

1 OBJETIVO

Establecer los lineamientos y responsabilidades para la identificación, clasificación, uso, protección, etiquetado y disposición final de los activos de información de la entidad, con el fin de garantizar su integridad, confidencialidad, disponibilidad y trazabilidad, de acuerdo con los principios de la seguridad de la información, las normas vigentes y las buenas prácticas aplicables.

2 ALCANCE

Inicia con la identificación y/o revisión de los activos de información y culmina con la consolidación de la matriz de inventario y valoración, incluyendo el etiquetado correspondiente. Aplica a todos los procesos y funcionarios de la Entidad, sin distinción de su tipo de vinculación. Así mismo, todos los contratistas están obligados a garantizar su cumplimiento en el marco de sus funciones y responsabilidades.

3 NORMATIVIDAD

Tipo	Número	Título	Fecha
Ley	594	Por medio de la cual se dicta la Ley General de archivos y se dictan otras disposiciones.	14/07/2000
Ley	1581	Por la cual se dictan disposiciones generales para la protección de datos personales.	17/10/2012
Ley	1712	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.	6/03/2014
Decreto	1377	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.	27/06/2013
Decreto	1081	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.	26/05/2015
Acuerdo AGN	001	Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado Colombiano y se fijan otras disposiciones	29/02/2024
Resolución Nacional MINTIC	1519	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos	24/08/2020
Resolución Nacional MINTIC	500	"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"	10/03/2021
Resolución MINTIC	02277	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia	03/06/2025

Resolución - COPNIA	R2024043248	Por medio de la cual se actualiza el Modelo Integrado de Planeación y Gestión del COPNIA y se reglamentan sus respectivos comités	02/10/2024
------------------------	-------------	---	------------

4 DEFINICIONES

- **ACTIVO:** Cualquier cosa que tenga valor para una persona, una organización o un gobierno. [ISO 27032:2012]
- **ACTIVO DE INFORMACIÓN:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).
- **CLASIFICACIÓN DE LA INFORMACIÓN:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.
- **CONFIDENCIALIDAD:** propiedad de la información que determina que esté disponible a personas autorizadas.
- **CONTROL:** medida que permite reducir o mitigar un riesgo.
- **CUSTODIO:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado
- **DATO:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **DATO PERSONAL:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada). Ejemplo: Nombres, apellidos, fecha y lugar de nacimiento, número de identificación, teléfono, e información asociada a sus actividades, registro multimedia, preferencias ideológicas, políticas, creencias religiosas, entre otros.
- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000]
- **INFORMACIÓN:** se refiere a un conjunto organizado de datos contenido en cualquier documento que los responsables y/o encargados del tratamiento generen, obtengan, adquieran, transformen o controlen.
- **INFORMACIÓN PÚBLICA:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Literal b, artículo. 6 de la Ley 1712 de 2014)
- **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 esta ley. (Literal c, artículo. 6 de la Ley 1712 de 2014)

- **INFORMACION 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 de la ley. (Literal d, artículo. 6 de la Ley 1712 de 2014)
- **INFRAESTRUCTURA CRÍTICA CIBERNÉTICA (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. (Decreto 338 de 2022).
- **INTEGRIDAD:** característica de los activos de información que salvaguarda la exactitud y estado completo de la información o activos.
- **MEDIO DE ALMACENAMIENTO ELECTRONICO DE DATOS:** son dispositivos físicos que permiten guardar información digital. Ejemplo: Discos duros, USB, tarjetas de memoria.
- **PRIVACIDAD DE LA INFORMACIÓN/DATOS:** es el aspecto de las tecnologías de la información (TI) que trata sobre la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático se pueden compartir con terceros.
- **PROPIETARIO DE LA INFORMACIÓN:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. [ISO/IEC 27000].
- **TABLAS DE RETENCIÓN DOCUMENTAL:** Es un conjunto de unidades documentales homogéneas emanadas por un mismo órgano o sujeto productor en ejercicio de sus funciones.
- **TRAZABILIDAD:** Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

5 CONDICIONES GENERALES

5.1 GENERALIDADES

- Todos los funcionarios son los responsables de la gestión de los activos de información
- La Oficina de Seguridad y Privacidad de la información realizará la coordinación y acompañamiento en la identificación, revisión, actualización y consolidación del inventario de activos de información.
- Las áreas productoras de activos de información documental (física y/o electrónica) deberán seguir los lineamientos del proceso de gestión documental a través de las Tablas de Retención Documental y/o las diferentes herramientas archivísticas adoptadas por la Entidad.
- El instrumento para realizar la clasificación y valoración de activos de información será la Matriz de Inventario de Activos de Información SPI-fr-10, a partir de este formato se mantendrán consolidados todos los activos de información de la Entidad, y será la única herramienta de control oficial. Por ende, el Registro de Activos de información y el índice de información Clasificada y Reservada conservarán el mismo formato y extraerán de dicha matriz la información de activos de tipo documental para publicarla conforme a lo establecido en la normativa archivística, como instrumento de información Pública. Solo se podrán publicar los activos de información de tipo Datos/información.
- El inventario de activos de información debe ser un documento clasificado como "Confidencial", y no debe tener características que lo permitan modificar por los usuarios no autorizados. Sólo tendrá de permisos de modificación a este documento el líder del proceso con previa autorización del profesional de gestión de la Oficina de Seguridad y Privacidad de la Información.
- Para determinar los activos de información que van a hacer parte del inventario, cada líder de proceso debe adelantar las actividades de identificación y/o revisión de los activos de información.
- Todos los funcionarios, para garantizar la protección de los activos de información almacenados en los equipos de cómputo, deberán bloquear la pantalla o cerrar la sesión del dispositivo cuando este se encuentre desatendido.
- Cuando un área, o secretaría seccional o regional de la Entidad vaya a firmar un convenio con otra Entidad que implique el intercambio de información, el supervisor o líder encargado debe informar previamente a la Oficina de Seguridad y Privacidad de la Información, mediante correo electrónico y/o memorando interno. Esta notificación debe hacerse antes de firmar el convenio y deberá incluir como mínimo los siguientes datos:
 - Nombre de la entidad con la que se va a firmar el convenio.
 - Propósito u objetivo del convenio.
 - Qué tipo de datos o información se van a intercambiar.
 - Quién será el responsable de hacer seguimiento al convenio (supervisor o líder encargado).
 - Duración del convenio. Si no tiene un tiempo definido, se debe informar a la Oficina de Seguridad y Privacidad cuando termine el convenio.

- Para la consolidación de la matriz de riesgos se deberá tener en cuenta los controles que mitiguen los riesgos asociados a los activos de información que para la Entidad tengan un valor Medio y Alto.

5.2 RESPONSABILIDADES

- La Oficina de Seguridad y Privacidad de la Información será la responsable de consolidar, controlar y custodiar el inventario de activos de información.
- Los propietarios de los activos de información son responsables de su clasificación, mantenimiento, actualización y documentación. Asimismo, les corresponde definir qué usuarios y sistemas de información pueden acceder a dichos activos, conforme a las funciones y competencias asignadas.
- El área Administrativa, a través del proceso de Administración de Bienes y Servicios, es la responsable de controlar, gestionar y garantizar el inventario de equipos de cómputo.
- El área Administrativa, a través del proceso de Gestión Documental, es la responsable de establecer los lineamientos para los activos de información documentales y garantizar el inventario de estos.
- El área de Tecnologías de la Información y las Comunicaciones es la responsable de administrar, gestionar e implementar medidas de seguridad, y controlar los accesos de los sistemas de información de la Entidad que garanticen la confidencialidad, integridad y disponibilidad de los activos de información.

5.3 ACTIVOS DE INFORMACIÓN.

Un activo de información es cualquier elemento (tangible o intangible) que para la Entidad genera valor y necesita proteger porque contiene o está relacionado con información crítica para su operación, objetivos y continuidad, para ello los activos de información pueden ser:

a) ACTIVOS HUMANOS

- **Empleados:** funcionarios de planta global, funcionarios de libre nombramiento y remoción.

b) ACTIVOS FÍSICOS

- **Infraestructura física y de TI (Hardware/Infraestructura):** Edificios, oficinas, centro de datos, cuartos de servidores y equipos, armarios de red (Racks), cableado, dispositivos de identificación y autenticación, control de acceso del personal. computadores de escritorio y portátiles, dispositivos de almacenamiento, servidores, firewall, routers, dispositivos de comunicaciones, impresoras, scanners, fotocopiadoras.
- **Datos/Información:** Procedimientos, programas, guías, formatos, manuales y demás documentación física de propiedad de la entidad conforme a la Tabla de Retención Documental.

c) ACTIVOS INTANGIBLES

- **Bases de Datos:** Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, puede ser utilizada en un formato de motor ya sea SQL, SQL Server, MySQL o en formato Excel.
- **Software / Aplicaciones informáticas:** Sistemas de información que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
- **Servicios:** Servicios de autenticación y administración de usuario, aplicaciones, servidores proxy, servicios de red, servicios web, servicios inalámbricos, antivirus, antispyware, antispam, detección y prevención de intrusiones, seguridad, FTP, bases de datos, correo electrónico y mensajería instantánea, contratos de soporte y mantenimiento de software.

5.4 USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

5.4.1 GENERALIDADES

- Los activos de información deben ser utilizados exclusivamente para el desarrollo de funciones institucionales y conforme a los fines misionales de la entidad.
- El acceso a los activos debe otorgarse en función de las responsabilidades del funcionario, contratista o tercero, y previa autorización del propietario del activo.
- Está prohibido utilizar los activos de información con fines personales, comerciales, políticos o cualquier otro propósito ajeno a los objetivos institucionales.
- Todos los funcionarios deben aplicar las medidas necesarias para prevenir el acceso no autorizado, modificación, pérdida o divulgación indebida de la información, tanto en medios físicos como digitales.
- Todo uso de activos debe respetar las políticas institucionales de seguridad de la información, protección de datos personales, gestión documental y las disposiciones legales aplicables.
- Cada usuario es responsable por el uso que haga de los activos asignados y debe reportar inmediatamente al jefe inmediato y a la Oficina de Seguridad y Privacidad de la información cualquier uso indebido, incidente o anomalía relacionada con los mismos.
- Está prohibido facilitar el acceso a activos de información a otros usuarios no autorizados, ya sea deliberadamente o por error.
- Todos los funcionarios, para garantizar la protección de los activos de información almacenados en los equipos de cómputo, deberán bloquear la pantalla o cerrar la sesión del dispositivo cuando este se encuentre desatendido.
- Todos los funcionarios deben garantizar el cumplimiento de los lineamientos para el uso de medios removibles que garanticen la protección de los activos de información, con el fin de evitar accesos no autorizados, daños, pérdida de información o extravío del medio.
- Emplear los medios removibles (USB, SD, Memory Stick, Micro SD, discos duros extraíbles, entre otras) sólo para la transferencia de datos y no como dispositivos de almacenamiento; la información transferida deberá ser eliminada de manera segura.
- Evitar la divulgación o entrega a terceros de la información clasificada como información pública reservada e información pública clasificada sin la correspondiente autorización del propietario del activo de información.
- Está expresamente prohibido retirar expedientes documentales de las instalaciones de la Entidad, salvo en los casos en que sea estrictamente necesario para el cumplimiento de funciones del servicio. En dichos casos, se deberá contar con una autorización previa y expresa, la cual debe ser solicitada mediante correo electrónico dirigido al jefe inmediato, con copia al jefe de dependencia correspondiente y al profesional de gestión del área

Administrativa. La autorización deberá ser emitida por el jefe inmediato a través del mismo medio, incluyendo copia a los mismos destinatarios, dejando constancia explícita del permiso para el retiro del expediente.

5.4.2 LINEAMIENTOS RESPECTO AL SOFTWARE

- Sólo está permitido el uso de software licenciado y/o aquel que sin requerir licenciamiento este permitido por el Profesional de Gestión del Área de Tecnologías de la Información y las Comunicaciones, y el Profesional de Gestión de Seguridad y Privacidad de la Información.
- Está prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas y/o de procedencia desconocida.
- Los funcionarios y/o contratistas no podrán efectuar ninguna de las siguientes acciones sin previa autorización de la Oficina de Seguridad y Privacidad de la información:
 - a. Usar licencias no autorizadas por el área de Tecnologías de la Información y las Comunicaciones.
 - b. Modificar, revisar, transformar o adaptar cualquier software propiedad de la Entidad.
 - c. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Entidad.
- El área de Tecnologías de la Información y las Comunicaciones es la única área autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Los contratistas de la entidad tendrán responsabilidad tanto civil como penal en lo relacionado al uso aceptable de los activos de información de la Entidad.
- La instalación de software y/o sistemas sólo podrán ser efectuadas por el área de Tecnologías de la Información y las Comunicaciones, siendo ésta quien efectúe las pruebas técnicas de la instalación, así como su mantenimiento y respaldos.

5.4.3 LINEAMIENTOS PARA EL USO DEL CORREO ELECTRÓNICO

- Todas las cuentas de correo electrónico institucional deben usarse de manera responsable y exclusivamente para fines propios del desarrollo de las funciones y responsabilidades asignadas por la Entidad. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
- Las cuentas de correo son personales e intransferibles y no se debe ceder el uso de la cuenta de correo a terceras personas.
- Al finalizar su vinculación todo funcionario y/o contratista, debe realizar la devolución de la cuenta de usuario de correo electrónico al jefe inmediato y/o supervisor para el cual laboraba, según los procedimientos establecidos.
- No se debe asociar el correo electrónico institucional a redes sociales, cuentas bancarias ni a ningún tipo de cuentas personales, salvo cuando estas estén directamente relacionadas con las funciones.
- Los siguientes usos del servicio de correo electrónico se consideran usos no autorizados y prohibidos:
 - o Envío de correos masivos sin autorización oficial.
 - o Es estrictamente prohibido el envío de cadenas.
 - o Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM.

- Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Entidad o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la entidad.
 - Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
 - Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
 - Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
- Para el caso de correos que contengan información confidencial o reservada según su clasificación de confidencialidad en el campo asunto del correo electrónico debe especificarse dicho nivel de clasificación de la información.
 - Se debe evitar el envío de información a destinatarios erróneos, por lo cual los usuarios deben revisar los destinatarios del mensaje antes de proceder con su envío.
 - Está prohibido el uso del correo electrónico personal para el envío o la recepción de cualquier tipo de información propia de la Entidad.

5.4.4 LINEAMIENTOS PARA EL ALMACENAMIENTO DE LA INFORMACIÓN

- El almacenamiento de expedientes documentales físicos debe cumplir con los lineamientos establecidos por el proceso de Gestión Documental.
- La información clasificada como reservada o confidencial no debe ser almacenada en los equipos de cómputo de manera local. Esta debe organizarse y conservarse dentro del expediente correspondiente en el gestor documental adoptado oficialmente por la Entidad, el cual garantiza los niveles adecuados de seguridad, preservación y trazabilidad. Aunque OneDrive puede utilizarse como un medio de almacenamiento temporal o de apoyo, no se considera un repositorio oficial. Por lo tanto, toda información de carácter reservado o confidencial debe ser gestionada exclusivamente a través del sistema documental institucional, en cumplimiento con las políticas de conservación y seguridad de la información
- Está prohibido el almacenamiento de información en recursos diferentes a los autorizados para este propósito.
- La información confidencial o reservada que de manera temporal deba ser almacenada en repositorios diferentes al gestor documental dispuesto por la Entidad debe:
 - Estar protegida contra accesos no autorizados
 - Emplear mecanismos de cifrado de la información para impedir la pérdida de la confidencialidad o integridad de esta.
 - Borrar o formatear los dispositivos de almacenamiento autorizados antes de realizar el copiado de la información.
- Cuando se requiera el envío físico de expedientes o documentos que contengan información confidencial o reservada de la Entidad, se deben utilizar servicios que permitan tener el seguimiento y trazabilidad del envío y en caso de hacer uso de los servicios postales contratados por la Entidad deberá realizarse por correo certificado.
- Los documentos que contengan información sensible se deben retirar de las impresoras inmediatamente.
- Es responsabilidad de los funcionarios y/o contratistas mantener copias de seguridad de la información contenida en sus equipos de cómputo y entregarlas al finalizar la vinculación

con la entidad. Estas copias de seguridad se refieren únicamente al uso de OneDrive para el almacenamiento de documentos de trabajo.

- Los funcionarios y/o contratistas no deben guardar ningún tipo de información personal en los equipos asignados, solo se permite la información necesaria relacionada con el cumplimiento de sus funciones.
- Emplear sólo para la transferencia de datos y no como dispositivos de almacenamiento, las memorias flash (USB, SD, discos duros extraíbles, entre otras) la información deberá ser eliminada de manera segura una vez transferida, para tal fin deberán solicitar apoyo al área de Tecnologías de la Información y las Comunicaciones.
- Mantener la información en el servidor, o servicios en la nube o equipos destinados para ello, ya que los medios removibles NO son alternativa de respaldo de información permanente

5.4.5 LINEAMIENTOS PARA LA ELIMINACIÓN DE ACTIVOS DE INFORMACIÓN

- Los medios de almacenamiento electrónico de datos y los medios físicos que tengan información confidencial o reservada, deben ser físicamente destruidos antes de su disposición final.
- El papel impreso con información confidencial o que contenga datos personales nunca debe ser reutilizado.
- Eliminar la información de los medios que contengan datos sensibles o de carácter confidencial, mediante técnicas de borrado seguro de datos, dejando registro de las acciones realizadas durante el proceso de eliminación, para facilitar la trazabilidad de eventos.
- El área de Tecnologías de la Información y Comunicaciones es la responsable de realizar un borrado seguro a los medios reutilizables, que contengan o hayan contenido información crítica o sensible y se van a retirar de las instalaciones y autorizar el retiro de dichos medios dejando registro de las acciones realizadas durante el proceso de eliminación, para facilitar la trazabilidad de eventos.
- El área de Tecnologías de la Información y las Comunicaciones es la responsable de emitir conceptos técnicos que determinen la disposición final de los activos de servicios, hardware o software.
- La eliminación de expedientes documentales físicos y digitales deberá realizarse de acuerdo con los lineamientos establecidos por el proceso de Gestión Documental y la normatividad del Archivo General de la Nación.

5.4.6 LINEAMIENTOS PARA LA DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN

- Todos los funcionarios, contratistas y terceros tienen la responsabilidad de devolver los activos de información que se encuentren a su cargo al terminar su empleo, contrato o vínculo con la Entidad.
- Es responsabilidad de los jefes de dependencias y líderes de áreas verificar el cumplimiento de procedimientos y actividades para la entrega y custodia de activos de información, conforme a los equipos de trabajo asignados a cada uno de ellos.
- Al momento de presentarse una novedad de retiro informada por el área de Gestión Humana a través del formato de novedades de personal (TIC-fr-02) conforme al procedimiento de desvinculación de personal GH-pr-05, el funcionario que tiene la novedad deberá devolver todos los activos de información así:
 - o Devolver los bienes incluyendo los equipos de cómputo y dispositivos de almacenamiento que se le hayan entregado en custodia para el desarrollo de sus funciones diligenciando el formato de Paz y Salvo de inventarios (AB-fr-01) en el cual

deberá quedar descrito el estado de los activos físicos al momento de la devolución que se encuentran bajo su responsabilidad.

- El funcionario que se retira deberá realizar la entrega al jefe inmediato de todos los expedientes en archivo de gestión, tanto físicos como digitales, que reposen bajo su custodia entregando la relación de estos, en el formato de acta de entrega de Cargo (Anexo 7.15 del procedimiento de desvinculación de funcionarios GH-pr-05) conforme a las Tablas de Retención Documental y a los lineamientos del proceso de gestión documental.
- El proceso de Gestión Documental deberá certificar la entrega del gestor documental que la Entidad tenga adoptado debidamente gestionado para lo cual diligenciará el formato GH-fr-47 Certificado administrativo para retiro de funcionarios en lo correspondiente a Gestión Documental.
- Una vez recibidos los equipos de cómputo y discos extraíbles por el área Administrativa, estos deberán ser entregados de manera inmediata al área de Tecnologías de la Información y las Comunicaciones, para que realice el Backup de la información contenida en los dispositivos móviles, la cual será salvaguardada en OneDrive en la cuenta que el área de Tecnologías de la Información y las Comunicaciones haya designado para este propósito, el cual deberá preservarse por al menos 5 años (dicho término se establece basado en la prescripción de acciones). Para los casos en que el funcionario retirado se haya considerado como activo de información el Backup deberá ser entregado a la Oficina de Seguridad y Privacidad de la información para su custodia en una cuenta especial destinada para tal fin. Cuando se haya finalizado dicho Backup el Profesional de Gestión del Área de Tecnologías de la información y las comunicaciones deberá diligenciar el formato GH-fr-47 *Certificado administrativo para retiro de funcionarios* en lo correspondiente al Área de Tecnologías de la información y las Comunicaciones - TICs.
- Después de realizado y asegurado el Backup, el área de Tecnologías de la Información y las Comunicaciones deberá realizar el formateo del dispositivo asegurando el borrado seguro de la información.
- En caso de que el funcionario retirado tenga asignado Certificado de firma digital, este deberá ser revocado de manera inmediata por parte del funcionario con acompañamiento del área de Tecnologías de la Información y las Comunicaciones. Dicha situación deberá quedar registrada en el formato GH-fr-47 *Certificado administrativo para retiro de funcionarios* en lo correspondiente al Área de Tecnologías de la información y las Comunicaciones TIC. Los certificados de firma digital físicos (Token) deberán ser entregados a la Oficina de Seguridad y Privacidad de la información para su custodia.
- Una vez conocida la novedad de personal de retiro, el área de Tecnologías de la información y las comunicaciones deberá deshabilitar los accesos a todos los sistemas de información de la Entidad (correo, VPN, gestor documental, etc)
- Si el funcionario retirado posee accesos privilegiados, o a otros sistemas de información externos en representación de la Entidad, estos deberán ser entregados al jefe inmediato y deberán cambiarse las contraseñas de dichos sistemas de información de manera inmediata. Es responsabilidad de los jefes inmediatos bloquear los accesos a sistemas de información externos que no son administrados por el área de Tecnologías de la información y las Comunicaciones.
- La Subdirección Administrativa y Financiera coordinará, a través del área Administrativa, la recepción de tarjetas de ingreso a las sedes y/o notificará a las administraciones del edificio la desvinculación del personal.
- En caso de que el Área de Tesorería haya asignado token de entidades financieras al funcionario retirado, una vez recibida la novedad de personal, deberá informar mediante correo electrónico al funcionario que se va a retirar con copia al jefe

inmediato para que realice la recepción de estos, la cual deberá quedar consignada en el acta de entrega de Cargo (Anexo 7.15 del procedimiento de desvinculación de funcionarios GH-pr-05). La entrega de los tokens deberá ser realizada al Profesional de Gestión del Área de Tesorería dejando como constancia un correo electrónico el cual deberá ser anexo al acta de entrega del cargo. El área de Tesorería deberá en todos los casos deshabilitar los accesos a las Entidades Financieras.

5.5 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

- La identificación de activos de información permite clasificar los activos que requieren mayor protección, pues permite determinar sus características y el rol que cumplen dentro de los procesos de la Entidad.
- La identificación y/o actualización del inventario de activos de información debe realizarse cuando se presente una o más de las siguientes situaciones:
 - o Ha transcurrido un período superior a un (1) año desde la última revisión del inventario correspondiente a cada proceso.
 - o Se realiza una actualización en un proceso existente.
 - o Existen cambios en la estructura organizacional o en los procesos de la Entidad (eliminación o creación de un área o proceso).
 - o Se presentan cambios tecnológicos que generen nuevos activos de información o que modifiquen los ya existentes.
 - o Cambios o migraciones de sistemas de información en dónde se almacenan o reposan activos de la ubicación ya inventariados.
 - o Entra en vigor una nueva norma o se modifica la normatividad aplicable.

En caso de que se identifique alguna de estas situaciones el líder de proceso deberá notificar a la Oficina de Seguridad y Privacidad de la Información para que se realice el acompañamiento para la actualización correspondiente al inventario de activos de información.

- La aprobación de la matriz del inventario y valoración de activos de información estará a cargo del Director General, previa revisión de la Subdirección de Planeación Control y Seguimiento, y Subdirección Administrativa y Financiera, quienes también deberán firmar dicha matriz junto con el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información. Las subdirecciones mencionadas deben firmar la matriz dado que en ellas se concentran los activos de información.
- La Entidad dentro de la identificación de activos de información tecnológicos no posee activos que puedan clasificarse como Infraestructura Crítica Cibernética Nacional conforme con Lineamiento para la identificación de infraestructuras críticas cibernéticas¹
- El inventario de activos de información de la entidad debe contener, como mínimo, los siguientes atributos para cada activo:
 - Información básica del activo: nombre, proceso, dependencia, descripción, tipo, formato, idioma, medio de conservación, ubicación (física y electrónica), entre otros.
 - Nivel de clasificación del activo, determinado con base en los criterios de confidencialidad integridad y disponibilidad, así como su nivel de criticidad.
 - Identificación del propietario y del custodio del activo.

¹ Lineamiento para la identificación de infraestructuras críticas cibernéticas establecido por MinTic (https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401778_recurso_1.pdf)

5.6 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La clasificación de los activos de información obedece a la calificación de los activos de acuerdo con la Ley de Transparencia y Acceso a la Información Pública, Ley de datos personales, y usos internos de la información basado en términos de Confidencialidad, Integridad y Disponibilidad de cada activo.

5.6.1 CLASIFICACIÓN DE ACUERDO CON LA CONFIDENCIALIDAD

La confidencialidad es la propiedad de la información que garantiza que esta no sea accesible ni divulgada a personas, entidades o procesos no autorizados. En este sentido, se establecen tres (3) niveles de confidencialidad, alineados con los tipos de información definidos en la Ley 1712 de 2014:

CLASIFICACIÓN	DESCRIPCIÓN
INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.

5.6.2 CLASIFICACIÓN DE ACUERDO CON LA INTEGRIDAD

La integridad es la propiedad de la información que garantiza su exactitud y completitud, conforme a la norma ISO 27000. Esta característica asegura que la información se mantenga precisa, coherente y completa desde el momento de su creación hasta su eventual eliminación. Con base en este principio, la información se clasifica en tres (3) niveles:

CLASIFICACIÓN	DESCRIPCIÓN
A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.

CLASIFICACIÓN	DESCRIPCIÓN
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

5.6.3 CLASIFICACIÓN DE ACUERDO CON LA DISPONIBILIDAD.

La disponibilidad es una característica fundamental de la información, la cual asegura que esta se encuentre accesible y utilizable por las personas, entidades o procesos debidamente autorizados, en el momento y la forma requeridos. Esta propiedad debe garantizarse tanto en el presente como en el futuro, junto con los recursos necesarios para su correcto uso y gestión:

Para tal fin, se determina la siguiente clasificación

CLASIFICACIÓN	DESCRIPCIÓN
1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

5.7 ETIQUETADO DE ACTIVOS DE INFORMACIÓN

El etiquetado de los activos de información consiste en asignar una clasificación visible y clara a cada activo, de acuerdo con los niveles de confidencialidad, integridad y disponibilidad previamente definidos. Este proceso permite identificar rápidamente el tipo de protección que requiere la información, facilitando su gestión segura y el cumplimiento de la normativa vigente. El etiquetado debe realizarse en el momento de creación o incorporación del activo, y actualizarse cada vez que cambien sus características o nivel de sensibilidad.

5.7.1 LINEAMIENTOS PARA EL ETIQUETADO DE ACTIVOS DE INFORMACIÓN

- Los propietarios y/o custodios de la información son responsables de etiquetar adecuadamente la información conforme a los criterios definidos.
- El etiquetado debe colocarse de acuerdo con el tipo de activo o medio que contiene la información clasificada.
- Cualquier excepción de etiquetado de la información debe ser informada al Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información con su respectiva justificación, quien analizará la viabilidad de la excepción y la autorizará en caso de darse

por un impedimento o situación de fuerza mayor. En caso de no poderse dar la autorización, dicho profesional considerará la pertinencia de elevar la situación al Subcomité de Seguridad de la Información en los casos en que el activo esté clasificado como de valor ALTO para la entidad.

- d) Los documentos de salida generados desde los sistemas de información adoptados por la Entidad deben, en lo posible, contener el etiquetado de la información.
- e) Los activos de información que sean clasificados como públicos no contendrán ninguna etiqueta conforme a su tratamiento, sin embargo deberán contener una marca de agua que indique es una copia no controlada.
- f) Para los documentos en formato físico, se deberán utilizar etiquetas visibles. En el caso de los medios electrónicos, se establecerá el uso de etiquetas mediante marcas de agua, símbolos o metadatos, de acuerdo con la posibilidad técnica de implementarlo.
- g) En el caso del gestor documental, el responsable del expediente deberá marcar el mismo conforme la clasificación de confidencialidad que dispone el sistema para que de esta manera los documentos hereden dicha clasificación.
- h) Para el caso de documentos, la etiqueta deberá estar impresa o incluida en la parte inferior izquierda
- i) Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado como si tuviera la clasificación de confidencialidad más alta establecido por la entidad.
- j) Para el caso de manuales, procedimientos o formatos adoptados por el Sistema de Gestión de Calidad, la etiqueta deberá estar incluida en el pie de página en el caso de manuales, procedimientos y formatos. Es importante señalar que los formatos publicados en la página web institucional no llevarán la etiqueta correspondiente, dado que se consideran anexos del procedimiento o manual asociado. No obstante, el formato original deberá conservar y garantizar su etiquetado conforme a la clasificación establecida en la matriz de inventario de activos de información. **NOTA:** El etiquetado de los documentos controlados por el Sistema de Gestión de la Calidad será de aplicación obligatoria a partir de la adopción del presente procedimiento, y regirá para todos los documentos que se emitan o actualicen en lo sucesivo.
- k) El etiquetado de la información se realizará basado en los siguientes criterios

Medio	Tipo de etiquetado
Físico electrónico (Ejemplo: Unidades de disco externo, USB, CD, DVD, entre otros)	Etiquetado físico
Papel	Etiquetado físico
Electrónico (Ejemplo: Documentos digitales, correo electrónico, publicaciones web)	Etiqueta electrónica.

- l) Para las etiquetas se deberá incluir la clasificación por Confidencialidad, Integridad y Disponibilidad así:

CLASIFICACIÓN	CRITERIO	ETIQUETA
CONFIDENCIALIDAD	Información Pública Reservada	IPR
	Información Pública Clasificada	IPC
	Información Pública	IPU
INTEGRIDAD	Alta	IA
	Media	IM
	Baja	IB

CLASIFICACIÓN	CRITERIO	ETIQUETA
DISPONIBILIDAD	Alta	DA
	Media	DM
	Baja	DB

Ejemplo: Para el caso del activo denominado: Paz y Salvo Administrativo la etiqueta sería IPR – IA - DA

- m) Con el fin de garantizar la autenticidad de documentos que deban ser publicados en la web y que no tengan un mecanismo de validación, estos deberán incluir una nota al pie de página que indique: "Al imprimir este documento se convierte en **COPIA NO CONTROLADA** del SIG y su uso es responsabilidad directa del usuario".

6 DESCRIPCIÓN DE LA ACTIVIDAD

No.	Nombre de la actividad	Descripción	Responsable	Registros
1	Identificar / inventario y/o actualización de activos de información	Identificar, y evaluar la inclusión en la matriz de inventarios de activos de información. NOTA: En caso de que se requiera registrar un nuevo activo de información, actualizar o modificar uno existente, o eliminar alguno previamente identificado que ya no esté en uso, se deberá enviar una solicitud mediante correo electrónico solicitando la actualización de la matriz al Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información, con copia al Grupo de Gestión Documental. Esto con el fin de evaluar de manera integral y sistémica la pertinencia de dicha actualización y mantener actualizados los registros en ambos procesos.	Profesional de gestión de la Oficina de Seguridad y Privacidad de la información / Líderes de proceso	Matriz de inventario de activos de información (SPI-fr-10) Correo electrónico de solicitud de modificación o actualización de la matriz de inventario de activos de información.
2	Clasificar los activos de información	Realizar, en la matriz de inventario de activos de información, la clasificación de activos de información calificando cada uno en términos de Confidencialidad, Integridad y Disponibilidad.	Profesional de Gestión Oficina de Seguridad y Privacidad de la Información	Matriz de inventario de activos de información (SPI-fr-10)

No.	Nombre de la actividad	Descripción	Responsable	Registros
			/ Líderes de proceso	
3	Consolidar el inventario de activos de información	<p>Consolidar en la matriz de inventario de activos de información, la información requerida por cada activo identificado.</p> <p>Una vez actualizada la información por el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información, el líder del proceso revisa, aprueba y envía la matriz del inventario de activos al Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información.</p>	<p>Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información / Líderes de proceso</p>	<p>Matriz de inventario de activos de información (SPI-fr-10)</p> <p>Correo de aprobación.</p>
4	Aprobar el inventario de activos de información	<p>Una vez validados los activos de información por parte de los líderes de proceso, se aprobará el inventario mediante firma de la matriz de inventarios de activos de información, la cual será firmada por el Profesional de gestión de la Oficina de Seguridad y Privacidad de la información, la Subdirectora de Planeación Control y Seguimiento, la Subdirectora Administrativa y Financiera, y el Director General.</p> <p>En caso de que se sugieran ajustes sobre la matriz de inventarios de activos de información, el Profesional de Gestión de la Oficina de Seguridad y Privacidad de la información y los líderes de proceso realizarán los ajustes que se consideren pertinentes.</p>	<p>Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información / Subdirectora de Planeación Control y Seguimiento / Subdirectora Administrativa y Financiera / Director general / Líderes de proceso</p>	<p>Matriz de inventario de activos de información (SPI-fr-10)</p>
5	Socializar el inventario de activos de información	<p>Solicitar la socialización de la matriz de inventarios de activos de información, mediante cápsula informativa al área de Relacionamento</p>	<p>Profesional de Gestión de la Oficina de Seguridad y</p>	<p>Matriz de inventario de activos de información (SPI-fr-10)</p>

No.	Nombre de la actividad	Descripción	Responsable	Registros
		Interinstitucional y Comunicaciones. NOTA: Teniendo en cuenta que la matriz de inventario de activos de información debe ser un documento clasificado como "Confidencial" este solo podrá ser divulgado para uso interno.	Privacidad de la Información	Correo de solicitud de socialización
6	Realizar etiquetado de la información	Realizar el etiquetado de la información conforme a los lineamientos establecidos.	Todos los funcionarios	Activos etiquetados.

7 ANEXOS

7.1 Matriz de Inventario de Activos de Información (SPI-fr-10)

8 CONTROL DE CAMBIOS

No.	Fecha	Descripción del cambio o modificación
1	Octubre/2025	Primera emisión

JOHANNA TRINIDAD CAÑÓN LONDOÑO <small>Firmado digitalmente por JOHANNA TRINIDAD CAÑÓN LONDOÑO Fecha: 2025.10.01 07:38:37 -05'00'</small>	 Firmado digitalmente por MARICELA OYOLA MARTINEZ MARICELA OYOLA MARTÍNEZ	 Firmado digitalment e por LUIS CARLOS CABEZAS PULECIO LUIS CARLOS CABEZAS PULECIO	 Firmado digitalmente por ANGELA PATRICIA ALVAREZ LEDESMA ÁNGELA PATRICIA ÁLVAREZ LEDESMA	 Firmado digitalmente por Rubén Darío Ochoa Arbeláez RUBÉN DARIO OCHÓA ARBELÁEZ
Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información	Subdirectora Administrativa y Financiera	Subdirector Jurídico	Subdirectora de Planeación, Control y Seguimiento	Director General
ELABORÓ	REVISÓ			APROBÓ

