TABLA DE CONTENIDO

1. OBJETIVO

Definir las pautas técnicas para la ejecución del borrado seguro de información en activos tecnológicos de la Agencia ATENEA, tanto en equipos físicos como en plataformas en la nube.

2. ALCANCE

El alcance de esta guía comprende el borrado seguro de la información almacenada en los activos tecnológicos de la Agencia ATENEA, en los siguientes contextos:

- Equipos que finalizan contrato de arrendamiento.
- Equipos dados de baja por obsolescencia, daño o reemplazo.
- Recursos digitales eliminados en entornos de nube (Oracle Cloud Infrastructure - OCI).

3. DEFINICIONES

- **Borrado seguro:** Conjunto de acciones técnicas destinadas a eliminar de manera definitiva la información contenida en un dispositivo o servicio, evitando su recuperación mediante técnicas forenses o herramientas especializadas.
- **Copia de seguridad** (Backup o Respaldo): Duplicado de los datos originales almacenado en un medio alterno seguro, realizado con el fin de poder recuperarlos en caso de pérdida, daño o fallo del sistema original. Es un mecanismo esencial de protección de la información.
- **Restauración** (Restore): Proceso de recuperar datos a partir de una copia de seguridad previamente realizada, devolviéndolos a su estado original o a un entorno operativo tras un incidente. Implica cargar o reintegrar la información respaldada en el sistema de producción para reanudar las operaciones.
- **Retención** (de respaldos): Periodo de conservación de las copias de seguridad antes de su eliminación o depuración. Una política de retención define cuánto tiempo se almacenan los respaldos (por ejemplo, 7 días, 1 mes, 1 año) antes de ser descartados automáticamente, asegurando un historial suficiente de versiones para recuperación.
- **Oracle Cloud**: Plataforma de servicios en la nube provista por Oracle, que incluye infraestructura como servicio (IaaS) –por ejemplo, instancias de cómputo (servidores virtuales), almacenamiento en bloque, redes– y plataformas de datos como bases de datos Oracle en la nube. En esta guía nos referiremos a Oracle Cloud para englobar todos estos servicios cloud bajo responsabilidad de la institución.
- **Microsoft 365**: Servicio en la nube de Microsoft que integra aplicaciones de productividad y colaboración (Exchange Online para correo, OneDrive y SharePoint para almacenamiento de archivos, Teams, entre otros). Aunque Microsoft 365 ofrece alta disponibilidad y ciertas capacidades nativas de retención, los datos alojados en esta plataforma también requieren de algunas configuraciones relacionadas con políticas de retención adicionales bajo responsabilidad de la institución.

4. NORMATIVIDAD ASOCIADA

- Resolución No. 2277 de 2025, “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”
- Acuerdo No 002 del 2023, proferido por la comisión distrital de transformación digital, por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
- Decreto 767 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.
- Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021
- Directiva Presidencial No. 02 de 2022: Reiteración de la Política pública en materia de seguridad digital
- Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones.

5. DESARROLLO

Este numeral describe las actividades técnicas que permiten la eliminación definitiva de la información en los diferentes entornos de la Agencia, evitando su recuperación mediante mecanismos de sobrescritura, destrucción de claves de cifrado o deshabilitación controlada, según aplique.

La ejecución de las actividades descritas en este numeral debe registrarse en el “Formato de borrado seguro”, el cual recopila la información mínima necesaria para dejar trazabilidad del borrado realizado, tales como: datos del activo o recurso, herramienta utilizada, número de pasadas (cuando aplica), fecha de ejecución, observaciones técnicas, evidencia de verificación y datos del responsable.

El profesional responsable de los activos tecnológicos de la Agencia ATENEA es el encargado de ejecutar las actividades establecidas en esta guía para el borrado seguro de la información.

En la siguiente tabla se resumen los entornos tecnológicos cubiertos por la guía, la tecnología involucrada en cada uno, el método de borrado seguro que debe aplicarse y la evidencia que se debe conservar como soporte de la ejecución del borrado seguro.

Entorno	Tecnología involucrada	Método de borrado seguro	Evidencia esperada
Equipos físicos	Discos SATA, SSD y NVMe	Cipher de Windows	Formato de borrado seguro
Oracle Cloud	OCI Volumes,file systems Buckets, DB, Vault	Eliminación + Borrado criptográfico	Logs de Auditorias - Formato de borrado seguro
Microsoft 365	OneDrive, SharePoint, Outlook, Teams	Inactivación de cuentas, retención y eliminación total	Capturas + Auditoría Formato de borrado seguro

5.1. Equipos físicos

Este apartado aplica a los dispositivos físicos de almacenamiento (HDD, SSD y NVMe), internos o externos, conectados a los equipos de cómputo institucionales de la Agencia ATENEA.

En este contexto se definen las actividades que debe realizar el personal técnico para efectuar el borrado seguro de la información, utilizando herramientas nativas del sistema operativo Windows. En particular, se emplea el comando cipher /w, que realiza una sobreescritura controlada del espacio libre del disco, evitando la recuperación de datos previamente eliminados, sin modificar los archivos vigentes ni comprometer la integridad del sistema.

Cuando, de acuerdo con los escenarios definidos en el alcance de esta guía, se determine que un equipo debe ser sometido a borrado seguro (por ejemplo, por finalización de contrato de arrendamiento, baja por obsolescencia o reemplazo), el personal técnico/profesional de la Subgerencia de Tecnologías de la Información y las Comunicaciones encargado de la administración de los equipos de cómputo institucionales realizará las siguientes actividades:

- Preparar el entorno

  - Iniciar sesión con una cuenta institucional que cuente con privilegios de administrador sobre el equipo. Estas cuentas son asignadas al profesional responsable de la Subgerencia de Tecnologías de la Información y las Comunicaciones, no a los usuarios finales.
  - Conectar el dispositivo físico de almacenamiento (HDD o SSD externo/interno).
  - Verificar que el sistema detecte correctamente el volumen, ejecutando en la consola de Windows el siguiente comando: `wmic logicaldisk get name, volumename`

    Este comando lista las unidades disponibles, su nombre, sistema de archivos, tamaño y espacio libre. Verifique que la unidad a limpiar use NTFS, ya que cipher /w solo opera sobre ese sistema.

  - Cerrar todas las aplicaciones que puedan estar accediendo al disco (bases de datos, sincronizadores, antivirus en escaneo, etc.).
  - Validar si es necesario contar con respaldo de cualquier información importante; los datos eliminados mediante las actividades descritas en esta guía no podrán recuperarse.

```
C:\Windows\System32>wmic logicaldisk get name,volumename
Name  VolumeName
C:
D:    Datos
E:    ATENEA
```

- Ejecuta el comando de borrado seguro
  - Abrir el Símbolo del sistema como administrador:
    Menú Inicio → escribir “cmd” → clic derecho → *Ejecutar como administrador*.
  - Ubicar la letra de la unidad a limpiar (por ejemplo, E:).
  - Ejecutar el comando: cipher /w:E:\

```
E:\>cipher /w:E:\
Para quitar todos los datos posibles, cierre todas las aplicaciones mientras
ejecuta CIPHER /W.
Escribir en 0x00
.....................
```

Donde E:\ es la ruta raíz del volumen que se limpiará.
El comando no borra los archivos actuales; únicamente sobrescribe el espacio libre.

- **Monitorear el proceso y finalización**
  La consola mostrará las pasadas
  - Las líneas de puntos (.....) indican el avance de cada fase de sobrescritura.
  - La duración puede ir de minutos a horas, según el tamaño del volumen y la cantidad de espacio libre disponible.

```
E:\>cipher /w:E:\
Para quitar todos los datos posibles, cierre todas las aplicaciones mientras
ejecuta CIPHER /W.
Escribir en 0x00
...............................................................................................
Escribir en 0xFF
...............................................................................................
Escribir en Números al azar
...............................................................................................

E:\>
```

- Interpretación de las pasadas. cipher /w ejecuta tres fases sobre el espacio libre del volumen: “Escribir en 0x00” (primera pasada con ceros), “Escribir en 0xFF” (segunda pasada con unos que refuerza la limpieza) y “Escribir en Números al azar” (tercera pasada con valores aleatorios para evitar patrones).

- Confirmación de éxito. El proceso se considera correcto cuando se visualizan las tres fases completas y la consola regresa al prompt (E:\> / C:\>) sin mensajes de error. Esto indica que el espacio libre fue sobrescrito y que los restos de archivos eliminados no son recuperables con herramientas estándar.

- El comando cipher /w realiza sobrescritura triple (0x00, 0xFF y aleatoria) exclusivamente sobre el espacio libre del volumen. La finalización sin errores y el retorno al prompt constituyen la evidencia de éxito. Este método se clasifica como Clear según NIST SP 800-88 Rev. 1 y es adecuado para limpieza rutinaria o preparación de medios para su reutilización

En los casos de borrado seguro ejecutados de manera masiva -por terminación de contratos de arrendamiento, renovación o devolución de equipos- las actividades descritas se aplican de forma agrupada para cada lote de dispositivos.

Una vez finalizadas las actividades sobre el dispositivo físico, se debe diligenciar el Formato de borrado seguro, incluyendo la identificación del equipo, la herramienta utilizada, el número de pasadas y la evidencia del resultado.

5.2. Entornos de nube – Oracle Cloud Infrastructure (OCI)

En Oracle Cloud Infrastructure (OCI), el borrado seguro de información se fundamenta en los controles nativos del proveedor, los cuales aseguran la protección y eliminación definitiva de datos tanto en almacenamiento en bloque como en objetos, siguiendo prácticas alineadas con estándares internacionales de sanitización de datos, como NIST SP 800-88 Rev. 1 y DoD 5220.22-M, que son implementados por el propio proveedor en su infraestructura.

Todos los volúmenes (block y boot) en OCI están automáticamente cifrados en reposo mediante el algoritmo AES-256 usando claves administradas por Oracle. Cuando se elimina un volumen, los datos ya cifrados en el disco quedan inaccesibles sin la clave de cifrado correspondiente. Por tanto, es prácticamente imposible recuperar la información. Este enfoque basado en cifrado proporciona una protección robusta ya que al eliminar o rotar las claves de cifrado, los datos anteriores resultan irrecuperables. Por eso, el cifrado por sí mismo refuerza el borrado seguro en estos casos.

Pasos para la eliminación del volumen:

- Ingresar al panel de OCI.
- Navegar a: Block Storage → Block Volumes.
- Seleccionar el volumen correspondiente.

- Hacer clic en “Terminate”.
- Confirmar la operación.

Importante: Esta acción no es reversible. Oracle impide el acceso posterior al volumen eliminado.

Las siguientes consideraciones aplican a los volúmenes y servicios de almacenamiento de Oracle Cloud Infrastructure (OCI) utilizados por la Agencia ATENEA. Su administración es realizada por el ingeniero de infraestructura de la Subgerencia de Tecnologías de la Información y las Comunicaciones con privilegios sobre la suscripción de Oracle Cloud, apoyándose en los mecanismos nativos de cifrado en reposo del proveedor.

a) Cifrado en reposo.

- Todos los volúmenes en OCI están cifrados por defecto con claves gestionadas por Oracle o el cliente.
- El borrado seguro de la clave de cifrado garantiza la destrucción lógica de los datos, incluso si existiera persistencia física.

File Storage: Estos también cuentan con el cifrado en reposo por defecto, ya sea con claves gestionadas por Oracle o con claves propias ubicadas en el Vault de Oracle. Al eliminar un file system, todo su contenido (y sus snapshots, si existen) se eliminan. Al igual que en los blocks volumes, el cifrado también refuerza la confidencialidad tras el borrado.

Object Storage (buckets): Cada objeto está cifrado individualmente con una clave de datos (DEK), que a su vez está cifrada con una clave maestra del bucket, ya sea gestionada por Oracle o por el cliente a través de un Vault de Oracle. Cuando se elimina un objeto o un bucket, los datos desaparecen de forma permanente, así, un bucket eliminado no puede recuperarse, y todo objeto y sus versiones quedan inaccesibles.

Bases de datos: Para las bases de datos como servicio PaaS, tales como Oracle DB System y MySQL DB System, todos los datos son almacenados en Block Storage cifrados en reposo con AES-256 y claves gestionadas por Oracle. Cuando se elimina una base de datos o el DB System completo, el volumen subyacente (boot y block) se destruye, y dado que los datos estaban cifrados, estos resultan inaccesibles al quedar desvinculados de la clave.

Para las bases de datos Autonomous Database (ATP, ADW, APEX, JSON, etc.), el cifrado en reposo está habilitado por defecto y no se puede desactivar. Cada base de datos autónoma utiliza Transparent Data Encryption (TDE) con claves maestras que se almacenan en un Oracle Key Vault. Cuando se elimina una base de datos autónoma, los datos cifrados y sus copias de respaldo asociadas se marcan para eliminación. Como las claves de TDE son únicas para cada instancia, al eliminar la base o revocar la clave en Vault, los datos anteriores quedan irrecuperables. Esto garantiza que el proceso de borrado se apoye no en sobreescritura física, sino en el modelo de “crypto-erasure” (los datos permanecen cifrados sin una clave válida).

Cada eliminación de volúmenes o recursos en OCI debe registrarse en el Formato de borrado seguro, reportando el tipo de recurso, fecha, acción realizada y la evidencia generada por la plataforma (por ejemplo, logs de auditoría).

5.3. Microsoft 365

La entidad utiliza la plataforma Microsoft 365 para correo electrónico, colaboración y almacenamiento de archivos (Exchange Online, OneDrive, SharePoint y Teams). Las configuraciones descritas a continuación corresponden a la implementación vigente realizada por la Subgerencia de Tecnologías de la Información y las Comunicaciones, en cumplimiento de la Política de Seguridad y Privacidad de la Información de la Agencia ATENEA; no constituyen una política independiente adicional.

En OneDrive y SharePoint se han configurado reglas de retención de datos que restringen la eliminación permanente de la información por parte de los usuarios y garantizan la conservación de los contenidos durante el tiempo definido institucionalmente.

En cuanto a las cuentas de correo, el funcionario o contratista deberá cumplir con lo descrito en el Procedimiento de Desvinculación o el Procedimiento de Supervisión e Interventoría según corresponda. Estos procedimientos establecen las actividades que la persona debe adelantar con el fin de que a través del trámite del formato de paz y salvo (funcionarios: Formato Paz y Salvo o Contratistas: Paz y salvo para contratistas) y las actividades descritas en los procedimientos, se notifique formalmente a la Subgerencia de Tecnologías de la Información y las Comunicaciones la novedad relacionada con la cuenta de correo.

A partir de esta notificación recibida a través de la mesa de ayuda en el caso de los Contratistas y por correo electrónico en el caso de los funcionarios, el profesional de la Subgerencia de Tecnologías de la Información y las Comunicaciones realiza las siguientes actividades sobre la cuenta de Microsoft 365:

- Se inactiva la cuenta de usuario y se bloquea el acceso interactivo.
- Se bloquea la recepción de mensajes mediante políticas de transporte, según aplique.
- Se retiran las licencias asociadas de Microsoft 365, de acuerdo con la administración de licenciamiento.
- Se genera y almacena un respaldo del buzón de correo, cuando aplica.

Transcurridos los periodos de retención definidos, la plataforma realiza la eliminación permanente de los datos mediante sus mecanismos internos de depuración, lo que complementa las medidas de borrado seguro descritas en esta guía.

6. ANEXOS

No aplica

7. DOCUMENTOS DE REFERENCIA

- Política de Seguridad y Privacidad de la Información

- Manual de Políticas de Seguridad de la Información
- Procedimiento de Desvinculación
- Procedimiento de Supervisión e Interventoría.

8. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
F1_G5_TIC	Formato de borrado seguro
F2_P4_TH	Formato Paz y Salvo
F2_P10_C	Formato de Paz y Salvo para Contratistas

9. CONTROL DE CAMBIOS

Fecha (De la Versión del documento que se está actualizando)	Versión (Relacionar la última versión y código del documento que se está actualizando)	Descripción del Cambio

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	María Alejandra Suarez	Profesional Contratista – Subgerencia de Tecnologías de la Información y las Comunicaciones	28/11/2025
Revisó	Juan Pablo Ceballos Sergio Cante Jair David Calderín Rojas	Profesionales Contratistas – Subgerencia de Tecnologías de la Información y las Comunicaciones	28/11/2025
Aprobó	Carlos Andrés Ballesteros	Subgerente de Tecnologías de la Información y las Comunicaciones	28/11/2025

Carlos Ballesteros

Firmado digitalmente por Carlos Andres Ballesteros Castañeda

NOMBRE Y FIRMA DEL LÍDER DE PROCESO