1. OBJETIVO

Establecer los pasos secuenciales para realizar el borrado seguro de información digital y software de la UAE Dirección de Impuestos y Aduanas Nacionales – DIAN, almacenada en dispositivos y medios sobrescribibles, garantizando que los datos eliminados no puedan ser recuperados ni restaurados, preservando así la confidencialidad de la información.

2. ALCANCE

Este instructivo establece los pasos a seguir para el borrado seguro de información digital y software categorizada como pública clasificada o pública reservada almacenada en dispositivos asignados a usuarios, funcionarios, contratistas, practicantes, supervisores, pasantes o terceros. Además, detalla los pasos a seguir para la reutilización de dispositivos o medios sobrescribibles que serán reasignados, dados de baja o enviados a garantía.

3. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Título	Modo de uso	Clasificación documento
Procedimiento	*PR-IIT-0460	Gestión de Requerimientos	Digital	Interno
Procedimiento	PR-IIT-0366	Gestión de Activos	Digital	Interno
Manual	MN-IIT-0072	Manual de Políticas y Lineamientos de Seguridad de la Información	Digital	Interno
Formato	FT-IIT-2847	Evidencia de borrado seguro	Digital	Interno

*Procedimiento al que pertenece este instructivo

4. DEFINICIONES Y SIGLAS

- **Borrado seguro:** es un proceso que permite eliminar datos de un dispositivo de almacenamiento de manera irreversible. Por tanto, es un control de seguridad que se aplica en los dispositivos y medios sobrescribibles que se van a reutilizar, que presentan algún daño o que van a ser dados de baja, con el cual se garantiza que la información que contienen se ha eliminado o sobrescrito correctamente, considerando que los formateos estándar no realizan esta tarea de manera adecuada; también, garantiza que los equipos averiados se someten a una evaluación de riesgos, antes entregarlos a terceros para una reparación. Lo anterior, con el fin de mantener la confidencialidad de la información contenida en el dispositivo o medio. Fuente: NTC-ISO 27002 Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información. A.7.14 Eliminación segura o reutilización de equipos, A.8.10 Eliminación de la información, A8.3.2 Eliminación segura de soportes de información.

- **Confidencialidad:** propiedad de la información que determina que esté disponible a personas autorizadas. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones - Glosario. Hipervínculo: https://www.mintic.gov.co/portal/inicio/Glosario/.

- **Copia de respaldo (Backup):** archivos, equipos, datos y procedimientos disponibles para su uso en caso de falla o pérdida, si los originales son destruidos o quedan fuera de servicio. Fuente: ISACA (Information Systems Audit and Control Association) Hipervínculo: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-spanish_mis_spa_0615.pdf

- **Datos sensibles:** para los propósitos del presente documento, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Fuente: Secretaría del Senado - Ley Estatutaria 1581 de 2012. Hipervínculo: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.htm

- **Información:** datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. Fuente: Ministerio de Tecnología y las Comunicaciones – Guía para la Gestión y Clasificación de Activos de Información. Hipervínculo: https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf?__noredirect=1

- **Información pública clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6). Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Hipervínculo: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- **Información pública reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6). Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Hipervínculo: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- **Medio de almacenamiento de datos:** se refiere a medios magnéticos, ópticos o mecánicos que registran y preservan información digital para operaciones en curso o futuras. Fuente: IBM Hipervínculo: https://www.ibm.com/mx-es/topics/data-storage

- **Métodos de borrado:** son técnicas empleadas para el borrado seguro. Se destacan las siguientes:

    - Método de Pases Únicos: este método implica una sola pasada de escritura sobre los datos con un patrón específico, como ceros o unos. Aunque es menos seguro que algunos métodos más avanzados, sigue siendo eficaz en muchos casos.
    - Método de Tres Pases (DoD 5220.22-M): este método sigue las directrices del Departamento de Defensa de los Estados Unidos y consiste en tres pases de escritura: un pase con ceros, un pase con unos y un pase con un patrón aleatorio. Luego se realiza una verificación.
    - Método de Siete Pases (Schneier's Method): propuesto por Bruce Schneier, este método implica siete pases de escritura con patrones específicos: ceros, unos, aleatorio, verificación, ceros, unos y aleatorio nuevamente.
    - Método de 35 Pases (Gutmann Method): desarrollado por Peter Gutmann, este método implica 35 pases de escritura con patrones específicos. Aunque es muy exhaustivo, puede considerarse excesivo para las necesidades actuales.
    - Método de Eliminación de Claves en SSD: específico para unidades de estado sólido (SSD), este método implica eliminar las claves de cifrado utilizadas en el controlador de la SSD, lo que hace que los datos sean prácticamente inaccesibles.

      Fuente: Elaboración propia de la Subdirección de Soluciones y Desarrollo – Dirección de Gestión de Innovación y Tecnología con base en Destroy Drive. (2024). Data wiping: 1 pass vs 3 pass vs 7 pass – Which method is best? Recuperado de https://destroydrive.com/blog/data-wiping-1-pass-vs-3-pass-vs-7-pass-which-methodis-best/; Jetico. (2023). DoD 5220.22-M explained – Data erasure standards. Recuperado de https://www.jetico.com/blog/dod-522022-m-explained-data-erasure-standards; Schneier, B. (1996). Applied cryptography (2.ª ed.). Wiley; BitRaser. (2024). Data erasure standards – Schneier's method. Recuperado de https://www.bitraser.com/data-erasure-standards.php; Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. Recuperado de 2025, de https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html; National Institute of Standards and Technology (NIST). (2014). Guidelines for media sanitization (Special Publication 800-88 Rev. 1). Recuperado de https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final.

- **Mesa de servicio:** se asemeja a la mesa de ayuda. Es un servicio de atención que gestiona los incidentes y solicitudes de los servicios que provee, da pronta respuesta y reacción por medio de sus puntos de contacto. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Hipervínculo: https://www.gobiernodigital.gov.co/623/articles-74967_recurso_24.pdf

5. DESARROLLO DEL TEMA

5.1 Generalidades del borrado seguro en la UAE Dirección de Impuestos y Aduanas Nacionales

- En atención con el Manual MN-IIT-0072 de Políticas y Lineamientos de Seguridad de la Información la Subdirección de Soluciones y Desarrollo de la Dirección General de Innovación y Tecnología – DGIT, o quien haga sus veces, es la responsable de adelantar el borrado seguro de información digital y software instalado en los equipos de cómputo que vayan a ser reasignados o dados de baja.

- Toda solicitud de borrado de información digital en los dispositivos de almacenamiento sobrescribibles debe cumplir con el requisito definido por la norma ISO/IEC 27001:2022, específicamente, en lo que refiere al control 8.10 del anexo A, que indica que los datos deben eliminarse cuando ya no sean necesarios, empleando métodos que pueden variar dependiendo del tipo de información y del medio en el que esté almacenada, para prevenir la exposición de información sensible. Por lo cual, la Dirección de Gestión de Innovación y Tecnología, en cumplimiento de lo anterior y de lo dispuesto en el MN-IIT-0072 Manual de políticas y lineamientos de seguridad de la información respecto al control de la eliminación segura o reutilización de equipos, garantiza el uso de técnicas y herramientas adecuadas para el borrado o sobre escritura segura de información, de acuerdo con la tecnología del medio de almacenamiento.

- El borrado seguro de la información debe efectuarse en el trascurso de los siguientes cinco (5) días hábiles, después de recibido el dispositivo o medio sobrescribible, bien sea para traslado, mantenimiento por terceras partes, o para baja.

- El funcionario que tenga asignado en su inventario el dispositivo o medio sobrescribible es responsable de realizar un borrado simple de cualquier tipo de información institucional previo a la entrega del dispositivo o medio bien sea por devolución, mantenimiento o baja. Se exceptúan los casos en los cuales el dispositivo o medio no es funcional, teniendo en cuenta que dicha situación le impida realizar la actividad.

- La Subdirección de Soluciones y Desarrollo efectúa el borrado por formateo simple de la totalidad de dispositivos o medios sobrescribibles de la UAE DIAN que sean objeto de reasignación, garantía o dada de baja. Posteriormente, de acuerdo con la gestión de activos de información, determina la necesidad de aplicar técnicas especializadas de borrado seguro.

- Los dispositivos o medios sobrescribibles que sean objeto de borrado seguro deben estar asignados a funcionarios que pertenezcan a dependencias que tengan activos de información categorizados como reservados y/o confidenciales. Si la solicitud proviene de una dependencia cuyos activos de información no se encuentren categorizados como tal, la dependencia debe aplicar lo definido en el Procedimiento PR-IIT-0366 Gestión de Activos para obtener dicha categorización. Esto no aplica para el Director General o Directores de gestión en cuyo caso

siempre se debe efectuar el borrado seguro en los dispositivos y medios sobrescribibles en los cuales se gestione su información, con el propósito de mitigar el riesgo de acceso y fuga de información confidencial y exposición de datos personales que pueda atentar contra la Administración Tributaria.

- Semestralmente, la Coordinación de Soporte Técnico al Usuario de la Subdirección de Soluciones y Desarrollo, debe solicitar a la Oficina de Seguridad de la Información – OSI el reporte de activos de información identificados como clasificados y reservados según el índice de información reservada y clasificada de la Entidad, dato indispensable para el desarrollo de las actividades previstas en este instructivo. Adicionalmente, se puede llegar a efectuar consultas puntuales a la OSI, si se recibe una solicitud de borrado seguro por un área que no figure en el reporte semestral. Esto con el fin de verificar si se han registrado cambios en los activos de información, con posterioridad a la generación del reporte.

- En caso de incidentes en la ejecución del borrado seguro que se presenten por pérdida, daño, robo o compromiso del dispositivo o medio sobre escribible que se encuentre dispuesto para el borrado seguro, la Subdirección de Soluciones y Desarrollo o quien haga sus veces, debe reportar esta situación como un evento de seguridad de la información a la Oficina de Seguridad de la Información (seguridaddigital@dian.gov.co) para que realice el estudio correspondiente de incidentes de seguridad de la información, de acuerdo con el Instructivo IN-IIT-0253 Gestión de Incidentes de Seguridad Digital.

5.2 Registro del requerimiento de borrado seguro

El Agente de Servicio, ubicado en la Coordinación de Soporte Técnico al Usuario de la Subdirección de Soluciones y Desarrollo o quien haga sus veces en las Direcciones Seccionales de Impuestos y Aduanas que se encuentre gestionando la reasignación, baja o garantía de un dispositivo o medio sobre escribible, debe registrar en la herramienta de mesa de servicio la gestión de borrado seguro para garantizar la trazabilidad de las actividades que se lleven a cabo. Así mismo, el jefe de área o dependencia que lo considere puede efectuar también este requerimiento sobre un dispositivo o medio sobre escribible que se encuentre asignado. En cualquier situación, se debe registrar el caso con la siguiente información mínima:

- Tipo de dispositivo o medio.
- Marca y modelo.
- Número de serie.
- Placa de inventario físico (si aplica).
- Funcionario responsable del dispositivo o medio (si no se cuenta con esta información, se debe indicar explícitamente la situación).
- Área del funcionario responsable del dispositivo o medio (si no se cuenta con esta información, se debe indicar explícitamente la situación).
- Ubicación física del dispositivo (nivel central – seccional).
- Razón del borrado (disposición para reasignación, dada de baja, envío a garantía). En caso de que la razón de borrado no corresponda a las anteriores, es decir que el caso no esté siendo registrado por un Agente de Servicio, sino por un jefe de área o dependencia con activos de

información categorizados como reservados y/o clasificados, en este campo debe incluir la justificación de la solicitud.

Si la solicitud se origina desde un área o dependencia, quien tenga asignado el dispositivo o medio sobrescribible, debe asegurarse de haber conservado una copia de respaldo de la información contenida, en los medios institucionales establecidos, ya que una vez se haya efectuado el borrado seguro la información no puede ser recuperada.

5.3 Verificación del requerimiento de borrado seguro

En los casos en los que el Agente de Servicio o quien haga sus veces, sea el responsable de registrar el requerimiento de borrado seguro en la herramienta de mesa de servicio, no aplica este punto.

En el caso de que el requerimiento de borrado seguro provenga de un jefe de área o dependencia, el Agente de Servicio o quien haga sus veces debe validar en un plazo máximo de 8 horas hábiles si el área se encuentra incluida dentro del listado, suministrado semestralmente por la OSI, que contiene las dependencias que poseen activos de información categorizados como Clasificados o Reservados. De no encontrarse en el listado, el Agente de Servicio debe comunicar a la OSI la solicitud, para que esta oficina valide si el reporte semestral tuvo alguna actualización y confirme si la dependencia tiene identificados activos con información clasificada o reservada para proceder con el caso. La solicitud debe ser atendida por la OSI y respondida en un plazo máximo de 8 horas hábiles.

En caso de obtener una respuesta negativa por parte de la OSI frente a la actualización de activos de información, el Agente de Servicio de acuerdo con lo previsto en el procedimiento PR-IIT-0460 Gestión de Requerimientos, debe proceder a cerrar el caso informándole al solicitante que para atender una solicitud de borrado seguro, se requiere que el propietario del activo de información, realice las actividades previstas en el Procedimiento PR-IIT-0366 Gestión de Activos para determinar si el activo de información, o la información que está contenida en el dispositivo a borrar, se encuentra enmarcada como Reservada o Clasificada y se registre su categorización en el inventario de activos de información de la entidad.

Una vez cumplida la anterior actividad, el solicitante puede registrar un nuevo caso en la herramienta de mesa de servicio.

5.4 Definición del método de borrado

El Agente de Servicio o quien haga sus veces, identifica el dispositivo o medio sobrescribible sobre el cual se solicita el borrado seguro y determina el método de borrado seguro que debe aplicar.

En la UAE Dirección de Impuestos y Aduanas Nacionales se aplican los siguientes criterios:

- Para **dispositivos de estado sólido o memorias USB**, se utiliza el método de eliminación segura disponible en la herramienta tecnológica habilitada para el borrado seguro de este tipo

de dispositivos por la Subdirección de Soluciones y Desarrollo - SSD de la Dirección de Gestión de Innovación y Tecnología - DGIT.

- Para **dispositivos HDD,** se utiliza el estándar de borrado DoD 5220.22-M, recomendado en la industria, el cual garantiza una sanitización correcta del disco duro manteniendo su vida útil. Este se aplica con la herramienta tecnológica habilitada por la Subdirección de Soluciones y Desarrollo - SSD de la Dirección de Gestión de Innovación y Tecnología - DGIT.

5.5 Borrado seguro y evidencia

El Agente de Servicio o quien haga sus veces, prepara el dispositivo o medio sobre escribible y demás herramientas necesarias para realizar el borrado seguro. Para el manejo de la herramienta tecnológica definida por la SSD, se debe seguir el paso a paso definido en el manual técnico el cual no se transcribe, teniendo en cuenta que la herramienta puede eventualmente variar.

Los dispositivos y medios sobrescribibles sobre los cuales se solicite el borrado, deben ser equipos funcionales, es decir, que permitan realizar operaciones de sobre escritura correctamente. En caso de que el requerimiento de borrado seguro se haya efectuado sobre un dispositivo o medio no funcional, el Agente de Servicio debe diligenciar el formato FT-IIT-2847 Evidencia de borrado seguro y notificarlo al superior jerárquico y a la OSI para que, a través de un análisis de eventos, se determine la presencia o no de un incidente de seguridad de la información y se determinen las estrategias de manejo del dispositivo o medio sobrescribible. La gestión de incidentes de seguridad digital se realizará mediante el procedimiento PR-IIT-0458 Gestión de Incidentes y el Instructivo IN-IIT-0253 Gestión de Incidentes de Seguridad Digital. La gestión adelantada, junto con el formato señalado, deben ser registradas en la herramienta de mesa de servicio para efectos de trazabilidad y posteriormente se debe efectuar el cierre del caso. Si aplica, se debe comunicar al solicitante el resultado no exitoso de la solicitud de borrado seguro y la gestión adelantada.

Si los dispositivos y medios sobrescribibles son funcionales, una vez efectuado el borrado seguro, se valida que este haya sido exitoso comprobando que los datos se eliminaron correctamente y que no pueden recuperarse. De no haber sido exitoso el borrado seguro, se debe reintentar nuevamente hasta por un máximo de tres (3) intentos. Si, posteriormente, no se consigue el borrado seguro del dispositivo o medio, se debe escalar son el superior jerárquico para determinar la acción a tomar con el propósito de lograr el borrado seguro.

Cuando el borrado seguro es exitoso, el Agente de Servicio o quien haga sus veces, debe extraer el registro de borrado de datos del dispositivo o medio sobrescribible (log o pantalla del resultado) y adicionalmente diligenciar el formato FT-IIT-2847 Evidencia de borrado seguro. Estos soportes, se adjuntan como evidencia en el caso registrado en la herramienta de mesa de servicio, y deben ser conservados en medio digital en el archivo del área para estar disponibles a efectos de trazabilidad o para ejercicios de auditoría, según se requiera.

Para el desarrollo de las actividades contenidas en este punto, el Agente de Servicio cuenta con un plazo máximo de treinta y dos (32) horas hábiles.

Una vez completadas estas actividades, continua con lo definido en el procedimiento PR-IIT-0460 Gestión de Requerimientos, en la actividad número siete (7) “Se solucionó el requerimiento”.

6. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	21/05/2025		Versión inicial	Esta versión corresponde a Información Pública

Elaboró:	Cristian Eduardo Zanguña Ruiz **Elaboración técnica**	Gestor IV	Subdirección de Soluciones y Desarrollo
	Julián Andrés Ruiz Méndez **Elaboración técnica**	Gestor III	Subdirección de Soluciones y Desarrollo
	Lizeth Cárdenas Cardozo **Elaboración metodológica**	Gestor II	Subdirección de Innovación y Proyectos
Revisó:	Yeni Marcela Arcos Casas	Gestor III	Subdirección de Innovación y Proyectos
	Tito Alejandro Menjura **Revisión metodológica**	Gestor II	Subdirección de procesos
	Cesar Augusto Garzón Baquero **Revisión metodológica**	Gestor I	Coordinación de Procesos y Riesgos Operacionales
	Nancy Paola Sanchez Moreno	Gestor II	Oficina de Seguridad de la Información
	Sandra Janette Piedrahíta Urueña	Gestor IV	Oficina de Seguridad de la Información
	Carlos Javier Ibáñez Serna	Gestor II	Oficina de Seguridad de la Información
Aprobó:	Antonio José Barrios Hoyos	Subdirector	Subdirección de Soluciones y Desarrollo

7. ANEXOS

No aplica.