BORRADO SEGURO DE DATOS PERSONALES

1. Objetivo

Establecer los procedimientos necesarios para el bloqueo y borrado seguro de los datos personales en posesión del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., que han cumplido los plazos de conservación, dejaron de ser necesarios para el cumplir de las finalidades previstas en Aviso de Privacidad, o bien para garantizar al titular el ejercicio de sus derechos de cancelación u oposición al tratamiento de datos personales.

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

2. Alcance

Las disposiciones previstas en este procedimiento son de carácter obligatorio para todo el personal que integra esta Sociedad Nacional de Crédito.

3. Políticas Particulares

Los datos de expedientes que causen baja, es decir, que su destino final sea la eliminación, se deberán eliminar también dichos expedientes en su formato electrónico y/o digital, siempre y cuando exista un dictamen y acta de baja documental emitido por el Archivo General de la Nación para el formato físico.

- ***BLOQUEO DE LOS DATOS PERSONALES***

CONSIDERACIONES GENERALES
Una vez cumplida la finalidad para la cual fueron recabados los datos personales, las Unidades Administrativas que integran Banjercito 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, las Unidades Administrativas de Banjercito 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, de conformidad con el catálogo de disposición documental vigente**.*

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 de Banjercito vigente, 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.

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

- ***PROCEDIMIENTO DE BLOQUEO EN MEDIOS DIGITALES***

I. *Las Unidades Administrativas generadoras de la información con apoyo de la Dirección de Tecnologías de la Información y Comunicaciones, así como del Oficial en Jefe de Seguridad de la Información, deben considerar una de las siguientes opciones o en su caso el medio que estas consideren para llevar a cabo lo siguiente:*

   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.*

- ***SUPRESIÓN DE LOS DATOS PERSONALES***

Transcurrido el periodo de bloqueo, las Unidades Administrativas de Banjercito 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, las Unidades Administrativas de Banjercito, 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 General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.*

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

- ***CONSIDERACIONES PARA LA ELIMINACIÓN EN MEDIOS DIGITALES***

Las Unidades Administrativas responsable de los datos personales en su posesión, con apoyo de la Dirección de Tecnologías de la Información y Comunicaciones, así como del Oficial en Jefe de Seguridad de la Información, deben 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, o en su caso el medio que estas consideren para llevar acabo lo siguiente:

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.*

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

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 de la Dirección de Tecnologías de la Información y Comunicaciones 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.

- ***PROCEDIMIENTO DE SUPRESIÓN EN MEDIOS ELECTRÓNICOS***

Las Unidades Administrativas responsables de los datos personales deben:

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 Banco****. Debido a que implica si el Banjercito 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.*

- ***TÉCNICAS DE ELIMINACIÓN DE DATOS PERSONALES***

En medios Digitales.

Las Unidades Administrativas generadoras de la información con apoyo de la Dirección de Tecnologías de la Información y Comunicaciones, así como del Oficial en Jefe de Seguridad de la Información, deben considerar una de las siguientes opciones o en su caso el medio que estas consideren para llevar acabo lo siguiente:

- ***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.*

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

- ***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.*

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.*

- ***MÉTODOS DE VERIFICACIÓN***

La Unidad de Transparencia, a través del Oficial de Protección de Datos Personales, en conjunto con la Dirección de Tecnologías de la Información y Comunicaciones y el Oficial en Jefe de Seguridad de la Información, verificará 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.*

- ***DOCUMENTACIÓN***

Para los datos personales contenidos en medios digitales:

Independientemente de la técnica aplicada en la eliminación de los datos personales las Unidades Administrativas responsables de los datos personales, deben generar un ***certificado (Anexo I)*** *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).*

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

- *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.*

Para los datos personales contenidos en medios impresos:

Se debe cumplir con lo indicado en los procedimientos de destrucción de documentos (expedientes) establecidos en el Manual Administrativo de Aplicación General en Materia de Archivos de la Subdirección de Gestión Documental.

- ***SELECCIÓN DEL MÉTODO DE ELIMINACIÓN BASADO EN EL NIVEL DE RIESGO***

El nivel de riesgo de los datos personales se determina con base en lo siguiente:

Las variables que el Oficial de Protección de Datos Personales tomará en consideración serán los criterios de sensibilidad por dato personal, siendo los siguientes:

Muy alto: *Los datos de mayor riesgo son aquellos que de acuerdo con su naturaleza derivan en mayor beneficio para un atacante en caso de obtenerlos, por ejemplo: información adicional de tarjeta bancaria (fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal PIN).*

Alto: *Esta categoría de datos contempla a los datos personales sensibles, tales como:*

- *Datos de salud*
- *Filosóficas y morales*
- *Información genética*
- *Afiliación sindical*
- *Origen racial o étnico*
- *Opiniones políticas*
- *Ideología*
- *Preferencia sexual*
- *Creencias religiosas*
- *Hábitos sexuales*
- *Cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.*

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

Medio: *Se incluyen los datos que permiten conocer la ubicación física de la persona, datos patrimoniales, de autenticación con información referente a los usuarios como son las contraseñas, además se incluye en este rubro la información biométrica, datos jurídicos y de la tarjeta bancaria.*

Bajo: *Integra los datos de identificación y contacto o información académica o laboral.*

Una vez identificado el riesgo, la Unidad Administrativa en conjunto con la Dirección de Tecnologías de la Información y Comunicaciones, así como el Oficial en Jefe de Seguridad de la Información y el Oficial de Protección de Datos Personales, seleccionará el método adecuado para eliminar la información contenida en el medio, considerar ando una de las siguientes opciones o en su caso el medio idóneo que estas consideren:

Identificación de la técnica de eliminación de datos personales con base en el nivel de riego.				
Nivel de riesgo	*El medio no permanecerá en Banjercito*		*El medio permanecerá en Banjercito*	
	Reutilizado	*No reutilizado*	*Reutilizado*	*No reutilizado*
Bajo	*Purgar*	*Purgar*	*Limpiar*	*Limpiar*
Medio	*Purgar*	*Destruir*	*Purgar*	*Destruir*
Alto	*Destruir*	*Destruir*	*Purgar*	*Destruir*
Muy alto	*Destruir*	*Destruir*	*Destruir*	*Destruir*

VERIFICACIÓN
La Unidad de Transparencia, a través del Oficial de Protección de Datos personales, en conjunto con personal designado por la Dirección de Tecnologías de la Información y Comunicaciones, así como del Oficial en Jefe de Seguridad de la Información llevarán a cabo una revisión anual 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.

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772

- CERTIFICADO DE ELIMINACIÓN DE DATOS PERSONALES

Una vez que se apruebe la eliminación de datos personales deberá emplearse el siguiente formato para documentar la misma:

Anexo I. Certificado de Eliminación de Datos Personales	
Fecha de Eliminación: ***DD/MM/AAAA***	*Numero de Control:* ***(Número asignado por la Unidad de Transparencia).***
Datos del personal que ejecuta la eliminación de datos	
Nombre completo:	*Cargo:*
Área:	*No. de empleado:*
Información del medio (Software o hardware donde se encuentra la información	
Nombre del medio de almacenamiento (carpeta, sistema, programa, archivo):	*Datos respaldados: No( ) Si( )* *Se desconoce( )*
Detalles de la eliminación	
Datos personales contenidos en el documento:	*Tipo de método:* *Desintegración( )* *Destrucción( )* *Fusión e incineración( )* *Trituración( )* *Purga( )* *Limpieza( )*
Herramienta empleada (número de versión):	*Sitio y hora de la destrucción:*
Verificación del método: *Completo( )* *Por muestreo( )* *Otro( )*	*Clasificación del medio posterior a la eliminación de datos:*
Observaciones:	
Destino del medio	
Reusó interno( ) Reusó externo( ) Reciclaje( ) ( ) Desecho	
Firmas	
Nombre y firma del Titular de la Unidad de Transparencia	*Nombre y firma del personal de la Unidad Administrativa dueña de la información.*
Nombre y firma del personal del Órgano Interno de Control	*Nombre y firma de Personal de la Unidad de Transparencia*
Nombre y firma del personal de la Gerencia de Coordinación de Archivos	

Av. Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, Ciudad de México, C.P. 11200, www.gob.mx/banjercito
Conmutador: (55) 5626 0500 y (55) 5557 9188 Fax: (55) 5557 8821 Banjetel: (55) 5328 2354 y 800 712 3772