

1. OBJETO:

Establecer los lineamientos y actividades para realizar el borrado seguro de la información de la UAESP almacenada en activos tecnológicos, garantizando su confidencialidad y evitando su recuperación posterior.

2. ALCANCE:

Este procedimiento aplica a todas las áreas de la UAESP que administren, utilicen o custodien información almacenada en activos tecnológicos y recursos digitales de la Entidad. El procedimiento comprende desde la solicitud y validación del borrado hasta su ejecución, verificación y generación de la evidencia correspondiente.

3. DEFINICIONES:

Activo de información: Cualquier elemento que tiene valor para la organización y que contiene, procesa o soporta información, incluyendo hardware, software, datos, servicios y recursos tecnológicos.

Baja de activos: Proceso administrativo y técnico mediante el cual un activo tecnológico es retirado definitivamente del inventario institucional.

Borrado común (no seguro): Proceso de eliminación de archivos mediante funciones del sistema operativo (delete, formateo rápido), que únicamente elimina referencias en el sistema de archivos sin borrar realmente los datos, permitiendo su recuperación posterior.

Borrado seguro: Proceso técnico mediante el cual la información contenida en un medio de almacenamiento es eliminada de forma irreversible, impidiendo su recuperación mediante herramientas o técnicas especializadas.

Cadena de custodia: Conjunto de procedimientos que garantizan el control, trazabilidad e integridad de los activos o medios de almacenamiento durante su traslado, manipulación, almacenamiento y destrucción.

Copia de respaldo: consiste en crear duplicados de archivos, aplicaciones o sistemas completos y almacenarlos en un lugar seguro, ya sea local, en la nube o en entornos híbridos, para poder restaurarlos en caso de pérdida, corrupción o ataque cibernético

Destrucción física: Proceso de eliminación del medio de almacenamiento mediante métodos mecánicos o físicos (tritución, pulverización, incineración), garantizando la imposibilidad de recuperación de la información.

Información personal: Cualquier información asociada a una persona natural identificada o identificable.

Información sensible: Información cuyo acceso, uso o divulgación no autorizada puede generar impactos legales, reputacionales, financieros o de seguridad para la entidad.

Log: es un archivo o base de datos donde se graban de manera cronológica todos los acontecimientos que afectan a un proceso particular, como una aplicación, un servidor o una red informática.

Medio de almacenamiento: Dispositivo físico o lógico utilizado para almacenar información, tales como discos duros, SSD, USB, cintas, almacenamiento en red o servicios en la nube.

Reasignación de activos: Proceso mediante el cual un activo tecnológico es transferido de un usuario, área o dependencia a otro, requiriendo previamente la eliminación segura de la información contenida.

Sobreescritura: Proceso de escritura de patrones de datos sobre la totalidad de la superficie de almacenamiento, con el fin de eliminar completamente la información previamente existente.

Tabla de Retención Documental (TRD): Instrumento archivístico que establece los tiempos de permanencia de la información en cada fase de su ciclo de vida y define su disposición final.

Verificación de borrado: Proceso mediante el cual se valida que la información ha sido eliminada correctamente, mediante herramientas técnicas de recuperación o auditoría.

4. NORMATIVA:

TABLA 1 NORMATIVA APLICABLE AL PROCEDIMIENTO

NUMERO	DESCRIPCIÓN
Ley 1273 del 05 de enero de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Estableciendo el marco legal para la identificación y reporte de incidentes de seguridad.
Ley 1581 del 17 de octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. Garantiza el tratamiento adecuado de la información en actividades de monitoreo, análisis y gestión de eventos de seguridad. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.
Ley 1712 del 06 de marzo de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1377 del 27 de junio de 2013	Reglamenta parcialmente la Ley 1581 de 2012, definiendo aspectos relacionados con la autorización del titular de los datos y las políticas de tratamiento

NUMERO	DESCRIPCIÓN
	de la información. Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto 1078 del 26 de mayo 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 415 del 07 de marzo de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.
Decreto 620 del 02 de mayo de 2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del párrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 338 del 08 de marzo de 2022	Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

NUMERO	DESCRIPCIÓN
Decreto 767 del 16 de mayo de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 del 11 de abril de 2016	Política nacional de seguridad digital.
CONPES 3995 del 01 de julio de 2020	Política nacional de transformación digital.
Resolución MinTIC 500 del 10 de marzo 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Resolución MinTIC 1117 del 05 de abril de 2022	Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.
Resolución MinTIC 460 del 15 de febrero de 2022	Por el cual se expide el Plan Nacional de Infraestructura de Datos (PNID) y su Hoja de Ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación. Impulsa la transformación digital del Estado y el desarrollo de una economía basada en los datos.
Resolución MinTIC 746 del 11 de marzo de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen los

NUMERO	DESCRIPCIÓN
	lineamientos adicionales a los establecidos en la Resolución 500 de 2019.
Resolución MinTIC 2277 del 03 de junio de 2025	Actualiza el Anexo 1 de la Resolución 500 de 2021, correspondiente al Modelo de Seguridad y Privacidad de la Información —MSPI—, alineándolo con estándares internacionales y lineamientos vigentes de seguridad digital para entidades públicas.
Directiva Presidencial 02 del 24 de febrero de 2022	Reiteración de la política pública en materia de seguridad digital.
ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27002:2022	Controles de seguridad de la información.

Fuente: Normograma UAESP

5. LINEAMIENTOS DE OPERACIÓN:

5.1 Tiempos de ejecución de la actividad

El borrado se realizará de acuerdo con los tiempos establecidos en el Catálogo de Servicios de TI, disponible en el Sistema Integrado de Gestión (SIG). Los tiempos de atención estarán sujetos al número de equipos que deban ser intervenidos. El proceso inicia con la apertura del caso en la Mesa de Servicios y finaliza con el cierre una vez ejecutadas y verificadas las actividades de borrado correspondientes.

5.2 Autorizaciones

La autorización para el borrado seguro de la información almacenada en los equipos se realizará de acuerdo con la situación que origine el proceso. En los casos de baja o retiro definitivo de los equipos, la autorización será otorgada por el almacenista, con fundamento en el acta del Comité Técnico de Sostenibilidad Contable en la cual se aprueba la baja.

Para los equipos devueltos por finalización de contrato que sean destinados a una nueva asignación, no se requerirá autorización específica para el borrado o formateo, teniendo en cuenta que la información institucional debe encontrarse previamente respaldada en los servicios de almacenamiento en la nube autorizados por la entidad.

Cuando se requiera el borrado de información contenida en un equipo, la solicitud deberá ser realizada por el jefe de oficina o el subdirector del área responsable de la información.

5.3 Situaciones en las que aplica procedimiento

El procedimiento se ejecutará en los siguientes casos:

- Eliminación de copias de respaldo y logs de auditorías en cumplimiento de los periodos de la Tabla de Retención Documental (TRD).
- Reasignación de equipos.
- Traslado de equipos entre dependencias.
- Baja definitiva de activos tecnológicos.
- Devolución de equipos a proveedores o terceros.
- Fallas técnicas que requieran formateo o reemplazo.
- Eliminación de información por requerimientos legales o de seguridad.
- Desmantelamiento de servicios o sistemas.

5.4 Solicitud

El borrado seguro de información deberá realizarse únicamente cuando exista una solicitud debidamente registrada a través de la mesa de servicios de la UAESP, especificando la siguiente información:

- Activo intervenido
- Serial o placa
- Justificación para la realización del proceso
- Soporte documental para los casos de baja de activos

Cuando el requerimiento no sea registrado inicialmente en Mesa de Servicios, el profesional o técnico de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) que reciba el equipo o medio de almacenamiento deberá abrir de oficio el respectivo caso en Mesa de Servicios.

5.5 Ejecución

La ejecución técnica del borrado seguro estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).

5.6 Verificación

El custodio o propietario del activo debe verificar que la información pueda ser eliminada y que no exista obligación de conservarla antes de solicitar el borrado seguro.

5.7 Respaldo de la información

En caso de ser requerido el respaldo de la información, se debe realizar de acuerdo con lo descrito en el procedimiento GTI-PC-11 Gestión de respaldos.

5.8 Método y herramientas de borrado

El método y las herramientas de borrado deberán seleccionarse de acuerdo con lo descrito en el instructivo GTI-IN-04 Soporte técnico.

5.9 Cierre de caso

El caso únicamente podrá cerrarse cuando se haya verificado el resultado del borrado y registro de la evidencia en el aplicativo de mesa de servicios de la entidad.

5.10 Roles a los que aplica

- Funcionarios
- Contratistas
- Terceros con acceso a información o activos tecnológicos propiedad de la UAESP

- Proveedores que gestionen almacenamiento o destrucción de medios propiedad de la UAESP

Queda excluida del alcance la información que no sea gestionada directamente por la UAESP o que se encuentren bajo la responsabilidad de terceros sin integración a las herramientas institucionales de monitoreo y seguridad.

6. DESCRIPCIÓN DE ACTIVIDADES:

TABLA 2 DESCRIPCIÓN DE ACTIVIDADES

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	Solicitar el borrado seguro Registra la solicitud de borrado seguro, identificando el activo o recurso tecnológico, la información objeto del borrado y la justificación de la solicitud.	Mesa de Servicios	Jefe o Subdirector responsable del activo de información Todos los procesos Almacenista general o delegado Subdirección Administrativa y Financiera	Caso registrado
2	Recibir y revisar la solicitud de borrado seguro Recibe la solicitud y revisa que contenga la información requerida y la autorización correspondiente para realizar el borrado.	Mesa de Servicios	Administrador Mesa de Servicios Oficina de Tecnología de la Información y las comunicaciones	

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	¿La solicitud cumple con los requisitos y cuenta con la autorización correspondiente? Sí: Continúa con la actividad No. 3. No: Devuelve y continúa con la actividad No. 1.			
3	Asignar el caso Asigna la solicitud al personal autorizado de la OTIC encargado de realizar el borrado seguro.	Mesa de Servicios	Administrador Mesa de Servicios Oficina de Tecnología de la Información y las comunicaciones	Caso asignado
4	Validar el método de borrado Identifica el tipo de activo, medio de almacenamiento o recurso tecnológico y determina el método de borrado seguro aplicable de acuerdo con sus características técnicas.	GTI-IN-04 Soporte técnico	Profesional técnico contratista designado de la Oficina de Tecnologías de la Información y las comunicaciones	
5	Realizar el borrado seguro Ejecuta el método de borrado definido sobre la información, medio de almacenamiento o recurso	Mesa de Servicios	Profesional técnico contratista designado de la Oficina de Tecnologías de la	Caso actualizado con la inclusión de evidencia de

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	tecnológico autorizado y genera las evidencias de la actividad realizada.		Información y las comunicaciones	ejecución del borrado
6	Verificar el resultado del borrado Comprueba que el proceso de borrado haya finalizado satisfactoriamente y registra el resultado de la verificación.	Mesa de Servicios Verifica el resultado obtenido y las evidencias generadas durante la ejecución del borrado	Profesional técnico contratista designado de la Oficina de Tecnologías de la Información y las comunicaciones	Caso actualizado con la inclusión de evidencia de ejecución del borrado
	¿El borrado fue satisfactorio? Sí: continúa con la actividad No. 7. No: Continúa con la actividad No. 4 para revisar el método de borrado aplicable.			
7	Cerrar y notificar el caso Registra el resultado final y las evidencias del borrado en la Mesa de Servicios, notifica al solicitante sobre la finalización de la	Mesa de Servicios	Profesional técnico contratista designado de la Oficina de Tecnologías de la	Caso cerrado

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	actividad y realiza el cierre del caso.		Información y las comunicaciones	

Fuente: UAESP

7. CONTROL DE CAMBIOS:

TABLA 3 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	09/09/2026	Adopción de procedimiento

Fuente: UAESP

8. AUTORIZACIONES:

TABLA 4 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Osbaldo Cortes Lozano	Profesional Universitario Oficina TIC	
	Victor Alfonso Gutiérrez Giraldo	Técnico Operativo (e) Oficina TIC	
Revisión	Jorge Alexis Rodríguez Meza	Jefe Oficina de Tecnologías de Información y las Comunicaciones	
	Luz Mary Palacios Castillo	Profesional Universitario Oficina Asesora Planeación	
Aprobó	Jesús Eduardo Gil Yaya	Jefe Oficina Asesora Planeación	