| CONTROL DE CAMBIOS | | |
|---|---|---|
| **VERSIÓN** | **FECHA** | **DESCRIPCIÓN DE LA MODIFICACIÒN** |
| 1 | 16-12-2019 | Versión inicial del documento |

| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Profesionales Dirección DTIC | Ing. Henry Díaz Dussán<br>Director de TIC | Ing. Henry Díaz Dussán<br>Director de TIC<br>Germán Uriel Rojas<br>Director de Planeación |

# TABLA DE CONTENIDO

## LISTA DE TABLAS



## LISTA DE ILUSTRACIONES

## 1. INTRODUCCION

Las organizaciones de cualquier tipo y tamaño (incluido el sector público y privado, comercial y sin ánimo de lucro) recolectan, procesan, almacenan y transmiten información en muchas formas, que incluyen los formatos electrónicos, físico, entre otros.

El valor de la información va más allá de las palabras escritas, números e imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas de información intangibles. En un mundo interconectado, la información y los procesos relacionados, los sistemas, las redes y el personal involucrado en su operación, el manejo y la protección de los activos que, como cualquier otro activo importante del negocio, son valiosos para una organización, y en consecuencia ameritan o requieren protección contra diversos peligros [ISO 27001:2013]

La norma ISO 27001: 2013, en su control A.8.1.1 “Inventario de activos”, establece que se deberían 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. Para lo anterior, una organización debería identificar los activos pertinentes en el ciclo de vida de la información, y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. La documentación se debería mantener en inventarios dedicados o existentes, según sea apropiado. Para dicha tarea se diligencia la matriz de identificación de activos de información basados en el Documento del Departamento Administrativo de la Función Pública DAFP, *“Guía para la administración del riesgo y el diseño de controles en Entidades públicas”* Versión N° 4 de octubre de 2018, así como los requerimientos específicos al interior de la Personería de Bogotá, D.C.

## 2. OBJETIVO GENERAL

Establecer los lineamientos para llevar a cabo las actividades de identificación y valoración de activos de la información en la Personería de Bogotá, D.C., de tal manera que se dé cumplimiento a la norma NTC-ISO/IEC 27001:2013, la Ley 1712 de 2014 (En lo que compete al Registro de Activos de Información), y la Ley 1581 de 2012 (En lo que compete a la protección de datos personales).

## 3. ALCANCE

La presente aplica para todos los procesos de la Entidad, quienes deberán tenerla en cuenta para realizar las actividades de creación y actualización del inventario de activos de información; inicia con la identificación de activos de información y finaliza con la valoración de los activos identificados.

## 4. RESPONSABLES

Serán responsables de la identificación de activos de Información todos los procesos que se encuentran dentro del alcance del Sistema de Gestión de Seguridad de la Información –SGSI para la Personería de Bogotá, D.C.

La Dirección de Tecnologías de Información y Comunicación DTIC deberá realizar la divulgación de la presente guía y será responsable de orientar y apoyar a los procesos en las actividades de levantamiento y actualización del inventario de activos de información.

## 5. DEFINICIONES

**Activo de Información**: Información y demás activos asociados tales como Software, Hardware Personas y Servicios, que almacenan, manipulan, modifican, ingresan, o transportan información, y que, en caso de verse afectada en su confidencialidad, integridad y/o disponibilidad, afectan a la Personería de Bogotá D.C., en menor o mayor medida.

**Clasificación de la Información**: Es la actividad por la cual se puede determinar que la información física y/o digital de la Entidad pertenece a uno de los niveles de clasificación estipulados por esta. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

**Confidencialidad**: Propiedad de la información que determina no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados. ISO/IEC 27001: 2013

**Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada ISO/IEC 27001: 2013.

**Información**: Datos relacionados que tienen valor 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. ISO/IEC 27001:2013.

**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[1].

**Información Pública Clasificada**: Información disponible para todos los procesos de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la Entidad o de terceros y puede ser utilizada por todos los funcionarios de la Entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario[2].

**Información Pública Reservada**: Información disponible sólo para un proceso de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica[3].

**Integridad**: Propiedad de la información relativa a su exactitud y completitud. ISO/IEC 27001: 2013

**Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas. ISO/IEC 27001: 2013

**SGSI**: Sistema de Gestión de Seguridad de la Información.

[1] Tomado de la Guía No. 5 para la Gestión y Clasificación de Activos de Información de MINTIC.
[2] Tomado de la Guía No. 5 para la Gestión y Clasificación de Activos de Información de MINTIC.
[3] Tomado de la Guía No. 5 para la Gestión y Clasificación de Activos de Información de MINTIC.

## 6. DESARROLLO DEL DOCUMENTO

### 6.1 DOCUMENTOS DEL SGSI ASOCIADOS CON LA GUIA

- Procedimiento de Gestión de Activos
- Tablas de Retención Documental
- Planilla Inventario de Activo Tipo Información
- Planilla Inventario de Activo de Tipo Talento Humano
- Normograma

### 6.2 METODOLOGÍA UTILIZADA

Para la elaboración del inventario de activos de información la Personería de Bogotá D.C., adopta la metodología establecida por el DAFP en la *"Guía para la administración del riesgo y el diseño de controles en Entidades públicas"*, y el anexo 4. *"Lineamientos para la gestión de riesgos de seguridad digital en Entidades públicas"* en su numeral 4.1.6. *"Identificación de activos de seguridad digital"*, la cual se ajustará si es necesario según los requerimientos y necesidades de la Entidad.

Para desarrollar el inventario de los activos de información se realizarán las actividades de identificación, clasificación y valoración establecidas en la guía metodológica del DAFP.

### 6.3 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

| IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ID Activo | Dependencia | Serie | Subserie | Nombre o Título de la Información | Descripción de la Información | Idioma | Medio de Conservación y/o Soporte | Formato | INFORMACIÓN | | Custodio de la Información |
| | | | | | | | | | Publicada | Disponible | |
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |

***Ilustración 1 Identificación de activos de información***

Consiste en reconocer y documentar los activos de información de la Personería de Bogotá, D.C., para esto es importante instruir a los líderes de los procesos o referentes en los conceptos generales sobre seguridad de la información.

La identificación del activo de información debe incluir todos aquellos atributos que permitan a la organización tener una percepción global sobre él. Para ello se diligencia en la Hoja *"2. Activos de Información"* del formato **03-FR-21** *"Matriz de inventario de activos de información*", los datos de los activos de tipo información

identificados, y con base en las Tablas de Retención Documental (en adelante TRD). Diligencie los siguientes campos:

**Dependencia**: Relacione el proceso al cual pertenece el activo de información identificado.

**Serie:** Número de serie del activo relacionada en la TRD.

**Subserie:** Número de subserie del activo relacionado en la TRD.

**Nombre o Título de la Información:** Nombre o título de la información con base en las TRD vigentes y/o asuntos manejados regularmente por la Entidad que no se encuentren definidos en las TRD.

**Descripción de la Información:** Descripción breve del contenido de la información, esta puede estar contenida en las TRD.

**Idioma:** Idioma, lengua o dialecto en que se encuentra la información, para Colombia se sugiere “Castellano”.

**Medio de Conservación y/o Soporte:** Medio y/o soporte en el que se encuentra la información; puede ser físico o electrónico, algunos ejemplos pueden ser: papel, disco duro, CD, Internet, Intranet, correo electrónico, microfilmación, etc.

**Formato:** Forma, tamaño o modo en que se presenta la información o se permite su visualización o consulta, tales como: hoja de cálculo (.xls, .xlsx), pdf, documento de texto (.txt, .doc, .docx), imagen (.JPG), audio, video (.MP4), cinta, entre otros.

**Información Publicada:** Marque con una “X” aquella información que se encuentra publicada para su consulta en algún medio de información de la Entidad.

**Información Disponible:** Marque con una “X” aquella información que no se encuentra publicada, pero que está disponible para ser solicitada por el público.

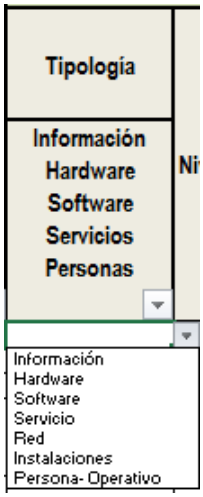
**Custodio de la Información:** Indicar la dependencia, proceso y/o cargo de la persona que custodia la información. La responsabilidad del custodio es aplicar las políticas, procedimientos y protocolos asociados al acceso a la información que se establezcan por parte de la Entidad y del propietario de la información (propietario de los activos), así como los relacionados con su trámite y conservación. Para definir esta persona es necesario tener en cuenta la localización del documento de archivo (registro).

## 6.4 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN


***Ilustración 2 Clasificación del activo***

Los activos de información identificados deben ser clasificados en términos de tipología, y normatividad aplicable por ley 1712 de 2014 y 1581 de 2012.

### 6.4.1. Clasificación Tipología




Seleccione el tipo de información del activo identificado de acuerdo con la siguiente clasificación[4]:

**Información:** Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información

[4] Tomado de Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas. 2018. Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.

**Hardware**: Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.

**Software**: Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

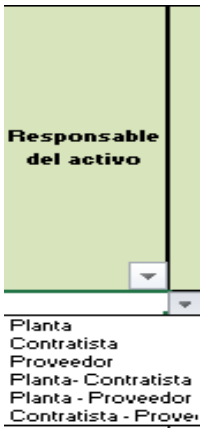
**Servicios**: Servicio brindado por parte de la Entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).

**Personas:** El activo persona se refiere al conocimiento no documentado que posee el funcionario o proveedor para realizar las funciones al interior de la Entidad.

> **Persona – Operativo:** Corresponde al personal que realiza tareas puntuales en cada uno de los procesos a los que pertenece. Se desarrolla a partir de los lineamientos proporcionados por los niveles de estratégico y táctico.[5]
>
> **Persona – Táctico:** Desarrolla detalladamente la planeación del funcionamiento de cada uno de los procesos de la Entidad a partir del marco de referencia elaborado en el nivel estratégico. Elabora la directiva para emplear los recursos asignados a cada proceso de la forma más efectiva posible para alcanzar los objetivos esperados.
> La diferencia básica con el nivel estratégico es que este se refiere a la gestión de toda la Entidad y se extiende en el tiempo, mientras que la segunda se refiere a la planeación de los productos y servicios específicos de la organización con tiempos y plazos determinados.[6]
>
> **Persona – Estratégico:** Personal cuyas funciones y/o actividades están relacionadas con la planeación con el fin de lograr los objetivos de la Entidad y su fin es establecer los planes de acción para el funcionamiento de la Entidad. Se basa en decidir los objetivos, definir los recursos que se usarán y las políticas y directrices para obtener y administrar dichos recursos.[7]

**6.4.2. Responsable del activo:** Es la persona o proceso responsable de alimentar o utilizar el activo de información

[5] Tomado de https://blog.acsendo.com/los-niveles-de-gestion-en-una-organizacion/, Julio 11 de 2019.
[6] Tomado de https://blog.acsendo.com/los-niveles-de-gestion-en-una-organizacion/,Julio 11 de 2019.
[7] Tomado de https://blog.acsendo.com/los-niveles-de-gestion-en-una-organizacion/, Julio 11 de 2019.




### 6.4.3. Respaldo:


Para el caso de activos de información tipo Información, Software, Hardware o Red hace referencia al respaldo que permite garantizar la continuidad de la Entidad.

Para el caso de activos de información tipo “persona” hace referencia a la persona o recurso al interior de la Entidad que está al tanto y puede realizar las actividades del activo tipo persona e incluso existe transferencia de conocimiento.

Se definen las siguientes categorías:

- **Existe transferencia del conocimiento:** Las actividades realizadas por la persona se encuentran documentadas y/o se ha realizado capacitación y transferencia del conocimiento considerado de valor a otras personas, de tal manera que en caso de ausencia las actividades y/o tareas pueden ser ejecutadas sin generar interrupciones en la operación normal del proceso o de la Entidad.

- **No existe transferencia del conocimiento:** Las actividades realizadas por la persona NO se encuentran documentadas ni se ha realizado capacitación o transferencia del conocimiento considerado de valor a otras personas, y en su ausencia se pueden presentar interrupciones en la prestación de los servicios o el desarrollo de actividades que afectarían la operación normal del proceso o de la Entidad

- **Tiene un respaldo:** Existe una persona que ha sido capacitada y entrenada para ejecutar las actividades de la persona identificada como activo de información, de tal manera que en caso de ausencia no se vean afectadas las operaciones normales de proceso o de la Entidad.

- **No tiene respaldo:** NO existe una persona capacitada y entrenada para ejecutar las actividades de la persona identificada como activo de información, y en caso de ausencia se pueden presentar interrupciones en la prestación de los servicios o el desarrollo de actividades que afectarían la operación normal del proceso o de la Entidad

Se debe elegir alguno de los valores anteriores y estos tendrán un peso en la valoración final del activo a saber:

| Categoría | Afecta la calificación final |
|---|---|
| **Existe transferencia del conocimiento** | Disminuye la criticidad del activo en 1 |
| **No existe transferencia del conocimiento** | Aumenta la criticidad del activo en 1 |
| **Tiene un respaldo** | Disminuye la criticidad del activo en 1 |
| **No tiene un respaldo** | Aumenta la criticidad del activo en 1 |

### 6.4.4. Clasificación de la Información Frente a Ley 1712 de 2014 y Ley 1581 de 2012

| Clasificacion de la Informacion Frente a Ley 1712 de 2014 y Ley 1581 de 2012 | | | | | |
|---|---|---|---|---|---|
| Nivel de Confidencialidad Ley 1712 de 2014 | | | Nivel de Proteccion de Datos Ley 1581 de 2012 | | |
| Pública | Pública Clasificada | Pública Reservada | Si contiene Datos personales | No contiene Datos personales | No Aplica |
| | | | | | |
| | | | | | |
| | | | | | |

Clasificar los activos de información identificados conforme a lo dispuesto en la Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública) y ley 1581 de 2012 (Ley de Protección de Datos Personales) y sus leyes y decretos regulatorios.

#### 6.4.4.1. Clasificación del nivel de confidencialidad según Ley 1712 de 2014

A nivel de confidencialidad del activo y de acuerdo con la Ley 1712 de 2014 los activos de información se clasificarán en pública, pública clasificada y pública reservada (Ver definiciones), y se asignará la siguiente escala de valores:

| Nivel de Confidencialidad Ley 1712 de 2014 | Valor |
|---|---|
| **Pública reservada** | 3 |
| **Pública clasificada** | 2 |
| **Pública** | 1 |

*Tabla 1 Esquema de clasificación por Ley 1712 de 2014*

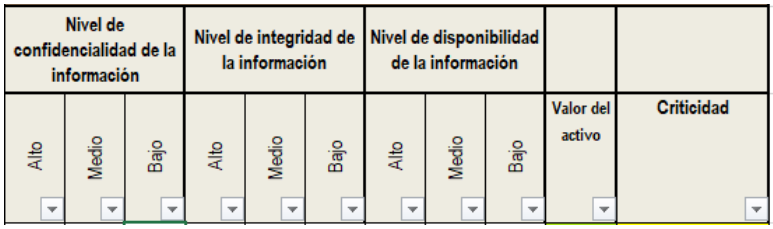
#### 6.4.4.2. Clasificación del nivel de protección de datos según Ley 1581 de 2012

A nivel de protección de datos personales los activos de información se clasificarán en los siguientes rangos y escala de valores:

| Nivel de Protección de Datos Ley 1581 de 2012 | Valor |
|---|---|
| **Si contiene datos personales** | 3 |
| **Si no contiene datos personales** | 2 |
| **Si no aplica** | 1 |

*Tabla 2 Esquema de clasificación por Ley 1581 de 2012*

## 6.5. VALORACIÓN DEL ACTIVO




En esta etapa se debe determinar la criticidad de activo de acuerdo a los niveles de confidencialidad, integridad y disponibilidad, determinando el grado de importancia de cada uno de ellos.

### 6.5.1. Valoración del nivel de criticidad respecto a la Confidencialidad

Como la Ley 1712 de 2014 Transparencia y del Derecho de Acceso a la Información Pública, determina una clasificación, el nivel de criticidad respecto a la confidencialidad se asignará en relación a esta con las escalas y valores de acuerdo a los criterios descritos en la siguiente tabla:

| Nivel de Confidencialidad | Valor | Clasificación según Ley 1712 de 2014 |
|---|---|---|
| **Alto** | 3 | Pública reservada |
| **Medio** | 2 | Pública clasificada |
| **Bajo** | 1 | Pública |

*Tabla 3 Esquema de valoración por Confidencialidad*

### 6.5.2. Valoración del nivel de criticidad respecto a la Integridad

La integridad se refiere a la propiedad de salvaguardar la exactitud y estado completo de los activos, para valorar su nivel de criticidad se tendrá en cuenta los siguientes criterios:

| Nivel de Integridad | Valor | Descripción |
|---|---|---|
| **Alto** | 3 | 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 o entes externos. |
| **Medio** | 2 | 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. |
| **Bajo** | 1 | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Entidad o entes externos. |

*Tabla 4 Esquema de valoración por Integridad*

### 6.5.3. Valoración del nivel de criticidad respecto a la Disponibilidad

La disponibilidad se refiere a la propiedad de que la información sea accesible y utilizable en el momento que sea requerido por persona(s) y/o Entidad(es) autorizada(s). Para valorar su nivel de criticidad se tendrá en cuenta los siguientes criterios:

| Nivel de Disponibilidad | Valor | Descripción |
|---|---|---|
| **Alto** | 3 | 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. |
| **Medio** | 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. |
| **Bajo** | 1 | 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. |

*Tabla 5 Esquema de valoración por Disponibilidad*

### 6.5.4. Valoración de criticidad del Activo

El valor de criticidad del activo está dado por la suma de los valores asignados a cada una de las clasificaciones dadas a los activos de información:

- Nivel de Confidencialidad Ley 1712 de 2014
- Nivel de Protección de Datos Ley 1581 de 2012
- Nivel de criticidad respecto a la confidencialidad
- Nivel de criticidad respecto integridad
- Nivel de criticidad respecto a la disponibilidad

Se tendrán en cuenta los siguientes valores para determinar el nivel de criticidad del activo:

| Valor de criticidad del activo | Rango |
|---|---|
| **Critico** | Sumatoria mayor Igual 11 |
| Moderado | Sumatoria menor igual a 10 |
| **Bajo** | Sumatoria menor igual a 5 |

*Tabla 6 Esquema de valoración de criticidad del activo*

El valor del activo permite determinar que activos (Valor critico Alto) se tendrán en cuenta para la identificación y valoración de riesgos de seguridad de la información.

Una vez se ejecute la identificación de los activos, la Entidad debe definir si gestionará los riesgos en todos los activos del inventario o si se tendrán en cuenta alguno(s) de los valores de criticidad resultante para cada activo.

## 7. NORMATIVIDAD APLICABLE

| TIPO DE NORMA | NÚMERO | AÑO | EMISOR | ARTÍCULOS (APLICACIÓN) |
|---|---|---|---|---|
| Ley | 1581 | 2012 | Congreso de la República | Toda la norma. |
| Ley | 1712 | 2014 | Congreso de la República | Toda la norma. |
| Norma técnica colombiana NTC-ISO-IEC | 27001 | 2013 | Information Technology Security Techniques | Toda la norma. |