CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital / Nombre: Ludís Elvira Agamez Ordóñez Cargo: Coordinadora Grupo Gestión Documental y Archivo	Nombre: Adriana Cetina Hernández Cargo: Jefe Oficina de Tecnología e Informática Nombre: Johana Elizabeth Duarte García Cargo: Directora Administrativa	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2024-05-31

1 OBJETIVO

Establecer las directrices y actividades generales para identificar, clasificar y valorar los activos de información de la Superintendencia de Industria y Comercio - SIC, a través de los lineamientos establecidos en este documento. Esta metodología orienta a los líderes de procesos en identificar los activos de información con el diligenciamiento del documento SC05-F03 **Registro de Activos de Información**, que ha sido establecido por la Entidad.

2 DESTINATARIOS

La metodología para la identificación, clasificación y valoración de activos de información de la Superintendencia de Industria y Comercio aplica a todos los procesos, bajo la responsabilidad de los líderes de cada proceso.

3 GLOSARIO

ACTIVO DE INFORMACIÓN: Es el elemento de información que se recibe o produce en el ejercicio de sus funciones incluye la información que se encuentre en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

AUTENTICIDAD DE LA INFORMACIÓN: Garantiza que los documentos o información son verdaderos o seguros (Departamento Nacional de Planeación, 2016).

CISO (Chief Information Security Officer): de acuerdo con (INCIBE, 2016): “Es el director de seguridad de la información”. Esencialmente corresponde al rol o perfil que es desempeñado a nivel ejecutivo y que como objetivo principal es engranar la seguridad de la información con los objetivos estratégico de la Entidad.

CONFIABILIDAD DE LA INFORMACIÓN: la confiabilidad permite certificar que el origen de la información creada sea apropiado para respaldar la toma de decisiones (Ministerio de Tecnologías de la Información y las Comunicaciones, 2019, pág. 4).

CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible, es decir, es divulgada a individuos, entidades o procesos que sean autorizados por la Entidad (Departamento Administrativo de la Función Pública, 2018, pág. 9).

CONTROL: Se interpretan como las medidas que transforman el riesgo. Los controles contienen los procesos, procedimientos, políticas, prácticas y dispositivos que cambian los riesgos (NTC-ISO:31000, 2018, pág. 9).

CUSTODIO DEL ACTIVO DE INFORMACIÓN: Como es mencionado por (Departamento Nacional de Planeación, 2016), es una porción determinada de la entidad, cargo, proceso, o grupo de trabajo delegado para gestionar y velar por el efectividad de los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado), que el responsable de la información diseñara para dicho fin, con los lineamientos de controles de seguridad estructurados por la entidad (pág. 9).

DATO PERSONAL: Según la directriz de (Ley N° 1581, 2012): “Es cualquier fragmento de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal” (pág. 2).

DATO PRIVADO: Se considera como cualquier información de naturaleza discreta o reservada solo para el titular (Ley N° 1266, 2008).

DATO PÚBLICO: Son todos aquellos datos que no sean semiprivado o privado y estén dentro del entorno de la constitución pública o la Ley. Los datos públicos están determinados entre la información relativa al estado civil de las personas, su profesión y a su calidad de comerciante o servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, como en registros públicos, documentos públicos, boletines oficiales y sentencias judiciales debidamente ejecutoriadas, que no estén sometidas a reserva (Ley N° 1266, 2008).

DATO SEMIPRIVADO: Se comprende como semiprivado los dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general (Ley N° 1266, 2008).

DATO SENSIBLE: Se entiende de acuerdo a la (Ley N° 1581, 2012), que: “afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, fla pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos”(pág. 4).

DISPONIBILIDAD: Comprende a la capacidad de los usuarios para acceder, utilizar o dar tratamiento a la información autorizada por la Entidad, en una ubicación determinada y en un formato correcto (NTC-ISO/IEC:27000, 2018).

HARDWARE: Determina el grupo de los elementos físicos que conforman el correcto funcionamiento de un entorno informático (redes, discos duros o extraíbles, impresoras, servidores, computadoras, dispositivos móviles, entre otros) (Departamento Administrativo de la Función Pública, 2014).

INFORMACIÓN: Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos misionales de la Superintendencia de Industria y Comercio.

En la ley 1712 de 2014 en el artículo 6, la define como: un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen obtenga, adquieran, transformen o controlen.

INFORMACIÓN PÚBLICA CLASIFICADA: 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 porque su acceso podrá ser negado o exceptuando siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 6 de la ley 1712 de 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 interés públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

IMPACTO: Se concibe como las consecuencias que puede originar o causar a la Entidad la materialización del riesgo (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, pág. 31).

INVENTARIO DE ACTIVOS: Consta del registro detallado de todos aquellos recursos tangibles e intangibles que den valor a la Entidad, y que estén dentro del alcance del Modelo de Seguridad y Privacidad de la Información.

INTEGRIDAD: Propiedad de la información referida a su exactitud o consistencia de los datos (NTC-ISO/IEC:27000, 2018).

LÍDER DE PROCESO: Se entiende por líder de proceso a los Jefes de Oficina y directores de oficinas o los que la Superintendencia de Industria y Comercio - SIC considere como líderes de proceso (Pueden ser coordinadores u otros cargos en la Entidad).

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una Entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

PROPIETARIO DE LA INFORMACIÓN: Delegatura, Oficina, Dirección o Grupo de Trabajo que tiene como responsabilidad la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos que tiene como responsabilidad velar por la protección del activo de información.
El Ministerio de Tecnologías de la Información y las Comunicaciones, 2016 menciona que: “es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida” (pág. 8).

SEGURIDAD DE LA INFORMACIÓN: Conservación de la confidencialidad, la integridad y la disponibilidad de los datos resguardados en los sistemas de información de cualquier amenaza o intenciones malintencionadas (NTC-ISO/IEC:27000, 2018).

SELECCIÓN DE CONTROLES: Proceso de elección de salvaguardo que aseguren la reducción de los riesgos a un nivel aceptable para evitar una pérdida o daño en un activo de información (Departamento Nacional de Planeación, 2016).

SERIE DOCUMENTAL: El Acuerdo N°027, 2006 indica que es: “un conjunto de unidades documentales de estructura y contenido homogéneos, emanadas de un mismo órgano o sujeto productor como consecuencia del ejercicio de sus funciones específicas” (pág. 10).

SUBSERIE DOCUMENTAL: El Acuerdo N° 027, 2006 menciona que es: “un conjunto de unidades documentales que forman parte de una serie, identificadas de forma separada de ésta por su contenido y sus características Específicas” (pág. 10).

SERVICIOS: Comprende las actividades ejecutadas o prestadas por las personas, dependencias (direcciones y oficinas) o entidades externas, que facilitan la administración o flujo de la información generada por el proceso. En esta tipología se encuentra la intranet, el internet, el correo electrónico, el servicio de

fotocopiado, el servicio de correspondencia, el servicio de ingreso a la entidad, entre otros (Secretaría Jurídica Distrital, 2019).

SISTEMA INTEGRADO DE GESTIÓN Y AUTOCONTROL: Por mención de la Secretaría Distrital de Planeación, 2019 es: “el conjunto de orientaciones, procesos, políticas, metodologías, instancias e instrumentos enfocados a garantizar un desempeño institucional articulado y armónico que busque de manera constatable la satisfacción de los grupos de interés".

SOFTWARE: Es un conjunto de programas, instrucciones y reglas informáticas, para realizar ciertas tareas en equipos de cómputo (Departamento Administrativo de la Función Pública, 2014).

TABLA DE RETENCION DOCUMENTAL: El Acuerdo N° 027, 2006 menciona que es Listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas (NTC-ISO/IEC:27000, 2018).

4 GENERALIDADES

La Superintendencia de Industria y Comercio - SIC, para dar cumplimiento al mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información, a través de la definición de un Sistema de Gestión de Seguridad de la Información (SGSI), tiene el compromiso de generar y actualizar los activos de información que son manejados en los procesos de la Entidad, a través de la identificación, clasificación y valoración de éstos.

La realización de un inventario de activos de información hace parte de la debida diligencia que a nivel estratégico ha considerado la Entidad, dentro de sus elementos a tratar con respecto a la seguridad y privacidad para los activos de información.
Las mejores prácticas sobre seguridad y privacidad de la información a nivel nacional e internacional recomiendan la realización de un inventario (identificación y/o actualización), clasificación y valoración de los activos de información de las organizaciones sean éstas públicas o privadas, para determinar cómo deben ser utilizados éstos en los procesos de la Entidad, los roles y las responsabilidades que tiene el personal (sean colaboradores o personal externo a la Entidad) sobre los mismos, reconociendo adicionalmente los niveles de confidencialidad, integridad y disponibilidad que a cada activo de información debe darse. Siendo construido con base en la siguiente normatividad:

- Modelo de Seguridad y Privacidad de la Información - MSPI.

- Ley 1712 de 2014, por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Por medio del registro de activos de información se puede determinar la información que debe ser protegida en la Entidad, las características de la misma, los responsables de su creación o custodia y el nivel de clasificación de cada activo de información.

Establecer un inventario de activos de información hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información y cuyo objetivo es apoyar la implementación de los siguientes controles de la Guía 8 - Controles de Seguridad de la Información de dicho modelo.

- 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.

De forma similar, en el Decreto 103 de 2015, capitulo 1, parágrafo 1 del artículo 38, se indica que una categoría de información *es "toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formatos o estructura)"*

Es de anotar que, una serie documental es un conjunto de unidades documentales homogéneas emanadas por un mismo órgano o sujeto productor en ejercicio de

sus funciones ejemplo: contratos, historias laborales, actas. Por consiguiente, las categorías a las que hace referencia el Decreto 103 de 2015, corresponde por definición a las series documentales.

4.1 ROLES Y RESPONSABILIDADES

Tabla Responsable y responsabilidades frente a los Activos de Información

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL ACTIVO DE INFORMACIÓN	NORMATIVIDAD
Estratégica	Comité Institucional de Gestión y Desempeño	• Toma de decisiones en los casos de incumplimiento de los procesos en la actualización de los activos de información presentados por el oficial de seguridad y las respectivas recomendaciones (Presentación del caso a asuntos disciplinarios, la implementación de acciones de mejora, la solicitud de informes, etc.) Aprobar la publicación de activos de información en la página de web.	• Ley 1712 de 2014 • Resolución Interna No. 89082 de 2018 • Resolución 20840 DE 2020
Primera Línea	Líderes de procesos	Líder del proceso: • Velar por la aplicación y cumplimiento de los lineamientos de la Metodología para la identificación, clasificación y valoración de activos al interior de su proceso. • Identificar, clasificar y valorar los activos de información de los procesos a su cargo y actualizarlos cada año o cuando (exista un cambio en las actividades del hacer del proceso, se determine que un activo de información no continúa siendo parte del inventario de activos, si se debe ingresar algún activo nuevo que se haya identificado, si hubo actualización de los instrumentos (Tabla de Retención Documental o del Índice de información clasificada y reservada), o si los valores de evaluación asignados deben ser modificados)	• Ley 1712 de 2014 • Anexo 4 - Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas • SC01-POL01 Política de Riesgos • SC01-P03 Metodología para la administración del riesgo • Resolución Interna No. 89082 de 2018 • Resolución 20840 DE 2020 • SC05-POL01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI (Apartado 6.6)
Segunda Línea	La OTI a través de la coordinación Grupo de Trabajo de Informática Forense y seguridad Digital	• Desarrollar una metodología para la identificación, clasificación y valoración de los activos de información. • Aprobar el inventario de activos de información de la SIC anualmente, o cuando se realiza actualizaciones al proceso al que pertenece el activo. • Asesorar y acompañar la identificación de activos de información, a los lideres de proceso en. • Consolidar los Activos de Información de la Entidad y enviar al Grupo de Trabajo de Gestión Documental y archivo, para el trámite correspondiente de publicación en la sección correspondiente de la página web. • Solicitar a la Oficina Asesora de Planeación, que se carguen los activos de información de cada proceso al aplicativo SIGI. • Presentar al Comité Institucional de Gestión y Desempeño, el seguimiento a la actualización e identificación de los activos de información,	• Ley 1712 de 2014 • Decreto 103 de 2015 • Anexo 4 - Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas • Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – 2022 • Resolución Interna No. 89082 de 2018 • Resolución 20840 DE 2020 • Políticas del Sistema de Gestión de Seguridad de la Información - SGSI Ítem 6.6 RESPONSABILIDADES SOBRE LOS ACTIVOS • Modelo de Seguridad y Privacidad de la Información. • ISO 27001

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL ACTIVO DE INFORMACIÓN	NORMATIVIDAD
		generando alertas de incumplimiento. • Capacitar a los líderes de los procesos y enlaces designados en la metodología de identificación clasificación y valoración de activos de información.	
	Secretaria General - Grupo de Trabajo de Gestión Documental y Archivo	• Apoyar a los líderes de los procesos en la identificación y actualización de las Tablas de Retención Documental. • Presentar al Comité de Institucional de Gestión y Desempeño, el consolidado de activos de información y solicitar su aprobación para publicar en la página web. • Solicitar a la Secretaria General o a quien esta designe, la publicación del consolidado de los activos de información en la sección correspondiente de la página web de la Entidad. • Solicitar copia del Acta del Comité Institucional de Gestión y Desempeño donde se aprobaron los activos de información a la OAP. • Enviar copia del Acta del Comité Institucional de Gestión y Desempeño donde se aprobaron los activos de información y certificado de la publicación al Grupo de Trabajo de Informática Forense y seguridad Digital.	• Ley 1712 de 2014 • Decreto reglamentario 1080 Artículo 2.8.5.1 - Título V Instrumentos de Gestión de Información Pública. • Resolución Interna No. 89082 de 2018 • Resolución 20840 DE 2020 • Programa de Gestión Documenta (GD01-F17)
	Oficina Asesora de Planeación	• Enviar al Grupo de Trabajo de Gestión Documental y Archivo, el acta del Comité Institucional de Gestión y Desempeño donde se presentaron y aprobaron los Activos de información para publicación en la página web. • Actualizar y publicar los Activos de información en el aplicativo SIGI, una vez el Grupo de Trabajo de Informática Forense y Seguridad Digital cite el No. de acta del Comité Institucional de Gestión y Desempeño donde se aprobaron los activos de información; y se adjunte el certificado de publicación en la página web. • Notificar la publicación de los activos de información en el aplicativo SIGI, al grupo de Grupo de Trabajo de Informática Forense y Seguridad Digital	• Ley 1712 de 2014 • Resolución Interna No. 89082 de 2018
Tercera Línea	Oficina de Control Interno	• Verificar y evaluar, a través de seguimientos o de auditorías internas, la adecuada identificación, clasificación y valoración de los activos de información, identificando las observaciones y oportunidades de mejora.	• ISO 27001

Fuente: Elaboración propia.

4.2 METODOLOGÍA PARA LA IDENTIFICACIÓN, CLASIFICACION Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Para realizar esta actividad debe desarrollarse completando los siguientes aspectos (Ilustración 1):

Ilustración 1.Aspectos de la metodología de inventario de activos de información.

Fuente: Elaboración propia.

Aspecto 1. Identificación de los activos de información: Deberán listarse todos los activos de información por cada proceso indicando como mínimo el nombre del activo y descripción breve del activo. Así mismo para cada uno de los activos identificados deberá asignar un propietario, si un activo no posee un propietario, nadie se hará responsable ni lo protegerá debidamente.

Aspecto 2. Alineación con tablas de retención documental: Identificarlos activos de información que sean documentos, en estos casos se debe incluir la información asociada a la serie y subserie según lo registrado en las tablas de retención documental.

Aspecto 3. Valoración del activo: Especificar la tipología del activo según su naturaleza, como, por ejemplo: Información, Software, Hardware, entre otros, así como evaluar las propiedades de confidencialidad, integridad y disponibilidad de acuerdo con los valores disponibles (Alto, Medio, Bajo, Sin clasificar), con la finalidad de que sea un insumo para el análisis de riesgos y generar la protección, dependiendo del activo de información.

Aspecto 4. Valoración de Protección de Datos Personales: Realizar la calificación de la información personal conforme al uso y tipo de datos personales que sean almacenados o capturados por el activo de información.

Aspecto 5. Alineación con Transparencia y Acceso a la información: Realizar la clasificación de la información conforme lo indican las Leyes, decretos y normas que apliquen.

Aspecto 6. **Datos abiertos**: Catalogar el activo de información como dato abierto en conformidad con la información conservada o contenida en el activo de información.

Aspecto 7. **Infraestructura Crítica**: Identificar si el activo de información puede ser catalogado como infraestructura critica de acuerdo con los criterios establecidos para tal fin.

4.3 FORMATO DE INVENTARIO DE ACTIVOS

En cada proceso de la Entidad se procede a llevar a cabo la identificación y/o actualización de los activos de información, para lo cual se debe llevar a cabo el diligenciamiento del documento SC05-F03 **Registro de Activos de Información**, que se encuentra publicada en la aplicación activa del Sistema Integral de Gestión Institucional, la cual contiene los siguientes aspectos y campos que deben ser diligenciados:

4.3.1 Campos generales para información del inventario (Tabla 1) (Ilustración 2).

Ilustración 2.Información general registro de activos de información.

PROCESO	
LIDER DE PROCESO O FUNCIONARIO DESIGNADO	
FECHA ÚLTIMA ACTUALIZACIÓN	

Fuente: Registro de Activos de Información.

Tabla 1. Información general del Registro de Activos de Información.

CAMPO	DEFINICIÓN	PROPIETARIO DE LIGENCIAMIENTO
PROCESO	Corresponde al nombre del proceso en el cual se está realizando el inventario y valoración de activos de información.	Líder de proceso / Funcionario designado / CISO
LIDER DE PROCESO O FUNCIONARIO DESIGNADO / CALIFICADO POR	Persona Propietario del (los) proceso (s) al interior de la oficina o dirección a la cual pertenece para la identificación/actualización, clasificación y valoración de los activos de información.	Líder de proceso / Funcionario designado / CISO
FECHA ÚLTIMA ACTUALIZACIÓN	Última fecha en la cual se llevó a cabo la identificación/actualización, clasificación y valoración de los activos de información de los procesos que tiene a cargo.	Líder de proceso / Funcionario designado / CISO

Fuente: Elaboración propia.

4.4 PERIODICIDAD PARA LA ACTUALIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

De acuerdo con el Modelo de Seguridad y Privacidad de la Información, la actividad de actualización 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 deben ser modificados. En general, el inventario de activos puede ser revisado anualmente o validado en cualquier momento por parte de la dependencia responsable. Algunas de las razones por las cuales se debería realizar la revisión o validación son las siguientes:

a) Actualizaciones al proceso al que pertenece el activo.
b) Adición de actividades al proceso.
c) Inclusión de nuevos registros, procesos y procedimientos.
d) Inclusión de un nuevo activo.
e) Supresión de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio.
f) Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
g) Cambios físicos de la ubicación de activos de información.

La actualización del registro de activos de información debe dar cumplimiento a lo establecido en la resolución 89082 del 07 de diciembre de 2018 en el artículo segundo, el cual ordena a todas las dependencias de la Superintendencia de Industria y Comercio a mantener actualizados los instrumentos documentales.

La frecuencia de actualización de los instrumentos se realizará anualmente o de acuerdo con la necesidad y/o cambios que se presenten en la información de la entidad, los cuales deberán ser aprobados previamente por el Comité Institucional de Gestión y Desempeño.

4.5 NORMATIVA APLICADA

Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
Guía No.5	2016	Guía para la Gestión y Clasificación de Activos de Información.		Aplicación total
NTC/ISO/IEC 27001	2013	Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.		Aplicación total

Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
NTC/ISO/IEC 27002	2013	Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información.		Aplicación total
NTC/ISO/IEC 27003	2017	Directrices para la implementación de un SGSI.		Aplicación total
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	Art. 13	Aplicación parcial
Decreto Nacional 1494	2015	Por el cual se corrigen yerros en la Ley 1712 de 2014.		Aplicación total
Decreto Nacional 103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.	Capítulo I Art. 37 Art. 38	Aplicación parcial
Decreto 1083	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.		Aplicación total
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.		Aplicación total
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.		Aplicación total
Resolución 89082	2018	Por la cual se adoptan los instrumentos de la Gestión de la Información Pública de la Superintendencia de Industria y Comercio.	Art. 2	Aplicación parcial

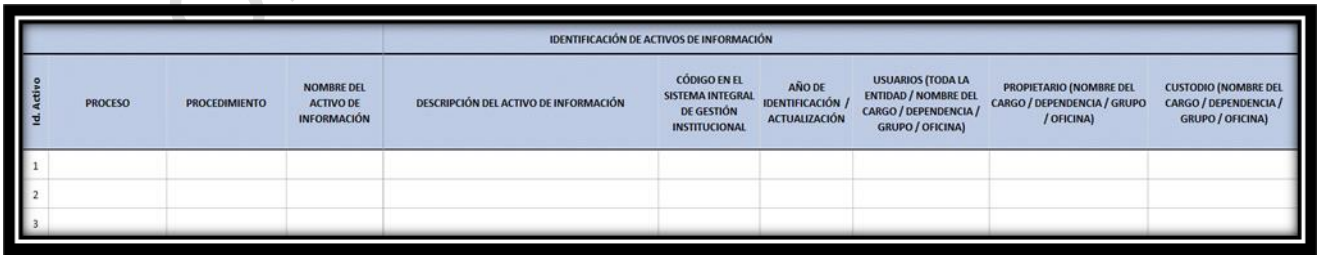
Jerarquía de la norma	Número/ Fecha	Título	Artículo	Aplicación Específica
Guía	2018	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital.	Anexo 4	Aplicación total
Modelo de Seguridad y Privacidad de la Información - MSPI	2021	Imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.		Aplicación total

5 DESCRIPCIÓN DE LAS ACTIVIDADES

5.1 IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN

5.1.1 Campos para la identificación de los activos (Tabla 2) (Ilustración 3).

Ilustración 3.Información de la identificación de activos de información.



	IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN								
Id. Activo	PROCESO	PROCEDIMIENTO	NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	CÓDIGO EN EL SISTEMA INTEGRAL DE GESTIÓN INSTITUCIONAL	AÑO DE IDENTIFICACIÓN / ACTUALIZACIÓN	USUARIOS (TODA LA ENTIDAD / NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)	PROPIETARIO (NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)	CUSTODIO (NOMBRE DEL CARGO / DEPENDENCIA / GRUPO / OFICINA)
1									
2									
3									

***Fuente**: Registro de Activos de información*

Tabla 2. Información para el registro e Identificación de activos.

INFORMACIÓN DE LOS ACTIVOS DE INFORMACIÓN		
CAMPO	**DEFINICIÓN**	**PROPIETARIO DE DILIGENCIAMIENTO**
ID. ACTIVO	Este es un indicador automático propio del registro.	Automático por herramienta
PROCESO	Proceso al cual pertenece activo de información.	Líder de proceso / Funcionario designado
PROCEDIMIENTO	Nombre del procedimiento en el que se encuentra referenciado o al que pertenece el activo de información.	Líder de proceso / Funcionario designado
NOMBRE DEL ACTIVO DE INFORMACIÓN	Denominación asignada al activo de información. Es necesario resaltar que este nombre en el caso de ser formatos o documentos puede ser diferente al nombre asignado al formato o documento.	Líder de proceso / Funcionario designado
DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	Descripción o detalle que permite contextualizar o proporcionar más información sobre el activo de información.	Líder de proceso / Funcionario designado
CÓDIGO EN EL SISTEMA INTEGRAL DE GESTIÓN INSTITUCIONAL	Código que haya sido asignado al documento, formato o archivo dentro Sistema Integral de Gestión Institucional.	Líder de proceso / Funcionario designado
USUARIO	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.	Líder de proceso / Colaborador designado
PROPIETARIO	Cualquier 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 del proceso, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.	Líder de proceso / Funcionario designado
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.	Líder de proceso / Funcionario designado

Fuente: Elaboración propia.

5.2 ALINEAR CON TABLAS DE RETENCIÓN DOCUMENTAL.

5.2.1 Campos requeridos para retención documental (Tabla 3) (Ilustración 4).

Ilustración 4.Información de tablas de retención documental.

***Fuente**: Registro de Activos de Información.*

Tabla 3. Información para alineación con tablas de retención documental.

RETENCIÓN DOCUMENTAL		
CAMPO	**DEFINICIÓN**	**PROPIETARIO DE DILIGENCIAMIENTO**
SERIE	Nombre asignado en la tabla de retención documental para la serie.	Líder de proceso / Funcionario designado
SUBSERIE	Nombre asignado en la tabla de retención documental para la subserie.	Líder de proceso / Funcionario designado

Fuente: Elaboración propia.

5.3 VALORAR EL ACTIVO

5.3.1 Categorías de Activos de información (Tabla 4).

Tabla 4. Clasificación de tipos de activos de información.

TIPO DE ACTIVOS	DESCRIPCIÓN
BASES DE DATOS	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, puede ser utilizada en un formato de motor ya sea SQL, SQL Server, MySQL o en formato Excel. **Ejemplos:** Bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, Base de datos Aprendices, Listado de proveedores, estados financieros) entre otros.
DATOS / INFORMACIÓN	Que es almacenado en equipos o soportes de información (normalmente agrupado como archivos o bases

TIPO DE ACTIVOS	DESCRIPCIÓN
	de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. **Ejemplo:** Copias de Respaldo, Archivos, 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, 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 integral de gestión institucional, formatos o formularios físicos o digitales.
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.
HARDWARE / INFRAESTRUCTURA	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 Propietarios 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 (host), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
INSTALACIONES	Lugares donde albergan los sistemas de información y comunicaciones. Ejemplo: Data Center, cuarto de comunicaciones, cuarto de cómputo.
REDES DE COMUNICACIONES	Infraestructuras 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, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (RDSI).
ROLES O CARGOS (RRHH)	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
SERVICIOS	Funciones que permiten suplir una necesidad de los usuarios del servicio. **Ejemplo:** Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de archivos, transferencia de archivos, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública), servicios relacionados con la enseñanza a los aprendices de la Entidad, servicios relacionados con los prestados por la Entidad hacia los grupos de valor, servicios relacionados para el desarrollo de las funciones de grupos de interés.
SOFTWARE / APLICACIONES INFORMÁTICAS	Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. **Ejemplo:** Aquellos utilizados para la enseñanza, para el desarrollo de aplicaciones, para la gestión o administración de bases de datos, para la gestión o administración de documentos, para la gestión del correo electrónico, para la navegación web, para el desarrollo de aplicaciones propias, para la gestión de

TIPO DE ACTIVOS	DESCRIPCIÓN
	respaldos de información, para la prevención de virus o infecciones informáticas, para conexiones o trabajos remotos, entre otros.
SOPORTES DE INFORMACIÓN	Dispositivos físicos o electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo y que posteriormente permiten recuperar la información contenida en ellos. **Ejemplo:** Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.

Fuente: Elaboración propia.

5.3.2 Criterios de clasificación de activos

La clasificación de activos de información tiene como objetivo asegurar que los activos reciben los niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características particulares requiere un tipo de manejo especial.

Cada nivel de clasificación establece requerimientos específicos de tratamiento durante el ciclo de vida del activo y cada activo, a su vez, debe estar clasificado en un único nivel de Confidencialidad, Integridad y Disponibilidad, ya sea Alta, Media, Baja de acuerdo con su criticidad.

- **Clasificación según la confidencialidad.**

La confidencialidad hace referencia a la protección de información para así evitar el acceso o la divulgación no autorizada (Tabla 5):

Tabla 5. Clasificación según la confidencialidad.

DESCRIPCIÓN	VALOR
Pública Reservada / Confidencial = Alta: 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. Por lo tanto, cuando un activo de información realice tratamiento de datos personales privados o sensibles el activo de Información deberá ser calificado como activo de información pública confidencial (ALTO).	**ALTO**

DESCRIPCIÓN	VALOR
Pública Clasificada / Uso Interno = Medio: 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. Por lo tanto, cuando un activo de información realice tratamiento de datos personales semiprivados, el activo de Información deberá ser calificado por lo menos como un activo de información pública de uso interno (MEDIO).	**MEDIO**
Pública / Pública = Baja: 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.	**BAJO**

Fuente: Elaboración propia.

- **Clasificación según la integridad.**

La integridad se define como la propiedad que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción (Tabla 6):

Tabla 6. Clasificación según la integridad.

DESCRIPCIÓN	VALOR
ALTO Información cuya modificación no autorizada, causa pérdida de exactitud y falta de datos, podría no repararse completamente, afecta a toda la organización generando retraso en las funciones, y los daños son casi irreparables, no se cuenta con los medios ni mecanismos para recuperar la información.	**ALTO**
MEDIO: Información cuya modificación no autorizada, pérdida de exactitud y falta de datos, podría repararse parcialmente, se afectan varios procesos generando retrasos en las actividades, se cuenta con un backup de la información.	**MEDIO**
BAJO Información cuya modificación no autorizada, pérdida de exactitud y falta de datos se puede remediar. Se afecta solo un porcentaje del proceso, no se pierde información, se puede seguir trabajando.	**BAJO**

Fuente: Elaboración propia.

- **Clasificación según la disponibilidad.**

La disponibilidad es la propiedad de la información que se refiere a que ésta debe estar en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso (Tabla 7):

Tabla 7. Clasificación según la disponibilidad.

DESCRIPCIÓN	VALOR
ALTO: Información donde la imposibilidad de acceso por menos de 1 día ocasiona pérdidas mayores y/o sanciones a la entidad.	**ALTO**
MEDIO Información donde la imposibilidad de acceso por un periodo de entre 2 y 7 días puede ocasionar pérdidas o sanciones la entidad. Indisponibilidad: entre 2 y 7 días calendario.	**MEDIO**
BAJO: Información donde la imposibilidad de acceso no afecta en forma significativa el movimiento de la entidad y puede no estar disponible más de una semana. Indisponibilidad: más de una semana (1 semana = 7 días calendario)	**BAJO**

Fuente: Elaboración propia.

- **Valor total del activo.**

El sistema de clasificación para la valoración del activo de información identificado y/o actualizado se basa en la confidencialidad como principio rector, e incluye el tratamiento de la información en cuanto a la Confidencialidad, Integridad y Disponibilidad de cada activo. Así mismo, contempla el impacto que causaría la perdida de alguna de estas propiedades, por lo tanto, se definieron tres (3) niveles que permiten determinar el valor general del activo en la entidad; es importante aclarar que los niveles son definidos a criterio del propietario del activo (Alta, Media, Baja), con el fin de identificar qué activos deben ser tratados de manera prioritaria (Tabla 8):

Tabla 8. Descripción del valor total del activo.

DESCRIPCIÓN	VALOR
Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad y disponibilidad) es alta.	**ALTO**
Activos de información en los cuales la clasificación es alta en (1) de sus propiedades o al menos una de ellas es de nivel medio.	**MEDIO**
Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.	**BAJO**

Fuente: Elaboración propia.

5.3.3 Campos requeridos para clasificación del activo

La clasificación de activos de información tiene como objetivo asegurar que los activos reciben los niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características particulares requiere un tipo de manejo especial (Tabla 9) (Ilustración 5):

Ilustración 5.Información de valoración de activos.

VALORACIÓN DEL ACTIVO					
Tipo de Activo	CRITICIDAD RESPECTO A LA CONFIDENCIALIDAD	CRITICIDAD RESPECTO A LA INTEGRIDAD	CRITICIDAD RESPECTO A LA DISPONIBILIDAD	Valor del Activo para el proceso	OBSERVACIONES

Fuente: Registro de Activos de Información.

Tabla 9. Información para valoración del activo de información.

VALORACIÓN DEL ACTIVO		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
TIPO DE ACTIVO	Define el tipo al cual pertenece el activo de acuerdo con las categorías de activos de información definidas.	Líder de proceso / Funcionario designado
CLASIFICACIÓN SEGÚN LA CONFIDENCIALIDAD	Se dará la calificación de acuerdo con los criterios establecidos para clasificar la confidencialidad.	Líder de proceso / Funcionario designado
CLASIFICACIÓN SEGÚN LA INTEGRIDAD	Se dará la calificación de acuerdo con los criterios establecidos para clasificar la integridad.	Líder de proceso / Funcionario designado
CLASIFICACIÓN SEGÚN LA DISPONIBILIDAD	Se dará la calificación de acuerdo con los criterios establecidos para clasificar la disponibilidad.	Líder de proceso / Funcionario designado
VALOR DEL ACTIVO PARA EL PROCESO	Este campo se calcula de manera automática como resultado final de la clasificación a nivel de las propiedades de: confidencialidad, integridad y disponibilidad.	Cálculo automático

VALORACIÓN DEL ACTIVO		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
OBSERVACIONES	En este campo se deben plasmar todas las observaciones que el dueño del activo de información considere necesarias con respecto al Activo de Información, puede anotarse también las razones por las cuales se realizaron las calificaciones, y qué se tuvo en cuenta para determinar las mismas.	Líder de proceso / Funcionario designado

Fuente: Elaboración propia.

5.4 VALORAR LOS ACTIVOS EN LA PROTECCIÓN DE DATOS PERSONALES.

5.4.1 Criterios y condiciones de valoración (Tabla 10).

Tabla 10. Información para valoración del activo de información.

DESCRIPCIÓN	VALOR	CONDICIÓN
El activo almacena o solicita Datos personales	SI / No	En este campo se indica si el activo de información almacena o solicita o recolecta datos de tipo personal. Ej. Datos de contacto, datos laborales, datos patrimoniales, datos académicos, entre otros.
Los datos almacenados o requeridos son públicos.	SI / No /	Este campo solamente es diligenciado cuando en el campo "**El activo almacena o solicita Datos personales"** se selecciona "Si". El campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado, permitiendo indicar si los datos personales que almacena, solicita o recolecta son de tipo público. Es decir, datos personales que la Entidad o las Leyes ha determinado expresamente como públicos.
Los datos almacenados o requeridos son Privados	SI / No /	Solamente es diligenciado cuando en el campo "**El activo almacena o solicita Datos personales"** se selecciona "Si". El campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado, permitiendo indicar si los datos personales que almacena, solicita o recolecta son de tipo privado. Es decir, datos personales que por su naturaleza son datos que solo le interesan al titular y no deberían ser conocidos por terceros.
Los datos almacenados o requeridos son Semiprivados	SI / No /	Solamente es diligenciado cuando en el campo "**El activo almacena o solicita datos personales"** se selecciona "Si". El campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado, permitiendo indicar si los datos que almacena, solicita o recolecta son de tipo semiprivados. Es decir, datos personales que por su naturaleza son datos que le interesan tanto al dueño de los datos como a

DESCRIPCIÓN	VALOR	CONDICIÓN
		terceros.
Los datos almacenados o requeridos son Sensibles	SI / No /	Solamente es diligenciado cuando en el campo "**El activo almacena o solicita Datos personales"** se selecciona "Si". El campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado, permitiendo indicar si los datos que almacena, solicita o recolecta son sensibles. Es decir, tipos de datos que, de acuerdo con la Ley de protección de datos colombiana, se han clasificado como sensibles, son de especial protección o pueden someter a discriminación.
Aviso de privacidad y autorización para el activo	SI / No / No Aplica No requiere / Si requiere y no está definido / Si requiere y está definido.	Solamente es diligenciado cuando en el campo "**Tipo de Activo"** se selecciona "Datos / Información" y cuando en el campo "El activo almacena o solicita Datos personales" se selecciona "Si", el campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado, permitiendo indicar el estado del aviso de privacidad para el activo de información.

Fuente: Elaboración propia.

5.4.2 Campos requeridos para protección de datos (Tabla 11) (Ilustración 6).

Ilustración 6.información protección de datos personales.

***Fuente**: Registro de Activos de Información.*

Tabla 11. Información para valoración de aspectos de protección de datos.

PROTECCIÓN DE DATOS PERSONALES		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
EL ACTIVO ALMACENA O SOLICITA DATOS PERSONALES	En este campo se indica si el activo de información almacena, solicita o recolecta datos de tipo personal. Ej. Datos de contacto, datos laborales, datos patrimoniales, datos académicos, entre otros.	Líder de proceso / Funcionario designado

PROTECCIÓN DE DATOS PERSONALES		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
LOS DATOS ALMACENADOS O REQUERIDOS SON PÚBLICOS	En este campo se indica si el activo de información almacena o requiere datos personales que, la Entidad o las leyes ha determinado expresamente como públicos, Ej., correos laborales, nombre, cargos o roles, datos de contacto definidos como públicos, sentencias judiciales, documentos públicos, datos de gacetas o boletines, entre otros.	
LOS DATOS ALMACENADOS O REQUERIDOS SON PRIVADOS	En este campo se indica si el activo de información almacena o requiere datos personales de tipo privado. Es decir, datos personales que por su naturaleza son datos que solo le interesan al titular y no deberían ser conocidos por terceros. Ej. Correo electrónico personal, teléfono, dirección de vivienda, datos laborales, nivel de escolaridad, sobre infracciones administrativas o penales, los datos administrados por algunas entidades como tributarias, financieras o de la seguridad social, fotografías, videos, y cualquier otro dato que referencien el estilo de vida de una persona.	
LOS DATOS ALMACENADOS O REQUERIDOS SON SEMIPRIVADOS	En este campo se indica si el activo de información almacena o requiere datos personales de tipo semiprivados. Es decir, datos personales que por su naturaleza son datos que le interesan tanto al dueño de los datos como a terceros. Ej. Datos financiero y crediticio de actividad comercial o de servicios, datos de contacto personal, entre otros.	
LOS DATOS ALMACENADOS O REQUERIDOS SON SENSIBLES	En este campo se indica si el activo de información almacena o requiere datos personales de tipo sensible. Es decir, tipos de datos que, de acuerdo con la Ley 1581 de protección de datos colombiana, se han clasificado como sensibles, son de especial protección o pueden someter a discriminación. Ej. Origen étnico o racial, datos de salud, preferencia sexual, filiación política, religión, ideología, afiliación a sindicatos, organizaciones sociales, datos biométricos, entre otros.	
AVISO DE PRIVACIDAD Y AUTORIZACIÓN PARA EL ACTIVO	En este campo se indica si el activo de información “No requiere”, “Si requiere y no está definido” o “Si requiere y está definido” el aviso de privacidad y autorización que se debe implementar cuando se solicite información personal a los titulares. Ej. Formularios de actualización de datos, listas de asistencia, formatos de inscripción, contratos, formatos de quejas y reclamos, formularios web, entre otros.	

Fuente: Elaboración propia.

5.5 ALINEAR CON LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

5.5.1 Criterios y condiciones de valoración (Tabla 12).

Tabla 12. Información para valoración de aspectos de protección de datos.

DESCRIPCIÓN	VALOR	CONDICIÓN
IDIOMA	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
MEDIOS DE CONSERVACIÓN Y/O SOPORTE	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
FORMATO	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
INFORMACIÓN PUBLICADA O DISPONIBLE	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
LISTADO DE RESPONSABLES DE LA PRODUCCIÓN DE LA INFORMACIÓN	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
RESPONSABLE DE LA PRODUCCIÓN DE LA INFORMACIÓN (MANUAL)	Digitado.	Solamente es diligenciado cuando en el campo "**Listado de responsables de la producción de la información"** se selecciona "Definido manualmente". El Campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado.
LISTADO DE LOS RESPONSABLES DE LA INFORMACIÓN:	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN (MANUAL)	Digitado.	Solamente es diligenciado cuando en el campo "**Listado de los responsables de la información:"** se selecciona "Definido manualmente". El Campo cambia de color gris a blanco con el fin de indicar que se ha habilitado y debe ser diligenciado.
CONDICIÓN LEGÍTIMA DE LA EXCEPCIÓN	Aquellos configurados en la lista despegable del registro de activos de información.	N/A

DESCRIPCIÓN	VALOR	CONDICIÓN
FUNDAMENTO CONSTITUCIONAL O LEGAL		Calculado automáticamente de acuerdo con lo diligenciado en el campo "**Condición legítima de la excepción:".** El campo trae la información configurada según el tipo de excepción seleccionada.
DESCRIPCIÓN DE CONDICIÓN LEGÍTIMA DE LA EXCEPCIÓN		Calculado automáticamente de acuerdo con lo diligenciado en el campo "**Condición legítima de la excepción:".** El campo trae la información configurada según el tipo de excepción seleccionada.
CALIFICACIÓN DEL ACTIVO DE ACUERDO CON TRANSPARENCIA LEY 1712		Calculado automáticamente de acuerdo con lo diligenciado en el campo "**Condición legítima de la excepción:".** El campo trae la información configurada según el tipo de excepción seleccionada.
PLAZO DE CLASIFICACIÓN O RESERVA		Calculado automáticamente de acuerdo con lo diligenciado en el campo "**Condición legítima de la excepción:".** El campo trae la información configurada según el tipo de excepción seleccionada.
CLASIFICACIÓN O RESERVA TOTAL O PARCIAL DE LA INFORMACIÓN	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
FECHA DE CALIFICACIÓN	Digitado.	N/A
FRECUENCIA DE ACTUALIZACIÓN	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
CATEGORÍA LUGARES DE CONSULTA	Aquellos configurados en la lista despegable del registro de activos de información.	N/A
DETALLE LUGAR DE CONSULTA		Debe ser coherente con la categoría seleccionada en el campo "**categoría lugares de consulta".**

Fuente: Elaboración propia.

5.5.2 Campos requeridos transparencia y acceso a la información (Tabla 13).

Ilustración 7.Información aspectos de transparencia y acceso a la información.

***Fuente**: Registro de Activos de Información.*

Tabla 13. Información para valoración y alineación con transparencia de información.

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
IDIOMA	Establece el Idioma, lengua o dialecto en que se encuentra la información.	Líder de proceso / Funcionario designado
MEDIO DE CONSERVACIÓN Y/O SOPORTE	Indicar si el activo se encuentra de forma: **Análogo:** si el documento de archivo - registro o activo de información se encuentra elaborado en soporte papel y cinta (video, casete, película, microfilm, entre otros). **Digital:** si el documento de archivo - registro o activo de información ha sido digitalizado o ha sufrido un proceso de conversión de una señal o soporte analógico a una representación digital (Archivo General de la Nación. Acuerdo 027 de 2006). **Electrónico:** si el documento de archivo - registro o activo de información es recibido, almacenado y comunicado se encuentra en medios electrónicos, y permanece en estos medios durante su ciclo vital (Archivo General de la Nación. Acuerdo 027 de 2006). **Hibrido Análogo Digital:** si el documento se encuentra en estos dos tipos de formatos. **Híbrido Análogo Electrónico:** si el documento se encuentra en estos dos tipos de formatos.	Líder de proceso / Funcionario designado
FORMATO	Se debe identificar la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: hoja de cálculo, imagen, video, documento de texto, etc. **Nota:** Si el documento es análogo se debe diligenciar no aplica (N.A.).	Líder de proceso / Funcionario designado

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
INFORMACIÓN PUBLICADA O DISPONIBLE	El Líder de proceso o encargado de calificar los activos de información seleccionará la opción con la cual la información puede encontrarse de manera ya sea pública o disponible para ser consultadas por terceros ya sean propios de la Entidad o ajenos a la misma.	Líder de proceso / Funcionario designado
FECHA DE GENERACIÓN DE LA INFORMACIÓN	Indique la fecha de creación del activo de información o base de datos dentro de la dependencia, en formato DD/MM/AAAA, si la fecha no es concreta o no se puede identificar fácilmente y este activo es parte constante en su gestión, defina la fecha desde el 1 de enero de la vigencia o en el caso que el activo de información sea generado, creado o expedido por una norma, establezca la fecha de generación a partir de la fecha de expedición de la norma.	Líder de proceso / Funcionario designado
LISTADO DE RESPONSABLES DE LA PRODUCCIÓN DE LA INFORMACIÓN	Es el nombre de la dependencia propietaria y por ende Propietario de la producción del documento de archivo -registro o activo de información, en virtud del cumplimiento de sus funciones, procesos y procedimientos. Además, está constituida por los competentes del trámite, administración, consulta y conservación durante su etapa de gestión. En caso de no encontrar la información disponible debe seleccionar la opción “Definido manualmente” para activar el campo “RESPONSABLE DE LA PRODUCCIÓN DE LA INFORMACIÓN (MANUAL)”.	Líder de proceso / Funcionario designado
RESPONSABLE DE LA PRODUCCIÓN DE LA INFORMACIÓN (MANUAL)	En el caso de no encontrarse en la lista del ítem anterior, se debe digitar de manera manual el responsable de producir la información.	Líder de proceso / Funcionario designado
LISTADO DE LOS RESPONSABLES DE LA INFORMACIÓN	Seleccione la Jefatura o dirección o entidad externa que crea o genera la información. En caso de no encontrar la información disponible debe seleccionar la opción “Definido manualmente” para activar el campo “NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN (MANUAL)	Líder de proceso / Funcionario designado
NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN (MANUAL)	Si de acuerdo con la opción anterior el Propietario no se encuentra en el listado, proceder a escribirlo de manera manual.	Líder de proceso / Funcionario designado
CONDICIÓN LEGÍTIMA DE LA EXCEPCIÓN	Se refiere a las normas de carácter reglamentario, jurisprudencia o doctrina.	Líder de proceso / Funcionario designado
FUNDAMENTO CONSTITUCIONAL O LEGAL	Corresponde al fundamento constitucional o legal que justifican la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara.	Líder de proceso / Funcionario designado

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
FUNDAMENTO JURÍDICO DE LA EXCEPCIÓN	Corresponde a la norma que sirve como fundamento jurídico para la clasificación o reserva de la información. Este campo se calcula de manera automática.	Líder de proceso / Funcionario designado
DESCRIPCIÓN DE CONDICIÓN LEGITIMA DE LA EXCEPCIÓN	Implica la mención de una o varias de las excepciones taxativas que se establecen en los artículos 18 y 19 de la Ley 1712. Es decir, las contenidas en los literales de los artículos mencionados.	Líder de proceso / Funcionario designado
CALIFICACIÓN DEL ACTIVO DE ACUERDO CON TRANSPARENCIA LEY 1712	**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 esta ley. **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 19 de esta ley.	Líder de proceso / Funcionario designado
PLAZO DE CLASIFICACIÓN O RESERVA	El tiempo que dura la clasificación. En el caso de la información clasificada, el término es ilimitado, al tenor de lo establecido en el parágrafo único del artículo 18 de la Ley 1712. Para la información reservada, el tiempo máximo es de 15 años, de acuerdo con el artículo 22 del mismo cuerpo normativo, pero siempre bajo el entendido de que el lapso puede ser menor, según las circunstancias de cada caso.	Líder de proceso / Funcionario designado
CLASIFICACIÓN O RESERVA TOTAL O PARCIAL DE LA INFORMACIÓN	Debe señalarse si la excepción al acceso aplica para toda la información o solamente para ciertos puntos específicos. En este último caso, debe señalarse expresamente cuáles.	Líder de proceso / Funcionario designado
FECHA DE CALIFICACIÓN	La fecha en que se califica la información como clasificada o reservada.	Líder de proceso / Funcionario designado

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
FRECUENCIA DE ACTUALIZACIÓN	Identifica la periodicidad o el segmento de tiempo en el que se debe actualizar la información, de acuerdo con su naturaleza y a la normatividad aplicable.	Líder de proceso / Funcionario designado
CATEGORÍA LUGARES DE CONSULTA	Incluir el enlace de consulta del documento de archivo (registro) en el caso en que se encuentre en línea, es decir, a través de la página web u otro medio habilitado para tal fin. De lo contrario escriba “No Aplica (N.A)”.	Líder de proceso / Funcionario designado
DETALLE LUGAR DE CONSULTA	Indicar si el documento de archivo (registro) se encuentra disponible (los usuarios pueden acceder a él en el lugar donde se ubica el documento original), publicado (los usuarios pueden acceder en línea al documento, es decir, a través de la página web u otro medio habilitado para tal fin), o disponible y publicado (puede presentarse que el original del documento de archivo (registro) se encuentre disponible, pero que exista publicada una copia del mismo).	Líder de proceso / Funcionario designado

Fuente: Elaboración propia.

5.5.3 Campos requeridos Datos abiertos (Tabla 14).

Ilustración 8.Información Datos abiertos.

Fuente: Registro de Activos de Información.

Tabla 14. Información para valoración y alineación con datos abiertos.

DATOS ABIERTOS		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**

El activo se cataloga como dato abierto	Seleccionar **SÍ** o **NO**, si la información documentada conservada contiene datos abiertos, los cuales son: todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. La Ley establece la obligatoriedad de las entidades públicas de **"divulgar datos abiertos"**, teniendo en cuenta las excepciones de acceso a la información, asociadas a información clasificada y reservada establecidas en su título tercero, Artículos 18 y 19 de la Ley 1712 de 2014.	Líder de proceso / Funcionario designado

Fuente: Elaboración propia.

5.5.4 Campos requeridos Infraestructura crítica (Tabla 15).

Ilustración 9.Información Infraestructura Crítica

Fuente: Registro de Activos de Información.

Tabla 15. Información para identificación de infraestructura crítica.

INFRAESTRUCTURA CRITICAS CIBERNETICAS - ICC		
CAMPO	**DEFINICIÓN**	**RESPONSABLE DE DILIGENCIAMIENTO**
IMPACTO SOCIAL **El daño, pérdida o deterioro** afectaría (0,5%) de la población nacional (250,000 personas)	Valorado en función de la afectación de la población (incluyendo la pérdida de vidas humanas, el sufrimiento físico y la alteración de la vida cotidiana). Valorado en función de la población total colombiana. Fuente: DANE. El daño, pérdida o deterioro del activo puede afectar a 250.000 o más personas.	Líder de proceso / Colaborador designado / CISO
IMPACTO ECONOMICO **Se podrían generar pérdidas, gastos o costos iguales o superiores** al PIB de un día o 0,123% del PIB Anual (464.619.736)	Valorado en función de la magnitud de las pérdidas económicas en relación con el producto interno Bruto de Colombia (PIB) Fuente: Banco Mundial. El daño, pérdida o deterioro del activo puede generar pérdidas, gastos o costos iguales o superiores a 464,619,736	Líder de proceso / Colaborador designado / CISO
IMPACTO AMBIENTAL Se requieren 3 años o más para la recuperación	Valorado en función de los años que tarda el medio ambiente en recuperarse. El daño, pérdida o deterioro puede generar un impacto ambiental que requiera 3 años o más para su recuperación.	Líder de proceso / Colaborador designado / CISO

Fuente: Elaboración propia.

5.6 PUBLICACIÓN ACTIVOS DE INFORMACIÓN

- La OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital, realiza la consolidación de los activos de información de la entidad y los envía a Secretaría General a través del Grupo de Trabajo de Gestión Documental y Archivo.
- Secretaria General a través del Grupo de Trabajo de Gestión Documental y Archivo, presenta al Comité Institucional de Gestión y Desempeño los activos de información para aprobación y publicación en la página de web.
- Oficina Asesora de Planeación, envía a Secretaría General a través del Grupo de Trabajo de Gestión Documental y Archivo, el acta del Comité Institucional de Gestión y Desempeño donde se presentaron los Activos y se aprobó su publicación en la página web.
- Secretaria General a través del Grupo de Trabajo de Gestión Documental y Archivo, Secretaría General o quien designe, verifica la ubicación en la que se debe ubicar la información en la página web de la entidad, así mismo se verifica que la publicación cumpla con la resolución 1519 de 2020.
- Secretaria General a través del Grupo de Trabajo de Gestión Documental y Archivo, enviara a la OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital, el Acta de Comité Institucional de Gestión y Desempeño donde se presentaron los Activos y se aprobó su publicación en la página web y el certificado de publicación en la página web.
- OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital, realiza la solicitud a la Oficina Asesora de Planeación, para la actualización de los activos de información de la entidad en el módulo SIGI, se debe citar el No. de Acta de Comité Institucional de Gestión y Desempeño donde se presentaron los Activos y se aprobó su publicación en la página web y adjuntar el certificado de publicación en la página web.

- La Oficina Asesora de Planeación notificara la actualización de activos de información en el módulo SIGI a OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital.

Nota: los activos de información de la entidad se actualizan en el módulo SIGI, una vez se publiquen en la página web.

6 DOCUMENTOS RELACIONADOS

GD01-F17 Programa de gestión documental.
SC05-F03 Registro de activos de información.
SC05-POL01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI
SC01-POL01 Política de Riesgos
SC01-P03 Metodología para la administración del riesgo

6.1 DOCUMENTOS EXTERNOS

No aplica.

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se realizó e incluyó tabla de roles y responsabilidades, ítem número 6 Publicación Activos de Información y se modificó las tablas de clasificación de integridad, disponibilidad y se elimina el nivel Sin clasificar.

_____
Fin documento