



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL - MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información
ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18



MAAGTICSI
Manual Administrativo de Aplicación General en Materia de Tecnologías
de la Información y Comunicaciones y de Seguridad de la Información

**ADMINISTRACIÓN DE LA SEGURIDAD DE LA
INFORMACIÓN (ASI)**

ASI FL - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
CLASIFICACIÓN DE LA INFORMACIÓN

POL-SGSI-PE-23



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

CONTENIDO

I. DESCRIPCIÓN GENERAL.....	3
II. PROPÓSITO	3
III. ALCANCE.....	4
IV. OBJETIVOS.....	4
V. POLÍTICA.....	4
i. Gestión de Inventario y Activos.....	4
ii. Clasificación de la Información	5
iii. Lineamientos Generales del Manejo y Clasificación de la Información	6
iv. Etiquetado de activos de información	6
v. Reclasificación y desclasificación de los activos de información	7
VI. TÉRMINOS Y DEFINICIONES	7
VII. BITÁCORA DE CAMBIOS.....	8



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

I. DESCRIPCIÓN GENERAL

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, establece en su Artículo 3 que *"Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y esta Ley, es pública, accesible a cualquier persona..."*, por lo tanto la información tratada en el Instituto está contemplada dentro del alcance definido por esta normativa y su propiedad corresponde al Estado Mexicano, en consecuencia este precepto también incluye a los activos de Información a cargo de la UTIC, los cuales deben ser protegidos de acuerdo a su valor y criticidad.

Cabe señalar que toda la información que las unidades administrativas del Instituto generan, obtienen, adquieren, transforman o conserven por cualquier título, es pública y la reserva de la misma se justifica estrictamente por excepción, por lo que en caso de clasificarse como reservada o confidencial requerirá fundarse y estará sujeta a un término para su desclasificación.

La presente política define las categorías de clasificación de la Información y las reglas de manejo en la UTIC tales como; copiado, almacenamiento, autorización de acceso y derecho a conocer la información facilitando así documentar la importancia que estos tienen para el Instituto.

II. PROPÓSITO

El propósito de la presente política es aplicar las medidas de seguridad ajustadas a cada activo de información, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, considerando para ello criterios de confidencialidad, integridad y disponibilidad, de esta manera se pueden tomar decisiones, por ejemplo: qué información debemos cifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuanto hacer respaldo, etc.

Además, al clasificar los activos de información se puede determinar la vigencia de su contenido, si el soporte tecnológico en el que se resguarda caduca antes que el contenido tendremos que regenerarlo en otro soporte. El ciclo de vida de la información determinará el momento en el cual dejará de ser útil, y por tanto cuándo tenemos que eliminarla convenientemente.

Esta política no pretende sustituir o reemplazar lo dispuesto en el marco legal aplicable en materia de transparencia, acceso a la información y protección de datos personales, en todo caso busca establecer los criterios relacionados con la clasificación de la información para etiquetar y categorizar la información de la UTIC en categorías para determinar el nivel de seguridad y tratamiento que se le debe dar a la misma de acuerdo al valor que tiene para el Instituto.



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

III. ALCANCE

Esta política es aplicable a toda la información propiedad y/o en custodia de la UTIC, en cualquier formato en que se encuentre es decir, a todos los tipos de información ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas y demás activos de información.

IV. OBJETIVOS

1. Establecer las bases de un sistema de clasificación de la información, tendiente a asegurar la confidencialidad, integridad y disponibilidad de la misma.
2. Clasificar la información con la finalidad de asegurar la prioridad y el grado de protección que ésta requiere, tomando en cuenta su valor, requerimientos legales y contractuales e importancia para el Instituto.
3. Establecer los principios, bases, lineamientos, procedimientos y normas necesarios para proteger la información y documentación sensible del Instituto, del conocimiento y divulgación a personas o instituciones no autorizadas.

V. POLÍTICA

Todo el personal de la UTIC que desarrolle, custodie y difunda información, deberá cumplir la presente política, observando sus requisitos y cumpliendo en el ámbito de competencia la cabalidad de las disposiciones vertidas en el presente documento.

i. Gestión de Inventario y Activos

- a) Todos los activos deberán estar claramente identificados y definiendo la importancia de estos para la UTIC, se deberá elaborar y mantener un inventario de los activos más importantes, que deberá incluir al menos:
 - Tipo de activo
 - Formato
 - Ubicación
 - Responsable del activo
- b) Se debe tener en cuenta que la clasificación de la información debe ser acordada y documentada para cada uno de los activos inventariados, tomando en consideración los siguientes criterios:
 - Importancia del activo
 - Valor de la información
 - Clasificación de seguridad



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

- Niveles de protección de acuerdo a la importancia
- c) En el inventario de activos, se debe especificar un custodio de la información, quien es el responsable del seguimiento de las tareas operativas y de seguridad en las que está involucrado el activo.
- d) Será responsabilidad del encargado de la seguridad de la información, en conjunto con los responsables de los activos, las actualizaciones de los inventarios de activos de información.
- e) Para el caso de los activos de información no inventariados o de aquellos documentos de carácter temporal o no oficial (borradores, proyectos, etc.) y que no posean un responsable específico, será responsabilidad de quien elabora la información la aplicación de los niveles de seguridad requeridos en el manejo y transmisión de la información generada.
- f) El propietario del activo de información o el custodio de la información deberá firmar una carta de responsabilidad que especifique los activos que se le asignaron.
- g) Los activos deben asignarse de acuerdo con el área, el puesto y las necesidades del puesto, los permisos y los derechos asignados a las funciones del servidor público.

ii. Clasificación de la Información

- a) La clasificación de la información se entiende como el acto de colocar los datos en categorías para determinar el nivel de seguridad y tratamiento que se le debe dar a la misma de acuerdo al valor que tiene para el Instituto.
- b) El INAI establece una clasificación de la información de la siguiente manera: Pública, Reservada y Confidencial:
 - 1. Información Pública: Información de uso general que por su contenido o contexto no requiere de protección especial y su distribución pública ha sido permitida a través de canales autorizados por el Instituto.
 - 2. Información Reservada: Se considera información cuya divulgación debe ser restringida únicamente al personal que la requiere conocer, previa autorización del responsable de la misma y, que se encuentra temporalmente sujeta a alguna de las excepciones previstas en la Ley Federal de Transparencia.
 - 3. Información Confidencial. Información que se encuentra protegida, intransferible e indelegable, queda prohibido su acceso, distribución, comercialización, publicación y difusión generales de forma permanente, con excepción de las autoridades competentes que, conforme a la Ley, tengan acceso a ella, y de los particulares titulares de dicha información.
- c) La información debe ser clasificada indicando la necesidad, prioridad y grado de protección para su manejo.



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

d) En la UTIC se reconocen 3 niveles básicos de activos de información:

1. Información en formato múltiple (impresa, escaneada, texto, imagen, audio, video, etc).
2. Equipos, sistemas, aplicativos e infraestructura que soportan o almacenan la información.
3. Las personas responsables del resguardo e integridad de la información.

iii. Lineamientos Generales del Manejo y Clasificación de la Información

- a) El usuario de los equipos e infraestructura a su cargo será el responsable de la información contenida en los mismos y quedará bajo su resguardo en todo momento.
- b) En caso de enviar equipos a mantenimiento o reasignar equipos a una persona, se deberá asegurar que, la información sea borrada de manera segura para que no sea posible su recuperación.
- c) Los equipos portátiles que contengan información, deben considerar mecanismos necesarios para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información almacenada.
- d) Se deberá minimizar el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
- e) Al término de la relación laboral, todo servidor público deberá restituir todos los bienes de propiedad del Instituto incluyendo todos los documentos y otros dispositivos que contengan información de cualquier naturaleza

iv. Etiquetado de activos de información

- a) Todos los Activos de Información deberán estar debidamente etiquetados y clasificados y asignados a un servidor público.
- b) Si un Activo de Información en formato impreso no se encuentra etiquetado deberá ser considerado como no clasificado.
- c) El sistema de clasificación de la información se basa en las características particulares de cada información, contempla la cultura y el funcionamiento interno y buscando dar cumplimiento a los requerimientos estipulados en los requisitos de los estándares 27001:2013, ISO 27002, e ISO 27005.
- d) Se etiquetarán todos los Activos de Información bajo los criterios de confidencialidad, Integridad y disponibilidad.



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

v. Reclasificación y desclasificación de los activos de información

- El propietario del activo de información es el único responsable de solicitar o aprobar una reclasificación o desclasificación de activos.
- Cualquier reclasificación o desclasificación de activos debe estar justificada por algún cambio relevante en la UTIC, proceso de negocio, cambio en la infraestructura tecnológica o cambio en las prioridades de la gestión de riesgos.
- Todas las reclasificaciones, desclasificaciones, modificaciones, retiros y adiciones de activos de información deben registrarse en el inventario de activos en función del proceso establecido por la UTIC.

VI. TÉRMINOS Y DEFINICIONES

Término	Descripción
Activos de Información	Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para el Instituto. En otras palabras, la información propiamente tal, en sus múltiples formatos, los equipos/sistemas que soportan esta información y las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Clasificación	Acto por el cual se determina que la información que posee una dependencia o entidad es reservada o confidencial, en términos de la legislación en materia de transparencia y acceso a la información pública gubernamental.
Documentos de archivo electrónico	Registra un acto administrativo, jurídico, fiscal o contable, creado, recibido, manejado y usado en el ejercicio de las facultades y actividades del Instituto, que precisa de un dispositivo electrónico para su registro, almacenamiento, acceso, lectura, impresión, transmisión, respaldo y/o preservación.
Formato electrónico	Codificación de un documento de archivo electrónico que define la manera como está organizada su información.
ISSSTE	Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
UTIC	La Unidad de Tecnologías de Información y Comunicaciones de las TIC en el Instituto
TIC	Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.



ISSSTE

INSTITUTO DE SEGURIDAD
Y SERVICIOS SOCIALES DE LOS
TRABAJADORES DEL ESTADO

**UNIDAD DE ADMINISTRACIÓN DE SISTEMAS DE
INFORMACIÓN Y PROCESOS TECNOLÓGICOS**
**ASI FL – MANUAL DE POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN**

Clasificación de la Información

ÚLTIMA ACTUALIZACIÓN: D.O.F. 23-JUL-18

VII. BITÁCORA DE CAMBIOS

DESCRIPCIÓN DEL CAMBIO	IMPACTO	APROBÓ	FECHA DE APLICACIÓN
V 1. Primera versión del documento.	De observancia para todas las áreas del ISSSTE	GESI	Noviembre 2019