Dumpster diving* o *Trashing***: Técnica utilizada por un tercero malintencionado que consiste en obtener información de la basura digital (discos duros, memorias USB, dispositivos ópticos, etc.) o de la papelería empleada en la oficina -generada en una organización- que puede contener información clasificada como reservada o confidencial, informes, entre otros.

xx. **DVD.** Disco de Video Digital. posee mayor capacidad de almacenamiento de datos que un CD.

xxi. **Eliminación segura.** Proceso a través del cual se hacen ilegibles o irrecuperables los datos en medios impresos o electrónicos, a pesar de aplicar un esfuerzo considerable al intentar recuperar los datos.

xxii. **Incineración.** Método de destrucción física para la eliminación segura de los datos; es el acto de quemar completamente y que el medio quede en cenizas.

xxiii. **Ingeniería social.** Acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo[1].

[1] Sandoval Castellanos, Edgar Jair. "Ingeniería Social: Corrompiendo la mente humana", Consultado en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

xxiv. **Instituto o INE.** Instituto Nacional Electoral

xxv. **Limpiar.** Método de eliminación que emplea técnicas lógicas para borrar de forma segura los datos en los medios de almacenamiento electrónico –a través de la sobre-escritura del dispositivo de almacenamiento o el reinicio del dispositivo con los valores de fábrica cuando la sobre-escritura no es soportada- que impide la recuperación de los datos a través de técnicas simples de recuperación no invasivas.

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

xxvii. **Lineamientos:** Lineamientos Generales de Protección de Datos Personales para el Sector Público.

xxviii. **Medio.** Material en el cual los datos son o pueden ser grabados, como papel, tarjetas perforadas, cintas magnéticas, discos magnéticos, dispositivos de estado sólido o discos ópticos.

xxix. **Órganos del Instituto**: órganos de dirección, ejecutivos, técnicos, de vigilancia, de transparencia, de control y otros órganos colegiados del INE.

xxx. **Técnica de eliminación**. Término referido a la acción tomada para que los datos escritos en un medio sean irrecuperables por mecanismos ordinarios y extraordinarios.

xxxi. **Medios de almacenamiento digital**. Dispositivos que almacenen información de manera permanente. Estos incluyen los medios magnéticos, los electrónicos y los ópticos.

xxxii. **Medios electrónicos.** Son los dispositivos que almacenan la información en circuitos electrónicos, como dispositivos de memoria *RAM*, *ROM, EEPROM*, memorias flash, y USB teléfonos celulares, dispositivos móviles, unidades de estado sólido (*SSD por sus siglas en inglés*), dispositivos de red entre otros.

xxxiii. **Medios impresos.** Se refiere a la representación física de la información, comúnmente asociada con impresiones en papel; se incluyen también los facsímiles, plásticos de tarjetas de pago, FAX y fotos.

xxxiv. **Medios magnéticos.** Tipo de medio que almacena la información por medio de ondas magnéticas, como los discos duros (*Hard Disk-HD*), Disquetes o discos flexibles (*Floppy Disks-FD*), cintas o casetes.

xxxv. **Medios ópticos.** Dispositivos de almacenamiento que escriben y leen la información mediante un rayo láser.

xxxvi. **Plazos de conservación.** Tiempo de prescripción legal o contractual, conforme al periodo de guarda de la documentación en los archivos de trámite y de

concentración e histórico, que se integra por la combinación de la vigencia documental, el término precautorio, el periodo de reserva, en su caso, y los periodos adicionales establecidos en los Lineamientos Generales para la Organización y Conservación de los Archivos de los Órganos Responsables en Materia de Transparencia del Instituto Federal Electoral (vigentes para el Instituto Nacional Electoral).

xxxvii. **Procedimiento.** Método de ejecución de bloqueo y supresión de los datos personales en posesión del Instituto.

xxxviii. **Propietario**: Es el área responsable de la información.

xxxix. **Purga.** aplicación de técnicas físicas o lógicas que hacen que la recuperación de los datos no sea factible usando técnicas de laboratorio de última generación.

xl. **Reglamento.** Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales.

xli. **Supresión:** Es la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los mismos bajo las medidas de seguridad previamente establecidas por el responsable.

xlii. **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.

xliii. **Usuario**: Es el área responsable autorizada para acceder a los datos personales, a través del personal y/o prestadores de servicios autorizados para ello.

2 OBJETIVO

Identificar los métodos y técnicas para el bloqueo en su caso y la supresión definitiva de los datos personales en posesión del Instituto Nacional Electoral que han cumplido con los plazos de conservación, de tal manera que recuperarlos o reutilizarlos sea improbable.

3 ALCANCE DE LOS PROCEDIMIENTOS

Las disposiciones previstas en los presentes Lineamientos son de carácter obligatorio para los órganos, personal y prestadores de servicios del Instituto Nacional Electoral.

La Ley General de Datos desarrolla una serie de principios y deberes que establecen obligaciones concretas para los responsables del tratamiento de datos personales, a fin de crear condiciones para la protección de los datos, evitar malos manejos de los mismos, y permitir que las personas ejerzan su derecho a la autodeterminación informativa.

Para efectos de los presente Lineamientos, se considerará el principio de calidad y el deber de seguridad.

Tomando en cuenta que los datos personales son un conjunto de la totalidad de la información que el Instituto tiene bajo su custodia, este documento abarcará las bases de datos físicas o digitales en posesión de los propietarios de la información que contienen datos personales en cualquier medio.

No serán aplicables respecto de la eliminación segura de información de equipos de cómputo personales (laptops o escritorios), dispositivos móviles, memorias flash/USB de uso diario de trabajo, impresoras y papel de reciclaje.

Tampoco serán aplicables a los archivos históricos del Instituto, en virtud de que los documentos contenidos en dichos archivos son catalogados como fuentes de acceso público por contener la memoria institucional del organismo de que se trate.

4 ALCANCE DEL PRINCIPIO DE CALIDAD

Durante el tratamiento de los datos personales, los Órganos del Instituto deberán adoptar las medidas necesarias para mantenerlos exactos, completos, correctos y actualizados, a efecto de no alterar la veracidad de los mismos. Lo anterior implica que los datos personales no presentan errores que pudieran alterar su veracidad; que estén completos para cumplir con las finalidades que motivaron su tratamiento y de las atribuciones que tiene conferidas el INE, y que reflejen fielmente la situación del titular de los datos.

Una vez que los datos personales dejaron de ser necesarios para el cumplir 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.

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

5 INTRODUCCIÓN

Para hacer posible el ejercicio del derecho de **cancelación** de los datos personales por parte su titular, el **propietario de los datos con apoyo de las áreas custodias**, deben implementar técnicas de eliminación segura de los datos, la cual es también una medida para garantizar su confidencialidad.

Debido a que una de las fuentes de recolección de información por personas no autorizadas es a través de la búsqueda de documentos que han sido desechados en la basura, en el caso de documentos en soporte en papel, o que sólo se han "borrado" del equipo de cómputo o medio de almacenamiento, es de suma importancia establecer procedimientos seguros para su eliminación.

La búsqueda de información con algún tipo de valor en la basura –la cual puede ser física o digital- es una práctica que puede resultar de alto riesgo para el Instituto, debido a que puede contener documentos confidenciales, configuraciones de equipos informáticos, correos electrónicos, computadoras en desuso, contraseñas, memorias de trabajo, entre otras. Esta información puede ser utilizada con el objetivo de robar o suplantar la identidad de una persona, ya que con sus datos personales es posible acceder a cuentas bancarias, tarjetas de crédito o acceso a instalaciones, servidores, cuentas de correos electrónicos, así como ser usada para ingeniería social.

Para evitar que algún tercero malintencionado obtenga información valiosa de los documentos desechados, en cualquier tipo de medio, se debe seguir un **procedimiento de seguridad para su eliminación**, en donde todo el papel -incluidas las impresiones- **se triture en una trituradora de corte transversal antes de ser reciclado, se eliminen todos los medios de almacenamiento y se concientice al personal sobre el peligro de no tener cuidado de la basura desechada**.

Por otro lado, el artículo 12 del Reglamento, también señala el **bloqueo** de los datos personales, motivo por el cual es necesario determinar la forma en la que se deberá llevar a cabo para garantizar su seguridad y que los datos no serán sujeto de tratamiento alguno hasta el cumplimiento del plazo establecido.

La terminología e información contenida en el presente documento se basa en estándares y buenas prácticas de seguridad de la información nacionales e internacionales.

6 ROLES Y RESPONSABILIDADES

a) **Grupo de Gobierno de Tecnologías de la Información**. Responsable de disponer a los propietarios de los datos, las soluciones (software/herramienta/tecnología) para ejecutar la eliminación segura de la información.
b) **Grupo de Gobierno de Seguridad de la Información**. Responsable de proponer y aprobar, en conjunto con la Unidad de Transparencia, las soluciones para la eliminación segura de los datos y la verificación de que la información no es recuperable.
c) **Unidad de Técnica de Transparencia**. Proporcionar asesoramiento en materia archivística y de protección de datos personales, de acuerdo a la normatividad aplicable al Instituto.
d) **Custodios de la información.** Apoyar a los propietarios de la información en la ejecución de la eliminación segura de los datos.
e) **Propietarios de la información**. Identificar el método de eliminación segura de los datos personales, con base en su clasificación, riesgo, tipo de medio, reutilización y si permanecerá o no en el Instituto, así como de los procesos de bloqueo y supresión, según lo indicado en el Cuadro General de Clasificación Archivística del Instituto y la normativa aplicable.
f) **Usuarios**. Conocer y entender la confidencialidad de la información que utilizan como parte de sus funciones y garantizar el manejo seguro de los datos, esto incluye no realizar copias no autorizadas de los datos personales a los que tenga acceso o difundir la información.

7 SUPRESIÓN DE LOS DATOS PERSONALES

7.1 CONSIDERACIONES GENERALES

Transcurrido el periodo de bloqueo, los Órganos del Instituto deberán realizar la supresión de los datos personales en la base de datos correspondiente.

La supresión de los datos personales deberá de ser de forma definitiva, de tal manera que la probabilidad de recuperarlos o reutilizarlos a través de técnicas forenses o de laboratorio sea mínima.

En la supresión de los datos personales, los Órganos del Instituto deberán tomar en cuenta como mínimo lo siguiente:

a) Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;
b) 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 Genera y los Lineamientos Generales.
c) Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios al medio ambiente.

7.2 CONSIDERACIONES PARA LA ELIMINACIÓN EN MEDIOS DIGITALES

El *propietario* de los datos, *con apoyo de las áreas custodias*, debe tener en cuenta las siguientes recomendaciones antes de llevar a cabo la eliminación segura de los datos personales, para determinar el tiempo y los recursos humanos, financieros y técnicos que se invertirán y estar en condiciones de cumplir con lo señalado en el artículo 12 del Reglamento:

a) Identificar el tipo y tamaño del medio de almacenamiento que requiere eliminación segura de datos.
b) Los requerimientos de confidencialidad para los datos almacenados en el medio, de acuerdo al nivel de riesgo de los datos contenidos.

Con base en estos requerimientos, se debe verificar la posibilidad de conocer, de manera anticipada, la cantidad de medios –clasificados por tipo de medios- que serán

sometidos a una eliminación segura, con lo cual se debe generar un **calendario de eliminación de medios**, a través del cual se podrá determinar lo siguiente:

a) La posibilidad de ejecutar la eliminación de la información en un ambiente controlado..
b) La disponibilidad de equipo y herramientas para la eliminación de la información.
c) Si la eliminación de la información puede ser realizada por personal del Instituto o se requiere un tercero.
d) El nivel de formación del personal con respecto al equipo/herramientas de eliminación de información.
e) El tiempo requerido para realizar la eliminación de los datos y
f) El costo de la eliminación de los datos en el medio, considerando las herramientas, la capacitación, verificación y su reutilización.

7.3 PROCEDIMIENTO DE SUPRESIÓN EN MEDIOS ELECTRÓNICOS

El *propietario* de los datos personales debe:

a. **Clasificar los datos personales e identificar el nivel de riesgo**. La técnica de eliminación de los datos debe determinarse por el riesgo inherente del dato, el cual, a su vez, está basado en la clasificación de los datos personales.
b. **Identificar el medio de almacenamiento**.
c. **Verificar si el medio de almacenamiento será reutilizado**. Analizar si el medio será reutilizado o reciclado. En caso de no ser así, se sugiere destruirlo.
d. **Verificar si el medio de almacenamiento saldrá del Instituto**. Debido a que implica si el Instituto tendrá o no control del medio.
e. **Seleccionar la técnica de eliminación**, y si será parcial –sólo un conjunto de datos de la base de datos o de un documento físico o digital- o total -la totalidad de la base de datos o de los documentos físicos o digitales.
f. **Seleccionar el método de verificación**. Se debe verificar que los datos no pueden ser recuperados aplicando un mínimo de esfuerzo.

7.4 TÉCNICAS DE ELIMINACIÓN DE DATOS PERSONALES

7.4.1 En medios Digitales.

- **Testar**. Técnica empleada para eliminar partes específicas de un documento digital que evita la visualización de los datos confidenciales durante un proceso de desclasificación. Esta técnica incluye el borrado de metadatos y la eliminación de imágenes y texto.
- **Borrar**. Esta técnica realiza un borrado sencillo que sólo elimina la referencia a los archivos en el sistema operativo (desindexación); los datos continúan en el medio de almacenamiento y éstos pueden ser recuperados aplicando técnicas de cómputo forense.
- **Limpiar**. Emplea procedimientos basados en software para la sobre-escritura de los datos en los medios de almacenamiento con la finalidad de que no puedan ser recuperados a través del uso de técnicas de cómputo forense. Lo anterior puede aplicarse a un archivo específico o el medio completo. Cuando la sobre-escritura no está soportada por el dispositivo, se reinicia con los valores de fábrica. Este método no puede ser utilizado para medios dañados o que no pueden ser sobre-escritos.
- **Purgar**. Emplea técnicas físicas o lógicas que evitan que los datos que contiene el medio sean recuperados empleando técnicas de laboratorio avanzadas. Se recomienda en caso de que el dispositivo sea reutilizado, reciclado o desechado. En esta categoría se encuentran la sobre-escritura, el borrado de bloque, el borrado criptográfico y la des-magnetización.

7.4.2 En medios físicos

- **Testar**. Aplica a medios físicos escritos. Consiste en el truncamiento de determinadas partes en un documento con la finalidad de prevenir revelaciones de información reservada o confidencial (datos personales).
- **Destruir**. Elimina los datos a través de la destrucción física del medio que los almacena, dejándolos inutilizables. Las técnicas de destrucción son las siguientes:
    - **Desintegración, incineración, pulverización, fundición**. Métodos diseñados para destruir de manera definitiva el medio de almacenamiento.
    - **Trituración**. Método diseñado para reducir el medio de almacenamiento de tal manera que no pueda ser reconstruido.

7.5 MÉTODOS DE VERIFICACIÓN

La Unidad de Transparencia, previa consulta al *Grupo de Gobierno de Seguridad,* debe verificar -posterior a la eliminación segura de los datos en el medio- que la técnica empleada garantice la confidencialidad de los datos eliminados.

Para tal efecto, existen dos métodos de verificación:

- **Completa**. Este método revisa de manera detallada cada dispositivo y garantiza la efectividad de la técnica aplicada en la eliminación segura de los datos. Se debe considerar que su aplicación toma mucho tiempo.
- **Por muestreo**. En este método se toma un subconjunto de los medios a los que se les aplicó la eliminación segura. Se recomienda que se verifiquen al menos el 25% de los dispositivos borrados. Su nivel de detalle es menor y por lo tanto requiere menos tiempo.

7.6 DOCUMENTACIÓN

a) Para los datos personales contenidos en medios digitales:

   Independientemente de la técnica aplicada en la eliminación de los datos personales, el *propietario* de los datos debe generar un certificado -que puede ser tanto un registro electrónico o un documento en papel- con, al menos, la siguiente información:

   - Datos del medio que contiene los datos personales:
     - Fabricado por / Marca.
     - Modelo.
     - Número de serie.
     - Número de inventario (en caso de que aplique).
   - Tipo de medio: impreso, magnético, óptico, electrónico.
   - Origen del medio: computadora personal, servidor, teléfono celular, etc.
   - Descripción de la técnica de eliminación: limpieza, purga, destrucción.
   - Método usado: des-magnetización, sobre-escritura, borrado de bloques, borrado criptográfico, trituración, etc.
   - Herramienta utilizada, incluyendo el número de versión.
   - Método de verificación.
   - Destino del medio posterior a la eliminación segura de la información.

- Respaldo. Indicar si la información se respaldó y de ser así, en dónde.
- Tanto para la eliminación segura y la verificación, incluir:
  - Nombre de quien realizó la eliminación
  - Nombre de quien validó la eliminación
  - Cargo y Área
  - Fecha
  - Localización
  - Teléfono y correo electrónico
  - Firma
- Incluir nombre, cargo y firma de quien autoriza la eliminación.

El Anexo III. incluye un formato de ejemplo.

b) Para los datos personales contenidos en medios impresos:
Se debe cumplir con lo indicado en los procedimientos de destrucción de documentos (expedientes) establecidos por el Archivo Institucional.

7.7 SELECCIÓN DEL MÉTODO DE ELIMINACIÓN BASADO EN EL NIVEL DE RIESGO

El nivel de riesgo de los datos personales se determina con base a la clasificación del dato personal. En el Anexo I. se describe la categorización de los datos personales y el valor del riesgo asociado.

Una vez identificado el riesgo, el *propietario* de los datos debe seleccionar el método adecuado para eliminar la información contenida en el medio (ver Tabla 1).

Tabla 1. Identificación de la técnica de eliminación de información con base en el nivel de riesgo

Nivel de Riesgo	El medio no permanecerá en el Instituto		El medio permanece en el Instituto	
	Reutilizado	No Reutilizado	Reutilizado	No reutilizado
Bajo	Purgar	Purgar	Limpiar	Limpiar

Tabla 1. Identificación de la técnica de eliminación de información con base en el nivel de riesgo				
Medio	Purgar	Destruir	Purgar	Destruir
Alto	Destruir	Destruir	Purgar	Destruir
Reforzado	Destruir	Destruir	Destruir	Destruir

8 BLOQUEO DE LOS DATOS PERSONALES

8.1 CONSIDERACIONES GENERALES

Una vez cumplida la finalidad para la cual fueron recabados los datos personales, los Órganos del Instituto deberán bloquear los datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

Previo al bloqueo de los datos personales, los Órganos del Instituto deberán:

a) Identificar los plazos de conservación de los datos personales, o bien, de los documentos y/o expedientes en los que obren los mismos.
b) Asegurarse de que los plazos de conservación atiendan y consideren:

i) las disposiciones aplicables en la materia de que se trate, y
ii) los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

c) Observar los plazos de prescripción previstos en la normativa que resulte aplicable o, en su caso, en las cláusulas contractuales, para efectos de las posibles responsabilidades.

El bloqueo de los datos personales, se realizará tomando en cuenta los plazos de conservación previstos en el Catálogo de Disposición Documental del Instituto Nacional Electoral que corresponda, tomando en cuenta el momento en que inició el tratamiento de los datos personales y el último uso de los mismos.

Durante el periodo de bloqueo, los datos personales no serán objeto de tratamiento, salvo disposición expresa de una ley o que exista una resolución judicial, orden o mandato, fundado y motivado, de autoridad competente.

El bloqueo de datos personales deberá realizarse tomando en cuenta los medios de almacenamiento físicos y/o electrónicos en los que se encuentran la información.

En el Anexo 2 se establecerán los procedimientos que los Órganos del Instituto llevarán a cabo para realizar el bloqueo en su caso, y supresión de los datos personales.

8.2 PROCEDIMIENTO DE BLOQUEO EN MEDIO DIGITALES

I. Las áreas propietarias de la información con apoyo de las áreas custodias, deben considerar una de las siguientes opciones:
    a. Trasladar temporalmente los datos seleccionados a otra base de datos.
    b. Aplicar técnicas de enmascaramiento de datos del registro(s) seleccionado(s) o de la base de datos.
    c. Cifrar la información del registro(s) seleccionado(s) o de la base de datos.
II. Impedir el acceso de usuarios a los datos personales seleccionados.
III. Si los datos se encuentran publicados en internet, retirarlos temporalmente.
IV. Indicar claramente, en el sistema informático y sus bases de datos, que los datos que se pretenden tratar se encuentran limitados en su tratamiento.
V. Establecer herramientas, procedimientos y protocolos que garanticen la autenticación, autorización y registro del acceso a las bases de datos (*Authentication, Authorization, Accounting-AAA*) que contengan datos bloqueados.

9 REVISIONES PERIÓDICAS PARA LA CONSERVACIÓN DE LOS DATOS PERSONALES

La Unidad de Transparencia, en conjunto con los órganos del Instituto y con el apoyo de los órganos especializados que aquella estime pertinentes, llevarán a cabo una revisión periódica de los procedimientos, métodos y técnicas para la conservación, bloqueo en su caso y supresión de los datos personales, cuyos resultados serán presentados ante el Comité de Transparencia.

10 MATERIAL DE APOYO

La Unidad de Transparencia, en conjunto con los órganos especializados, desarrollará el material de apoyo (manuales, guías, y cualquier otro que resulte necesario) para la implementación de los procedimientos enunciados en el presente documento.

11 ANEXOS

11.1 ANEXO I. CATEGORIZACIÓN DELOS DATOS PERSONALES Y VALOR DE RIESGO ASOCIADO

11.1.1 Clasificación por tipo de dato personal

De acuerdo al INAI, los datos se clasifican en los siguientes niveles (INAI, 2015):

I. **Estándar**. Datos de **identificación y contacto, laborales y académicos**, como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.
II. **Sensible.** Contempla los siguientes datos:

a. **De Ubicación física** de la persona, como la dirección física, relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más (dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.).
b. **De patrimonio**. Todos aquellos que permitan inferir el patrimonio de una persona, incluye entre otros, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, número de tarjeta bancaria de crédito y/o débito.
c. **De autenticación,** información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.
d. **Jurídicos,** como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
e. Todos aquellos que afecten la esfera más íntima de su titular, es decir, los que puedan dar **origen a discriminación** o conlleven un **riesgo grave a la integridad del titular**, como revelar aspectos del origen racial o étnico, estado de salud, pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales, entre otros.

III. Especial. Son todos los datos que, debido a su naturaleza o bien debido a un cambio excepcional en el contexto de las operaciones usuales, pueden causar daño directo a los titulares, como información adicional de la tarjeta bancaria -número de tarjeta de crédito o débito más cualquier otro dato relacionado o contenido en la misma (fecha de vencimiento, código de seguridad, datos de la banda magnética, número de identificación personal PIN)-.

NOTA. Lo anterior es sólo una guía ya que, como lo señala el INAI, es posible que ciertos datos personales que, en principio no se consideran sensibles, pueden llegar a serlo dependiendo del contexto en el que la información sea tratada.

11.1.2 Identificación del nivel de riesgo

Posteriormente, se identifica el resigo inherente a los datos de acuerdo a su criticidad (INAI, 2015):

II. **Bajo**. Considera información general como datos de identificación y contacto o información académica o laboral.
III. **Medio**. Contempla los datos:
    a. De ubicación física,
    b. De patrimonio,
    c. De autenticación,
    d. Jurídicos.
IV. **Alto**. Datos personales que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular.
V. **Reforzado**. Son **todos los considerados *datos especiales***.

11.2 Anexo II. Técnica de eliminación por tipo de medio

11.2.1 Medios físicos

	Limpiar	Purgar	Destruir
Papel	NA	NA	Destrucción del papel mediante trituradoras de corte transversal que produzcan partículas de 1mmx5mm o menores o pulverizar/desintegrar materiales de papel utilizando dispositivos desintegradores equipados con una pantalla de seguridad de 2.4 mm.
Microfilms, microfichas o negativos	NA	NA	Incinerar.

11.2.2 Medios digitales

	Limpiar	Purgar	Destruir
Medios Magnéticos			
Floppies	Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a través de un software aprobado por el Instituto.	Desmagnetizar el medio en un desmagnetizador aprobado por el Instituto.	Incineración de los discos o triturar con un proveedor con licencia.
Discos magnéticos (externos o internos)	Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a	Desmagnetizar el medio en un desmagnetizador aprobado por el Instituto.	Incineración de los discos o triturar con un proveedor con licencia.

	Limpiar	Purgar	Destruir
	través de un software aprobado por el Instituto.		
Cintas magnéticas con formato de carrete y cassette	Re-grabar todos los datos en la cinta usando un patrón aprobado por el Instituto, utilizando un sistema con características similares con el que originalmente fueron grabados los datos.	Desmagnetizar el medio en un desmagnetizador aprobado por el Instituto.	Incineración o triturar las cintas a través de un proveedor con licencia.
Discos duros ATA	Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a través de un software aprobado por el Instituto.	Si el medio lo soporta, emplear alguna de las siguientes opciones: 1. Usar alguno de los siguientes comandos de ATA Sanitize Device: a. Utilizar el comando de sobre-escritura EXT. b. Si el dispositivo soporta borrado criptográfico, utilizar el comando CRYPTO SCRAMBLE EXT. 2. Ejecutar el comando SECURE ERASE UNIT. 3. Ejecutar el borrado criptográfico a través de la interface de Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) o Enterprise SSC.	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia.

	Limpiar	Purgar	Destruir
		4. Desmagnetizar el medio en un desmagnetizador aprobado por el Instituto. Referirse a TCG y a los fabricantes de los dispositivos para mayor referencia.	
Discos duros SCSI	Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a través de un software aprobado por el Instituto.	Si el medio lo soporta, emplear alguna de las siguientes opciones: 1. Utilizar acciones de SCSI SANITIZE: a. Ejecutar el comando SANITIZE del servicio OVERWRITE. Una sobre-escritura simple de ceros o un patrón pseudo-aleatorio es suficiente. b. Ejecutar el comando SANITIZE del servicio CRYPTOGRAPHIC ERASE Referirse a TCG y a los fabricantes de los dispositivos para mayor referencia.	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia.
Medios ópticos			
CD, DVD,BD	NA	NA	Se recomienda la destrucción a través de alguno de los siguientes métodos: 1. Eliminar las capas portadoras de información de medios de CD

	Limpiar	Purgar	Destruir
			usando un dispositivo abrasivo comercial de disco. Esta opción sólo aplica a CD, no así a DVD o BD. 2. Incinerar el disco óptico a cenizas, usando proveedores autorizados. 3. Utilizar dispositivos de desintegración o trituración de discos ópticos, que permita reducir las partículas a 0.5 mm^2 o más pequeñas.
Dispositivos de almacenamiento basados en memoria flash			
Dispositivo de Estado Sólido ATA (SSD)	Seleccionar alguno de los siguientes métodos: 1. Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a través de un software aprobado por el Instituto. 2. Si el dispositivo lo soporta, utilizar el conjunto de comandos SECURITY ERASE UNIT.	Seleccionar una de las opciones: 1. Aplicar alguno de los comandos de *ATA sanitize*: a. Comando de borrado por bloques (*BLOCK ERASE*). b. Comando de borrado criptográfico (*CRYPTOGRAPHIC ERASE*, conocido también como *CRYPTO SCRAMBLE*). 2. Borrado criptográfico (CRYPTOGRAPHIC ERASE) a través de la interfaz de *TCG Opal SSC* o *Enterprise SSC*.	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia.

	Limpiar	Purgar	Destruir
		Referirse a TCG y a los fabricantes de los dispositivos para mayor referencia	
Dispositivo de Estado Sólido SCSI (SSSD)	1. Sobre-escribir el medio con, al menos, un algoritmo de nivel 6 (3 pasadas de sobre-escritura), a través de un software aprobado por el Instituto.	Seleccionar una de las dos opciones: 1. Si el medio lo soporta, aplicar el comando SCSI SANITIZE, a través de la ejecución de alguno de las siguientes opciones: a. Ejecutar el comando SANITIZE con el servicio BLOCK ERASE. b. Si el dispositivo soporta cifrado, aplicar el servicio CRYPTOGRAPHIC ERASE 2. Borrado criptográfico (*CRYPTOGRAPHIC ERASE*) a través de la interfaz de *TCG Opal SSC* o *Enterprise SSC*. Referirse a TCG y a los fabricantes de los dispositivos para mayor referencia	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia.
Memorias Flash embebidas en tableros y dispositivos **(incluye tarjetas madre y tarjetas de periféricos ,como adaptadores de**	Si el dispositivo lo soporta, reiniciarlo a las configuraciones de fábrica en su estado original.	NA. Si se puede identificar y remover, la memoria debe ser destruida.	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia.

	Limpiar	Purgar	Destruir
red o cualquier adaptador que contiene memoria flash no volátil)			
Dispositivos de almacenamiento basados en RAM y ROM			
Memoria de Acceso Aleatorio Dinámico (DRAM)	Apagar el dispositivo, remover la fuente de energía, remover la batería (en caso de tenerla). Como alternativa, remover la DRAM del dispositivo. La DRAM debe permanecer sin energía por un periodo de al menos cinco minutos	Aplicar los mecanismos especificados en el apartado Limpiar.	Triturar, desintegrar o pulverizar.
PROM Alterable Electrónicamente (EAPROM)	Realizar una purga completa del chip según la hoja de datos del fabricante	Aplicar los mecanismos especificados en el apartado Limpiar	Triturar, desintegrar o pulverizar.
PROM Borrable Electrónicamente (EEPROM)	Sobre-escribir el medio mediante el uso de software de sobre-escritura aprobado por el Instituto.	Aplicar los mecanismos especificados en el apartado Limpiar.	Triturar, desintegrar, pulverizar, o incinerar a través de un proveedor con licencia

11.3 ANEXO III. CERTIFICADO DE ELIMINACIÓN DE DATOS

Certificado de eliminación de datos	
Datos del personal que ejecuta la eliminación de datos	
Nombre completo:	Puesto/Área:
Localización:	Teléfono:
Información del medio	
Fabricante:	Número de modelo:
Número de serie:	Número de inventario:
Tipo de medio:	Origen:
Clasificación:	Dueño de los datos que contiene el medio:
Datos respaldados: □ Sí □ No □ Se desconoce	Localización del respaldo:
Detalles de la eliminación	
Tipo de método □ Limpieza □ Purga □ Destrucción	
Método aplicado □ Desmanetización □ Sobre-escritura □ Borrado por bloques □ Borrado criptográfico □ Otro. Especifique:	
Detalle del método aplicado:	
Herramienta utilizada (incluir número de versión):	
Verificación del método □ Completo □ Por muestreo □ Otro	
Clasificación del medio posterior a la eliminación de los datos:	
Observaciones:	
Destino del medio	
□ Reuso interno □ Reuso externo □ Instalaciones de reciclaje □ Fabricante □ Otro. Especifique:	
Validación	
Nombre completo:	Puesto/Área
Localización	Teléfono
Fecha	
Firmas	

Ejecución	Validación
_____	_____
Nombre y firma	Nombre y firma

Autorización

_____

Nombre, cargo y firma

12 REFERENCIAS

Feldman, L., & Witte, G. (5 de February de 2015). *NIST SP 800-88, Revision 1: Guidelines for Media Sanitization.* Obtenido de National Insitute of Standars and Technology: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

INAI. (Junio de 2015). *Guía para implentar un Sistema de Gestión de Seguridad de Datos Personales.* Recuperado el 20 de Mayo de 2018, de INAI: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

INAI. (Junio de 2015). *Metodología de Análisis de Riesgo BAA.* Recuperado el 25 de mayo de 2018, de INAI: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf