ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

INSTRUCTIVO
CLASIFICACIÓN ACTIVOS DE INFORMACIÓN

INSTITUTO PARA LA ECONOMIA SOCIAL PES

Bogotá, 2026

Elaboró	Revisó:	Aprobó:
Michael Brayan Pinilla Coy Contratista GIRT - SDAE	Hans Lwver Carlosama Alferez Profesional Especializado GIRT - SDAE	Adriana Villamizar Subdirectora GIRT - SDAE

TABLA DE CONTENIDO

1. OBJETIVO....3
2. ALCANCE....3
3. RESPONSABLES....3
4. DEFINICIONES....4
5. ABREVIATURAS....5
6. CONDICIONES GENERALES....6
7. DESARROLLO....6
8. DOCUMENTOS ASOCIADOS....20
9. MARCO NORMATIVO DE REFERENCIA....20
10. ANEXO — TABLA RESUMEN DE TIPIFICACIÓN DE ACTIVOS DE INFORMACIÓN IPES....21
11. CONTROL DE CAMBIOS....22

1. OBJETIVO

Definir, implementar, mantener y mejorar los lineamientos para la identificación, inventario y clasificación de los activos de información e infraestructura crítica cibernética del Instituto para la Economía Social – IPES, garantizando niveles apropiados de confidencialidad, integridad y disponibilidad de la información institucional, conforme a los lineamientos de la NTC/ISO-IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, la Ley 1712 de 2014 sobre acceso a la información pública y la Ley 1581 de 2012 sobre protección de datos personales.

2. ALCANCE

El presente instructivo aplica a todos los procesos, dependencias, servidores públicos, contratistas y proveedores del Instituto para la Economía Social – IPES que produzcan, custodien, traten o utilicen activos de información en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI del IPES.

3. RESPONSABLES

- **Subdirección de Diseño y Análisis Estratégico (SDAE):** Como representante de la Dirección General para el desarrollo e implementación del Sistema Integrado de Gestión, se encargará de revisar y mantener actualizado el presente instructivo, y brindará asesoría y herramientas a los procesos para su correcta aplicación.

- **Oficial de Seguridad de la Información / Equipo Operativo del SIG:** Será responsable del desarrollo, coordinación e implementación del instructivo; recogerá iniciativas y armonizará los ejercicios de inventario y clasificación de activos de información en todos los procesos del IPES.

- **Líderes de Proceso y Jefes de Dependencia:** Son los propietarios de los activos de información de sus respectivas áreas. Deberán identificar, clasificar y actualizar los activos a su cargo en la Matriz de Inventario, validar la información producida por sus equipos y aprobar el inventario de su dependencia antes de su consolidación.

- **Servidores públicos y contratistas:** Todos los colaboradores del IPES que produzcan o custodien información son responsables de clasificar los activos de información bajo su cargo siguiendo los criterios establecidos en este instructivo, bajo la coordinación del Equipo Operativo del SIG.

- **Asesor de Control Interno:** Velará por la adecuada elaboración de las actividades de clasificación de activos de información, promoviendo su apropiación, entendimiento y evaluación.

4. DEFINICIONES

- **Activo de información:** Cualquier información o elemento relacionado con el tratamiento de ésta —sistemas, soportes, instalaciones, personas, entre otros— que tenga valor para la organización. *(ISO/IEC 27001:2022)*

- **Propietario del activo:** Persona, área o dependencia responsable de la producción del activo de información y de autorizar su acceso, uso y protección. Es quien conoce el valor del activo para la organización. *(ISO/IEC 27001:2022, Control A.5.9; MinTIC Lineamientos v5, 2025)*

- **Custodio del activo:** Área, proceso o dependencia encargada de la custodia, control e implementación de controles de protección sobre el activo de información. Puede ser diferente al propietario. *(MinTIC Lineamientos v5, 2025)*

- **Clasificación de la información:** Ejercicio mediante el cual se determina que un activo de información pertenece a uno de los niveles de clasificación definidos por la entidad, con el objetivo de asegurar que recibe el nivel de protección adecuado conforme a sus características de confidencialidad, integridad y disponibilidad. *(ISO/IEC 27001:2022, Control A.5.12)*

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. *(ISO/IEC 27001:2022)*

- **Integridad:** Propiedad de salvaguardar la exactitud y completitud de la información a lo largo de todo su ciclo de vida. *(ISO/IEC 27000:2018)*

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, en el momento y forma en que se requiera. *(ISO/IEC 27001:2022)*

- **Criticidad del activo:** Nivel de importancia estratégica y operativa de un activo de información para la entidad, determinado como resultado de la valoración combinada de sus propiedades de confidencialidad, integridad y disponibilidad. Puede ser Alta, Media o Baja.

- **Etiquetado de la información:** Procedimiento mediante el cual se marca la información de acuerdo con su nivel de clasificación, para asegurar un tratamiento diferenciado y consistente según su sensibilidad. *(ISO/IEC 27001:2022, Control A.5.13)*

- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones (TIC) o Tecnologías de Operación (TO), 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)*
- **Infraestructura Crítica Cibernética Nacional (ICCN):** Infraestructura soportada por las TIC y tecnologías de operación cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado, y cuya afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones y de la administración pública. *(MinTIC Lineamientos v5, 2025; Decreto 338 de 2022)*
- **Dato público:** Dato calificado como tal según los mandatos de la ley o la Constitución Política, y todos aquellos que no sean semiprivados o privados. *(Ley 1266 de 2008, art. 3)*
- **Dato semiprivado:** Dato que no tiene naturaleza íntima, reservada ni pública, y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general. *(Ley 1266 de 2008, art. 3)*
- **Dato privado:** Dato que por su naturaleza íntima o reservada solo es relevante para el titular. *(Ley 1266 de 2008, art. 3)*
- **Dato sensible:** Dato personal que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación; incluye datos sobre origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, datos de salud, vida sexual y datos biométricos. *(Ley 1581 de 2012, art. 5)*
- **No repudio:** Propiedad que garantiza que, cuando se realiza un intercambio de información, ninguna de las partes puede negar haberla enviado o recibido.

5. ABREVIATURAS

- **IPES:** Instituto para la Economía Social
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información
- **SDAE:** Subdirección de Diseño y Análisis Estratégico
- **SIG:** Sistema Integrado de Gestión
- **TRD:** Tabla de Retención Documental
- **CID:** Confidencialidad, Integridad, Disponibilidad
- **ICC / ICCN:** Infraestructura Crítica Cibernética / Nacional

- **SIC:** Superintendencia de Industria y Comercio
- **RNBD:** Registro Nacional de Bases de Datos
- **NNA:** Niños, niñas y adolescentes

6. CONDICIONES GENERALES

El presente instructivo se enmarca en las siguientes condiciones que deben ser observadas por todos los colaboradores del IPES en el ejercicio de identificación, inventario y clasificación de activos de información:

- El inventario y clasificación de activos de información es una actividad obligatoria para todos los procesos del IPES incluidos en el alcance del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, conforme a lo establecido en la NTC/ISO-IEC 27001:2022 (Control A.5.9) y los lineamientos del MSPI del MinTIC.

- El instrumento oficial para el registro del inventario de activos de información del IPES es la Matriz de Inventario y Clasificación de Activos de Información dispuesta por el MinTIC (formato articles-401780), que constituye el formato institucional adoptado por el IPES para este fin.

- Todos los activos de información deben ser identificados, tipificados, clasificados y valorados conforme a los criterios de Confidencialidad, Integridad y Disponibilidad – CID establecidos en este instructivo.

- Cada activo de información debe tener un propietario y un custodio claramente definidos. Ningún activo puede quedar sin responsable asignado.

- Los activos de información que no hayan sido clasificados deben tratarse como Información Pública Reservada en confidencialidad, como Alta en integridad y como Alta en disponibilidad, hasta tanto se realice su clasificación formal.

- El inventario de activos debe revisarse y actualizarse al menos una vez al año, o cada vez que se presenten las causales de actualización definidas en la sección (CAUSALES DE ACTUALIZACIÓN DEL INVENTARIO) del presente instructivo.

- Los activos de información que contengan datos personales deben ser reportados ante la Superintendencia de Industria y Comercio a través del Registro Nacional de Bases de Datos – RNBD, conforme al Decreto 1074 de 2015.

- El presente instructivo debe leerse y aplicarse en conjunto con el PA03-MN-001 V5 Manual del Sistema de Gestión de Seguridad y Privacidad de la Información del IPES.

7. DESARROLLO

El proceso de inventario y clasificación de activos de información del IPES se estructura en las siguientes etapas, que corresponden a las fases del formato oficial MinTIC:

- **IDENTIFICACIÓN Y TIPIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

  - **Fuentes para la identificación:**
    Los propietarios y custodios de la información de cada dependencia deben identificar los activos de información tomando como fuentes:

    - Las Tablas de Retención Documental – TRD vigentes del IPES, que contemplan las series, subseries y tipos documentales de la información producida, su medio de conservación y preservación.
    - Los sistemas de información y plataformas tecnológicas utilizadas en cada proceso.
    - Los procesos y procedimientos del Sistema Integrado de Gestión del IPES.
    - Las fuentes de valor no contempladas en las TRD, que deben ser identificadas por los líderes de proceso en coordinación con el proceso Grupo de la Información y Recursos Tecnológicos (GIRT) y el Equipo de planeación de la Subdirección de Diseño y Análisis Estratégico.

    Es importante identificar primero la información como activo primario y luego determinar los activos secundarios que participan en su tratamiento. Por ejemplo: la información de beneficiarios de un programa del IPES se almacena en una base de datos, que reside en un servidor alojado en un centro de datos, al que se accede a través de una aplicación web. En este caso deben identificarse como activos: la información, el gestor de base de datos, el servidor, el datacenter, la aplicación y las redes por donde fluye la información, dado que los controles de seguridad para cada activo son diferentes.

  - **Tipificación de activos**

    De acuerdo con los lineamientos de la NTC/ISO-IEC 27001:2022 y el MinTIC, los activos de información del IPES se clasifican en los siguientes 7 tipos:

    - **Información:** Corresponde a datos e información almacenada o procesada, tanto en medios físicos como electrónicos. Incluye: bases de datos, archivos de gestión, contratos, documentación de sistemas, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos, planes de continuidad, acuerdos sobre retiro y pruebas de auditoría, entre otros. Es el activo primario a partir del cual se identifican los demás activos.

- **Hardware:** Medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta el IPES. Incluye: servidores, routers, módems, computadores de escritorio, computadores portátiles, tabletas, teléfonos IP, celulares, impresoras, periféricos, medios de almacenamiento (discos duros externos, USB, cintas, NAS, SAN).

- **Software:** Programas, aplicativos y sistemas de información que soportan las actividades del IPES y la prestación de sus servicios. Incluye: sistemas operacionales, software de administración de hardware, utilitarios de usuario final (ofimática, navegadores, antivirus, herramientas de desarrollo), aplicaciones de negocio (sistemas misionales, software financiero, gestión de talento humano, sistemas de gestión, bases de datos, correo electrónico, página web).

- **Servicios:** Servicios de computación, comunicaciones y utilidades que apoyan o soportan a los demás activos de información. Incluye: servicio de internet, intranet, directorios compartidos, páginas de consulta, así como servicios de soporte físico como iluminación, refrigeración, energía y aire acondicionado para las instalaciones de procesamiento.

- **Recurso Humano:** Personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información. Incluye: funcionarios de planta, contratistas y proveedores cuyo conocimiento aporta de manera relevante a la gestión misional institucional.

- **Instalaciones:** Lugares donde se almacenan o resguardan los sistemas de información y comunicaciones del IPES. Incluye: centros de cómputo, centros de cableado, datacenter, cuartos de servidores y demás áreas seguras donde se procese o almacene información institucional.

- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por TIC o Tecnologías de Operación (TO), cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos o en el funcionamiento efectivo del IPES como entidad pública. Su identificación se desarrolla en la sección (IDENTIFICACIÓN DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA) del presente instructivo.

- **DILIGENCIAMIENTO DE LA MATRIZ DE INVENTARIO Y CLASIFICACIÓN**

La Matriz de Inventario y Clasificación de Activos de Información del IPES corresponde al formato oficial dispuesto por el MinTIC. Está organizada en cuatro secciones y contiene 38 campos que se describen a continuación.

- **SECCIÓN A - IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN**
  (Ley 594 de 2000 · Ley 1712 de 2014 · Decreto 103 de 2015 · Decreto 1080 de 2015 · ISO 27001:2022)

  - **Campo 1 - Macroproceso:** Macroproceso del IPES al que pertenece el activo, según el mapa de procesos institucional vigente. En caso de que el IPES no tenga macroprocesos definidos, se puede dejar en blanco o consignar el nombre del proceso misional o de apoyo correspondiente.

  - **Campo 2 - Proceso:** Nombre del proceso del IPES al que pertenece el activo de información, conforme al Sistema Integrado de Gestión.

  - **Campo 3 - Identificador:** Código único del activo. Se sugiere construirlo como una concatenación del código de la dependencia según la TRD vigente del IPES más un número consecutivo. Ejemplo: PA03-001, PA03-002.

  - **Campo 4 - Tipo**: Tipo de activo conforme a la tipificación definida en la sección (Tipificación de activos). Los valores válidos son: Información, Hardware, Software, Servicios, Recurso Humano, Instalaciones, Infraestructura Crítica Cibernética.

  - **Campo 5 - Dependencia:** Nombre de la dependencia, área o proceso del IPES responsable del activo.

  - **Campo 6 - Serie documental:** Serie documental del área o proceso según la TRD vigente del IPES. Aplica principalmente para activos de tipo Información.

  - **Campo 7 - Subserie documental:** Subserie documental correspondiente según la TRD vigente del IPES. Aplica principalmente para activos de tipo Información.

  - **Campo 8 - Nombre:** Nombre completo y descriptivo del activo de información, suficientemente claro para identificarlo sin ambigüedad.

  - **Campo 9 - Descripción:** Descripción resumida del activo que permita entender su contenido, función o propósito dentro del proceso del IPES.

  - **Campo 10 - Nombre del responsable de la producción de la información (Propietario del activo):** Nombre del área, dependencia, proceso o cargo responsable de producir el activo de información y de autorizar su acceso y uso.

Este campo debe corresponder a un rol o cargo institucional, no a una persona natural específica, para garantizar la continuidad ante cambios de personal.

- **Campo 11 - Fecha de generación de la información:** Fecha en la que el activo de información fue incluido por primera vez en el inventario. Formato: DD/MM/AAAA.

- **Campo 12 - Nombre del responsable de la información (Custodio del activo):** Nombre del área, proceso o dependencia encargada de la custodia, control e implementación de controles de protección del activo. Al igual que el propietario, debe corresponder a un rol o cargo institucional.

- **Campo 13 - Fecha de ingreso del activo al archivo:** Fecha en la que el activo ingresó al archivo de gestión. Aplica para activos de tipo Información. Formato: DD/MM/AAAA.

- **Campo 14 - Soporte de registro:** Medio en el que se encuentra el activo. Los valores válidos son: Físico (análogo), Digital o Electrónico, o N/A (para activos que no sean de tipo Información, como Hardware, Software, Recurso Humano, etc.).

- **Campo 15 - Medio de conservación:** Lugar o sistema donde se conserva el activo. Ejemplos: Archivo de gestión, Sistemas de información corporativos, Unidades compartidas, Drive, servidor local, datacenter, etc.

- **Campo 16 - Formato:** Forma o modo en que se presenta la información o se permite su visualización. Ejemplos: hoja de cálculo, imagen, audio, video, documento de texto, base de datos, aplicación web, etc.

- **Campo 17 - Idioma:** Idioma en que se encuentra la información. Para el IPES será Español en la generalidad de los casos.

- **SECCIÓN B - CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN**
  (NTC/ISO-IEC 27001:2022)

  - **Campo 18 - Confidencialidad:** Nivel de confidencialidad del activo conforme al esquema definido en la sección **(Clasificación por Confidencialidad).** Los valores válidos son: Información Pública Reservada, Información Pública Clasificada, Información Pública, No Clasificada.

  - **Campo 19 - C (valor):** Valor numérico correspondiente al nivel de confidencialidad asignado, según la escala definida por el IPES en su metodología de valoración.

- **Campo 20 - Integridad:** Nivel de integridad del activo conforme al esquema definido en la sección **(Clasificación por Integridad)**. Los valores válidos son: Alta, Media, Baja, No Clasificada.

- **Campo 21 - I (valor):** Valor numérico correspondiente al nivel de integridad asignado.

- **Campo 22 - Disponibilidad:** Nivel de disponibilidad del activo conforme al esquema definido en la sección **(Clasificación por Disponibilidad)**. Los valores válidos son: Alta, Media, Baja, No Clasificada.

- **Campo 23 - D (valor):** Valor numérico correspondiente al nivel de disponibilidad asignado.

- **Campo 24 - Criticidad del activo:** Nivel de criticidad general del activo, resultado de la valoración combinada de las tres propiedades CID. Los valores son: ALTA, MEDIA o BAJA, conforme a los criterios de la sección **(Determinación de la Criticidad del Activo)**.

- **Campo 25 – Impacto Social:** El daño, perdida o deterioro afectaría (0,5%) de la población nacional (250,000 personas).

- **Campo 26 – Impacto Económico:** Se podrían generar pérdidas, gastos o costos iguales o superiores al PIB de un día o 0,123% del PIB Anual (464.619.736)

- **Campo 27 – Impacto Ambiental:** Se requieren 3 años o más para la recuperación

- **Campo 28 - ¿Es Infraestructura Crítica Cibernética?:** Indicar Sí o No según si el activo forma parte de la infraestructura crítica cibernética del IPES, conforme a los criterios de la sección **(IDENTIFICACIÓN DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA)**.

- **Campo 29 - Información publicada:** Indicar si la información está publicada y el medio: Publicada (Interno - Intranet), Publicada (Externo-Internet), No publicada.

- **Campo 30 - Lugar de consulta o ubicación:** URL, ruta de red, sistema de información, ubicación física o digital donde puede consultarse el activo. Ejemplo: https://www.ipes.gov.co, Unidad compartida Drive IPES, Archivo central, Sede Principal.

- **SECCIÓN C - ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA** *(Decreto 103 de 2015, compilado en el Decreto 1080 de 2015)*

Esta sección aplica únicamente para los activos clasificados como Información Pública Reservada o Información Pública Clasificada. Para los demás activos se diligencia N/A.

- **Campo 31 - Objeto legítimo de la excepción:** Descripción del objeto que justifica la reserva o clasificación de la información conforme a la Ley 1712 de 2014.

- **Campo 32 - Fundamento constitucional o legal:** Norma constitucional o legal que ampara la excepción al acceso a la información. Ejemplo: Artículo 74 de la Constitución Política; Ley 1712 de 2014.

- **Campo 33 - Fundamento jurídico de la excepción:** Artículo o disposición específica que sustenta la excepción. Ejemplo: Artículo 18 de la Ley 1712 de 2014.

- **Campo 34 - Excepción total o parcial: Indicar si la reserva aplica sobre la totalidad del activo o solo sobre una parte de su contenido: Total o Parcial.**

- **Campo 35 - Fecha de clasificación:** Fecha en la que se clasificó el activo como reservado o clasificado. Formato: DD/MM/AAAA.

- **Campo 36 - Tiempo de clasificación:** Plazo legal durante el cual se mantiene la reserva o clasificación, conforme a lo establecido en la Ley 1712 de 2014. Ejemplo: 15 años.

- **SECCIÓN D - DATOS PERSONALES**
  (Ley 1581 de 2012)

  Esta sección aplica para todos los activos. Si el activo no contiene datos personales, los campos 35 a 38 se diligencian con N/A.

  - **Campo 37 - ¿Contiene datos personales?: Indicar Sí o No.**

  - **Campo 35 - ¿Contiene datos personales de niños, niñas o adolescentes (NNA)?:** Indicar Sí o No. Este campo requiere especial atención dado el régimen de protección reforzada que establece la Ley 1581 de 2012 para datos de NNA.

  - **Campo 38 - Tipos de datos personales:** Indicar la categoría del dato personal contenido en el activo: Dato público, Dato semiprivado, Dato privado o Dato sensible, conforme a las definiciones de la sección (**DEFINICIONES Y ABREVIATURAS)** de este instructivo y la Ley 1581 de 2012.

- **Campo 39 - Finalidad de la recolección de los datos personales:** Descripción clara y específica del propósito para el cual el IPES recolecta o trata los datos personales contenidos en el activo.

- **Campo 40 - ¿Existe autorización para el tratamiento de los datos personales?:** Indicar Sí, No o N/A según si existe autorización expresa del titular para el tratamiento de sus datos, conforme al artículo 9 de la Ley 1581 de 2012.

- **Nota importante:** Los activos que contengan datos personales, especialmente aquellos con información pública clasificada o reservada, deben ser reportados ante la Superintendencia de Industria y Comercio a través del Registro Nacional de Bases de Datos – RNBD, conforme al Decreto Único 1074 de 2015.

- **CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

La clasificación de activos de información tiene como objetivo asegurar que cada activo recibe el nivel de protección adecuado de acuerdo con sus características particulares. El sistema de clasificación del IPES se basa en tres propiedades fundamentales de la seguridad de la información conforme a la NTC/ISO-IEC 27001:2022: Confidencialidad, Integridad y Disponibilidad – CID.

Para cada propiedad se establecen niveles que permiten determinar el valor general o criticidad del activo en el IPES, con el fin de identificar qué activos deben ser tratados de manera prioritaria.

- **Clasificación por Confidencialidad**

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados (ISO/IEC 27001:2022).

La clasificación por confidencialidad del IPES se define en cuatro niveles, los tres primeros alineados con los tipos de información declarados en la Ley 1712 de 2014:

Nivel	Descripción
INFORMACIÓN PÚBLICA RESERVADA	Información que no debe ser divulgada debido a que puede causar daño a intereses públicos. Solamente la Constitución o la ley pueden definir qué información es de carácter reservado. Su acceso está restringido

	únicamente al personal autorizado del proceso que la genera.
INFORMACIÓN PÚBLICA CLASIFICADA	Información que no debe ser divulgada porque puede vulnerar derechos de personas naturales o jurídicas, tales como: derecho a la intimidad, a la vida, salud o seguridad, y los secretos comerciales, industriales y profesionales. Corresponde al ámbito propio, particular y privado de una persona natural o jurídica conforme al artículo 18 de la Ley 1712 de 2014.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del IPES, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de información incluidos en el inventario que aún no han sido clasificados. Deben tratarse como Información Pública Reservada hasta tanto se realice su clasificación formal. Aplica típicamente para activos de tipo Hardware, Recurso Humano e Instalaciones.

Clasificación de datos personales conforme a la Ley 1581 de 2012:

Los activos clasificados como Información Pública Clasificada pueden contener datos personales, los cuales se subdividen en:

- **Dato semiprivado:** No tiene naturaleza íntima ni pública; su conocimiento puede interesar a cierto sector o grupo de personas. Ejemplo: datos financieros y crediticios.

- **Dato privado:** Por su naturaleza íntima o reservada, solo es relevante para el titular. Solo puede obtenerse por orden de autoridad judicial.

- **Dato sensible:** Afecta la intimidad del titular o su uso indebido puede generar discriminación. Incluye datos sobre origen racial o étnico, orientación política, convicciones religiosas, datos de salud, vida sexual y datos biométricos. Su tratamiento está prohibido salvo las excepciones establecidas en el artículo 6 de la Ley 1581 de 2012.

Nota: Para los activos que contengan información pública clasificada, pública reservada o datos personales, se debe identificar qué criterios del Índice de Información Clasificada y Reservada (Decreto 103 de 2015, compilado en el Decreto 1080 de 2015) y de la Ley 1581 de 2012 les aplican, y realizar el reporte correspondiente ante la SIC a través del RNBD (Decreto 1074 de 2015).

- **Clasificación por Integridad**

  La integridad se refiere a la exactitud y completitud de la información a lo largo de todo su ciclo de vida, desde su creación hasta su destrucción (ISO/IEC 27000:2018).

- El IPES adopta el siguiente esquema de clasificación:

Nivel	Descripción
A - ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar las funciones del IPES, o generar pérdidas de imagen severas ante entes externos.
M - MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar funciones, o generar pérdida de imagen moderada para funcionarios o procesos del IPES.
B - BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para el IPES o entes externos.
NO CLASIFICADA	Activos de información incluidos en el inventario que aún no han sido clasificados. Deben tratarse como integridad ALTA hasta tanto se realice su clasificación formal.

- **Clasificación Clasificación por Disponibilidad**

  La disponibilidad es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, en el momento y forma en que se requiera (ISO/IEC 27001:2022). El IPES adopta el siguiente esquema de clasificación:

Nivel	Descripción

1 - ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar las funciones del IPES, o generar pérdidas de imagen severas ante entes externos.
2 - MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar funciones, o generar pérdida de imagen moderada del IPES.
3 - BAJA	La no disponibilidad de la información puede afectar la operación normal del IPES o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de información incluidos en el inventario que aún no han sido clasificados. Deben tratarse como disponibilidad ALTA hasta tanto se realice su clasificación formal.

- **Determinación de la Criticidad del Activo**

La criticidad del activo es el resultado de la valoración combinada de las tres propiedades CID y determina la prioridad con que el IPES debe gestionar los controles de seguridad sobre ese activo. Se determinan tres niveles:

Criticidad	Descripción
ALTA	Activos en los cuales la clasificación es Alta en dos o en las tres propiedades (confidencialidad, integridad y disponibilidad).
MEDIA	Activos en los cuales la clasificación es Alta en una sola propiedad, o al menos una de ellas es de nivel Medio.
BAJA	Activos en los cuales la clasificación en todas sus propiedades es Baja.

Nota: Los activos con criticidad ALTA deben ser tratados de manera prioritaria en la gestión de riesgos de seguridad de la información del IPES, y son los candidatos principales para la identificación de Infraestructura Crítica Cibernética conforme a la sección (IDENTIFICACIÓN DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA).

- **CAUSALES DE ACTUALIZACIÓN DEL INVENTARIO**

El inventario de activos de información del IPES debe revisarse y actualizarse, además de la revisión anual obligatoria, cada vez que se presente alguna de las siguientes situaciones:

- Actualizaciones al proceso al que pertenece el activo de información.
- Adición de nuevas actividades al proceso o inclusión de nuevos registros de calidad, referencia o procedimientos.
- Inclusión de un nuevo activo de información no contemplado previamente.
- Desaparición de un área, proceso o cargo que tenía asignado el rol de propietario o custodio del activo (cambios organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos ya inventariados.
- Cambios físicos en la ubicación de activos de información.
- Vinculación de nuevas aplicaciones de terceros que traten información del IPES o bajo su custodia, para las cuales deberá además asegurarse el cumplimiento de las políticas de seguridad de la información institucionales.
- Cambios normativos o de política que afecten la clasificación de la información.

- **IDENTIFICACIÓN DE INFRAESTRUCTURA CRÍTICA CIBERNÉTICA**

Una vez ejecutada la identificación y clasificación de activos, el IPES debe determinar si alguno de sus activos corresponde a Infraestructura Crítica Cibernética – ICC, entendida como aquellos sistemas y activos, físicos o virtuales, soportados por TIC o Tecnologías de Operación (TO), cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos o en el funcionamiento efectivo del IPES como entidad pública (Decreto 338 de 2022).

Para su identificación el IPES deberá:

- Determinar si gestionará los riesgos sobre todos los activos del inventario o únicamente sobre aquellos con criticidad Alta. Esta decisión debe estar debidamente documentada y aprobada por la Alta Dirección del IPES.
- Aplicar los criterios y la metodología de identificación de infraestructura crítica cibernética establecidos por el ColCERT, los cuales deben consultarse en cada ejercicio de actualización del inventario de activos.
- Identificar si los componentes de la posible ICC son de naturaleza TI (como servidores y aplicaciones) o de naturaleza TO (como sistemas de control o sensores), documentando cada componente en la matriz de inventario en el campo "¿Es Infraestructura Crítica Cibernética?".

- Si el IPES determina que posee Infraestructura Crítica Cibernética Nacional – ICCN, deberá reportarlo a las instancias y autoridades respectivas del Gobierno Nacional (ColCERT), conforme al Decreto 1078 de 2015 adicionado por el Decreto 338 de 2022.

- **ETIQUETADO DE LOS ACTIVOS DE INFORMACIÓN**

Conforme al Control A.5.13 de la NTC/ISO-IEC 27001:2022, el IPES debe desarrollar e implementar procedimientos para el etiquetado de la información de acuerdo con su esquema de clasificación. Se aplicarán los siguientes lineamientos:

- Se deben etiquetar todos los activos de información clasificados conforme al esquema CID del IPES.
- Un activo de información en formato impreso que no se encuentre etiquetado debe tratarse como si tuviera la clasificación de confidencialidad más alta (Información Pública Reservada – IPR).
- Las etiquetas de confidencialidad a utilizar son:

  - **IPR:** Información Pública Reservada
  - **IPC:** Información Publica Clasificada
  - **IP:** Información Publica.

  Las etiquetas de integridad a utilizar son: A (Alta), M (Media), B (Baja). Las etiquetas de disponibilidad a utilizar son: A (Alta), M (Media), B (Baja).

  Las etiquetas se combinan para reflejar la clasificación completa del activo. Ejemplo: un activo clasificado como Información Pública Reservada, con integridad Alta y disponibilidad Alta se etiquetaría: IPR – A – A.

- **LINEAMIENTOS COMPLEMENTARIOS**

- **Activos en la nube:** El IPES debe identificar y clasificar los activos de información almacenados, procesados o transmitidos mediante servicios en la nube (SaaS, PaaS, IaaS), aplicando los mismos principios de seguridad de los activos locales. Para cada servicio en la nube utilizado se debe documentar: tipo de servicio, responsable, niveles de disponibilidad esperados, mecanismos de respaldo, condiciones de monitoreo continuo, y consideraciones específicas de soberanía, cifrado, control de accesos y cumplimiento contractual con el proveedor. (ISO/IEC 27001:2022, Control A.5.23)

- **Eliminación segura de activos:** El IPES debe definir e implementar procedimientos para la eliminación segura de información contenida en activos físicos y digitales, asegurando que los datos no puedan ser recuperados una vez descartados. Estos procedimientos deben considerar el tipo de activo (papel, disco duro, dispositivos USB, nube), su nivel de clasificación, y el método de eliminación adecuado (desmagnetización, destrucción física, borrado certificado, entre otros). Toda eliminación debe estar documentada y respaldada por registros auditables. (ISO/IEC 27001:2022, Control A.7.10)

- **Activos no estructurados:** El IPES debe identificar, clasificar y controlar los activos digitales no estructurados, tales como archivos ofimáticos, correos electrónicos, presentaciones, grabaciones y otros documentos generados en la operación diaria que no estén formalizados en un sistema de gestión documental. Estos activos deben estar incorporados en el inventario y estar sujetos a revisión periódica.

- **REVISIÓN, APROBACIÓN Y PUBLICACIÓN DEL INVENTARIO**

El proceso de revisión, aprobación y publicación del inventario de activos de información del IPES sigue el siguiente flujo:

- **Elaboración:** El líder de cada proceso o su delegado elabora y actualiza el inventario de activos de su dependencia en la Matriz de Inventario y Clasificación de Activos de Información, con el apoyo del Equipo Operativo del SIG.

- **Validación del jefe de dependencia:** El jefe de cada dependencia valida y aprueba el inventario de activos de su área antes de su remisión para consolidación.

- **Consolidación:** El Equipo Operativo del SIG o el Oficial de Seguridad de la Información consolida los inventarios de todas las dependencias en una única matriz institucional.

- **Validación jurídica:** La Oficina Asesora Jurídica valida el inventario consolidado en lo referente a la correcta aplicación de las excepciones de información reservada y clasificada (Ley 1712 de 2014) y al cumplimiento de la Ley 1581 de 2012 en materia de datos personales.

- **Aprobación institucional:** El inventario consolidado y validado se presenta al Comité Institucional de Gestión y Desempeño para su aprobación formal, conforme al Decreto 1083 de 2015 modificado por el Decreto 1499 de 2017.

- **Publicación:** Una vez aprobado, el custodio del inventario remite el consolidado a la Oficina Asesora de Comunicaciones o quien haga sus veces, para su publicación en: el sitio web institucional del IPES, el enlace de Transparencia y Acceso a la Información Pública, el Portal de Datos Abiertos del Estado colombiano, y la intranet institucional. La publicación debe respetar las restricciones de acceso según la clasificación de cada activo, anonimizando o restringiendo los datos que así lo requieran conforme a la Ley 1581 de 2012.

8. DOCUMENTOS ASOCIADOS

Codigo	Documento
PA03-MN-001 V5	Manual del Sistema de Gestión de Seguridad y Privacidad de la Información — IPES
PA03-PD-009	Implementación de la Continuidad de la Seguridad de la Información
PA08-FO-010 V2	Acuerdo de Confidencialidad

9. MARCO NORMATIVO DE REFERENCIA

Norma / Estándar	Descripción
NTC/ISO-IEC 27001:2022	Sistema de Gestión de Seguridad de la Información — Requisitos
ISO/IEC 27000:2018	Vocabulario y definiciones de seguridad de la información
ISO/IEC 27002:2022	Controles de seguridad de la información — Guía de implementación
Ley 594 de 2000	Ley General de Archivos
Ley 1266 de 2008	Ley de Hábeas Data — Datos financieros
Ley 1581 de 2012	Protección de Datos Personales

Ley 1712 de 2014	Transparencia y Acceso a la Información Pública Nacional
Decreto 103 de 2015	Reglamentación parcial de la Ley 1712 de 2014 — Índice de Información Clasificada y Reservada
Decreto 1074 de 2015	Decreto Único Reglamentario del Sector Comercio — RNBD
Decreto 1080 de 2015	Decreto Único Reglamentario del Sector Cultura (compilación Decreto 103 de 2015)
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector de Función Pública, modificado por el Decreto 1499 de 2017
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC
Decreto 338 de 2022	Seguridad Digital — Infraestructura Crítica Cibernética Nacional
Resolución 500 de 2021	MinTIC — Lineamientos y estándares para la estrategia de seguridad digital

10. ANEXO — TABLA RESUMEN DE TIPIFICACIÓN DE ACTIVOS DE INFORMACIÓN IPES

La siguiente tabla constituye la guía de referencia rápida para que los líderes de proceso del IPES identifiquen correctamente el tipo al que pertenece cada activo de información al momento de diligenciar la Matriz de Inventario.

Tipo de Activo	Descripción	Ejemplos en el contexto IPES
Información	Datos e información almacenada o procesada en medios físicos o electrónicos, que constituye el activo primario a partir del cual se identifican los demás activos.	Bases de datos de beneficiarios, contratos, expedientes, manuales de procedimientos, informes de gestión, actas, resoluciones, registros de nómina, planes institucionales, acuerdos de confidencialidad
Hardware	Medios materiales físicos que soportan	Servidores de aplicaciones, equipos de

	directa o indirectamente los servicios que presta el IPES. Se registra por grupos o categorías funcionales, no equipo por equipo.	escritorio por dependencia, computadores portátiles, equipos de red (switches, routers), impresoras, teléfonos IP, dispositivos de almacenamiento.
Software	Programas, aplicativos y sistemas de información que soportan las actividades del IPES y la prestación de sus servicios.	Sistemas de información misionales, software financiero, sistema de gestión documental, correo electrónico institucional, sistemas operativos, antivirus, herramientas de ofimática, aplicaciones web.
Servicios	Servicios de computación, comunicaciones y utilidades que apoyan a los demás activos de información.	Servicio de internet, intranet institucional, servicio de nube (SaaS/PaaS/IaaS), servicio de energía regulada, aire acondicionado para datacenter, servicios de telecomunicaciones.
Recurso Humano	Personas cuyo conocimiento, experiencia y criticidad para el proceso las convierten en activos de información. Se registran por roles o cargos, no por nombre de personas.	Oficial de Seguridad de la Información, administrador de sistemas, gestor de base de datos, líderes de procesos misionales, contratistas con acceso a información crítica, proveedores estratégicos.
Instalaciones	Lugares donde se almacenan, procesan o resguardan los sistemas de información y comunicaciones del IPES	Datacenter o cuarto de servidores, centro de cableado, archivos físicos, sede principal, sedes operativas donde se procese información institucional.
Infraestructura Crítica Cibernética (ICC)	Sistemas y activos, físicos o virtuales, soportados por TIC o Tecnologías de Operación (TO), cuya afectación tendría un impacto grave en el funcionamiento del IPES o en la prestación de sus servicios esenciales a la ciudadanía.	Plataformas tecnológicas que soportan servicios esenciales del IPES a la ciudadanía, sistemas de control de acceso físico, infraestructura de red crítica, sistemas de continuidad del negocio.

11. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
01	07/03/2021		Elaboración de documento

02	20/04/2022		Ajuste general al documento
03	18/10/2023		Ajuste general al documento
04	12/04/2026	Todo el documento	Actualización a NTC/ISO-IEC 27001:2022. Incorporación de lineamientos MinTIC v5 (2025). Adopción del formato oficial MinTIC como instrumento institucional de inventario. Incorporación de secciones de Infraestructura Crítica Cibernética, Etiquetado de activos y Lineamientos complementarios (nube, eliminación segura, activos no estructurados). Actualización de tipificación de activos, definiciones y marco normativo. Actualización de referencias al PA03-MN-001 V5.