Instituto Nacional de Medicina Genómica
20 AÑOS INMEGEN 2004 – 2024

Política para el Borrado Seguro de Datos INMEGEN

INSTITUTO NACIONAL DE MEDICINA GENÓMICA

2024

Contenido

GLOSARIO

Activos de TIC: Los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Aplicativo de Cómputo: El software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo a requerimientos previamente definidos.

Borrado Seguro: El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.

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. Art. 3 fracción IX LGPDPPSO.

Documento Electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.

Información Pública: Toda información generada, obtenida, adquirida, transformada o en posesión de sujetos obligados. Art. 4 LGTAIP

Información Reservada: Es aquella información que se encuentra prevista en alguna de las causales de los artículos 113 LGTAIP y 110 LFTAIP.

Información Confidencial: Es la información que contiene los datos personales de una persona identificada o identificable. Art. 166 LGTAIP.

INMEGEN: Instituto Nacional de Medicina Genómica.

LFTAIP: Ley Federal de Transparencia y Acceso a la Información Pública.

LGTAIP: Ley General de Transparencia y Acceso a la información Pública.

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

Medios de almacenamiento: Todo dispositivo para en el cual se puede leer y escribir información con el propósito de almacenarla permanentemente o no, pueden ser tipo ópticos, magnéticos, electrónicos o en la nube.

Medio óptico: Dispositivo de almacenamiento como los CD's, DVD's, BluRay.

Medio magnéticos: Dispositivo de almacenamiento como los discos rígidos, cintas magnéticas, diskettes.

Medio electrónicos: Dispositivo de almacenamiento como los discos de estado sólido (SSD por sus siglas en inglés), memorias de estado sólido USB, tarjeta digital segura (SD).

Medio de almacenamiento en la nube: Servicio que permite almacenar datos transfiriéndose a través de Internet o de otra red a un sistema de almacenamiento que mantiene el proveedor del servicio.

Medio Extraíble: Todo dispositivo que permita almacenar o transportar información, como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos.

Espacio de Trabajo: Lugar dispuesto para que los usuarios realicen las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.

Responsable de la información: El servidor público que para el desempeño de empleo, cargo o comisión brinda tratamiento.

Responsable del borrado seguro: El personal designado para atender la solicitud de borrado seguro quien deberá generar evidencia auditable del proceso de borrado seguro.

Responsable de datos personales: Son los sujetos obligados por la Ley General de Protección de Datos Personales en posesión de sujetos obligados que deciden sobre determinado tratamiento de datos personales.

Introducción:

El borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos, de modo que la probabilidad de recuperarlos sea mínima, el proceso de borrado seguro consiste en sobrescribir al menos una vez con un valor definido, por ejemplo 0, la información almacenada en el medio.

Por lo que resulta importante el establecimiento de una eliminación adecuada de los medios de almacenamiento en desuso de los datos, porque representa una medida de seguridad efectiva para minimizar las fugas y/o el mal uso de los datos personales por parte de una persona mal intencionada, o no autorizada.

Normatividad Aplicable

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Archivos
- Ley General de Responsabilidades Administrativas
- Ley Federal de Entidades Paraestatales
- Ley de los Institutos Nacionales de Salud
- Lineamientos Generales de Protección de Datos Personales para el
- Sector Público
- Estatuto Orgánico del Instituto Nacional de Medicina Genómica.
- Políticas y Disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal
- Documento de Seguridad de Datos Personales del Instituto Nacional de
- Medicina Genómica
- Reglas internas de uso de software, equipos y servicios de cómputo.
- Reglas de propiedad intelectual del Instituto Nacional de Medicina Genómica.
- Código de Ética del Instituto Nacional de Medicina Genómica.

Objetivo

Establecer las obligaciones, atribuciones y procedimiento para el borrado seguro.

Alcance

Toda la información o medio de almacenamiento digital del Instituto Nacional de Medicina Genómica.

1. Descripción

Para completar el ciclo de vida de la información es necesario pasar por el proceso de destrucción o eliminación de la misma.

Se deberán utilizar métodos de borrado seguro para garantizar que la información y/o los medios que la contienen o almacenan no se puedan recuperar, para ello se implementarán procedimientos específicos según tecnología y clasificación de la información a ser eliminada.

En todos los casos de destrucción electrónica, se debe borrar la información original, todas sus copias y sus respectivos respaldos de seguridad. En el caso de la destrucción impresa se deberán eliminar todas las copias y respaldo existentes.

Durante la destrucción de la información, se deberá velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a su divulgación y acceso.

2. Gestión de soportes adecuada:

Se realizará un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el INMEGEN.

Se llevará a cabo la supervisión de los dispositivos que almacenen las copias de seguridad de estos datos, de acuerdo con las leyes, normativas, procesos y procedimientos vigentes (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).

Controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, entre otros.

En los traslados de los dispositivos de almacenamiento a instalaciones externas al INMEGEN se deberá asegurar que se cumpla la cadena de custodia de los mismos, para evitar fugas de información.

3. Registro de las operaciones de borrado

Deberá existir una solicitud formal indicando los medios o información a destruir dirigida al propietario del activo. La solicitud debe identificar en forma unívoca al medio o la información que requiere destrucción.

Al seleccionar una herramienta de borrado, se deberá elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.

El propietario del activo y la persona responsable de su destrucción deberá tomar en cuenta los decretos, leyes u otra normativa vigente y evaluar si corresponde la destrucción de dicha información.

En cada proceso de destrucción se deberá generar un reporte de actuación que identifique al personal actuante y la metodología empleada para la destrucción de la información, así como las observaciones que éste considere pertinente. Se deberá identificar claramente que el proceso se ha efectuado.

Si la destrucción no se puede realizar correctamente, por ejemplo, por falla en la destrucción de la información contenida en un medio lógico, entonces esta situación deberá quedar documentada y deberá utilizar otros medios de destrucción, como por ejemplo físicos, para asegurar la adecuada destrucción del medio.

4. Gestión adecuada del soporte

Deberá realizarse un adecuado control y mantenimiento de los dispositivos de acuerdo con las leyes, normativas, procesos y procedimientos vigentes: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En caso de traslados de soportes físicos, lógicos y/o información almacenada externa a "La Organización", se deberá asegurar el cumplimiento de la cadena de custodia de los mismos, para evitar fugas de información.

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

Medios de almacenamiento físico
Los medios de almacenamiento físico 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.

Podemos considerar entre estos medios:

1) Archiveros
2) Gavetas
3) Cajones
4) Bodegas
5) Estantes
6) Oficinas

Medios de almacenamiento electrónico
Los medios de almacenamiento electrónico, es 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 los datos personales.

Podemos considerar entre estos medios:

Medios magnéticos
- Discos duros internos (tanto los propios del equipo de cómputo como los portátiles)
- Disco duro externo o portátil
- Cintas magnéticas

Medios ópticos
- CD's,
- DVD's
- Blu-rays entre otros.

Medios de estado sólido
- Memorias USB
- Disco duro SD.
- Servicios de almacenamiento en línea.

9. Destrucción errónea de medios de almacenamiento físico

La destrucción manual: Romper archivos y documentos a mano, con tijeras o rasgarlos con un cúter es un método inseguro para desechar este tipo de activos. Este método permite que una persona mal intencionada pueda recuperar los fragmentos de la basura y los ensamble a modo de rompecabezas para extraer información importante.

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.

10.- Destrucción errónea de medios de almacenamiento electrónico

Los sistemas operativos de los equipos de cómputo o dispositivos ordenan la información en archivos dentro de sus medios de almacenamiento (por ejemplo, en un disco duro). Para encontrar estos archivos en el espacio correspondiente, el sistema operativo acude a la "lista de archivos", donde se indica tanto el nombre del archivo como su ubicación dentro del espacio de almacenamiento.

Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo, la eliminación se realiza exclusivamente en la "lista de archivos" sin que se borre realmente el contenido del archivo que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo. Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la "lista de archivos" como del contenido del mismo, no consigue destruir eficazmente dicha información de forma específica:

Los comandos de borrado por defecto de los sistemas operativos: Cuando se utiliza un comando o el botón de "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".

"Formatear": Cuando se formatea un medio de almacenamiento, se eliminan 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.

¿Cómo borrar de manera segura los datos personales?

La destrucción y borrado de información es un tema de vital importancia para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los datos

personales, por esta razón, los sujetos obligados deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren.

Las técnicas de borrado seguro 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 para este tipo de destrucción 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.

A continuación, se detallan los diferentes métodos de Borrado Seguro, a fin de que los responsables de borrado seguro puedan seleccionar aquéllos que mejor se ajusten a sus necesidades.

<table>
<tr><th colspan="4">Métodos para el Borrado Seguro de los Datos Personales</th></tr>
<tr><td colspan="2">Métodos Físicos</td><td colspan="2">Métodos Lógicos</td></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 almacenados</td></tr>
<tr><td>Destrucción de los medios de almacenamientos físicos</td><td>Destrucción de los medios de almacenamientos electrónicos</td><td>Desmagnetización</td><td>Sobreescritura</td></tr>
</table>

11. - Métodos Físicos de Borrado

Los Métodos Físicos son aquellos que implican un daño irreversible o la destrucción total de los medios de almacenamiento, tanto físico como electrónico.

Destrucción de los medios de almacenamiento físico

Dentro de las técnicas de destrucción para los medios de almacenamiento físico se encuentran:

1) Trituración

Uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivos, es la trituración.

Las principales características que se deben considerar para la adquisición de una trituradora son el tipo y tamaño del corte o "partícula", así como la capacidad de la trituradora.

Considerando el tipo de corte, existen dos tipos principales 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 los fragmentos.

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

La norma DIN 32757 es un estándar que se ha adoptado a nivel mundial para la destrucción de documentos, creada por el Instituto Alemán para la Estandarización. Esta norma establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de la criticidad de la información.

Además, de acuerdo con la Guía para el SGSDP10 se sugiere 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.

A continuación, se ofrecen ejemplos de categorías para los sistemas de tratamiento de datos personales según su riesgo inherente:

a) Nivel estándar

Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal 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.

b) Nivel sensible

Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país.

También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los 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 y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito.

Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos jurídicos tales 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.

Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como 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 y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

c) Nivel especial

Esta categoría corresponde a los 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 los titulares, por ejemplo la Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las categorías antes descritas de la Guía para el SGSDP son sólo una orientación, ya que el Pleno del INAI no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles o de alto riesgo, podrían llegar a serlo dependiendo del contexto en que se trate la información.

En la tabla siguiente se muestra una relación entre el nivel de seguridad que se debe utilizar para destruir documentos, de acuerdo a la norma DIN 32757, dependiendo de la clasificación asignada a cada medio de almacenamiento en los sistemas de tratamiento.

Nivel de riesgo por sistema de tratamiento	Nivel del estándar	Tamaño máximo del fragmento	Tipo de documento
No recomendable	1. General	Tiras de 12 mm de ancho.	Documentos generales que deben hacerse ilegibles.
No recomendable	2. Interno	Tiras de 6 mm de ancho	Documentos internos que deben hacerse ilegibles.
Estándar	3. Confidencial	Tiras de 2 mm de ancho.	Partículas de 4x80 mm. Documentos confidenciales.
Sensible	4. Secreto	Partículas de 2x15 mm.	Documentos de importancia vital para la organización que deben mantenerse en secreto.
Especial	5. Alto Secreto	Partículas de 0.8x12 mm.	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas.

En general, para la protección de los datos personales, se recomienda utilizar la clasificación que sugiere la Guía para el SGSDP, respecto a los sistemas de tratamiento de datos personales según su riesgo inherente, en combinación con la norma DIN 32757, o cualquier otro estándar internacional o mejores prácticas en la materia.

2) Incineración

La incineración de medios de almacenamiento físico consiste en 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 recomendable por temas ecológicos.

b) Destrucción de los medios de almacenamiento electrónicos

La destrucción de medios de almacenamiento electrónico utiliza técnicas tales como:

- **Desintegración.** Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
- **Trituración o Pulverización.** Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas.
- **Abrasión.** Acción de arrancar, desgastar o pulir algo por rozamiento o fricción.
- **Fundición o Fusión.** Paso de un cuerpo del estado sólido al líquido por la acción del calor.

La destrucción de medios de almacenamiento electrónico tiene el carácter de un proceso industrial robusto, por lo que a la mayoría de las organizaciones les puede resultar más práctico la subcontratación del servicio, además de que la eliminación definitiva del activo puede contar con opciones de tratamiento de desperdicios y de reciclaje para hacer que el proceso sea más amigable con el ambiente.

Cuando se trate de un proceso más pequeño, por ejemplo, el de desechar un disco duro del equipo personal, es recomendable aplicar algún método lógico (que se verán en la siguiente sección) y posteriormente realizar una destrucción minuciosa del dispositivo (por ejemplo, haciendo varios hoyos en el dispositivo con un taladro), antes de enviarlo a un centro de reciclaje o depositarlo en algún contenedor genérico de "basura electrónica".

Métodos lógicos de Borrado

Los métodos lógicos son aquellos que implican la sobreescritura o modificación del contenido del medio de almacenamiento electrónico.

a) Desmagnetización

Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizado. 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 a utilizar 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 equipo necesario para este proceso, suele utilizarse bajo un esquema de contratación del servicio.

b) Sobreescritura

Consiste en sobrescribir todas las ubicaciones de almacenamiento 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 sobreescritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobreescrituras o "pasadas" con variaciones en los caracteres grabados al medio de almacenamiento.

Una ventaja particular de la sobreescritura es que las herramientas se pueden utilizar para borrar un archivo o carpeta específica, sin necesidad de alterar o detener la operación de todo un medio de almacenamiento o equipo de cómputo.

Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política regulada en el presente documento, El director podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

Responsabilidades

De conformidad con el artículo 3 fracción XXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los servidores públicos del INMEGEN que traten datos personales en el ejercicio de sus funciones y de las atribuciones de la Unidad Administrativa a la que se encuentran adscritos observarán al menos las medidas de seguridad técnicas siguientes:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware y
d) Gestionar comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En ese sentido, se informa que las responsabilidades de los servidores públicos involucrados son:

1. Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
2. Verificar que el inventario de datos personales y los sistemas de tratamiento de los mismos, a los que tienen acceso se encuentren actualizados.
3. Identificar a los servidores públicos que acceden a los datos personales.
4. En caso de presentarse algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento, informar dicho incidente a la Unidad de Transparencia.
5. Llevar a cabo las medidas de seguridad administrativas, físicas y técnicas para la protección de los datos personales.
6. Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

Anexo Formato de solicitud de borrado seguro

Fecha: _____ **Cantidad de bienes: _____**

Marcar con una X el tipo de borrado que se requiere:

1. **Sistemas Windows.**
   - **a.** _____ Borrado parcial (carpetas)
   - **b.** _____ Borrado total (formato bajo nivel)
2. **Sistemas MAC.**
   - **a.** _____ Borrado parcial (carpetas)
   - **b.** _____ Borrado total (formato bajo nivel)
3. **Sistemas Linux.**
   - **a.** _____ Borrado parcial (carpetas)
   - **b.** _____ Borrado total (formato bajo nivel)
4. **Borrado en dispositivo externo.**
   - **a.** ___ Electrónico
   - **b.** ___ Magnético
   - **c.** ___ Óptico
   - **d.** ___ Nube

Área solicitante	**Área que atiende**
Nombre, firma y cargo	**Nombre, firma y cargo**