SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

FASE DE PLANIFICACION

GUIA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

ALCALDÍA DE PEREIRA

PROCESO
PROMOCIÓN DEL DESARROLLO ECONÓMICO

SUBPROCESO
SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

FORMATO PRELIMINAR DEL DOCUMENTO

Título:	**GUIA PARA LA GESTIÓN Y CLASIFICACION DE ACTIVOS DE INFORMACION.**				
Fecha de elaboración	Febrero de 2018				
Sumario	Este documento contiene las instrucciones relacionadas con la gestión y clasificación de los Activos de Información y los registros asociados al mismo, en el Sistema de Seguridad y Privacidad de la Información de la ESE SALUD PEREIRA.				
Palabras Claves	Activos de Información Sistema de Gestión Seguridad de la Información Privacidad de la Información Norma ISO 27001:2013				
Formato:	PDF y DOC		Lenguaje:	Español	
Dependencia:	Secretaría de Tecnologías de Información y Comunicaciones				
Código:	N/A	Versión	1.0	Estado	En Aprobación
Categoría	Documento Técnico, Implementación de la Estrategia de Gobierno Digital en la Alcaldía de Pereira: Componente: Seguridad y Privacidad de la Información. Herramienta: NTC-ISO-IEC 27001:2013, M.SPI Modelo de Seguridad y Privacidad de la Información para GEL – Guía 3 Procedimientos de Seguridad de la Información. – Guía 5. Guía para la Gestión y Clasificación de Activos de Información. - articles-5482_Implementación_Políticas				
Autor (es):	Rubialba Ocampo Foronda Magister Carlos Mario Arteaga Pacheco				
Revisó:	Carlos Andrés Álvarez Palomino Director Operativo de Información y Servicios Digitales. Mesa de trabajo de Gobierno Digital				
Aprobó:	Fredy Eduardo Ruano López Secretario Tecnologías de Información y Comunicaciones				

TABLA DE CONTENIDO

CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	01/02/2018	Versión inicial del documento
2.0.0	11/08/2020	Se incorpora el cuerpo del documento, capítulo del 5 al 9 y se actualiza el formato de calidad.

1. INTRODUCCIÓN

Los procedimientos para el mantenimiento y gestión del inventario de activos de información son buenas prácticas, guías y estándares que se deben efectuar para realizar acertadamente el mantenimiento y gestión del inventario de activos de información en todos las acciones que realiza la Alcaldía de Pereira, por lo tanto, se encontrará a continuación un conjunto de protocolos que constituyen una base sólida para que quede documentado y debidamente elaborado el inventario de activos de información en la entidad.

2. OBJETIVO

Documentar y establecer buenas prácticas para la continua actualización del inventario de activos de información en todas las dependencias, Secretarías de despacho, oficinas asesoras y demás que la Alcaldía de Pereira tenga dentro de su organigrama con el fin de garantizar una buena gestión de los riesgos de los activos de información.

3. ALCANCE

Los procedimientos tienen como ámbito de aplicación el sector central de la Alcaldía de Pereira tal como lo dicta el artículo 24 “Estructura de la Administración Municipal de Pereira, Risaralda” del Decreto 834 de 2016 “Por el cual se dictan normas generales sobre la organización y funcionamiento de la administración municipal de Pereira, Risaralda, se crean sectores administrativos, se determina la estructura de la administración y las funciones generales de sus dependencias, y se dictan otras disposiciones”.

Los servidores públicos, contratistas, practicantes, pasantes, proveedores y terceros, que creen, procesen, transmitan y/o almacenen información de la Alcaldía de Pereira tienen el compromiso de manipular y tratar los activos de información de acuerdo con el cumplimiento de la presente política.

4. DEFINICIONES

- **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 sami-privado 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.
- **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.
- **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.

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

5. IDENTIFICACION DE ACTIVOS

La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Las actividades a realizar para obtener el inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

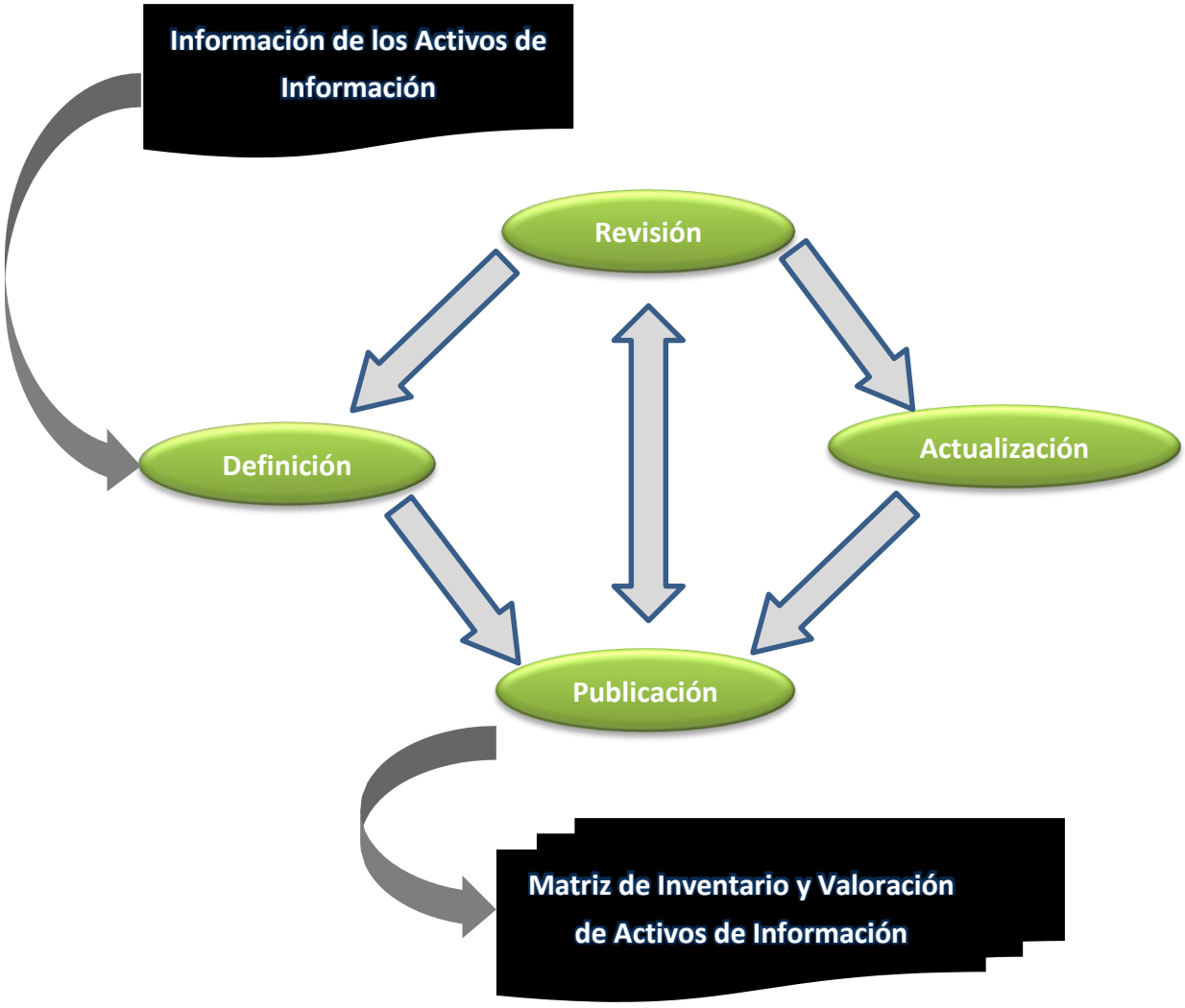

Imagen 1. Procedimiento Para Inventario de Activos.
Fuente de información MIntic Guía Nro.5

5.1 DEFINICIÓN

El inventario se efectuará mediante una muestra de los activos, no a la totalidad, por ser demasiado extensa, esta tarea será liderada por la Dirección de Información y Servicios Digitales de la Secretaria de Tecnologías de la Información y la Comunicación, y contará con el apoyo de los líderes de cada proceso (o quien haga sus veces, líder requerido en gestión de calidad) que coadyuven 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.

La definición del inventario se efectuará una vez por año teniendo en cuenta los siguientes aspectos.

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.

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

Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario

Fecha salida del Activo: Fecha de exclusión del activo de información del inventario.

5.2 REVISIÓN

El inventario de activos podrá 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.

Las razones para solicitar o efectuar 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 ó procesos y procedimientos.
- Inclusión de un nuevo activo.

- Desaparición de un área, proceso 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.

5.3 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.

5.4 PUBLICACIÓN

El inventario de activos de información es un documento clasificado como "***Confidencial"***, por lo tanto no tiene características que lo permitan ser modificado por los usuarios autorizados. Sólo tiene acceso de modificación a este documento Director Operativo de Información y Servicios Digitales de la Secretaria de Tecnologías de la Información y la Comunicación o los líderes de los procesos con previa autorización del Comité de Seguridad y Privacidad e la Información.

6. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

El sistema de clasificación de la información se efectuará teniendo en cuenta las características particulares de la información y buscando 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.

6.1 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, Esta se debe definir de acuerdo con las características de los activos que se manejan en la entidad.

Se toma como base el siguiente esquema de clasificación de tres (3) niveles:

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 PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de 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.
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.

Tabla3. Esquema de clasificación por confidencialidad
Fuente de información MIntic Guía Nro.5

6.2 DE ACUERDO CON LA INTEGRIDAD

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Se toma como base el siguiente esquema de clasificación de tres (3) niveles:

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.

Tabla4. Esquema de clasificación por Integridad
Fuente de información MIntic Guía Nro.5

6.3 DE ACUERDO CON 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.

Se toma como base el siguiente esquema de clasificación de tres (3) niveles:

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.

Tabla5. Esquema de clasificación por Disponibilidad
Fuente de información MIntic Guía Nro.5

7. ETIQUETADO DE ACTIVOS DE INFORMACIÓN

Para realizar el etiquetado de los Activos de Información se aplicarán las siguientes pautas generales:

6.3.1 Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.

6.3.2 Se etiquetará el nivel de clasificación en relación a Confidencialidad, Integridad y Disponibilidad.

6.3.3 Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.

6.3.4 Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma: {Clasif.Confidencialidad}-Clasif.Integridad} - {Clasif.Disponibilidad}

6.3.5 Para los activos clasificados en confidencialidad como INFORMACION PUBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACION PUBLICA CLASIFICADA IPC y INFORMACION PUBLICA, IPB.

6.3.6 Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.

6.3.7 Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.

8. FORMATO INVENTARIO DE ACTIVOS DE INFORMACION

Este formato está compuesto por diferentes campos que recogen las diferentes características de los Activos de Información; a continuación, se detallaran estos campos para su correcto diligenciamiento.

COLUMNA	DESCRIPCIÓN	OPCIONES
Macro proceso:	Son los procesos principales que forman parte fundamental de la misión y visión de la Alcaldía de Pereira	Estratégicos Misionales Apoyo Evaluación y Seguimiento
Proceso:	conjunto de acciones o actividades sistematizadas que se realizan dentro de los diferentes procesos de la Alcadía de Pereira	Acorde con el Mapa de Procesos Vigente
Localización	Es la ubicación física donde se encuentra el activo	Sede y oficina
Funcionario que genera el activo	Hace referencia a la persona vinculada a la Alcaldía de Pereira y que crea el Activo de Información	Funcionarios y contratistas de la Alcaldía de Pereira.
Responsable de la seguridad	Es el funcionario jefe de la secretaría en la cual se generara el Activo de Información.	Jefes de área
Id	Es el código o número de identificación asignado al Activo de Información.	Número de placa, serial o código de barras
Nombre del activo	Es el nombre asignado al Activo de Información	Archivador, pc de escritorio, portátil, servidor, nas, centros de archivo
Descripción	Indica la información que contiene el activo	Carpetas
Categoría	determina el tipo de información que contiene el activo	Digital o impresa

COLUMNA	DESCRIPCIÓN	OPCIONES
Estado	Indica la forma en que se encuentra el activo	B = bueno, R= regular, M= malo
Requerimiento legal	El activo debe cumplir alguna norma o ley.	Ley decreto, articulo (internacional, nacional, o generado por la empresa entidad)
Relevancia del Archivo	Determina cual es la importancia del activo para el desarrollo normal de las actividades diarias de la empresa.	Baja, poco importante, importante, muy importante, critica
Datos abiertos	Información que puede ser publicada o no, según los requerimientos o exigencias de normas o leyes	No Si
Clasificación de la seguridad	son los nivele s de protección de la información de la Alcaldía de Pereira de acuerdo a su manejo y tratamiento	P= Datos e información publicable Np= datos e información no publicable PS= datos e información personal semi privada
Criticidad Confidencialidad	Determina que tan crítico es el activo de acuerdo a la integridad	A= Alta M= media B= baja
Criticidad integridad	Determina que tan crítico es el activo de acuerdo a la integridad	A= Alta M= media B= baja
Criticidad disponibilidad	Determina que tan crítico es el activo de acuerdo a la Disponibilidad	A= Alta M= media B= baja

9. ANEXO A

INVENTARIO DE ACTIVOS DE INFORMACIÓN - ETAPA DE PLANIFICACIÓN - BUENAS PRÁCTICAS SGSI																
UBICACIÓN			TALENTO HUMANO		DESCRIPCIÓN DEL ACTIVO											
MACROPROCESO	PROCESO	LOCALIZACIÓN	FUNCIONARIO QUE GENERA EL ACTIVO	RESPONSABLE DE LA SEGURIDAD	ID	NOMBRE DEL ACTIVO	DESCRIPCIÓN	CATEGORÍA	ESTADO	REQUERIMIENTO LEGAL	RELEVANCIA DEL ACTIVO	Datos Abiertos	Clasificación de Seguridad	Criticidad Confidencialidad	Criticidad Integridad	Criticidad Disponibilidad