	GESTIÓN DE TECNOLOGÍA E INFORMACIÓN	CÓDIGO: PA-TI-G06
	INVENTARIO DE ACTIVOS DE LA INFORMACIÓN DE LAS TIC (TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN)	VERSIÓN: 1
		FECHA: 15/Abr/2019

Objetivo

Suministrar criterios para identificar, valorar y clasificar los activos de información de las TIC (Tecnologías de la Información y la Comunicación) del Instituto Nacional Penitenciario y Carcelario en cuanto a su confidencialidad, integridad y disponibilidad; con el propósito de cumplir con los requisitos para la gestión efectiva de la seguridad y privacidad de la información y así mantener la protección adecuada de los activos de la entidad.

Marco Legal

- [Ver normograma del Instituto Nacional Penitenciario y Carcelario](#)

Glosario

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, software, hardware, datos de información, servicios, edificios, personas, etc.) que tenga valor para la organización.
- **Activo de información:** elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organización. En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en una organización en el cumplimiento de sus funciones.
- **Confidencialidad:** hace referencia a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control:** medida que modifica el riesgo. Políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.

- **Disponibilidad:** hace referencia a que la información sea accesible y utilizable por solicitud de una persona o entidad autorizada.
- **Integridad:** hace referencia a la propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Hardware:** partes físicas, tangibles, de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos
- **Software:** es todo equipo o soporte lógico (intangibles) de un sistema informático que abarca el conjunto de los componentes que son necesarios para la realización de tareas específicas.

1.Generalidades

Este documento presenta una guía para realizar el inventario y clasificación de los activos de información de las TIC; el oficial o responsable de seguridad de la información del instituto liderara el inventario junto con la Oficina de Sistemas de Información orientado y apoyando a los líderes de cada proceso, con el fin de determinar la valoración, clasificación y la criticidad de los activos, lo anterior teniendo en cuenta la norma técnica NTC ISO/IEC 27001:2013 anexo A dominio A.8 Gestión de Activos. La norma establece tres características para la clasificación del activo que son: la confidencialidad, integridad y disponibilidad

Lo anterior es base fundamental para el Sistema de Gestión de Seguridad de la Información para establecer los riesgos y su tratamiento.

2. Consideraciones previas al inventario de activos de información.

Los activos de información son aquellos que tienen valor para el instituto y que utiliza el Sistema de Gestión de Seguridad de la Información para que el INPEC funcionen y cumpla con los objetivos propuestos en sus diferentes planes. Por lo anterior tenga en cuenta las diferentes características y tipos de activos, así:

- **Software de:**
 - **Sistema:** es aquel que permite a los usuarios interactuar con el sistema operativo así como también controlarlo. Este sistema está compuesto por una serie de programas que tienen como objetivo administrar los recursos del hardware y, al mismo tiempo, le otorgan al usuario una interfaz. El sistema operativo permite facilitar la utilización del ordenador a sus usuarios ya que es el que le da la posibilidad de asignar y administrar los recursos del sistema, como ejemplo de

esta clase de software se puede mencionar a Windows, Linux y Mac OS X, entre otros. Además de los sistemas operativos, dentro del software de sistema se ubican las herramientas de diagnóstico, los servidores, las utilidades.

- **Aplicación:** aquí se incluyen todos aquellos programas que permiten al usuario realizar una o varias tareas específicas. Programas que los usuarios usan de manera cotidiana como: procesadores de texto, hojas de cálculo, editores, telecomunicaciones, software de cálculo numérico y simbólico, entre otros.
- **Programación:** son aquellas herramientas que un programador utiliza para poder desarrollar programas informáticos. Para esto, el programador se vale de distintos lenguajes de programación. Como ejemplo se pueden tomar compiladores, programas de diseño asistido por computador, paquetes integrados, editores de texto, enlazadores, depuradores, intérpretes, entre otros.

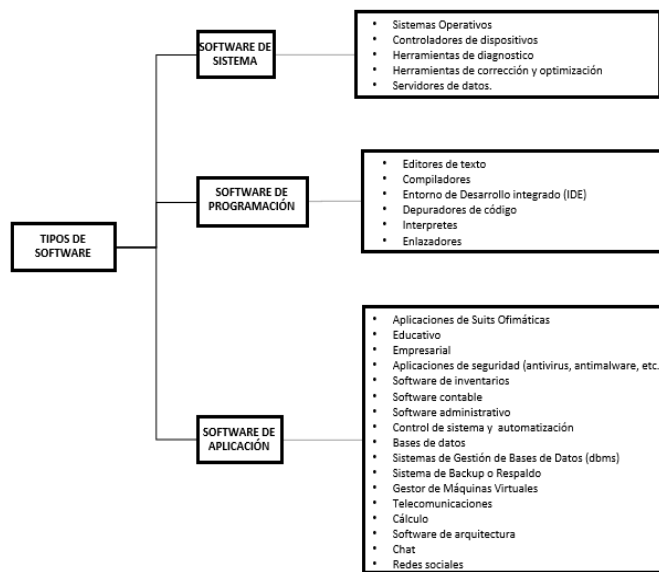


Figura No 1. Fuente propia

- **Hardware:**

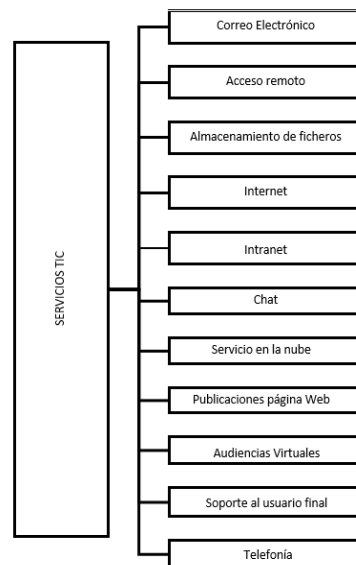
- Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Ejemplo: servidores (host), equipos de escritorio (Pc), equipos portátiles (Laptop), dispositivos móviles, equipos de respaldo, periféricos, dispositivos criptográficos, dispositivos biométricos,

servidores de impresión, impresoras, escáneres, equipos virtuales (vhost), soporte de la red (Network), módems, concentradores, conmutadores (switch), encaminadores (router), pasarelas (bridge), firewall, central telefónica, telefonía IP, access point, disco duro removible, vídeo beam,, fotocopidora entre otros.

- **Servicios:**

- Se pueden definir como el conjunto de actividades que buscan responder a las necesidades que presenta un usuario interno o externo con la aplicación de tecnologías requeridas para la gestión y transformación de la información, incentivando el valor de estos sin que los clientes asuman el riesgo y costo

Figura No 2. Fuente propia



- **Redes de Comunicaciones:**

- Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. Ejemplo: red telefónica, red inalámbrica, telefonía móvil, satélite, canales dedicados, red local (LAN), red metropolitana (MAN), Internet, radio comunicaciones, punto a punto, ADSL, red digital (rdsi).

- **Activos Esenciales:**

- Datos importantes o vitales para la administración de la entidad: aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustentan la naturaleza legal de la organización o de sus usuarios.
 - Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012).
 - Datos clasificados o calificados: aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
- **Datos / Información:**
 - Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplo: copias de respaldo, ficheros, datos de gestión interna, datos de configuración, credenciales (contraseñas), datos de validación de credenciales (autenticación), datos de control de acceso, registros de actividad (Log), matrices de roles y privilegios, código fuente, código ejecutable, datos de prueba, información de bitácoras, entre otros.
- **Personas:**
 - Usuarios internos, usuarios externos, operadores, administradores de sistemas, administradores de comunicaciones, administradores de bases de datos, administradores de seguridad, líder de proyectos, programadores, contratistas, proveedores, conocimiento. En general, todos aquellos que tengan acceso de una manera u otra a la entidad. Se valora el cargo, rol y perfil o conocimiento de la persona
- **Soportes de Información:**
 - Dispositivos físicos electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo. Ejemplo: Discos, discos virtuales, almacenamiento en red (SAN), memorias USB, CDRom, DVD, cinta

magnética (tape), tarjetas de memoria, tarjetas inteligentes, material impreso, microfilmaciones.

- **Claves criptográficas:**

- Esenciales para garantizar el funcionamiento de los mecanismos criptográficos. Ejemplo: claves de cifrado, claves de firma, protección de comunicaciones (claves de cifrado de canal), cifrado de soportes de información, certificados digitales, certificados de claves, claves de autenticación.

- **Equipos Auxiliares:**

- Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.

- **Instalaciones:**

- Lugares donde albergan los sistemas de información y comunicaciones. Ejemplo data center, centro de cableado, etc.

3. Roles y responsabilidades

Los activos de información deben ser justificados y valorados en cuanto a su confidencialidad, integridad y disponibilidad por los propietarios, custodios o en su defecto los usuarios, como lo recomienda la norma ISO/IEC 27001:2013 en su anexo A numeral A.8.1.2 "Propiedad de los activos", la norma ISO/IEC 27002:2013 en su numeral 8. Gestión de activos ítem 8.1.2 "Propiedad de los activos" y en la guía No. 5 para la Gestión y Clasificación de Activos de Información en su numeral 6. Inventario de activos, ítem 6.1 Definición de MINTIC.

Por lo anterior, se describe las partes que intervienen en la clasificación de activos, sus responsabilidades y roles; este análisis debe estar a cargo del oficial o responsable de la seguridad de la información con el apoyo de la Oficina de Sistemas de Información para orientar a los líderes de procesos, directivos, asesores, jefes de dependencias, coordinadores, directores regionales, directores de establecimientos de orden nacional y Dirección Escuela de Formación (Escuela Penitenciaria Nacional), según sea el caso.

PROPIETARIO DEL ACTIVO	RESPONSABILIDADES	ROLES
<p>Identifica un cargo, área, dependencia, proceso o grupo de trabajo responsable del activo. (el término "propietario" no significa que la persona disponga de los derechos de propiedad reales del activo. ISO/IEC 27002)</p>	<ul style="list-style-type: none"> *- Garantizar que los los activos de información se clasifiquen adecuadamente. *Definir controles y el uso adecuado de los activos de información identificados. *Tomar decisiones sobre el buen uso del activo de información. *Definir uso aceptable de los activos de información. * Hacer mantenimiento periódico y evaluar clasificación y valoración de los activos de información 	<p>Identificar, actualizar y definir los controles de los activos de información que hacen parte de su área, dependencia o grupo de trabajo</p>

CUSTODIO DEL ACTIVO DE INFORMACIÓN	RESPONSABILIDADES	ROLES
Identifica un cargo, área, dependencia o grupo que custodia el activo de información. (las labores rutinarias se pueden delegar, por ejemplo un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del propietario. ISO/IEC 27002) el custodio generalmente se define donde reposa el activo original.	<ul style="list-style-type: none"> * Administrar y hacer efectivo los controles que el propietario del activo haya definido. * Ejecutar las actividades propias de su cargo, de acuerdo a la custodia del activo de información. * Cumplir con los controles de seguridad establecidos para la protección de los activos de información. * Garantizar que los activos de información se encuentre disponible e íntegros y que solo personal autorizado acceda a ellos. 	Verificar y mantener la protección y privacidad de los activos de información que están bajo su custodia.
USUARIO	RESPONSABILIDADES	ROLES
Identifica al colaborador que hace uso del activo de información. (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 institución, para propósitos propios de su labor.)	<ul style="list-style-type: none"> * Hacer buen uso de los activos de información asignados. * Reportar cualquier evento o incidente que atente contra la seguridad del activo de información. *Garantizar la confidencialidad, integridad y disponibilidad del activo de información. 	* Cumplir con las políticas, controles o buenas practicas establecidas para el buen uso del activo de información.

Tabla No 1. Roles y responsabilidades. Fuente propia

4. Inventario de activos de información

El inventario y clasificación de los activos de información es la base para la gestión de riesgos de seguridad de la información, para determinar los niveles de protección requeridos. Las actividades a realizar para obtener un inventario de activos inician con la Definición, Revisión, Actualización y Publicación.

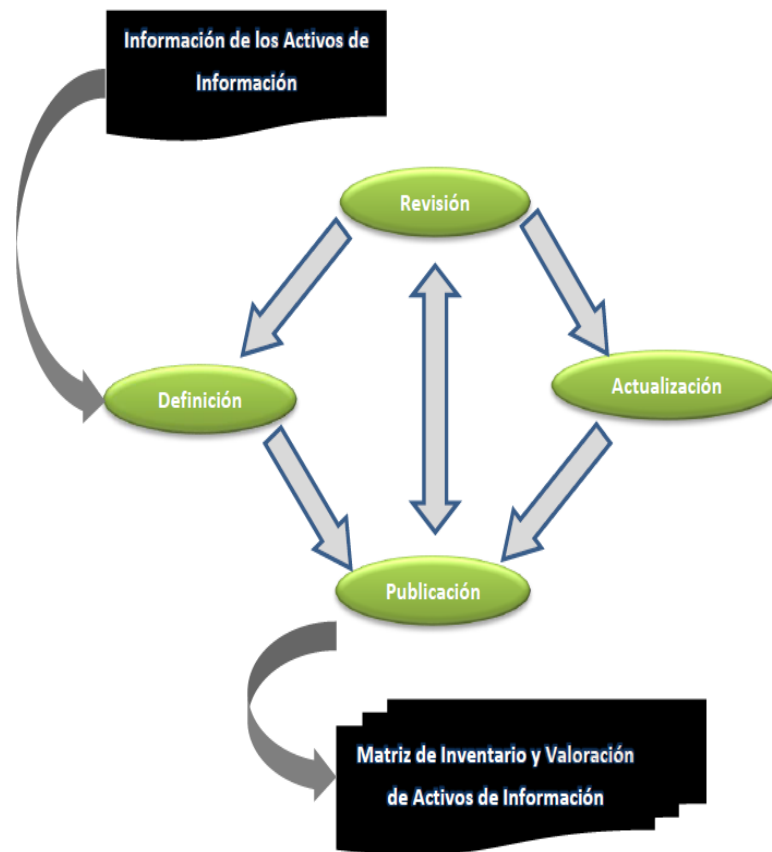


Imagen 1. Procedimiento Para Inventario de Activos.

Imagen No 1. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

4.1 Definición

Determinar qué activos de información van a hacer parte del inventario. En esta actividad el oficial o responsable de seguridad de la información del instituto con el apoyo de la Oficina de Sistemas de Información debe establecer con los colaboradores designados por los líderes de procesos, directivos, asesores, jefes de dependencias, coordinadores, directores regionales, directores de establecimientos de orden nacional o Dirección Escuela de Formación (Escuela Penitenciaria Nacional) según sea el caso, la inclusión de los activos en la Matriz inventario de activos de la información de las TIC (Tecnologías de la Información y la Comunicación), de acuerdo con las variables establecidas en este instrumento para lograr identificar la clasificación, valoración y cuales activos son de mayor criticidad para el Instituto.

El propietario, custodio o el usuario que tiene la responsabilidad de administrar el activo de información, debe clasificar y valorar el activo, con la orientación y apoyo del oficial o responsable de la seguridad de la información del instituto y con el apoyo de la Oficina de Sistemas de Información en caso de requerirse. La definición del inventario se debe realizar por lo menos una vez al año o cada vez que ingrese o salga un activo de un proceso, dependencia, regional,

establecimiento o Dirección Escuela de Formación (Escuela Penitenciaria Nacional) ; activad que debe ser definida y reportada por los líderes de procesos, directivos, asesores, jefes de dependencias, coordinadores, directores regionales, directores de establecimientos de orden nacional o Dirección Escuela de Formación (Escuela Penitenciaria Nacional) o a quien se le asigne esta actividad y reportarla al oficial o responsable de la seguridad de la información con conocimiento a la Oficina de Sistemas de Información. A continuación, se hace referencia a la información mínima o básica a tener en cuenta para definir el activo de información:

- **Proceso:** nombre del proceso al que pertenece el activo de información.
- **Líder del proceso:** nombres y apellidos del líder del proceso; quien es el propietario de la información (propietario de los activos de información).
- **Cargo Líder del Proceso:** denominación del cargo del líder del proceso.
- **Dependencia/Grupo/Regional/Establecimiento:** digite le nombre de la dependencia, grupo, regional, establecimiento al cual pertenecen los activos de información.
- **Fecha de elaboración / validación:** registrar la fecha de elaboración y validación del registro de activos de información.
- **Nombre Activo:** nombre de identificación del activo dentro del proceso al que pertenece.
- **Descripción del Activo de Información:** realizar la descripción general del activo de información.
- **Tipo de Activo:** seleccionar el tipo de activo teniendo en el ítem **2. Consideraciones previas al inventario de activos de información.**
- **Clasificación del activo de información:** de acuerdo a la confidencialidad, integridad y disponibilidad.
- **Valoración de la clasificación:** 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.
- **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.
- **Ubicación del activo de información:** indicar la ubicación física o digital del activo de información.
- **Propietario:** cargo, área, dependencia, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifiquen adecuadamente.

- **Custodio:** del activo de información: cargo del custodio de la información, es decir la persona que realiza el control en el acceso al activo de información. En caso de que el custodio sea un tercero, indicar la empresa y cargo del mismo.
- **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.
- **Fecha de ingreso:** del activo de información en el inventario.
- **Fecha salida del Activo:** fecha de exclusión del activo de información del inventario

4.2 Revisión

Se verifica si el activo de información debe o no permanecer en el inventario, o si los valores de evaluación asignados deben ser modificados. Esta revisión debe ser ejecutada por líderes de procesos, directivos, asesores, jefes de dependencias, coordinadores, directores regionales, directores de establecimientos de orden nacional, Dirección Escuela de Formación (Escuela Penitenciaria Nacional) o a quien se le asigne esta actividad y reportarla al oficial o responsable de la seguridad de la información con conocimiento a la Oficina de Sistemas de Información. Se debe realizar cada año o cuando sea necesario.

Las razones por las cuales se debe realizar una revisión o validación son:

- Actualización del proceso que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros, procesos o procedimientos.
- Adición de actividades al proceso.
- Desaparición de una dependencia, grupo o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

4.3 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.

4.4 Publicación.

El inventario de activos de información debe ser un documento clasificado como “Confidencial”, y no debe tener características para ser modificado, ni consultado por usuarios no autorizados. Por lo anterior el oficial o responsable de seguridad de la información orienta y apoya a los líderes de procesos, directivos, asesores, jefes de dependencias, coordinadores, directores regionales, directores de establecimientos de orden nacional o Dirección Escuela de Formación (Escuela Penitenciaria Nacional) en la utilización de métodos de seguridad para garantizar la confidencialidad tales como nombre de usuario y contraseña, entre otros.

Una vez realizado el inventario de activos de información, el oficial o responsable de seguridad, consolidara la información y la enviara al administrador de la página web del instituto para la respectiva publicación; teniendo en cuenta que por tratarse de un documento confidencial y sin infringir la Ley 1712 de 2014, se publicaran aquellos campos de la Matriz inventario de activos de la información de las TIC (Tecnologías de la Información y la Comunicación), que no afecten la seguridad y privacidad de la información del instituto.

5. Clasificación de los activos de información

La clasificación de activos de información tiene como objetivo asegurar que la información reciba los niveles de protección adecuados, ya que con base en su valor y de acuerdo a características particulares como el funcionamiento interno, requiere un de manejo especial, así mismo busca dar cumplimiento a los requerimientos estipulados en el ítem relacionado con la Gestión de Activos de los estándares 27001:2013, ISO 27002, e ISO 27005. y los lineamientos de la política de Gobierno Digital de MINITC. Se toma como referencia los niveles de clasificación y valoración de la Guía No. 5 para la Gestión y Clasificación de Activos de Información de MINTIC.

5.1 Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

INFORMACION PUBLICA 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.
INFORMACION PUBLICA CLASIFICADA	<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.</p> <p>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>
INFORMACION 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.

Tabla No 2. Esquema de clasificación por confidencialidad. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

5.2 Clasificación de acuerdo con la integridad

La integridad se refiere a la exactitud y no modificación y destrucción sin autorización de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

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.

Tabla No 3. Esquema de clasificación por integridad. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

5.3 Clasificación de acuerdo a la disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

ALTA (1)	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.
MEDIA (2)	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.
BAJA (3)	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.

Tabla No 4. Esquema de clasificación por disponibilidad. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

6. Valoración de Activos de Información

Se debe cuantificar la importancia de los activos de información, su valoración y clasificación a través de diferentes dimensiones que trae la matriz de inventario de activos de la información de las TIC (Tecnologías de la Información y la Comunicación). Los tres criterios básicos son: la confidencialidad, la integridad y la disponibilidad. Para cada propiedad se establecen criterios específicos y lineamientos para el tratamiento adecuado del activo de la siguiente manera:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla No 5. Criterios de Clasificación. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

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.

Tabla No 6. Niveles de Clasificación. Fuente: Guía No. 5 para la Gestión y Clasificación de Activos de Información. MINTIC

Anexo

- [PA-TI-G06-F01 V01 Inventario de activos de la información de las TIC \(Tecnologías de la Información y la Comunicación\)](#)

Lista de Versiones

Versión	Fecha de Emisión	Motivo de la Modificación	Modificaciones
1	04/Abr/2019	Creación del documento.	N.A

Elaboró	Revisó	Aprobó
Nombre: María Cristina Reyes Castillo Cargo: Técnico Operativo Fecha: 04/Abr/2019	Nombre: Angélica María Patiño García Cargo: Profesional Especializado Fecha: 05/Abr/2019 Nombre: Juan Manuel Riaño Vargas Cargo: Jefe Oficina Asesora de Planeación Fecha: 05/Abr/2019	Nombre: Adriana Cetina Hernández Cargo: Jefe Oficina Sistemas de Información Fecha: 15/Abr/2019

TXTCopiaControlada