

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	1 de 6

1. OBJETIVO

Establecer los lineamientos, métodos, controles y pasos para realizar la eliminación segura (sanitización) de la información contenida en los activos de TI de la Contaduría General de la Nación (CGN), así como en los medios de almacenamiento que se encuentren en proceso de reasignación, reintegro, sustitución o baja administrativa (dispuestos como residuos de aparatos eléctricos y electrónicos (RAEE) con el fin de asegurar que la información no pueda ser recuperada por personal no autorizado que emplee técnicas convencionales o especializadas y así mantener la integridad, confidencialidad y disponibilidad de la información, reduciendo el riesgo de recuperación de datos por personal no autorizado. Así como, proteger la información clasificada y/o reservada almacenada en estos medios, evitando que quede expuesta a terceros y pueda ser utilizada de manera perjudicial para la imagen de la entidad o con fines lucrativos.

2. ALCANCE

Aplica a todos los medios de almacenamiento de información de la entidad, propios o arrendados, independientemente de su tecnología: discos duros magnéticos (HDD), unidades de estado sólido, memorias USB, tarjetas de memoria, medios ópticos, cintas magnéticas, discos de servidores y arreglos de almacenamiento (RAID). También para el caso de los equipos de seguridad perimetral (firewall, WAF) y dispositivos de red que cuenten con sistema de almacenamiento interno.

Su cumplimiento es obligatorio para servidores públicos, y contratistas que intervengan en la sanitización o destrucción de los medios de almacenamiento de la CGN.

3. DEFINICIONES

Sanitización: Proceso mediante el cual se hace inviable la recuperación de la información contenida en un medio de almacenamiento, para un nivel de esfuerzo determinado. Comprende las categorías Eliminación, Purga y Destrucción.

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	2 de 6

Categorías de sanitización: Eliminación (Clear): sobrescritura del espacio direccionable, impide la recuperación con software convencional. Purga (Purge): técnicas que impiden la recuperación incluso en laboratorio. Destrucción (Destroy): inutilización física del medio.

Sobrescritura: Escritura de patrones de datos sobre el área direccionable del medio para reemplazar la información previamente almacenada.

Comando de sanitización del firmware: Función del fabricante que borra el medio de forma integral (ATA Secure Erase, ATA/NVMe Sanitize), incluidas las áreas no direccionables por el sistema operativo.

Borrado criptográfico (Crypto Erase): Destrucción segura de la clave de cifrado del medio, que deja ilegible la información. Requiere que el medio haya estado cifrado desde su puesta en servicio.

Desmagnetización (Degaussing): Exposición de un medio magnético a un campo intenso que destruye la información y por lo general inutiliza el medio. No aplica a medios de estado sólido.

Formateo rápido: Operación que solo elimina las referencias del sistema de archivos, dejando los datos recuperables mediante herramientas de recuperación de uso común. No constituye borrado seguro.

RAEE: Residuos de aparatos eléctricos y electrónicos, sujetos a gestión ambiental especializada conforme a la normatividad vigente.

4. LINEAMIENTOS

4.1. Solicitud de servicios de borrado seguro

La solicitud se gestiona en el aplicativo GLPI de mesa de servicio, utilizando el formulario Borrado seguro, cuando los activos vayan a ser reasignados, sean reintegrados, se den de baja por obsolescencia o se destinen para RAEE.

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	3 de 6

4.2. Identificación y gestión del activo

El equipo de Gestión de servicios de TI identifica el activo (marca, modelo, serial, tipo y capacidad) y determina las acciones a ejecutar sobre el activo de TI, de acuerdo con los siguientes casos:

- Traslado, reintegro o reasignación del activo de un usuario a otro.
- Activo obsoleto o disposición para RAEE.

Nota: el proceso de traslado, reintegro o reasignación de los activos debe ser solicitado por el coordinador del GIT correspondiente a través de la mesa de servicio.

Cuando un activo sea reintegrado por obsolescencia, el equipo de Gestión de Servicios de TI del GIT de Apoyo Informático deberá remitir al almacén un correo electrónico con el concepto técnico que sustente la solicitud de baja.

El concepto técnico deberá estar debidamente soportado y orientado al trámite de baja correspondiente, de conformidad con lo establecido en el procedimiento GAD-PRC19 – Baja de bienes inservibles y obsoletos.

4.3. Autorización de borrado de información

Con la aprobación de la solicitud generada en el numeral 4.1.

4.4. Selección de la herramienta

Al seleccionar una herramienta de borrado se debe elegir una que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando el resultado del proceso.

Existen algunas condiciones generales que se deben tener en cuenta a la hora de realizar borrado de información en medios de almacenamiento, donde se hace uso de técnicas y herramientas adecuadas de borrado seguro o sobre-escritura de acuerdo con la tecnología del medio de almacenamiento.

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	4 de 6

Nota: Solo se utilizarán herramientas de software (propietario o libre) que cuenten con la debida autorización y licencia, dando estricto cumplimiento a las leyes de derechos de autor.

4.5. Ejecución del borrado seguro o destrucción de la información

En caso de que se requiera reasignación del PC se realizará el proceso de borrado mediante formateo rápido o eliminación de datos, según corresponda. El usuario deberá dejar la información en una ubicación específica del equipo, la cual se le ha comunicado con anterioridad, posteriormente el equipo de Gestión de Servicios de TI realizará la copia de la información allí contenida.

Nota: el formateo rápido se utiliza considerando que los usuarios estándar no cuentan con permisos para instalar software que permita la recuperación de la información eliminada mitigando así el riesgo de restauración no autorizada de datos.

Para los casos de baja de activos, el proceso de formateo a bajo nivel lo realizará el funcionario asignado el cual deberá documentar el resultado del proceso de manera detallada dejando evidencia del procedimiento ejecutado en GLPI.

4.6. Verificación de borrado seguro

El equipo de Gestión de Servicios de TI será responsable de verificar la correcta ejecución del proceso de borrado seguro aplicado a los activos de información.

Para ello, el equipo responsable deberá adelantar las siguientes acciones:

- Validar que el método de borrado aplicado corresponda al autorizado para el tipo de activo (reasignación, baja o disposición final).
- Verificar que el medio de almacenamiento no contenga información.
- Confirmar que el proceso se haya ejecutado conforme a los lineamientos definidos por la Entidad y las buenas prácticas de seguridad de la información.

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	5 de 6

4.7. Recuperación de Datos

El equipo de Gestión de Servicios de TI, en conjunto con el equipo de seguridad de la información realizará la validación de la imposibilidad de recuperación de datos del activo mediante herramientas especializadas de recuperación de datos.

Para la ejecución de esta validación, se deberán considerar las siguientes acciones:

- Aplicar herramientas de recuperación de datos autorizadas o validadas por la Entidad.
- Intentar la recuperación de información sobre el medio de almacenamiento intervenido.
- Verificar que no sea posible acceder, reconstruir o visualizar datos previamente almacenados.

En caso de que se logre recuperar total o parcialmente información del medio de almacenamiento, se deberán ejecutar nuevamente las actividades descritas en el numeral 4.5, utilizando una herramienta de borrado diferente.

4.8. Documentar el proceso realizado

El equipo de Gestión de Servicios de TI deberá documentar de manera detallada la ejecución del proceso de borrado seguro o eliminación de la información en el aplicativo GLPI de Mesa de Servicios, garantizando la trazabilidad, integridad y disponibilidad de los registros generados durante la actividad.

Como parte de la documentación, se deberán adjuntar las evidencias que demuestren la correcta ejecución del proceso de borrado seguro y/o eliminación segura.

Una vez verificadas y almacenadas las evidencias, se procederá a retirar el activo de TI del inventario institucional mediante la eliminación de su registro en el módulo de Activos de la herramienta GLPI.

BORRADO Y/O ELIMINACIÓN SEGURA			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	SEGURIDAD DE LA INFORMACIÓN		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
08/09/2026	GTI10-INS01	03	6 de 6

4.9. Actualizar información del Activo

El equipo de Gestión de Servicios de TI envía diligenciado el formato GAD22-FOR01 Reintegro de Elementos al Almacén con las observaciones respectivas al Grupo Interno de Trabajo de Servicios Generales, Administrativos y Financieros de la Secretaría General (almacén).

5. DOCUMENTOS RELACIONADOS

- [GTI02-MAN01 Anexo Términos y Definiciones – Manual del Sistema de Gestión de Seguridad de la información y Ciberseguridad.](#)