

CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

**GESTIÓN DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN**



ALCALDÍA MUNICIPAL DE
SOACHA

**EL CAMBIO
AVANZA** >>>

2021

Tabla de contenido

1. OBJETIVO.....	3
2. ALCANCE	3
3. RESPONSABLES.....	4
4. DEFINICIONES Y ABREVIATURAS	4
5. CONDICIONES GENERALES	5
6. PUBLICACION	6
7. REVISIÓN	6
8. ACTUALIZACIÓN.....	6
9. DESARROLLO	8
9.1. DEFINICIÓN	8
Información básica	9
Propiedad.....	10
Acceso	10
Gestión	10
Identificación del nivel soporte del Activo de información	10
Identificación del tipo de activo según su composición	11
Identificación del activo de acuerdo con su función:.....	11

1. OBJETIVO.

Definir, implementar, mantener y mejorar controles para la clasificación de los activos de información del Instituto Municipal para la Recreación y el Deporte de Soacha – IMRDS, que permitan alcanzar niveles apropiados de integridad, disponibilidad y confidencialidad de la información institucional, en consideración con la normatividad vigente relacionada con seguridad y privacidad de la información.

2. ALCANCE

El presente instructivo aplica para la clasificación de los activos de información en del Instituto Municipal para la Recreación y el Deporte de Soacha – IMRDS, en el marco del Subsistema de Gestión de Seguridad de la Información del IMRDS.

La clasificación de activos de información se debe realizar acorde con el alcance definido para la implementación del Manual del Subsistema de Seguridad y Privacidad de la Información; por otro lado, la gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del modelo de seguridad y privacidad de la información, para garantizar el cumplimiento de los puntos descritos a continuación:

- ✓ **Inventario de activos:** Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
- ✓ **Propiedad de los activos:** Los activos mantenidos en el inventario deberían tener un propietario.
- ✓ **Uso aceptable de los activos:** Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- ✓ **Devolución de activos:** Todos los contratista y funcionarios o de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Etiquetado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Manejo de activos: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

3. RESPONSABLES

La Subdirección Administrativa y Financiera como representante de la Dirección General para el desarrollo e implementación del Sistema Integrado de Gestión se encargará de revisar y adecuar el instructivo de clasificación de activos de información a las necesidades del IMRDS, también brindará la asesoría y las herramientas a los procesos para su correcta elaboración.

El Equipo de Gestión Documental y Gestión TIC, serán los encargados del desarrollo e implementación del instructivo de clasificación de activos de información, estos deberán recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación efectiva de las actividades de clasificación de los activos información del IMRDS.

El Equipo Directivo o Comité de Gestión y Desempeño Institucional se encargará del monitoreo constante y todos los servidores involucrados en cada proceso serán los encargados de clasificar los activos de información con el fin de implementar los controles necesarios para proteger a los mismos de los riesgos identificados en la Matriz de Riesgos Institucionales, bajo la coordinación del líder MIPG y la Subdirección Administrativa y Financiera.

El equipo de seguimiento y evaluación está conformado por la asesoría de Control Interno, los funcionarios y contratistas de su oficina, quienes velarán por la adecuada elaboración de las actividades de clasificación de los activos de información del IMRDS, promoviendo su apropiación, entendimiento y evaluación del mismo.

4. DEFINICIONES Y ABREVIATURAS

Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados 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.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y

privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

Información pública reservada: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley".

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.

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.

- a) **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.
- b) **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.
- c) **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- d) **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- e) **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

5. CONDICIONES GENERALES

- ✓ Cumplimiento de la normatividad vigente relacionada con gestión de activos, clasificación de activos de información.
- ✓ Desarrollar mecanismos para identificar, clasificar y proteger los diferentes tipos de activos de información a cargo del IMRDS.

6. PUBLICACION

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 autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien haga sus veces.

7. REVISIÓN

La actividad de revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el equipo de gestión de activos lo solicita a algún líder de proceso o el oficial de seguridad de la información si así lo requiere.

Las razones por las cuales debería realizarse una revisión o validación son:

- ✓ Actualizaciones al proceso al que pertenece el activo.
- ✓ Adición de actividades al proceso.
- ✓ Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- ✓ Inclusión de un nuevo activo.

8. ACTUALIZACIÓN

Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de la entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013:4

- ✓ **Inventario de activos:** todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos.

- ✓ **Propiedad de los activos:** los activos de información del inventario deben tener un propietario.
- ✓ **Clasificación de la información:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- ✓ **Etiquetado y manipulado de la información:** Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
 - El inventario de activos de información de la entidad debería especificar para cada activo:
 - Información básica del activo (nombre, observaciones, proceso, entre otras).
 - El nivel de clasificación de la información.
 - Información relacionada con su ubicación, tanto física como electrónica.
 - Su propietario y su custodio.
 - Los usuarios y derechos de acceso.

El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Para cada propiedad se deben establecer criterios específicos y lineamientos para el tratamiento adecuado del activo. Asimismo, en esta guía se definieron tres (3) niveles que permiten determinar el valor general del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria (ver Tabla: Niveles de evaluación).

Tabla 1: Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)

INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 2: Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

9. DESARROLLO

A continuación, se describen las actividades que se desarrollan para realizar la identificación y clasificación de los activos de información en el IMRDS. El siguiente esquema de clasificación atiende a los requerimientos de clasificación de los activos de información con el fin de realizar una adecuada gestión de riesgos de seguridad de la información y clasificación de la información almacenada en los activos.

9.1. DEFINICIÓN

La definición consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder de cada proceso ayude en realización de la actividad.

En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol.

Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.

Información básica

La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente:

Identificador: Número consecutivo único que identifica al activo en el inventario.

Proceso: Nombre del proceso al que pertenece el activo.

Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.

Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.

Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- ✓ Alta: Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- ✓ Media: Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- ✓ Baja: Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Propiedad

Propietario: 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 el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

Acceso

Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Gestión

Identificación del nivel soporte del Activo de información

Los activos de información del IMRDS se clasifican en dos grandes grupos que determinan el nivel de soporte del activo al cumplimiento de la función misional del IMRDS

- ✓ **Activos Primarios:** Corresponden a los activos esenciales para el cumplimiento de la función misional del IMRDS, en esta categoría se catalogan: La información, los procesos y procedimientos del IMRDS.
- ✓ **Activos de Soporte:** En esta categoría se clasifican los activos que permiten el tratamiento de la información del IMRDS, empleando los procesos y procedimientos del Sistema Integrado de Gestión de la entidad.

Identificación del tipo de activo según su composición

Una vez se ha determinado si el activo es primario o de apoyo se determina la estructura o forma que tiene dicho activo.

La clasificación para los activos primarios contiene:

- ✓ Información.
- ✓ Procesos y procedimientos.

Los activos de soporte se categorizan en los siguientes grupos, atendiendo a las recomendaciones que formulan las normas técnicas de gestión de la seguridad de la información.

- ✓ Hardware
- ✓ Software
- ✓ Redes
- ✓ Servicios
- ✓ Personal
- ✓ Ubicaciones físicas
- ✓ Estructura Organizacional

Identificación del activo de acuerdo con su función:

Cuando se identifican la composición del activo, se puede proceder a su clasificación de acuerdo con su función. Las categorías inicialmente definidas se describen a continuación, en conjunto con los responsables del sistema integrado de gestión del IMRDS se pueden definir nuevas categorías que deben ser aprobadas oficialmente por el IMRDS.

Hardware

- Equipos portátiles: Aquellos equipos como computadores portátiles, tabletas, teléfonos inteligentes, cuyo propósito permitir la portabilidad de los mismos con sus usuarios
- Equipo estático: Aquellos equipos como estaciones de trabajo, servidores y demás equipos de procesamiento de información destinado a permanecer en una ubicación física y cuyo fin no es la portabilidad con sus usuarios.
- Periféricos: Dispositivos destinados a apoyar la entrada y salida de datos hacia los equipos de procesamiento de información. En esta categoría están elementos como impresoras, scanner, cámaras fotográficas, pistolas lectoras de datos.
- Medios de almacenamiento: Son equipos cuyo fin primordial es el almacenamiento de información como cintas, discos extraíbles, sistemas de almacenamiento NAS, SAN entre otros.

Software

- Sistemas operacionales: Software cuyo propósito es permitir tener acceso al software y hardware que procesa la información en el hardware.
- Software de administración de hardware: Software cuyo propósito es permitir la operación y control del hardware que procesa la información.
- Utilitarios para usuario final: Software que es empleado el usuarios finales y administradores de sistemas de información para realizar las actividades definidas en los procedimientos y procesos del Sistema Integrado de Gestión del IMRDS. En esta categoría se encuentra el software de ofimática como procesadores de texto, presentadores de diapositivas, hojas electrónicas, navegadores web, software para consulta de correo electrónico, antivirus y herramientas de desarrollo de software.
- Aplicaciones de negocio: Software cuya función específica es realizar o apoyar las actividades de los procesos y procedimientos de la entidad que han sido automatizada. En esta categoría están: sistemas de información misionales, software para control de inventarios, sistemas financieros, sistemas para gestión de talento humano, software para implementación de sistemas de gestión, sistemas de bases de datos y software específico para prestar servicios en el IMRDS como correo electrónico, página de Internet, sistemas de seguridad.

Redes

De la categoría de redes se clasifican los medios de transmisión que soportan a las redes y los equipos activos que permiten la transmisión de datos sobre las redes.

Servicios

Los servicios están compuestos por facilidades que apoyan o soportan a los demás tipos de activos de información: iluminación, calefacción, refrigeración, energía o aire acondicionado.

Los grupos Personal y estructura organizacional se dividen de acuerdo con las directrices que define la estructura orgánica del IMRDS.

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Una vez identificados los activos de información, su nivel de soporte, composición, función, se deben establecer niveles de protección para asegurar que la información institucional se encuentre protegida contra divulgación no autorizada, exposición, pérdida, robo o daño intencional o accidental, teniendo en cuenta las características y lineamientos de los estándares y normatividad relacionada con seguridad y privacidad de la información.

NTC-ISO/IEC 27001 establece la seguridad de la información como la “preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.”, para lo cual se establecen criterios para la valoración y clasificación de los activos teniendo en cuenta estas características principales.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Tabla3. Esquema de clasificación por confidencialidad

<p>INFORMACIÓN PÚBLICA RESERVADA</p>	<p>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.</p>
<p>INFORMACIÓN PÚBLICA CLASIFICADA</p>	<p>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 la misma. 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.</p>

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 PUBLICA RESERVADA.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Tabla4. Esquema de clasificación por Integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, 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 a funcionarios de la entidad.
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.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Tabla5. Esquema de clasificación por Disponibilidad.

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.

BIBLIOGRAFIA:

- Guía para la Gestión y Clasificación de Activos de Información
https://www.mintic.gov.co/gestioni/615/articles-5482_G5_Gestion_Clasificacion.pdf

CONTROL DE CAMBIOS			
VERSIÓN	FECHA DE APROBACIÓN DD/MM/AA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
01	14/12/2021	Creación Clasificación de activos de la Información	Líder Oficina TIC

TABLA DE APROBACIÓN		
ELABORÓ	REVISIÓN	APROBÓ
Nombre: Edwin Zapata Cargo: Líder de Sistemas Firma: <i>Original Firmado</i> Fecha: 14/12/2021	Nombre: Karen Mora Cruz Cargo: Líder MIPG Firma: <i>Original Firmado</i> Fecha: 14/12/2021	Nombre: Comité Institucional de Gestión y Desempeño. Acta No. 08/2021 Fecha: 14/12/2021