

“ITFIP”

INSTITUCIÓN DE EDUCACIÓN SUPERIOR



**METODOLOGÍA PARA LA IDENTIFICACIÓN,
CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS
DE INFORMACIÓN.**





**METODOLOGÍA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN Y
VALORACIÓN DE ACTIVOS DE INFORMACIÓN**

Versión:

Diseño y elaboración:

LUIS ALBERTO VASQUEZ GUERRA
Asesor de Planeación

Aprobado
MARIO FERNANDO DIAZ PAVA
Rector

Espinal, Agosto de 2022

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS

INTRODUCCION

Este documento se elaboró como guía para identificar, registrar, clasificar y valorar los activos de información, que el Instituto Tolimense de Formación Técnica Profesional – ITFIP, genera, obtiene, adquiere, transforma o controla en su calidad.

La Institución de Educación Superior ITFIP, se orienta con la guía No. 5, del Ministerio de Educación, donde estipula los lineamientos básicos que deben ser utilizados por los responsables de la Seguridad de la Información para poner en marcha la gestión y clasificación de activos de información, cuyo objetivo es dar cumplimiento a 4 puntos principales:

- Inventario de activos.
- Propiedad de los activos.
- Clasificación de la Información.
- Etiquetado y Manipulado de la información.

La información debe ser clasificada y valorada por el criterio de la entidad, donde sea evaluada por unos ítems: Alta, Media, Baja, No clasificada.

La actividad del levantamiento de la información, será desarrollada con cada líder de los procesos misionales de la institución, quienes identificarán y evaluarán su información de acuerdo a los criterios de la entidad.

Activo de información: Es "Toda información que tenga valor para la organización". No obstante, este concepto es bastante amplio debe ser limitado por una serie de consideraciones:

- El impacto que para la organización supone la pérdida de confidencialidad, integridad y/o disponibilidad de cada activo.
- El tipo de información que maneja.
- Sus productores y consumidores.

La norma ISO 27001 establece 2 tipos de activos a saber:

Activos de información primarios: Dentro de estos activos se encuentra la información que se genera, procesa y se almacena en bases de datos, archivos de datos, contratos, acuerdos, documentación de sistemas de información, procedimientos operativos y las caracterizaciones de los procesos que ejecuta el MEN.

Activos de información secundarios: Dentro de estos activos se encuentra el recurso humano (servidores de planta, contratistas y proveedores), tecnología (Software, Hardware y Redes de Comunicaciones) y la infraestructura (edificios y puestos físicos de trabajo, PBX, telefonía, servicios de energía, calefacción, iluminación).

CONTENIDO

1. OBJETIVO
2. DESTINATARIOS
3. GLOSARIO
4. GENERALIDADES
 - 4.1 REGISTRO DE ACTIVOS DE INFORMACIÓN DE TIPO DOCUMENTAL, SOFTWARE, PERSONA, SERVICIOS, FISICO Y RED DE DATOS
 - 4.2 RESPONSABILIDADES
 - 4.3 PERIODICIDAD PARA LA ACTUALIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN.
5. DESCRIPCIÓN DE ACTIVIDADES
 - 5.1 VERIFICAR CAMBIOS EN EL REGISTRO DE ACTIVOS DE INFORMACION
 - 5.2 REALIZAR MESAS DE TRABAJO
 - 5.3 APROBAR Y PUBLICAR EL VERSIONAMIENTO
 - 5.4 DESCRIPCIÓN DEL FORMATO DE REGISTRO DE ACTIVOS DE INFORMACIÓN.
 - 5.5. FORMATO

1. OBJETIVO

Establecer los lineamientos básicos y actividades generales para identificar, clasificar y valorar los activos de información de la Institución de Educación Superior-ITFIP, a través de los lineamientos establecidos en este documento con guía del Ministerio, para la seguridad y privacidad de la información, los cuáles serán utilizados por los servidores públicos, contratistas y terceros de la Entidad.

2. DESTINATARIOS

Servidores públicos, contratistas y terceros de la Institución de Educación Superior ITFIP.

3. GLOSARIO

ACTIVO: Cualquier cosa que tiene valor para una organización¹.

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, transmitida 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.

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta que tenga valor para la entidad, por ejemplo: archivos, bases de datos, expedientes, entre otros.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CUSTODIO: Identifica la 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 de privilegios de acceso, modificación y borrado.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DISPOSITIVO: Cualquier componente de hardware que sea necesario para efectuar o complementar operaciones sobre algún activo de información.

¹ INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C.: ICONTEC, 2013. p. 2 (NTC-ISO/IEC 27001)

DOCUMENTO FÍSICO: Cualquier conjunto de información que conforme una unidad significativa y que se encuentre en medio impreso.

DOCUMENTO DIGITAL: Cualquier conjunto de información que conforme una unidad significativa y que se encuentre en digital (videos, multimedia, presentaciones, entre otros).

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

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, obtengan, adquieran, transformen o controlen”*².

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 2014.³

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 2014.⁴

PROPIETARIO DEL ACTIVO DE INFORMACIÓN: Grupo de trabajo, Oficina, Dirección o Delegatura, que tiene como responsabilidad velar por la protección del activo de información. Tiene responsabilidad de controlar la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

RECURSO HUMANO: Hace referencia a cualquier colaborador tenga un vínculo con la Organización. Los privilegios de acceso se encuentran sujetos al rol y a las responsabilidades para el cumplimiento de sus actividades.

SISTEMA DE ALMACENAMIENTO DE INFORMACIÓN: Hace referencia a cualquier sistema o tecnología para el almacenamiento de datos que sea necesaria para efectuar o complementar alguna operación sobre los activos de información.

SISTEMA DE INFORMACIÓN: Todo sistema que realice operaciones, transacciones y que requiera la interacción de uno o más activos de información para efectuar sus tareas.

SOFTWARE: Cualquier software de cliente final como: suites de ofimática, correo, edición de documentos, etc.

² COLOMBIA CONGRESO DE COLOMBIA, Ley 1712 de 2014. Artículo 6. Definiciones Literal a.

³ Op.Cit. 2

⁴ Op. Cit. 2

TABLA DE RETENCIÓN DOCUMENTAL - TRD: 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.⁵

GENERALIDADES

Este documento orienta la identificación, clasificación y registro de los activos de información que son gestionados en la Institución de Educación Superior ITFIP. 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.
- Norma ISO 27000, que son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC)⁸.

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 que a cada activo de información debe dársele.

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 lineamientos de la Guía 5 - Seguridad y Privacidad 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.

⁵ COLOMBIA. CONGRESO DE COLOMBIA. Ley 594 del 2000 " por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Artículo 3 Definiciones.

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

De otra parte, se debe tener en cuenta que el registro de activos de información está relacionado con el Decreto 103 de 2015, capítulo 1, artículo 37, el cual lo define como “*el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal*”⁶.

El Registro de Activos de Información debe contener, como mínimo, los siguientes componentes:

1. Todas las categorías de información del sujeto obligado.
2. Todo registro publicado.
3. Todo registro disponible para ser solicitado por el público.

De forma similar, en el Decreto 103 de 2015, capítulo 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.⁷ Por consiguiente, las categorías a las que hace referencia el Decreto 103 de 2015, corresponde por definición a las series documentales.

La seguridad de la información, se basa en la preservación de su confidencialidad, integridad y disponibilidad, para cualquier tipo de empresa, u organización.

⁶ COLOMBIA CONGRESO DE COLOMBIA, Decreto Nacional 103 de 2015. Artículo 37.

⁷ COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 027 de 2006. p 43

⁹ NORMAS ISO SOBRE GESTION DE SEGURIDAD DE LA INFORMACIÓN.

REGISTRO DE ACTIVOS DE INFORMACIÓN DE TIPO DOCUMENTAL, SOFTWARE, PERSONA, SERVICIOS, FISICO Y RED DE DATOS

La Organización Internacional de Estandarización (ISO), a través de las normas ISO 27001/ ISO 27002, nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger de la información.

Los Objetivos del SGSI son preservar la Confidencialidad, Integridad, y Disponibilidad de la información.

Con relación a la información que se recibe, transforma y produce en la Entidad, se reconocen los siguientes tipos de activos de información:

- **Documental:** se realiza a través del reconocimiento de la producción documental de la Entidad. En este sentido, dadas las características de esta entidad, la totalidad de la producción documental hace parte de los activos de información, toda vez que se desarrollan a través de procesos, procedimientos y funciones establecidas por la normatividad vigente.
- **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en un computador.
- **Físico: (Hardware)** Medio utilizado para realizar la captura, procesamiento, almacenamiento, difusión y divulgación de la información, es deseable que se utilicen las tecnologías de punta para lograr una gestión oportuna y eficiente en almacenaje y procesamiento de datos y en la ampliación de la cobertura de información a difundir. En este sentido, se refiere a todos los elementos físicos que permiten el correcto funcionamiento de un medio informático. Incluye redes de datos, discos duros o extraíbles, impresoras, servidores, computadores, dispositivos móviles, entre otros. Para facilidad de manejo de este tipo de activos, los mismos pueden ser agrupados según sus características (por ejemplo: equipos de cómputo personales; dispositivos móviles o celulares).
- **Persona:** Cargo de aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- **Servicios:** Hace referencia a aquellas actividades realizadas por personas, dependencias o entidades ajenas al proceso, 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.
- **Red de datos:** Elementos de la infraestructura de telecomunicaciones.

En el siguiente cuadro, se presentan las propiedades de seguridad aplicables, según el tipo de activo de información.

Categoría del activo	Propiedades aplicables		
	Confidencialidad	Integridad	Disponibilidad
Físico			X
Documental	X	X	X
Personal			X
Servicio			X
Software			X
Red			X
Otros	X	X	X