Programa de capacitación en Seguridad de la Información para la Implantación del MAAGTICSI

Módulo 1: Introducción a la seguridad de la información y el MAAGTICSI

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Objetivo

- Facilitar la implantación del MAAGTICSI en las instituciones de la Administración Pública Federal:
  - Sensibilizar sobre la importancia de la seguridad de la información
  - Asegurar la comprensión de procesos y disposiciones de seguridad de la información
  - Establecer bases para la creación de una cultura de seguridad de la información

Agenda

Programa de capacitación en Seguridad de la Información para la implantación del MAAGTICSI	Horario
Día 1	
Registro.	8:20 – 8:50
Apertura del programa de capacitación – Presentación del Presídium.	9:00
Palabras de los representantes de las instituciones participantes en el diseño e impartición del programa de capacitación.	9:10 – 9:50
Despedida del Presídium – Receso.	9:50 – 10:00

Apertura del programa de capacitación

Presentación Presídium

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

Autoridades que nos acompañan

SFP
SECRETARÍA DE LA FUNCIÓN PÚBLICA

SEMAR

Almirante C.G.DEM. Carlos Federico Quinto Guillén
Director del Centro de Estudios Superiores Navales
Vice-Almirante Jorge Burguete Kaller
Jefe de la Unidad de Comunicaciones e Informática

SFP

Mtro. Carlos Viniegra Beltrán
Titular de la Unidad de Gobierno Digital

GOBIERNO FEDERAL

SEGOB

Lic. Jorge Colín Elías
Secretario Técnico del CESI

SEDENA

Gral. de Brigada
Ing. Ind. Francisco Fernando Escalante Sánchez
Director General de Informática

SSP

Ing. David Jiménez Domínguez
Director General del
Centro Especializado en Respuesta Tecnológica, Policía Federal

Participación de las instituciones

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

SFP

Módulo 1
Introducción a la seguridad de la información y el MAAGTICSI

SEGOB

Módulo 2
Sistema de Gestión de Seguridad de la Información

SEDENA

Módulo 3
Identificación de Infraestructuras Críticas

SEMAR

Módulo 4
Análisis de riesgos

SSP

Módulo 5
Desarrollo de los Equipos de respuesta a incidentes de seguridad en cómputo

GOBIERNO FEDERAL

Introducción a la seguridad de la información y el MAAGTICSI

Recomendaciones…

- Asistencia y puntualidad
- Gafete de identificación
- Celulares y Laptops
- Dudas y sugerencias
- Instalaciones y servicios

Agenda

Programa de capacitación en Seguridad de la Información para la implantación del MAAGTICSI	Horario
Día 1	
Modulo 1, primera parte – Antecedentes, objetivos del programa , conceptos y definiciones de seguridad de la información en el MAAGTICSI.	10:00 – 11:15
Receso.	11:15 – 11:30
Modulo 1, segunda parte – Estructura general de un SGSI, elementos y relaciones entre los elementos del mismo.	11:30 – 12:45
Receso.	12:45 – 13:00
Modulo 1, tercera parte– Disposiciones contenidas en los acuerdos que dan lugar al MAAGTICSI. Relación e Integración de los procesos de seguridad de la información en los cuatro niveles de gestión del MAAGTICSI.	13:00 – 14:00
Final de la sesión del día 1.	14:00

Agenda

Programa de capacitación en Seguridad de la Información para la implantación del MAAGTICSI	Horario
Día 2	
Registro.	8:20 – 8:50
Modulo 1, cuarta parte – Alcance y estructura de los procesos ASI/OPEC. Mapeo de Roles.	9:00 – 11:00
Receso.	11:00 – 11:20
Modulo 1, quinta parte – Interrelación entre los procesos ASI y OPEC, relación de éstos con los demás procesos del marco rector del MAAGTICSI.	11:20 – 12:30
Receso.	12:30 – 12:45
Modulo 1, sexta parte – Formatos para los nuevos procesos de seguridad de la información.	12:45 – 13:30
Preguntas y respuestas.	13:30 – 14:00
Fin del módulo y agradecimiento.	14:00

Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, primera parte

- Antecedentes.
- Objetivo del módulo.
- Conceptos de la seguridad de la información.
- Definiciones relacionadas utilizadas en el MAAGTICSI.

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Objetivos

- Proveer de una visión general de los principales retos y conceptos de la seguridad de la información.
- Revisar los acuerdos que han dado lugar a las diversas versiones del manual.
- Revisar los procesos y los roles que requieren establecer las instituciones para implantar adecuadamente el MAAGTICSI en la materia de seguridad de la información.
- Asegurar que los RSII de las instituciones así como el Titular de la UTIC conozcan el alcance del acuerdo y del manual en materia de Seguridad de la Información.

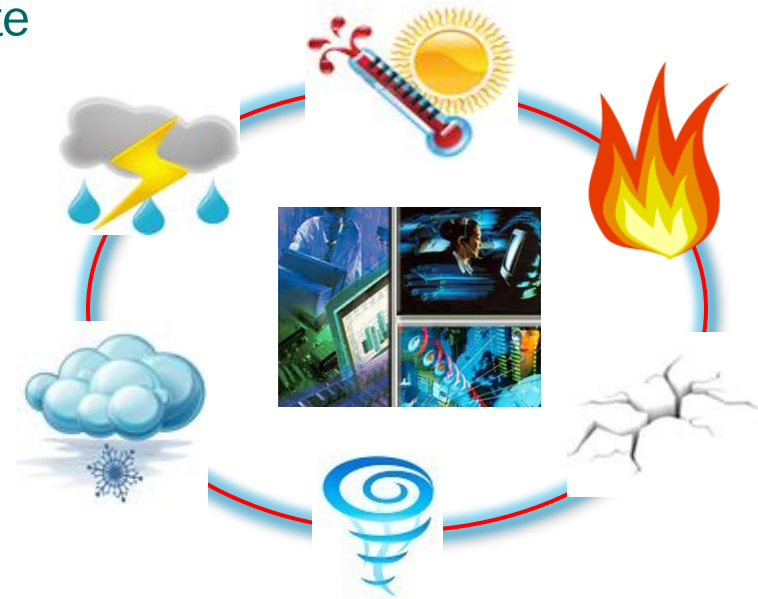
Problemática

En el “Entorno externo” :

- Las TIC evolucionan aceleradamente
- La información se vuelve cada vez mas valiosa:
  - múltiples beneficios de su uso
- Las instituciones públicas y las organizaciones privadas requieren intercambiar información oportuna y ágilmente

Amenazas

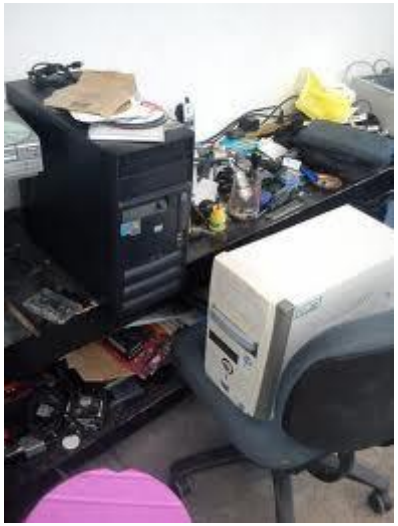
Agentes amenazantes



Problemática

Al interior de las instituciones:

- TIC´s limitadas o tienden a la obsolescencia
- Procesos informales o con escaso orden
- Personal insuficiente o con capacidades deficient



Vulnerabilidades

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Incidentes de seguridad

Antecedentes

Problemática

Cada vez es mas común escuchar o ser víctima de:

- Sabotaje a sitios gubernamentales
- Robo de información “electrónica”
- Fraudes cibernéticos
- Suplantación de identidad
- Otros…

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Toma de decisión ante una situación crítica

Antecedentes

Acciones

Integrar elementos como punto de partida hacia una solución:

- Ley de Seguridad Nacional
- Consejo de Seguridad Nacional
- Grupo Técnico Especializado en Seguridad de la Información (GTECSI):
  - Generador de disposiciones específicas en materia de seguridad de la información
- Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones

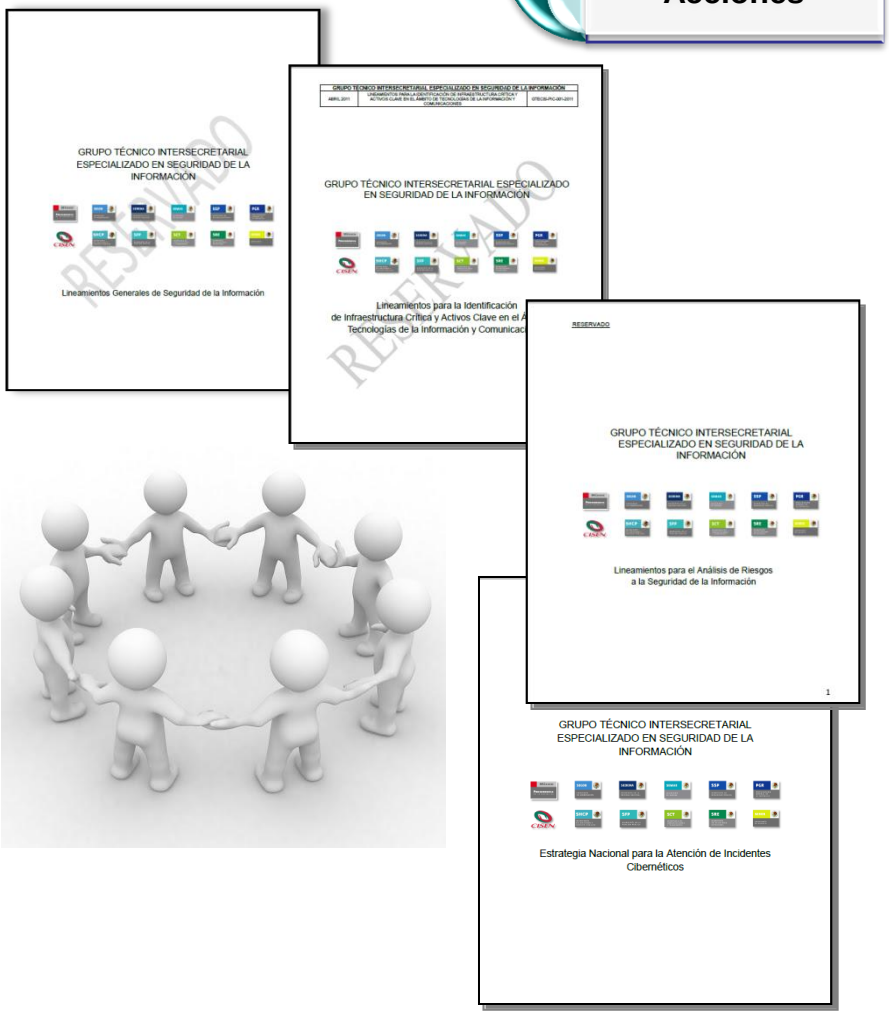
GOBIERNO FEDERAL

Elaboración de un marco de solución e integración armonizada en el MAAGTICSI

Antecedentes

Acciones

- 4 documentos normativos elaborados por el GTECSI, que se integraron al manual, para dar lugar al MAAGTICSI.
- En consecuencia, el alcance del Manual se extiende a dos materias:
  - Las Tecnologías de la Información y Comunicaciones.
  - La Seguridad de la Información, incluyendo aquella considerada de Seguridad Nacional.

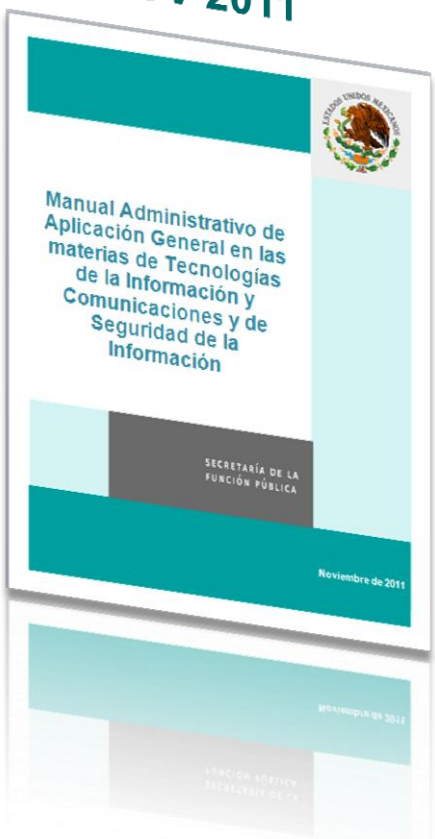


Integración armonizada en el MAAGTICSI

Antecedentes

Acciones

- En el manual se contienen los procesos para garantizar la seguridad de la información, de las infraestructuras críticas y de los activos de información.
- En el Acuerdo por el que se expide el manual se contienen, entre otras, las disposiciones específicas para la seguridad de la información considerada de seguridad nacional.



Seguridad de la Información

Seguridad de la Información

Conceptos

"La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma."

Características de la información

Confidencialidad: La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

Integridad: Mantener la exactitud y corrección de la información y sus métodos de proceso.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Seguridad de la información…

Seguridad de la Información

Conceptos

…así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.”

- ✓ Identificar mediante un nombre de usuario y contraseña.
- ✓ Aceptar o denegar el acceso de un usuario.
- ✓ Registrar la totalidad de actividades de usuarios.
- ✓ Asegurar que el emisor no pueda negar un envío o que el receptor no pueda negar una recepción de mensaje.

Seguridad de la información...

Amenaza: Cualquier posible acto que pueda causar algún tipo de daño a los Activos de información de la Institución.

Vulnerabilidad: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los Activos de TIC, a la Infraestructura crítica, así como a los Activos de información.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los Activos de TIC, las Infraestructuras críticas o los Activos de información de la Institución.

Seguridad de la información...

Seguridad de la Información

Conceptos

Evento: Suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Incidente: La afectación o interrupción a los Activos de TIC, a las Infraestructuras críticas, así como a los Activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Seguridad de la información...

Impacto: El grado de los daños y/o de los cambios sobre un Activo de información, por la materialización de una amenaza.

Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, segunda parte

- Estructura general de un SGSI.
  - Elementos del SGSI.
  - Relaciones entre los elementos del SGSI.
  - Aspectos de implantación.
  - Aspectos de evaluación.

Secretaría de Marina
Centro de Estudios Superiores Navales

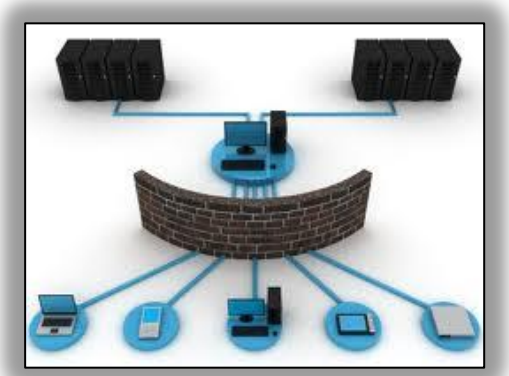
Ciudad de México,
abril - mayo de 2012

Enfoque de proceso, articulación de un SGSI

SGSI

Elementos

"Establecer un SGSI que proteja los Activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad."

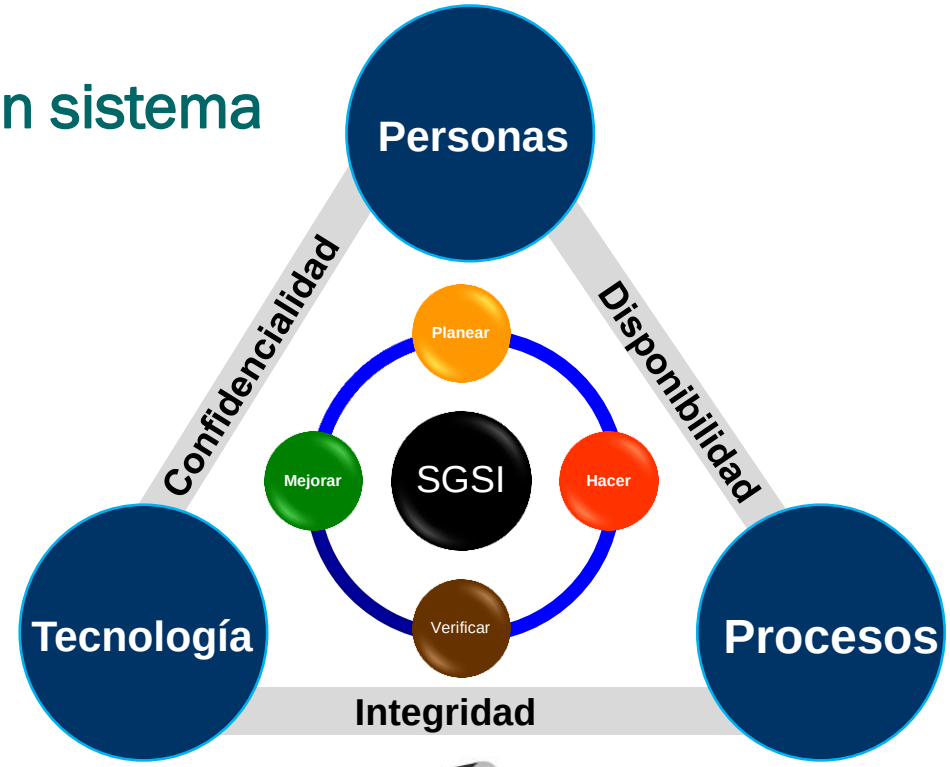


Estructura general del SGSI

SGSI
Elementos

Enfoque de proceso, articulación de un sistema

... articulación de un sistema



Estructura general del SGSI

Elementos del proceso

SGSI

Enfoque de proceso

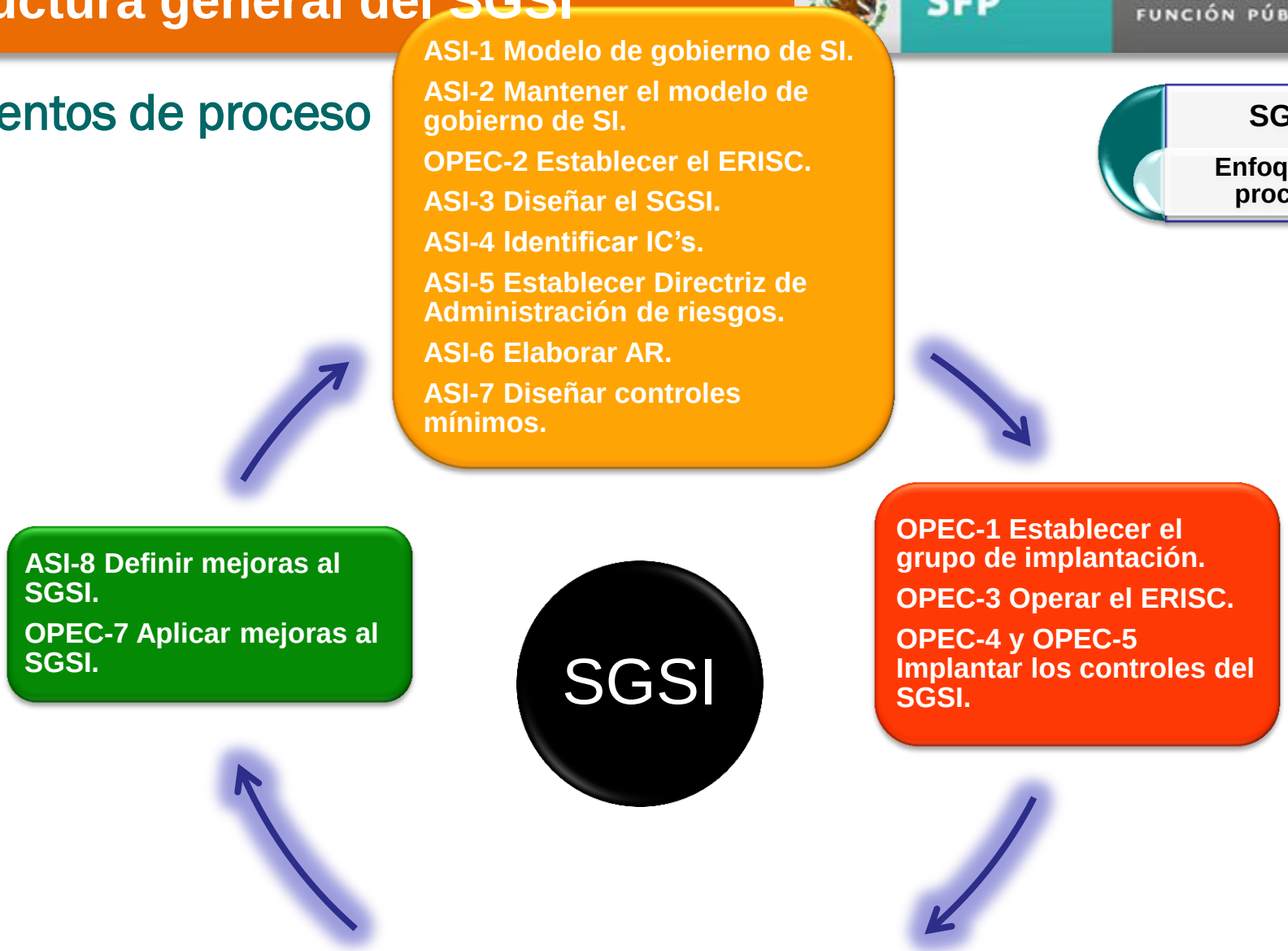
Estructura general del SGSI

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Elementos de proceso

SGSI

Enfoque de proceso



Aspectos relevantes para la implantación

SGSI

Implantación

- ✓ Compromiso de la Dirección con la gestión de la seguridad de la información (gobierno de la SI).
- ✓ Entendimiento de los requerimientos de seguridad en la Institución.
- ✓ Manejo de la adaptación al cambio.
- ✓ Formación de cultura de Seguridad de la Información.
- ✓ Asignación de recursos.
- ✓ Se asignen roles y responsabilidades.
- ✓ Exista documentación plena del SGSI que garanticen su implantación.
- ✓ Establecimiento de indicadores.

Aspectos relevantes de la evaluación

SGSI

Evaluación

- ✓ Ejecutar revisiones objetivas al SGSI.
- ✓ Asegurar la consistencia de los datos que se utilizarán para la evaluación.
- ✓ Registrar la totalidad de los datos de eventos e incidentes.
- ✓ Medir la efectividad de los controles implantados.
- ✓ Analizar los resultados de las evaluaciones y obtener acciones de mejora

Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, tercera parte

- Disposiciones contenidas en los Acuerdos que dan lugar al MAAGTICSI.
- Relación e integración de los procesos de seguridad de la información en los 4 niveles de gestión del MAAGTICSI.

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

Contexto del manual

El MAAGTICSI forma parte de los 9 Manuales Administrativos de Aplicación General con enfoque a procesos, derivados de la tala regulatoria y orientados a la mejora regulatoria.

No.	MAAG´s
1	Adquisiciones
2	Obra Pública
3	Recursos Financieros
4	Recursos Humanos
5	Recursos Materiales
6	Tecnologías de la Información y Comunicaciones y Seguridad de la Información
7	Transparencia
8	Auditoria
9	Control

Disposiciones en los Acuerdos

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Primer acuerdo publicado en el DOF el 13 de julio de 2010

Consta de Cuatro capítulos, nueve artículos y expide el manual:

- CAPITULO I. Objeto, Ámbito de Aplicación y Definiciones.
- CAPITULO II. De los Responsables de su Aplicación.
- CAPITULO III. Procesos.
- CAPITULO IV. Interpretación, Seguimiento y Vigilancia.

Primero al quinto Transitorios: Sobre su entrada en vigor, procesos y actos iniciados, procesos optimizados, recursos y cronogramas de implantación.

(Segunda Sección) DIARIO OFICIAL Martes 13 de julio de 2010

SECRETARIA DE LA FUNCION PUBLICA

ACUERDO por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones: (Continúa en la Segunda Sección)

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de la Función Pública.

SALVADOR VEGA CASILLAS, Secretario de la Función Pública, con fundamento en lo dispuesto por el artículo 37, fracciones VI y XXVI de la Ley Orgánica de la Administración Pública Federal; 1 y 6, fracciones I y XXIV del Reglamento Interior de la Secretaría de la Función Pública, y

CONSIDERANDO

Que el Plan Nacional de Desarrollo 2007-2012, establece como estrategia para lograr el objetivo 10 del Eje Rector "Estado de Derecho y Seguridad", la ampliación de los programas de simplificación administrativa y mejora regulatoria en toda la administración pública, procurando que los cambios tengan un impacto directo en el combate a la discrecionalidad, la arbitrariedad o la corrupción;

Que en ese sentido, el Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012, en su estrategia 2.3 "Simplificar la regulación que rige a las instituciones y su interacción con la sociedad", establece como una línea de acción, mejorar el marco normativo de las instituciones a través del proceso de calidad regulatoria para lograr mayor agilidad, certidumbre y menores costos de operación para la institución y los particulares;

Que asimismo el referido Programa, reconoce como postulado para mejorar la gestión de las instituciones, reformar el marco regulatorio de aplicación obligatoria a toda la Administración Pública Federal, mediante las estrategias tendientes a simplificar la regulación que rige a las instituciones y su interacción con la sociedad, así como a mejorar las políticas, normas y disposiciones de carácter general que emiten las instancias globalizadoras o instituciones coordinadoras de sector;

Que el Ejecutivo Federal, en su mensaje dirigido a la Nación con motivo de la presentación al H. Congreso de la Unión del Tercer Informe de Gobierno, se comprometió a llevar a cabo un proceso de desregulación a fondo de la normatividad de la Administración Pública Federal, con el objetivo de reducir y simplificar al máximo las disposiciones administrativas, eliminar toda aquella regulación, requisitos, duplicidad de información y trámites innecesarios que permitan consolidar un régimen de certidumbre jurídica, en donde la plena eficacia de las normas aplicables a particulares y a gobernantes, les garantice el ejercicio pleno de sus derechos y libertades. Este proceso de desregulación implica dejar sin efectos una de cada dos disposiciones;

Que la Secretaría a mi cargo cuenta con atribuciones para organizar y coordinar el desarrollo administrativo integral de las dependencias y entidades de la Administración Pública Federal, a fin de que los recursos humanos, patrimoniales y los procedimientos técnicos de la misma, sean aprovechados y aplicados con criterios de eficiencia, buscando en todo momento la eficacia, descentralización, desconcentración y simplificación administrativa, así como para realizar o encomendar las investigaciones, estudios y análisis que al efecto se requieran, y dictar las disposiciones administrativas correspondientes para las propias dependencias y entidades;

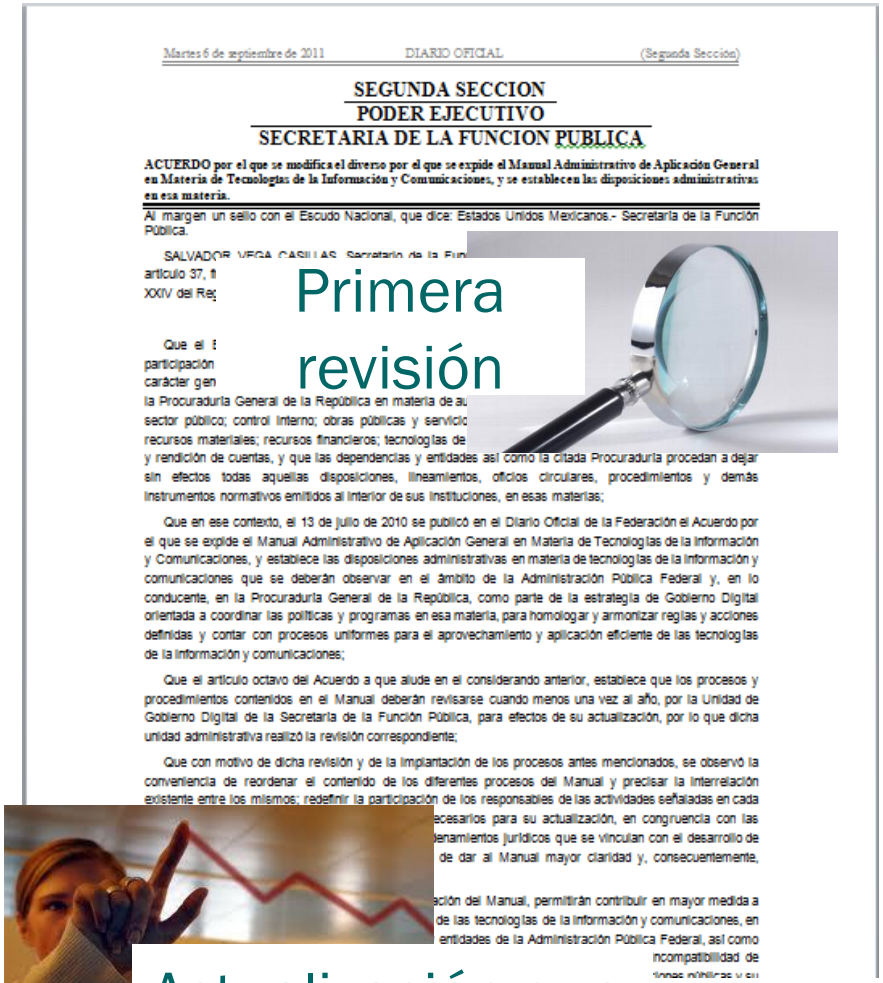
Que en este sentido, el Ejecutivo Federal instruyó a esta Secretaría para emitir, por sí o con la participación de las dependencias competentes, disposiciones, políticas o estrategias, acciones o criterios de carácter general y procedimientos uniformes para la Administración Pública Federal y, en lo conducente, para la Procu... sector p... recursos... y rendic... sin efe... instrume...

Que ... comunic... interno, ...

Que ... tecnolog... Pública ... de gob... armoniz... eficient... políticas ... institucio...

GOBIERNO FEDERAL

Acuerdo publicado en el DOF el 6 de septiembre de 2011



Martes 6 de septiembre de 2011 DIARIO OFICIAL (Segunda Sección)

SEGUNDA SECCION
PODER EJECUTIVO
SECRETARIA DE LA FUNCION PUBLICA

ACUERDO por el que se modifica el diverso por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y se establecen las disposiciones administrativas en esa materia.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de la Función Pública.

SALVADOR VEGA CASILLAS, Secretario de la Fun
artículo 37, f
XXIV del Reg

Que el
participación
carácter gen
la Procuraduría General de la República en materia de au
sector público; control interno; obras públicas y servicio
recursos materiales; recursos financieros; tecnologías de
y rendición de cuentas, y que las dependencias y entidades así como la citada Procuraduría procedan a dejar sin efectos todas aquellas disposiciones, lineamientos, oficios circulares, procedimientos y demás instrumentos normativos emitidos al interior de sus instituciones, en esas materias;

Que en ese contexto, el 13 de julio de 2010 se publicó en el Diario Oficial de la Federación el Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y establece las disposiciones administrativas en materia de tecnologías de la información y comunicaciones que se deberán observar en el ámbito de la Administración Pública Federal y, en lo conducente, en la Procuraduría General de la República, como parte de la estrategia de Gobierno Digital orientada a coordinar las políticas y programas en esa materia, para homologar y armonizar reglas y acciones definidas y contar con procesos uniformes para el aprovechamiento y aplicación eficiente de las tecnologías de la información y comunicaciones;

Que el artículo octavo del Acuerdo a que alude en el considerando anterior, establece que los procesos y procedimientos contenidos en el Manual deberán revisarse cuando menos una vez al año, por la Unidad de Gobierno Digital de la Secretaría de la Función Pública, para efectos de su actualización, por lo que dicha unidad administrativa realizó la revisión correspondiente;

Que con motivo de dicha revisión y de la implantación de los procesos antes mencionados, se observó la conveniencia de reordenar el contenido de los diferentes procesos del Manual y precisar la interrelación existente entre los mismos; redefinir la participación de los responsables de las actividades señaladas en cada
cesarios para su actualización, en congruencia con las
enamientos jurídicos que se vinculan con el desarrollo de
de dar al Manual mayor claridad y, consecuentemente,

ación del Manual, permitirán contribuir en mayor medida a
de las tecnologías de la información y comunicaciones, en
entidades de la Administración Pública Federal, así como
ncompatibilidad de

Primera revisión

Actualización que agrega claridad

Artículo primero (único):

- Señala que se reforman los artículos primero, sexto, octavo y el anexo único.

  … en el sexto, se adiciona un párrafo el cual establece que contrataciones de servicios a terceros que integren algún proceso del manual, deberán establecerse en las convocatorias de los procedimientos de contratación…

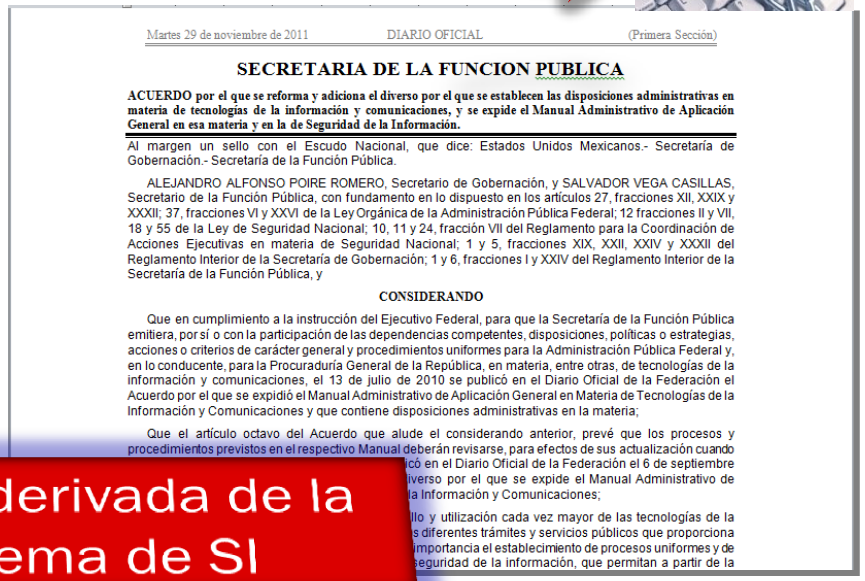
- El anexo da lugar a la nueva versión del manual y suprime un proceso.

Único transitorio: entrada en vigor.

Acuerdo publicado en el DOF el 29 de noviembre de 2011

A fin de fortalecer los procesos de seguridad de la información:

- Con base en los documentos técnicos del GTECSI, se integra la materia de seguridad de la información,
- las disposiciones para armonizar las dos materias,
- y se establecen disposiciones de seguridad de la información considerada de seguridad nacional.



Martes 29 de noviembre de 2011 DIARIO OFICIAL (Primera Sección)

SECRETARIA DE LA FUNCION PUBLICA

ACUERDO por el que se reforma y adiciona el diverso por el que se establecen las disposiciones administrativas en materia de tecnologías de la información y comunicaciones, y se expide el Manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Gobernación.- Secretaría de la Función Pública.

ALEJANDRO ALFONSO POIRE ROMERO, Secretario de Gobernación, y SALVADOR VEGA CASILLAS, Secretario de la Función Pública, con fundamento en lo dispuesto en los artículos 27, fracciones XII, XXIX y XXXII; 37, fracciones VI y XXVI de la Ley Orgánica de la Administración Pública Federal; 12 fracciones II y VII, 18 y 55 de la Ley de Seguridad Nacional; 10, 11 y 24, fracción VII del Reglamento para la Coordinación de Acciones Ejecutivas en materia de Seguridad Nacional; 1 y 5, fracciones XIX, XXII, XXIV y XXXII del Reglamento Interior de la Secretaría de Gobernación; 1 y 6, fracciones I y XXIV del Reglamento Interior de la Secretaría de la Función Pública, y

CONSIDERANDO

Que en cumplimiento a la instrucción del Ejecutivo Federal, para que la Secretaría de la Función Pública emitiera, por sí o con la participación de las dependencias competentes, disposiciones, políticas o estrategias, acciones o criterios de carácter general y procedimientos uniformes para la Administración Pública Federal y, en lo conducente, para la Procuraduría General de la República, en materia, entre otras, de tecnologías de la información y comunicaciones, el 13 de julio de 2010 se publicó en el Diario Oficial de la Federación el Acuerdo por el que se expidió el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y que contiene disposiciones administrativas en la materia;

Que el artículo octavo del Acuerdo que alude el considerando anterior, prevé que los procesos y procedimientos previstos en el respectivo Manual deberán revisarse, para efectos de sus actualización cuando

ió en el Diario Oficial de la Federación el 6 de septiembre

iverso por el que se expide el Manual Administrativo de

la Información y Comunicaciones;

llo y utilización cada vez mayor de las tecnologías de la

s diferentes trámites y servicios públicos que proporciona

importancia el establecimiento de procesos uniformes y de

seguridad de la información, que permitan a partir de la

Actualización derivada de la criticidad del tema de SI

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones:

- En el articulo primero se contiene el señalamiento sobre aquellas instituciones que deberán observar el acuerdo y el manual, y extiende el ámbito de ambos instrumentos a la materia de seguridad de la información.
- Se reforma el artículo segundo a fin de integrar definiciones para hacer congruente el uso de las voces necesarias para la materia de seguridad de la información.
- El articulo cuarto se reforma para dar cabida al ordenamiento de dejar sin efectos aquellas disposiciones y procesos de ambas materias, que no deriven de facultades expresamente previstas en leyes y reglamentos.
- Se reforma el artículo quinto para señalar a qué áreas o servidores públicos corresponde la aplicación del manual: áreas de TIC y servidores cuyas funciones se vinculen con las TIC y con la seguridad de la información.

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones *(continuación)*:

- El articulo sexto se reforma en su primer párrafo para dar lugar en el manual a los procesos de seguridad de la información mas allá del alcance previo sujeto a las TIC.
- Se adiciona el Capítulo III bis, para dar lugar a las *Disposiciones específicas para la seguridad de la información considerada de seguridad nacional*,
  - El Sexto bis aplica a las instancias consideradas de seguridad nacional:

    "las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquéllas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional";

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones *(continuación)*:

Sin embargo en el penúltimo y último párrafos del mismo artículo se cita:

> *"Las dependencias y entidades que, aún sin tener el carácter de Instancia de seguridad nacional, generen o sean destinatarias de información considerada de seguridad nacional, deberán observar lo establecido en este artículo en los casos en que compartan o transmitan dicha información."*
>
> *"Lo dispuesto en este artículo se aplicará sin perjuicio de lo establecido en la Ley Federal de Trasparencia y Acceso a la Información Pública Gubernamental y demás disposiciones aplicables."*

Debiendo entonces las instituciones cuidar la observancia de estas disposiciones para el caso de resguardar o ser destinataria de información considerada de seguridad nacional.

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones *(continuación)*:

Sexto bis…

…establece las disposiciones que incluyen aquellas necesarias para el control de:

- los sujetos habilitados para su manejo, su identificación y registro;
- La asignación de niveles de diseminación, de acuerdo a la clasificación de la información generada o custodiada en las instituciones;
- Los señalamientos para precisar y controlar a los destinatarios que tienen necesidad de conocer la información a diseminar y las responsabilidades que adquieren.
- El manejo y protección de la información física o electrónica, para que ésta conserve su carácter.

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones *(continuación)*:

- El artículo Sexto ter cita:

  "Las dependencias y entidades deberán comunicar al Centro, los datos de los servidores públicos que designen como Responsables de la seguridad de la información; así como de los enlaces responsables de mantener comunicación con los Equipos de respuesta a incidentes de seguridad en TIC, para efectos de su registro."

- Cabe hacer notar en este mismo sentido el primero y segundo artículos transitorios del mismo Acuerdo:

  "Primero.- El presente Acuerdo entrará en vigor el día 2 de enero de 2012."

  "Segundo.- En la fecha de entrada en vigor del presente Acuerdo, las dependencias y entidades deberán comunicar al Centro los datos de los servidores públicos designados como responsables de la seguridad de la información y de los enlaces responsables a los que se refiere el artículo Sexto Ter del presente ordenamiento."

Acuerdo publicado en el DOF el 29 de noviembre de 2011

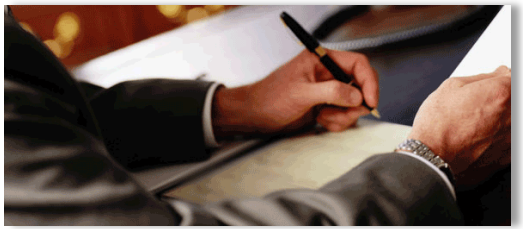
Reformas y adiciones *(continuación)*:

- Los artículos séptimo y octavo se reforman:
  - Respecto de la interpretación del acuerdo y del manual, para efectos administrativos y resolución de casos no previstos, se establece en el séptimo, que:
    - ✓ *En materia de TIC y de seguridad de la información, corresponde a la SFP, a través de la Unidad de Gobierno Digital.*
    - ✓ *En materia de seguridad de la información considerada de seguridad nacional, a la SEGOB, a través del Centro.*
  - Respecto de la revisión y actualización del acuerdo y el manual, el artículo octavo, señala que éstos deberán revisarse, y de ser el caso, actualizarse, por las instancias en concordancia con el artículo anterior, cuando menos una vez al año.

Acuerdo publicado en el DOF el 29 de noviembre de 2011

Reformas y adiciones *(continuación)*:

- El artículo noveno no se reformó, sin embargo sobre éste cabe hacer notar recordar que se refiere a la función que los Órganos internos de control en las instituciones deben observar: vigilar el cumplimiento del acuerdos, los diversos que lo modifican, así como del manual.
- Asimismo, deben vigilar, al respecto del tema de tala regulatoria y contención de la expedición de regulaciones que ya estén contenidas en el manual así como dejar sin efectos aquellas que puedan contraponerse a los mismos.



Acuerdo publicado en el DOF el 29 de noviembre de 2011

Regresemos a las definiciones, el artículo segundo define, entre otras:

- Diseminación: la transmisión o entrega de información considerada de seguridad nacional, a quienes cumplan con los requisitos para conocer esa información, de acuerdo con el nivel de acceso autorizado.
- Infraestructura de TIC: el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.
- Instancias de seguridad nacional: las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquéllas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional.
- Seguridad nacional: las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de lo dispuesto en el artículo 3 de la Ley de Seguridad Nacional.

Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, cuarta parte

- Elementos de los procesos de administración de la seguridad de la información (ASI) y operación de los controles de seguridad de la información y del ERISC (OPEC).
  - Alcance y estructura
  - Mapeo de roles.

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

La seguridad de la información…

… en los procesos del MAAGTICSI…

Objetivo General

"Definir los procesos que en materia de TIC y de seguridad en la información regirán hacia el interior de la Institución, con el propósito de **lograr la cobertura total de la gestión de ambas materias…**

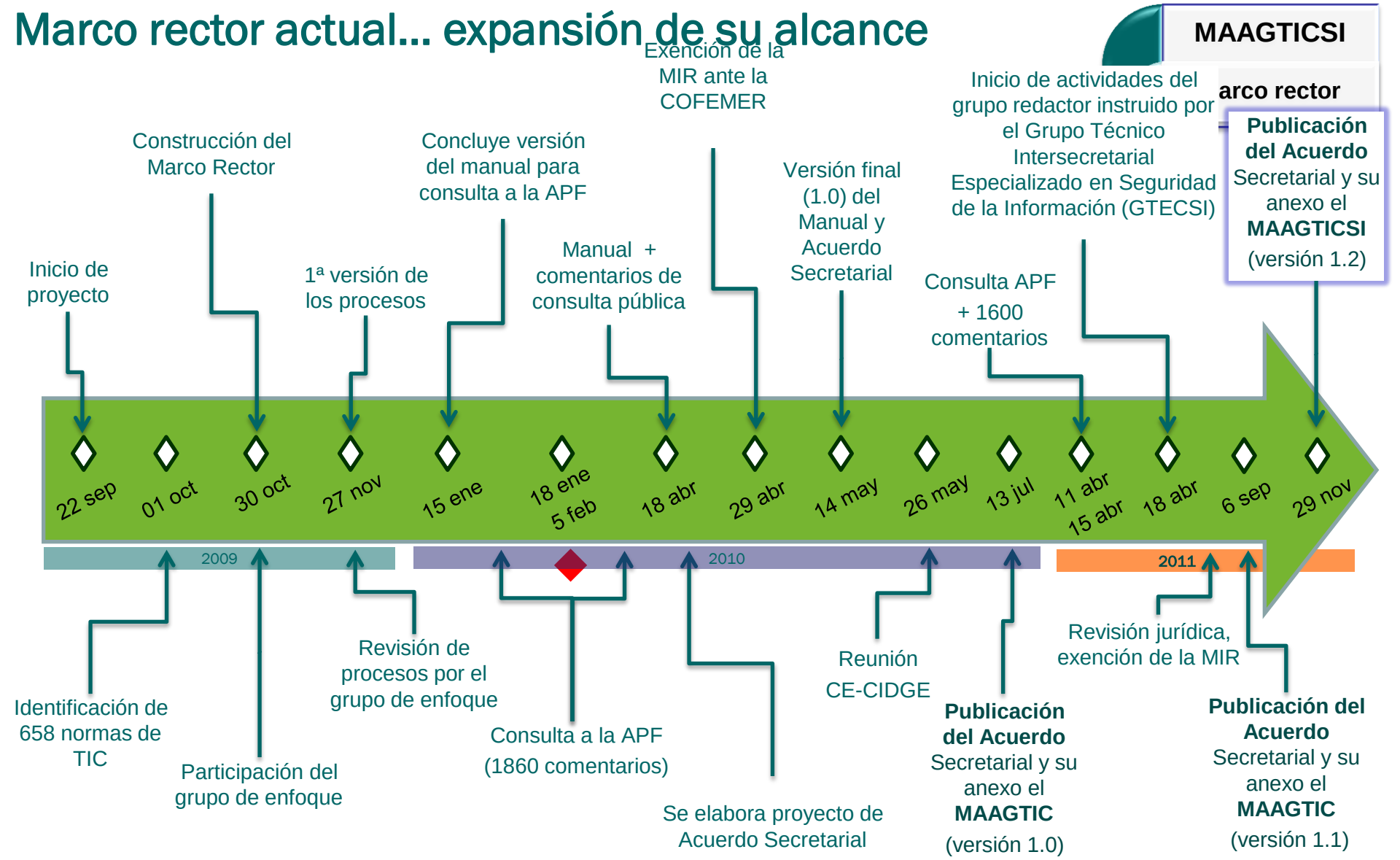
…cohesión de los procesos para una mejor gestión"

Objetivos Específicos

Procesos simplificados y homologados en las materias de TIC y de seguridad de la información	Indicadores homologados para medición de resultados	Mayor eficiencia orientada al servicio y satisfacción del ciudadano

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Marco rector actual… expansión de su alcance



Evolución del marco rector…

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

MAAGTIC Versión 1.0

4 Niveles de Gestión, 11 Grupos de procesos y 30 procesos

GOBIERNO

Dirección

- Establecimiento del modelo de gobernabilidad de TIC
- Planeación estratégica de TIC
- Determinación de la Dirección Tecnológica

Control

- Administración de la evaluación de TIC
- **Administración de riesgos de TIC**

ORGANIZACÍON Y ESTRATEGIA

Administración de Proyectos

- Administración del portafolio de proyectos de TIC
- Administración de proyectos de TIC

Administración de procesos

- Operación del sistema de gestión y mejora de los procesos de la UTIC

Administración de recursos

- Administración del presupuesto de TIC
- Administración de proveedores de productos y servicios de TIC
- Administración de adquisiciones de TIC

Administración de Servicios

- Administración del portafolio de servicios de TIC
- Diseño de servicios de TIC

EJECUCIÓN Y ENTREGA

Administración del desarrollo de soluciones

- Definición de requerimientos de soluciones
- Desarrollo de soluciones tecnológicas
- Calidad de soluciones tecnológicas

Transición y entrega

- Administración de cambios
- Liberación y entrega
- Transición y habilitación de la operación
- Administración de la configuración

Operación de Servicios

- Operación de la mesa de servicios
- Administración de servicios de terceros
- Administración de niveles de servicios
- **Administración de la seguridad de los sistemas informáticos**

SOPORTE

Administración de Activos

- Administración de dominios tecnológicos
- Administración del conocimiento
- Integración y desarrollo del personal

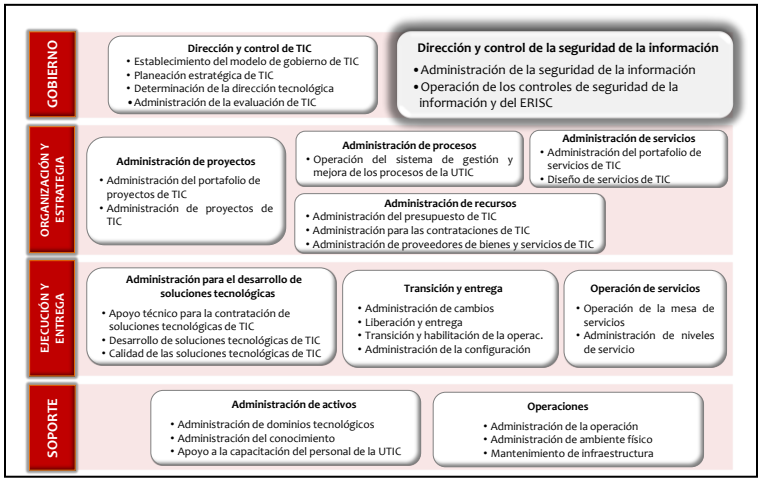
Operaciones

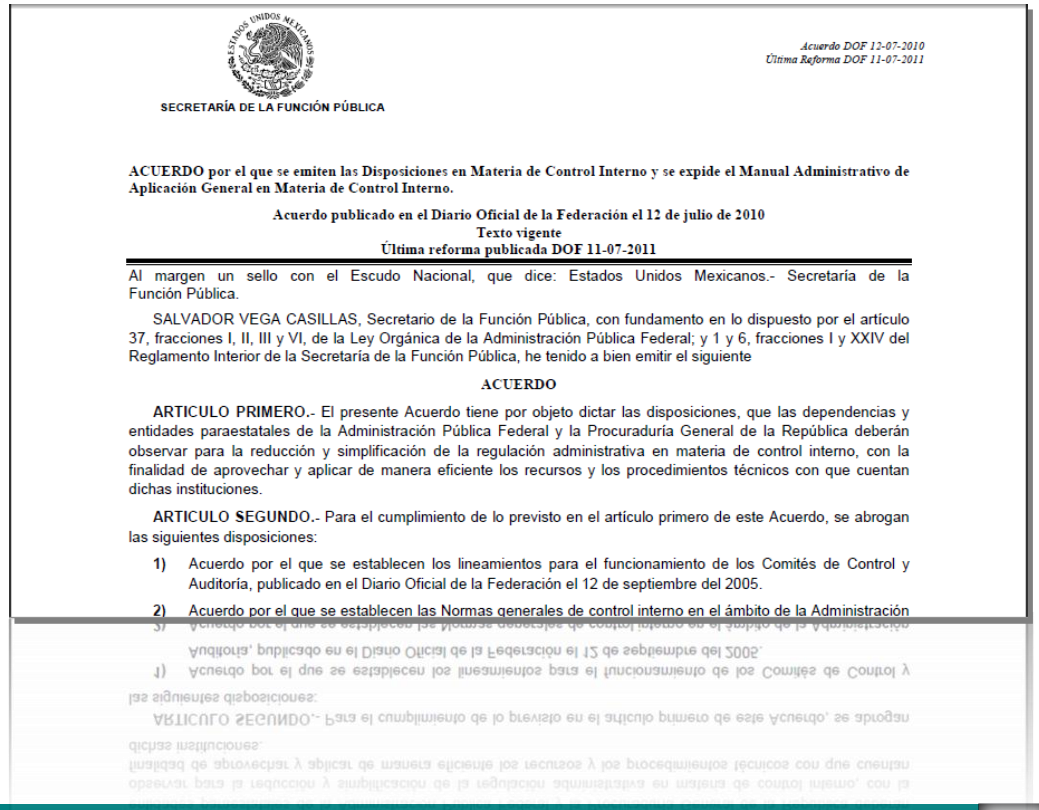
- Administración de la operación
- Administración de ambiente físico
- Mantenimiento de Infraestructura

Elementos de los procesos

Marco rector actual... expansión de su alcance

Acuerdo y manual de control interno





SECRETARÍA DE LA FUNCIÓN PÚBLICA

Acuerdo DOF 12-07-2010
Última Reforma DOF 11-07-2011

ACUERDO por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno.

Acuerdo publicado en el Diario Oficial de la Federación el 12 de julio de 2010
Texto vigente
Última reforma publicada DOF 11-07-2011

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de la Función Pública.

SALVADOR VEGA CASILLAS, Secretario de la Función Pública, con fundamento en lo dispuesto por el artículo 37, fracciones I, II, III y VI, de la Ley Orgánica de la Administración Pública Federal; y 1 y 6, fracciones I y XXIV del Reglamento Interior de la Secretaría de la Función Pública, he tenido a bien emitir el siguiente

ACUERDO

ARTICULO PRIMERO.- El presente Acuerdo tiene por objeto dictar las disposiciones, que las dependencias y entidades paraestatales de la Administración Pública Federal y la Procuraduría General de la República deberán observar para la reducción y simplificación de la regulación administrativa en materia de control interno, con la finalidad de aprovechar y aplicar de manera eficiente los recursos y los procedimientos técnicos con que cuentan dichas instituciones.

ARTICULO SEGUNDO.- Para el cumplimiento de lo previsto en el artículo primero de este Acuerdo, se abrogan las siguientes disposiciones:

1) Acuerdo por el que se establecen los lineamientos para el funcionamiento de los Comités de Control y Auditoría, publicado en el Diario Oficial de la Federación el 12 de septiembre del 2005.

2) Acuerdo por el que se establecen las Normas generales de control interno en el ámbito de la Administración

La seguridad de la información…

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Marco rector actual... expansión de su alcance

MAAGTICSI

Marco rector

4 Niveles de Gestión, 11 Grupos de procesos y 29 procesos

GOBIERNO

Dirección y control de TIC
- Establecimiento del modelo de gobierno de TIC
- Planeación estratégica de TIC
- Determinación de la dirección tecnológica
- Administración de la evaluación de TIC

Dirección y control de la seguridad de la información
- Administración de la seguridad de la información
- Operación de los controles de seguridad de la información y del ERISC

ORGANIZACIÓN Y ESTRATEGIA

Administración de proyectos
- Administración del portafolio de proyectos de TIC
- Administración de proyectos de TIC

Administración de procesos
- Operación del sistema de gestión y mejora de los procesos de la UTIC

Administración de servicios
- Administración del portafolio de servicios de TIC
- Diseño de servicios de TIC

Administración de recursos
- Administración del presupuesto de TIC
- Administración para las contrataciones de TIC
- Administración de proveedores de bienes y servicios de TIC

EJECUCIÓN Y ENTREGA

Administración para el desarrollo de soluciones tecnológicas
- Apoyo técnico para la contratación de soluciones tecnológicas de TIC
- Desarrollo de soluciones tecnológicas de TIC
- Calidad de las soluciones tecnológicas de TIC

Transición y entrega
- Administración de cambios
- Liberación y entrega
- Transición y habilitación de la operac.
- Administración de la configuración

Operación de servicios
- Operación de la mesa de servicios
- Administración de niveles de servicio

SOPORTE

Administración de activos
- Administración de dominios tecnológicos
- Administración del conocimiento
- Apoyo a la capacitación del personal de la UTIC

Operaciones
- Administración de la operación
- Administración de ambiente físico
- Mantenimiento de infraestructura

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Roles que se requiere alinear para la implantación del MAAGTICSI

Versiones anteriores, proceso ARTI y ASSI:	
1.1	Responsable del proceso ARTI- Administración de riesgos de TIC.
1.2	Grupo de trabajo para la dirección de TIC.
1.3	Grupo de trabajo de riesgos de TIC.

Versión actual, procesos ASI y OPEC:	
1.1	Responsable de la seguridad de la información en la Institución o RSII.
1.2	Grupo estratégico de seguridad de la información o GESI.
1.3	Equipo de trabajo de infraestructuras críticas.
1.4	Equipo de trabajo de análisis de riesgos.
1.5	Equipo de respuesta a incidentes de seguridad o ERISC.

GOBIERNO FEDERAL

Mapeo de roles

Roles que se requiere alinear para la implantación del MAAGTICSI

Versiones anteriores, proceso ARTI y ASSI:	
1.1	Grupo de trabajo de seguridad de la información.
1.2	Responsable del SGSI.
1.3	Responsables de los procesos de la UTIC.

Versión actual, procesos ASI y OPEC:	
1.1	Grupo de trabajo para la implantación de la seguridad de la información.
1.2	Responsable del Grupo de trabajo para la implantación de la seguridad de la información.
1.3	ERISC.

Elementos de los procesos

Producto (Insumo)-Entrada-Proceso-Salida-Producto

MAAGTICSI
Marco rector

Reglas del proceso

Entradas

Proceso

Actividad 1
- *Factores Críticos*

Actividad 2
- *Factores Críticos*

Actividad n …
- *Factores Críticos*

Productos

Roles

Indicadores

Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, quinta parte

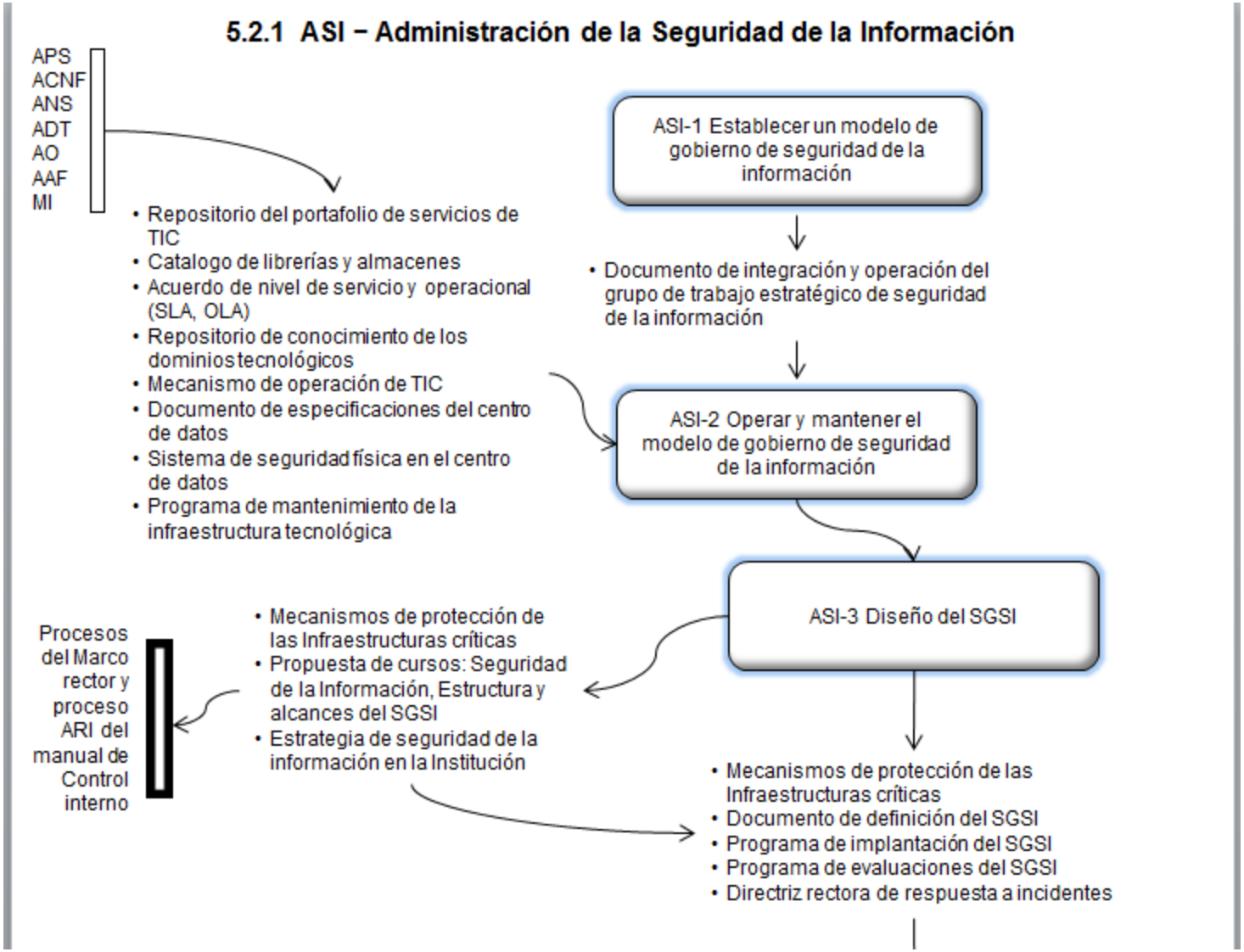
- Interrelación entre los procesos ASI y OPEC; y relación éstos, con el resto de los procesos del marco rector del MAAGTICSI.

Secretaría de Marina
Centro de Estudios Superiores Navales

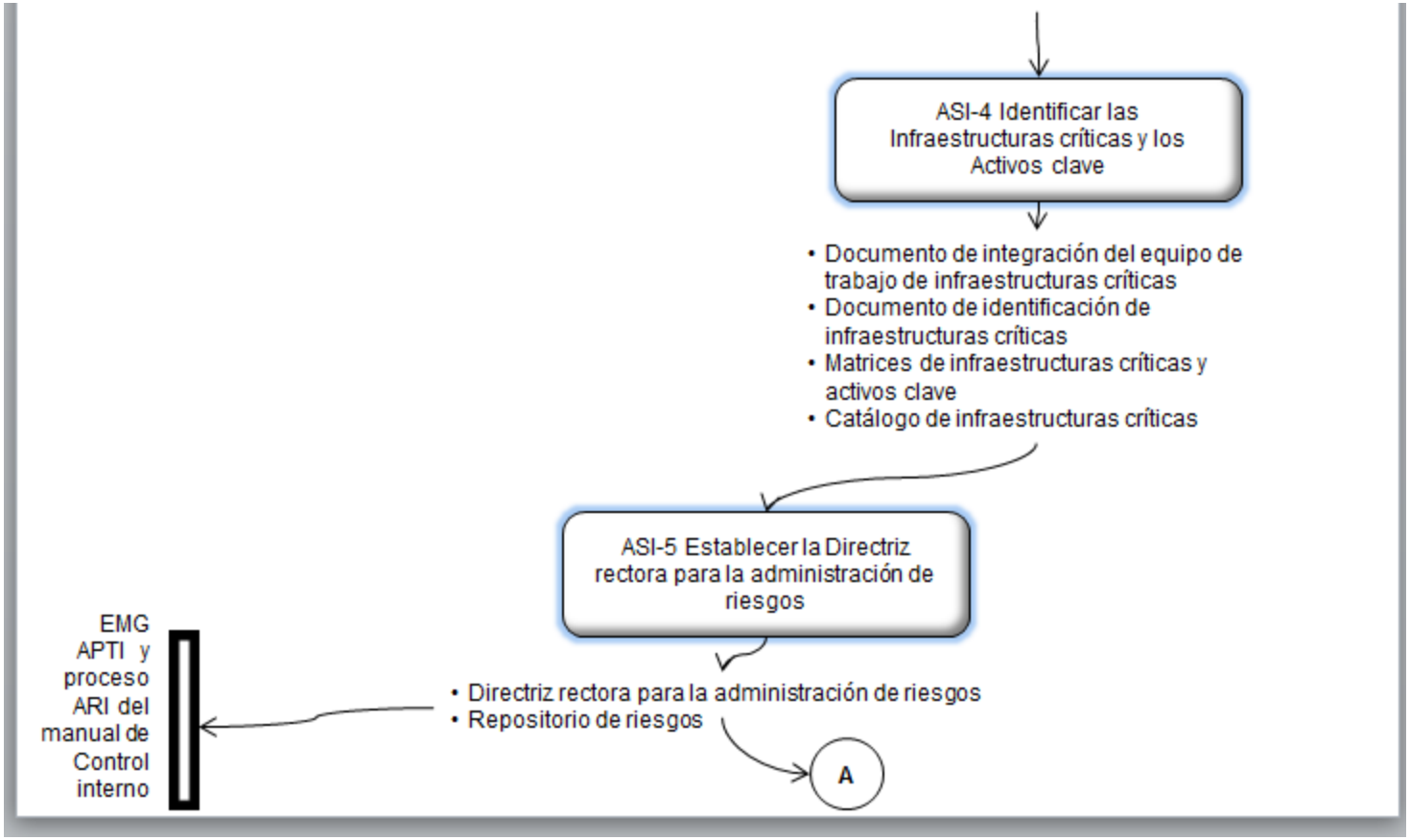
Ciudad de México,
abril - mayo de 2012

Diagramas de flujo de información

Interrelaciones proceso ASI

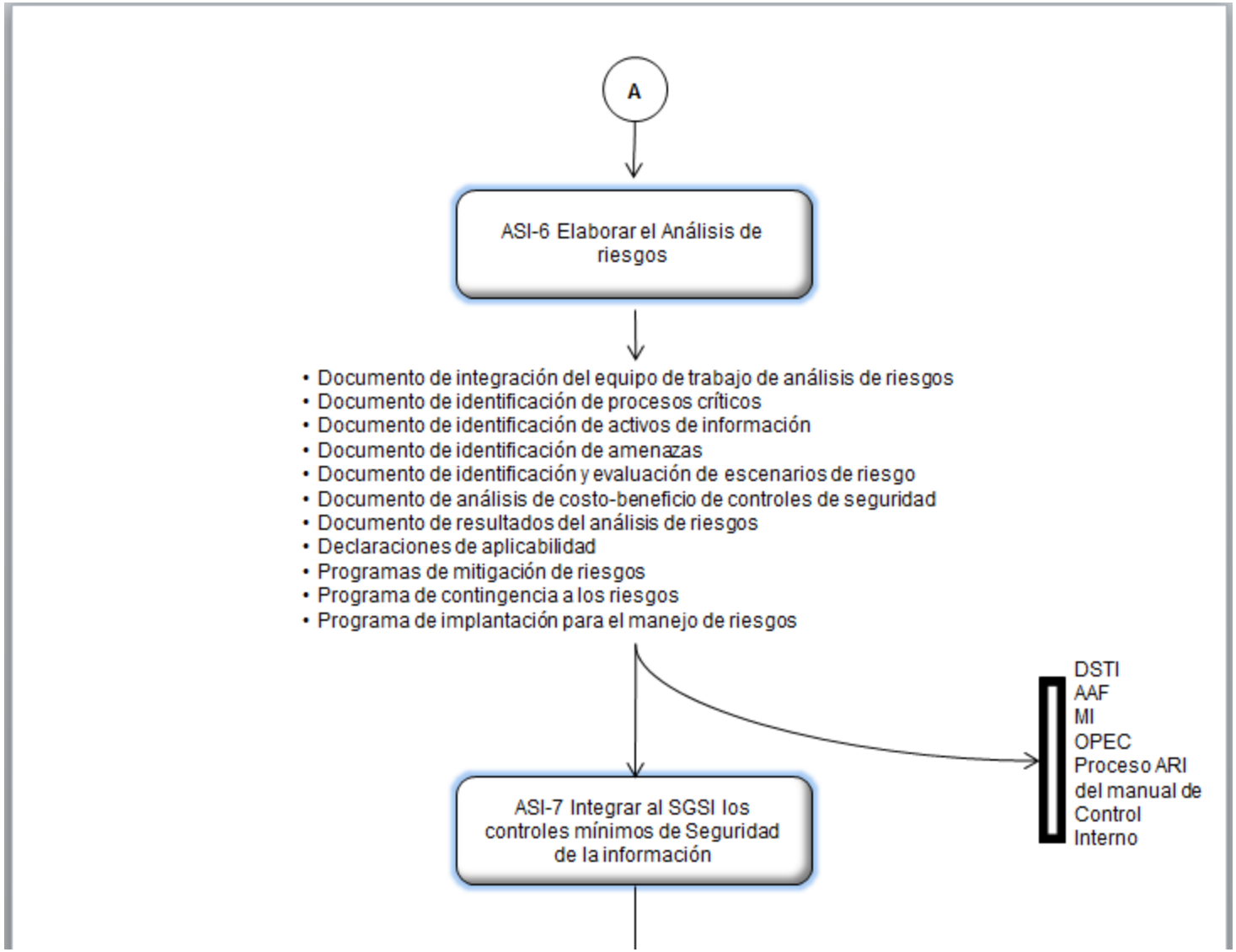


Interrelaciones proceso ASI *(continuación)...*

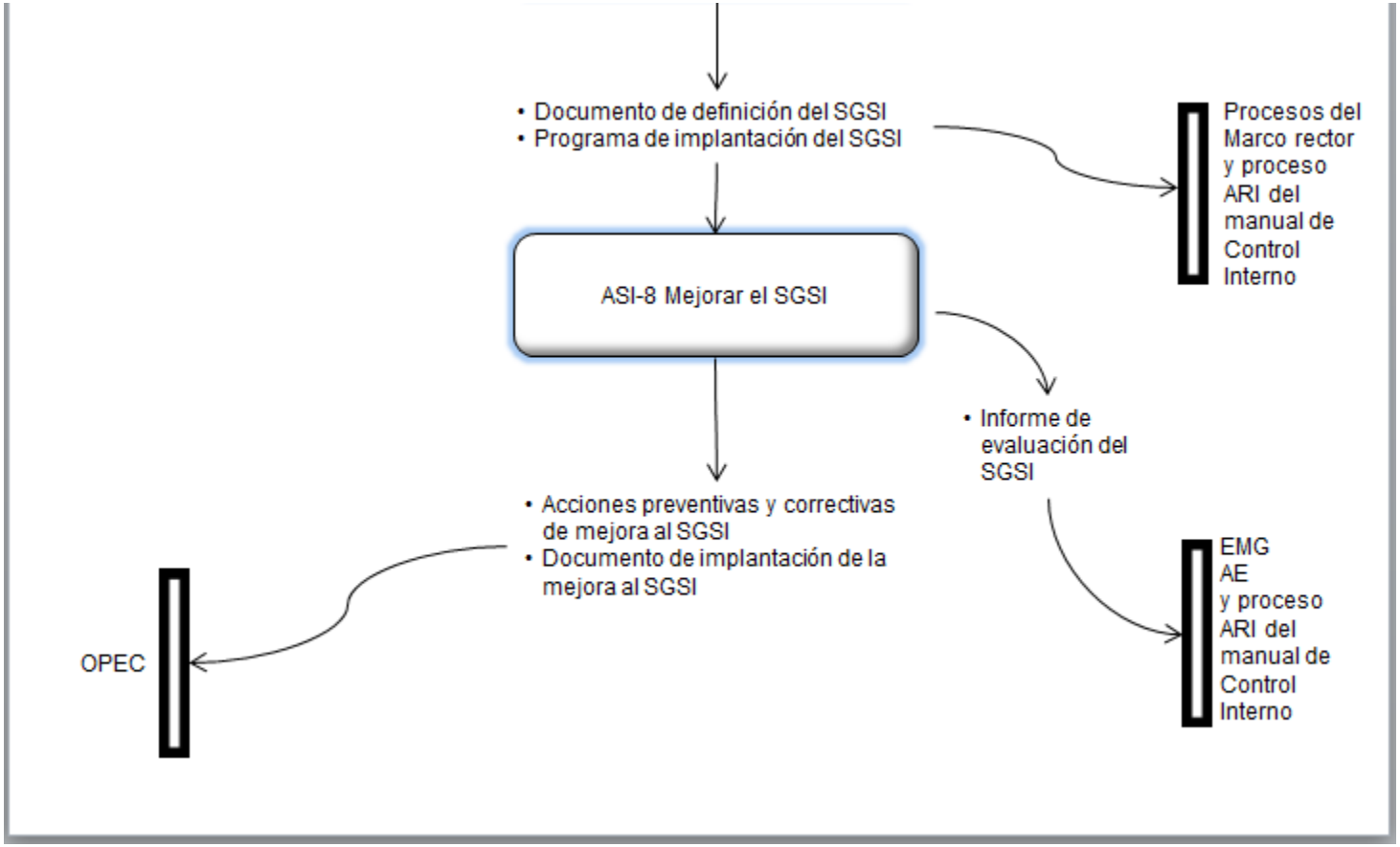


Diagramas de flujo de información

Interrelaciones proceso ASI *(continuación)...*

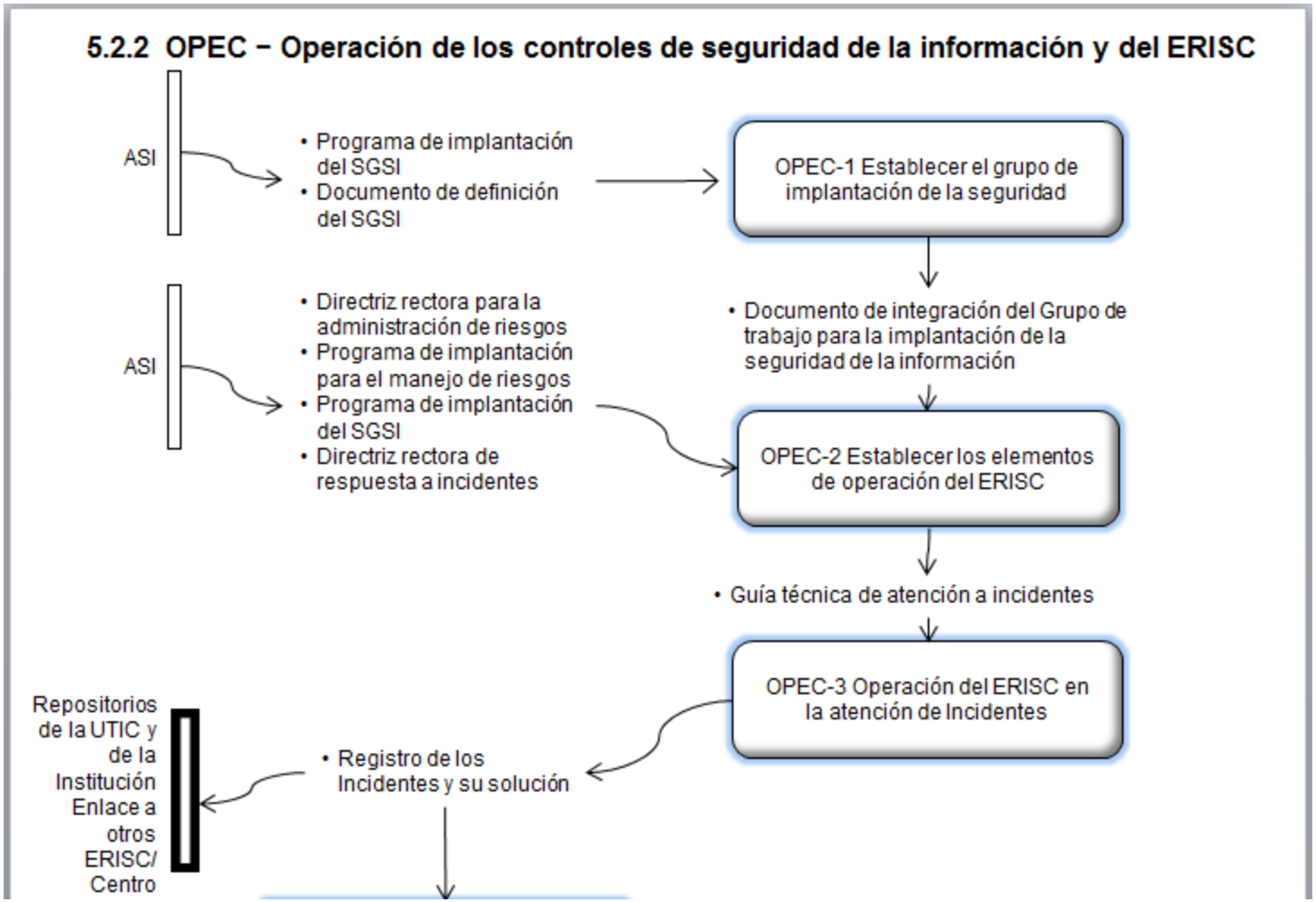


Interrelaciones proceso ASI *(continuación)...*

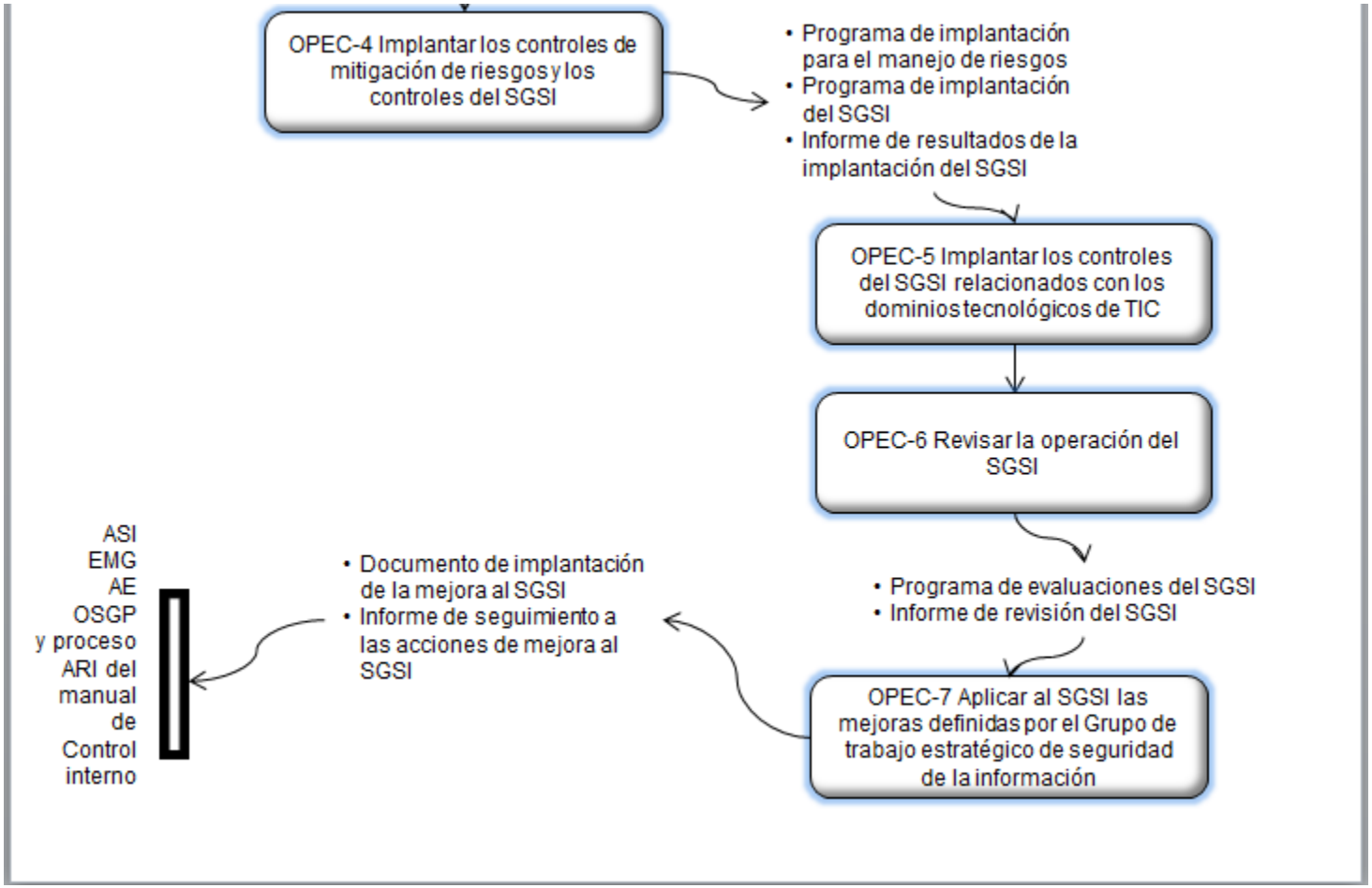


Diagramas de flujo de información

Interrelaciones proceso OPEC



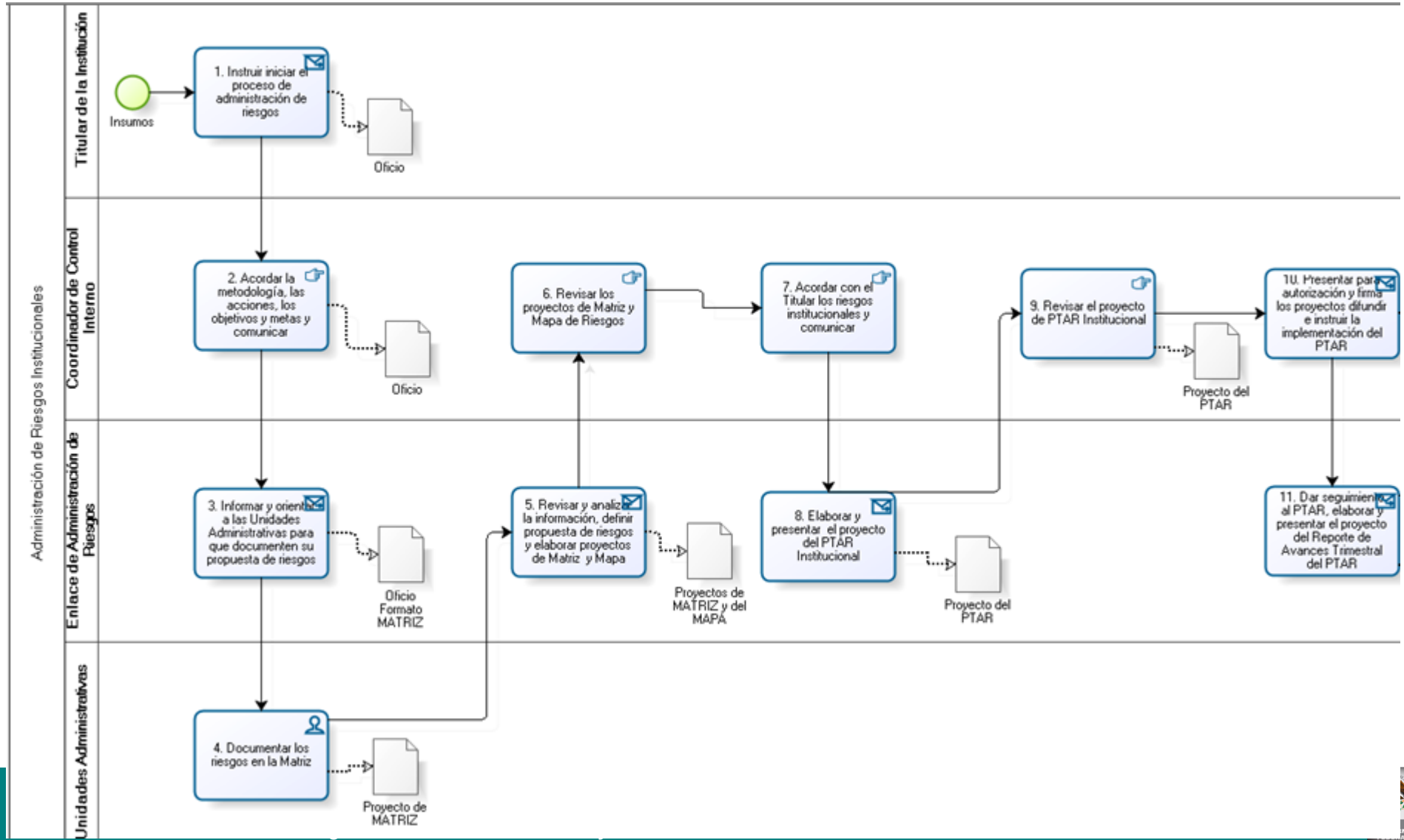
Interrelaciones proceso OPEC *(continuación)...*



Elementos de los procesos

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

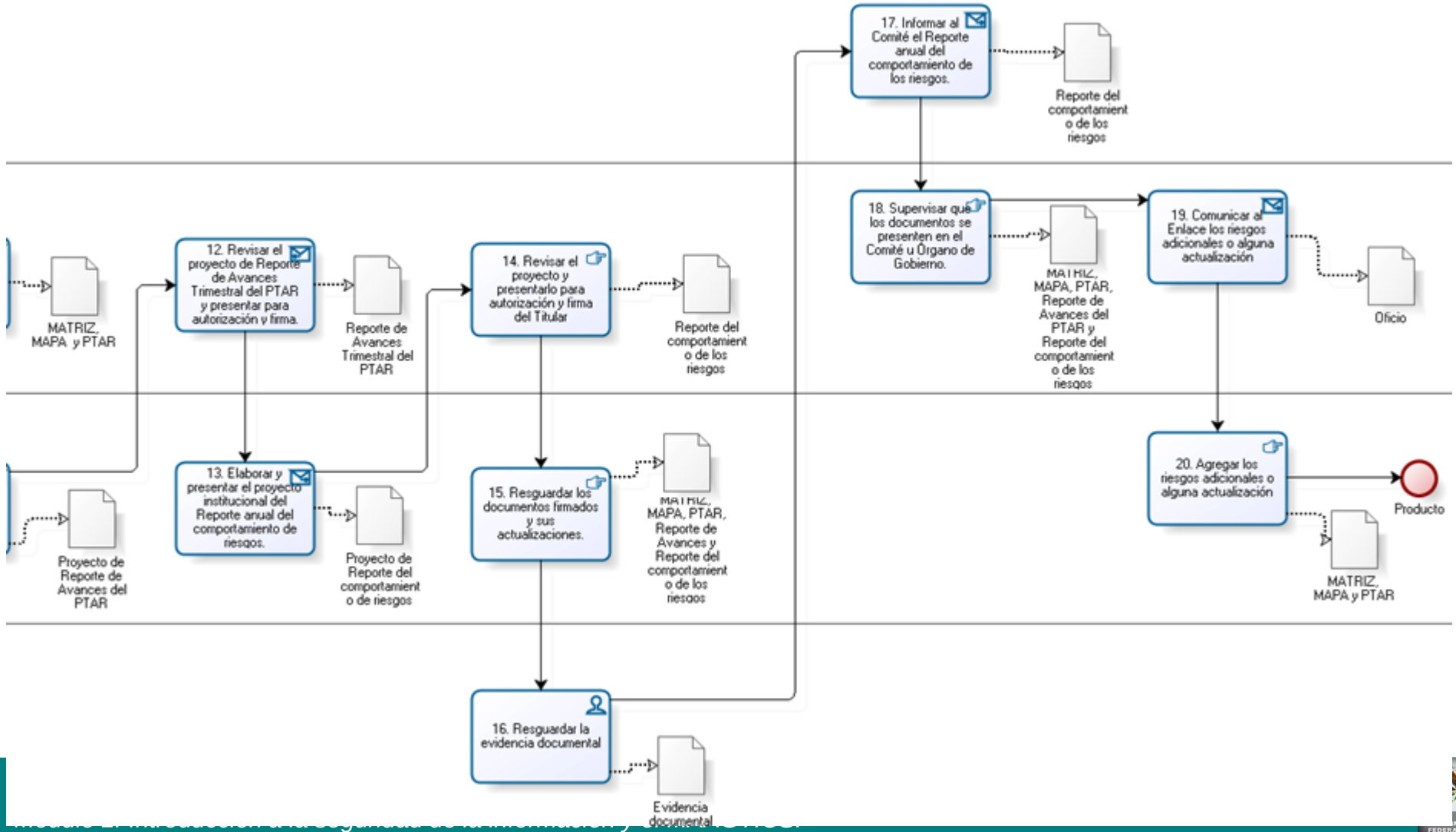
..proceso de Administración de Riesgos Institucionales del Manual de Control Interno.



Elementos de los procesos

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

..proceso de Administración de Riesgos Institucionales del Manual de Control Interno.



SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Formatos del proceso de administración de riesgos, control interno

	A	B	C	D	E	F	G	H	I	J
25	El Formato de Matríz de Administración de Riesgos se Imprime en Formato Tamaño Oficio				I. EVALUACIÓN RIESGOS					
26	No. de Riesgo	Unidad Administrativa	Alineación a Estrategias, Objetivos, o Metas Institucionales		RIESGO	Nivel de decisión del Riesgo	Clasificación del Riesgo		F A	
27			Selección	Descripción			Selección	Especificar Otro	No. de Factor	Descripción
28										
29										
30										
31										
32										
33										
34										
35										
36										
37										
38										
39										
40										
41										
42										
43										
44										
45										
46										
47										
48										
49										
50										
51										
52										
53										

GOBIERNO FEDERAL

Formatos del proceso de administración de riesgos, control interno

No es necesario requisitar ningún dato, ya que el Mapa de Riesgos está vinculado con la información que se registre previamente en la Matriz de Administración de Riesgos

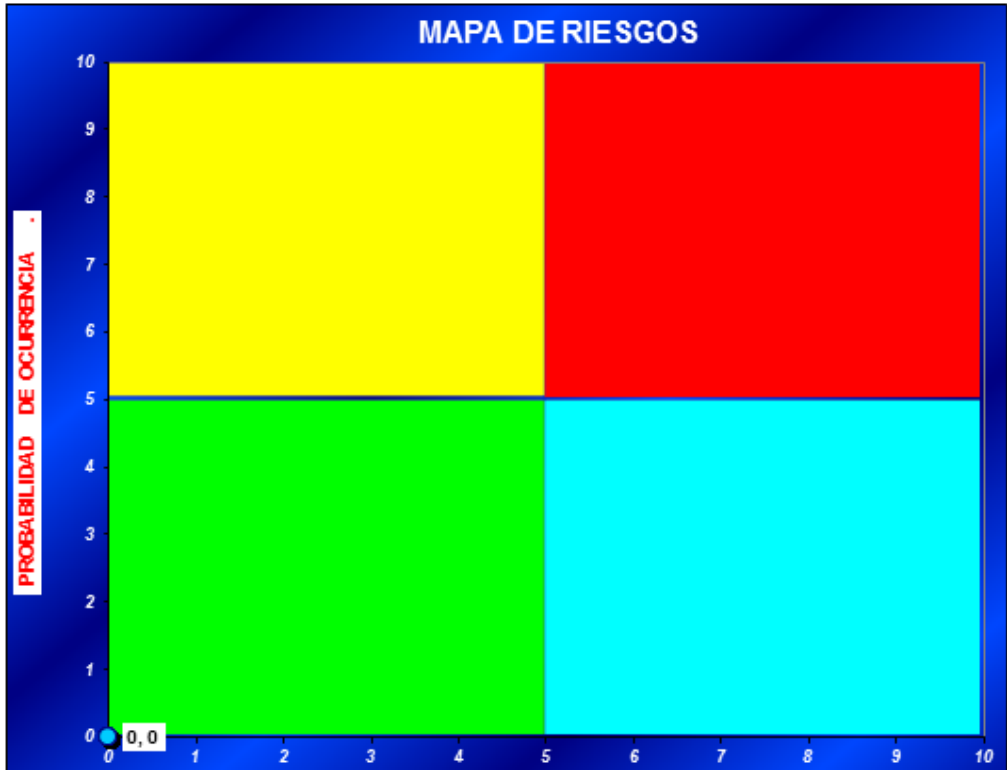
El Mapa de Riesgos se Imprime en Formato Tamaño Carta

MAPA DE RIESGOS INSTITUCIONAL 2010

RAMO / SECTOR:

INSTITUCIÓN:

No. de Riesgo	RIESGO	III. VALORACIÓN DE RIESGOS VS. CONTROLES	
		Valoración Final	
		GRADO DE IMPACT	PROBABILIDAD DE



Introducción a la seguridad de la Información y el MAAGTICSI

Modulo 1, sexta parte

- Elementos de los procesos de administración de la seguridad de la información (ASI) y operación de los controles de seguridad de la información y del ERISC (OPEC).
  - Procesos, productos/formatos para los nuevos procesos de seguridad de la información.

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012

Procesos, nivel de gestión Gobierno

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Procesos que requirieron adecuaciones con la integración de la SI

4 Niveles de Gestión, 11 Grupos de procesos y 29 procesos

GOBIERNO

Dirección y control de TIC
- Establecimiento del modelo de gobierno de TIC
- Planeación estratégica de TIC
- Determinación de la dirección tecnológica
- Administración de la evaluación de TIC

Dirección y control de la seguridad de la información
- Administración de la seguridad de la información
- Operación de los controles de seguridad de la información y del ERISC

ORGANIZACIÓN Y ESTRATEGIA

Administración de proyectos
- Administración del portafolio de proyectos de TIC
- Administración de proyectos de TIC

Administración de procesos
- Operación del sistema de gestión y mejora de los procesos de la UTIC

Administración de servicios
- Administración del portafolio de servicios de TIC
- Diseño de servicios de TIC

Administración de recursos
- Administración del presupuesto de TIC
- Administración para las contrataciones de TIC
- Administración de proveedores de bienes y servicios de TIC

EJECUCIÓN Y ENTREGA

Administración para el desarrollo de soluciones tecnológicas
- Apoyo técnico para la contratación de soluciones tecnológicas de TIC
- Desarrollo de soluciones tecnológicas de TIC
- Calidad de las soluciones tecnológicas de TIC

Transición y entrega
- Administración de cambios
- Liberación y entrega
- Transición y habilitación de la operac.
- Administración de la configuración

Operación de servicios
- Operación de la mesa de servicios
- Administración de niveles de servicio

SOPORTE

Administración de activos
- Administración de dominios tecnológicos
- Administración del conocimiento
- Apoyo a la capacitación del personal de la UTIC

Operaciones
- Administración de la operación
- Administración de ambiente físico
- Mantenimiento de infraestructura

Procesos que requirieron adecuaciones con la integración de la SI

Gobierno

Dirección y control de TIC

Grupo: Dirección y control de TIC

Establecimiento del modelo de gobierno de TIC	Planeación estratégica de TIC	Determinación de la dirección tecnológica	Administración de la evaluación de TIC

Procesos

Objetivo general

Gobierno

Dirección y control de TIC

- *Establecer un modelo de gobierno de TIC en la Institución, mediante la conformación de dos grupos de trabajo para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos.*

Actividad EMG-3, modificada

Entradas → EMG-1 Establecer un modelo de gobierno de TIC → EMG-2 Establecer y mantener una adecuada organización de la UTIC

EMG-3 Operar y mantener el modelo de gobierno de TIC → Salidas

Gobierno

Dirección y control de TIC

Grupo de trabajo para la dirección de TIC

- Tomar acuerdos sobre los asuntos en materia de TIC
- Participará en el proceso de Administración del portafolio de proyectos y de servicios de TIC
- Aprobar el PETIC
- Aprobar el sistema de gestión y mejora de los procesos de la UTIC y los indicadores del cuadro de mando de la UTIC
- **Establecer la coordinación necesaria con el RSII para armonizar el gobierno de TIC, la administración de riesgos y el SGSI**
- **Conocer los criterios técnicos que proponga el RSII para gestionar los riesgos**
- Informar al Titular de la Institución acerca de los resultados, recomendaciones y acuerdos del Grupo de trabajo para la dirección de TIC

Reglas del proceso que se adecuaron....

Gobierno

Dirección y control de TIC

- El Titular de la UTIC es el Responsable de este proceso.
- Los roles que se señalan en cada uno de los procesos del MAAGTICSI, con excepción de los mencionados en los procesos ASI- Administración de la seguridad de la información y OPEC- Operación de los controles de seguridad de la información y del ERISC, serán asignados a los servidores públicos de la UTIC en este proceso. Para cualquier cambio en su asignación será necesario considerar los resultados del proceso OSGP- Operación del sistema de gestión y mejora de los procesos de la UTIC.
- Los servidores públicos de la UTIC, así como los de otras áreas o unidades administrativas de la Institución serán responsables, de acuerdo a los roles que les sean asignados, de las actividades que en los diversos procesos del MAAGTICSI se señalan para dichos roles.
- El Grupo de trabajo para la dirección de TIC deberá apoyar la implantación, operación y mejora del SGSI, así como las acciones que realice el Grupo de trabajo estratégico de seguridad de la información.

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Procesos de seguridad de la información rediseñados

Gobierno

Dirección y control de la SI

Grupo: Dirección y control de la seguridad de la información

ASI − Administración de la seguridad de la información	OPEC − Operación de los controles de seguridad de la información y del ERISC

Procesos

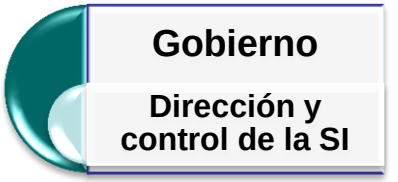
Objetivo general

Gobierno

Dirección y control de la SI

- *Establecer y vigilar los mecanismos que permitan la administración de la Seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad nacional.*

Objetivos específicos



1. Establecer, operar y mantener un modelo de gobierno de Seguridad de la información.
2. Efectuar la identificación de Infraestructuras críticas y Activos clave de la Institución y elaborar el Catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un SGSI que proteja los Activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
5. Establecer mecanismos para la respuesta inmediata a Incidentes a la seguridad de la Información.
6. Vigilar los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.
7. Fomentar una cultura de Seguridad de la información en la Institución.

Definiciones...

Gobierno

Dirección y control de la SI

- **Activos de información:** Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- **Análisis de riesgos:** El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los Activos de TIC, a la Infraestructura crítica o a los Activos de información; efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Actividades del proceso

Gobierno

Dirección y control de la SI

Entradas

ASI-1**:** Establecer un modelo de gobierno de seguridad de la información

ASI-2: Operar y mantener el modelo de gobierno de seguridad de la información

ASI-3: Diseño del SGSI

ASI-4: Identificar las Infraestructuras críticas y los Activos clave

ASI-5: Establecer la Directriz rectora para la administración de riesgos

ASI-6: Elaborar el Análisis de riesgos

ASI-7: Integrar al SGSI los controles mínimos de Seguridad de la información

ASI-8: Mejorar el SGSI

Salidas

Actividades del proceso

Titular de la Institución

Responsable de seguridad de la información en la Institución

Responsable de seguridad de la información en la Institución

Gobierno

Dirección y control de la SI

Grupo de trabajo estratégico de seguridad de la información

ASI-1: Establecer un modelo de gobierno de seguridad de la información

- Designar al RSII, quien deberá tener nivel jerárquico mínimo de DG o equivalente
- Establecer el Grupo de trabajo estratégico de seguridad de la información, integrado por servidores públicos que conozcan los procesos institucionales y tengan conocimientos en materia de seguridad de la información
- Encabezar el Grupo de trabajo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas

ASI-2: Operar y mantener el modelo de gobierno de seguridad de la información

Grupo de trabajo estratégico de seguridad de la información

- Coordinar la elaboración del Catálogo de IC de la Institución
- Establecer, con los Responsables de los grupos de procesos PR, AS, TE, OS, AA y OP, así como con los servidores públicos que administren Activos de información, mecanismos para garantizar la protección de las IC bajo su responsabilidad
- Vigilar que los controles de seguridad de la información que se definan e implanten, consideren los mecanismos establecidos, así como el Análisis de riesgos de ASI-6
- Constatar que se efectúe la implantación de SGSI en la Institución y que se lleven a cabo revisiones al mismo
- Dar seguimiento a las acciones de mejora continua derivadas de las revisiones al SGSI

ASI-3: Diseño del SGSI

- Diseñar la Estrategia de seguridad de la información que será implantada en la Institución
- Integrar el Documento de definición del SGSI y el Programa de implantación del SGSI
- Presentar una propuesta para que se integren al programa de capacitación institucional, los cursos para difundir los conceptos e importancia de la Seguridad de la información, así como la estructura y alcances del SGSI
- Elaborar el Programa de evaluaciones del SGSI
- Elaborar, probar y mantener actualizada una Directriz rectora de respuesta a incidentes, en coordinación con el ERISC
- Elaborar el Programa de evaluaciones del SGSI y difundirlo en la Institución

Actividades del proceso

Gobierno

Dirección y control de la SI

Grupo de trabajo estratégico de seguridad de la información

Equipo de trabajo de infraestructuras críticas

Responsable de seguridad de la información en la Institución

Grupo de trabajo estratégico de seguridad de la información

ASI-4: Identificar las Infraestructuras críticas y los Activos clave

- Establecer el Equipo de trabajo de IC
- Identificar y listar los procesos críticos de la Institución en el Documento de IIC
- Identificar, a partir de los procesos críticos, aquéllos vinculados con la integridad, estabilidad y permanencia del Estado Mexicano
- Identificar las actividades críticas de los procesos contenidos en el Documento de IIC
- Identificar los Activos de información involucrados en los procesos de seguridad nacional
- Efectuar la valoración de los Activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad para identificar Activos de información clave

- Identificar la criticidad de una infraestructura, los tipos de impacto potencial que podrían ocurrir ante la presentación de un Incidente
- Representarlos en las matrices de impacto del documento Matrices de infraestructuras críticas y activos clave
- Determinar el nivel de criticidad de cada infraestructura, mediante la identificación de su Interdependencia y el nivel de Impacto que tenga con cada una de las infraestructuras con las que se relacione
- Elaborar el Catálogo de IC, con base en la información contenida en el Documento de identificación de IC y en el de Matrices de IC y activos clave
- Presentar a la aprobación del Titular de la Institución, el Catálogo de IC's

ASI-5: Establecer la Directriz rectora para la administración de riesgos

Responsable de seguridad de la información en la Institución

- Elaborar y mantener actualizada la Directriz rectora para la administración de riesgos
- El Responsable de la Seguridad de la Información deberá autorizar la Directriz rectora para la administración de riesgos
- Difundir la Directriz rectora para la administración de riesgos y sus actualizaciones a los involucrados y a los integrantes del Grupo de trabajo para la dirección de TIC
- Establecer el Repositorio de riesgos e integrar la información de la Directriz rectora para la administración de riesgos

Actividades del proceso

Grupo de trabajo estratégico de seguridad de la información

Equipo de trabajo de análisis de riesgos

Gobierno

Dirección y control de la SI

ASI-6: Elaborar el Análisis de riesgos

- Integrar el Equipo de trabajo de AR y seleccionar a su líder
- Integrar la información anterior al Documento de Integración del equipo de trabajo de AR
- Elaborar el Documento de identificación de procesos críticos, integrando aquellos procesos de los que la Institución depende para alcanzar sus objetivos y niveles de servicio comprometidos, así como procesos críticos vinculados con la seguridad nacional
- Identificar los Activos de información e incluirlos al Documento de identificación de activos de información
- Identificar y documentar las Vulnerabilidades y Amenazas sobre los Activos de Información

- Elaborar el Documento de identificación y evaluación de escenarios de riesgo
- Elaborar el Análisis de costo-beneficio de controles de seguridad
- Elaborar el Documento de resultados del AR
- Obtener del GESI, la aprobación del Documento de resultados del AR
- Seleccionar de los controles recomendados, aquéllos a implantar de acuerdo a las capacidades y recursos de las áreas involucradas
- Justificar los controles no seleccionados
- Elaborar el Programa de implantación para el manejo de riesgos

- Obtener del GESI la aprobación del Programa de implantación para el manejo de riesgos y verificar su adecuada integración con las demás actividades de implantación o mejora de los controles del SGSI
- Cuidar que el análisis de riesgos se realice o actualice conforme a los factores críticos de esta actividad, una vez al año, o en caso de un cambio en los procesos, Activos de Información o cuando se detecte una nueva Amenaza o Vulnerabilidad a la seguridad de la información y/o los Activos de TIC que la soportan
- Asegurar que se obtengan y actualicen los productos de la actividad y se documente, en su caso, la mejora continua que se efectúe derivada del factor crítico anterior
- Vigilar que se actualice el Repositorio de riesgos

Actividades del proceso

Gobierno

Dirección y control de la SI

Grupo de trabajo estratégico de seguridad de la información

ASI-7: Integrar al SGSI los controles mínimos de Seguridad de la información

- Definir los controles de seguridad necesarios para salvaguardar a los Activos de TIC, las Infraestructuras críticas y los Activos de información de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para: la designación de personal en áreas relacionadas con el manejo y gestión de los Activos de información de la Institución, la instalación y configuración de software, el ingreso y salida de Activos de información, el borrado seguro de dispositivos de almacenamiento, entre otros
- Documentar los controles determinados en el Documento de definición del SGSI y elaborar con los responsables de los procesos institucionales el Programa de implantación del SGSI

Grupo de trabajo estratégico de seguridad de la información

ASI-8: Mejorar el SGSI

- Constatar con las áreas y unidades administrativas involucradas, que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica de la Institución se apliquen y hacer del conocimiento del Titular de la misma el cumplimiento de los controles de seguridad establecidos
- Obtener, del Informe de evaluación del SGSI, los datos sobre su desempeño, a fin de definir y documentar las acciones correctivas y preventivas para ajustar el mismo, e integrarlas al documento Acciones preventivas y correctivas al SGSI
- Elaborar el Documento de implantación de la mejora al SGSI y utilizarlo para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas

- Comunicar las mejoras que deberán aplicarse al SGSI al Responsable del grupo de trabajo para la implantación de la seguridad de la información, previsto en la actividad OPEC-1, por medio de los productos: Acciones preventivas y correctivas al SGSI y el Documento de implantación al SGSI
- Vigilar la implantación de las mejoras mediante el Informe de seguimiento a las acciones de mejora al SGSI

Productos

Gobierno

Dirección y control de la SI

- "Documento de integración y operación del grupo de trabajo estratégico de seguridad de la información"
- "Directriz rectora para la administración de riesgos
- "Documento de integración del equipo de trabajo de infraestructuras críticas"
- "Documento de identificación de infraestructuras críticas"
- "Matrices de infraestructuras críticas y activos clave"
- "Catálogo de infraestructuras críticas"

Productos

Gobierno

Dirección y control de la SI

- “Documento de integración del equipo de trabajo de análisis de riesgos”
- “Documento de identificación de procesos críticos”
- “Documento de identificación de activos de Información”
- “Documento de identificación de amenazas”, formato sugerido
- “Documento de identificación y evaluación de escenarios de riesgo”
- “Documento de análisis de costo-beneficio de controles de seguridad”
- “Declaraciones de aplicabilidad”
- “Programas de mitigación de riesgos”
- “Programa de contingencia a los riesgos”
- “Documento de resultados del análisis de riesgos”
- “Programa de implantación para el manejo de riesgos

Productos

Gobierno

Dirección y control de la SI

- "Documento de definición del SGSI"
- "Programa de implantación del SGSI"
- "Programa de evaluaciones del SGSI"
- "Directriz rectora de respuesta a incidentes"
- "Informe de evaluación del SGSI"
- "Acciones preventivas y correctivas de mejora al SGSI"
- "Informe de seguimiento a las acciones de mejora al SGSI"
- "Documento de implantación de la mejora al SGSI"

Indicadores

Gobierno

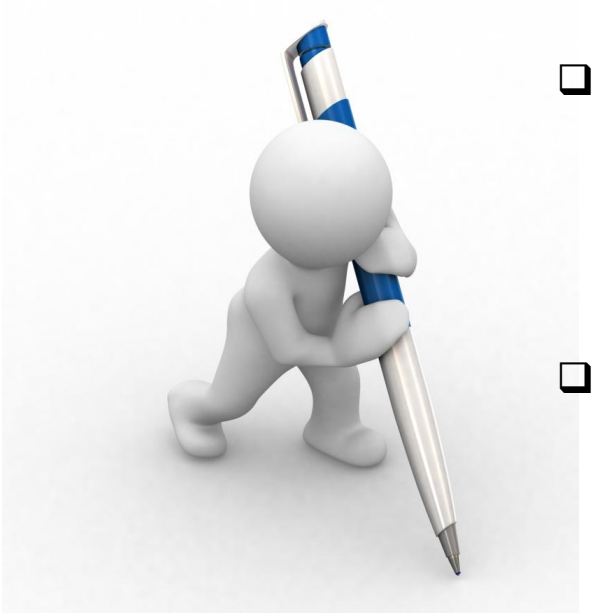
Dirección y control de la SI

Indicador	Fórmula	Periodicidad
Cumplimiento del proceso ASI- Administración de la seguridad de la información	% eficacia= (Controles implantados / Controles programados para su implantación) X 100	Anual

Reglas del proceso

Gobierno

Dirección y control de la SI



- El Responsable de la seguridad de la información en la Institución es el responsable de este proceso.
- En los casos en que el Titular de la Institución tenga un nivel jerárquico equivalente o inferior a Director General, el servidor público que éste designe como Responsable de la seguridad de la información en la Institución deberá tener un nivel inmediato inferior al del Titular.
- El Responsable de este proceso se deberá asegurar de que las acciones y productos que sean resultado de su ejecución, sean consecuentes con lo previsto en el Acuerdo por el que se emiten las *Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno*, en lo relativo a la Administración de Riesgos y Seguridad de la información, y de que los mismos se comuniquen al Coordinador de Control Interno de la Institución que se designe conforme a lo establecido en dicho ordenamiento.

Reglas del proceso

Gobierno

Dirección y control de la SI

- En caso de que la Institución cuente con Infraestructuras críticas que impactan a la Seguridad nacional, el Responsable de la seguridad de la información se asegurará de que el Análisis de riesgos previsto en este proceso se enfoque a éstas; y en caso contrario que dicho análisis se oriente a sus Activos de información clave.

- El Responsable de este proceso deberá establecer el Equipo de respuesta a incidentes de seguridad de TIC (ERISC) y definir los roles y responsabilidades de sus integrantes, así como asegurase de que éstos conozcan las reglas de operación del mismo, así como la Guía técnica de atención a incidentes.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Responsable de la seguridad de la información de cada Institución será quien mantendrá comunicación con el Centro de Investigación y Seguridad Nacional para la atención de cualquier Incidente de seguridad de la información que implique una amenaza a la seguridad nacional; y designará un enlace para que se coordine con los ERISC de las demás Instituciones en la atención de otros incidentes que así lo requieran.

- El Responsable de la seguridad de la información de las Instituciones que tengan el carácter de Instancia de seguridad nacional, deberá coordinarse con las diversas Instancias de seguridad nacional involucradas cuando se presente un Incidente de seguridad que supere su capacidad de respuesta.

- El Grupo de trabajo estratégico de seguridad de la información deberá asegurarse de que se integre al SGSI un control de seguridad para evitar intrusiones a la Infraestructura de TIC, incluyendo ataques externos vía Internet, Intranet o Extranet.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Grupo de trabajo estratégico de seguridad de la información deberá asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de Vulnerabilidades.

- El Responsable de este proceso deberá hacer del conocimiento de las autoridades competentes, los intentos de violación a los controles de seguridad y los incidentes de seguridad, incluido el acceso no autorizado a la infraestructura y servicios de TIC y a la información contenida en éstos, para que se determinen, en su caso, las responsabilidades que correspondan conforme a las disposiciones jurídicas aplicables.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Grupo de trabajo estratégico de seguridad de la información deberá constatar que los controles de seguridad que se hayan establecido para el Repositorio de configuraciones, se implementen de igual manera, para activos y elementos de configuración de los ambientes de desarrollo, pruebas y preproducción.

- El Grupo de trabajo estratégico de seguridad de la información deberá coordinarse con los Responsables de los grupos de procesos PR, AD y TE, para que se implanten controles de seguridad que impidan que el código de las soluciones tecnológicas, sus componentes y productos, y demás elementos relacionados, se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Grupo de trabajo estratégico de seguridad de la información deberá coordinarse con los Responsables de los grupos de procesos PR y AD, para que se implanten controles de seguridad orientados a que las herramientas para el desarrollo de las soluciones tecnológicas, sus componentes y productos, únicamente estén disponibles para los involucrados en su desarrollo y a la conclusión de éste, tales herramientas sean borradas de modo seguro de cualquier equipo del ambiente de trabajo.

- El Grupo de trabajo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implante un control para elaboración y conservación de Bitácoras de seguridad para los sistemas identificados como parte de una Infraestructura crítica, en éstas se registrará el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras tendrán un tiempo mínimo de almacenamiento de un año.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Grupo de trabajo estratégico de seguridad de la información de Instituciones que tengan el carácter de Instancia de seguridad nacional, deberá recomendar que en los procedimientos de contratación de soluciones tecnológicas o servicios de TIC prevista, se incluyan los requerimientos de continuidad de la operación, niveles de servicio y tiempos de respuesta a interrupciones, en concordancia con la criticidad de los procesos institucionales que los bienes o servicios objeto de las contrataciones soportarán.

Objetivo general

Gobierno

Dirección y control de la SI

- *Implantar y operar los controles de seguridad de la información de acuerdo al Programa de implantación del SGSI, así como los correspondientes a la capacidad de respuesta a Incidentes.*

Objetivos específicos

Gobierno

Dirección y control de la SI

1. Implantar y operar los controles de seguridad de la información.
2. Definir y aplicar la planeación para la mitigación de riesgos por incidentes.
3. Implantar las mejoras recibidas del proceso ASI- Administración de la seguridad de la información, para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la Información en operación.

Definiciones...

Gobierno

Dirección y control de la SI

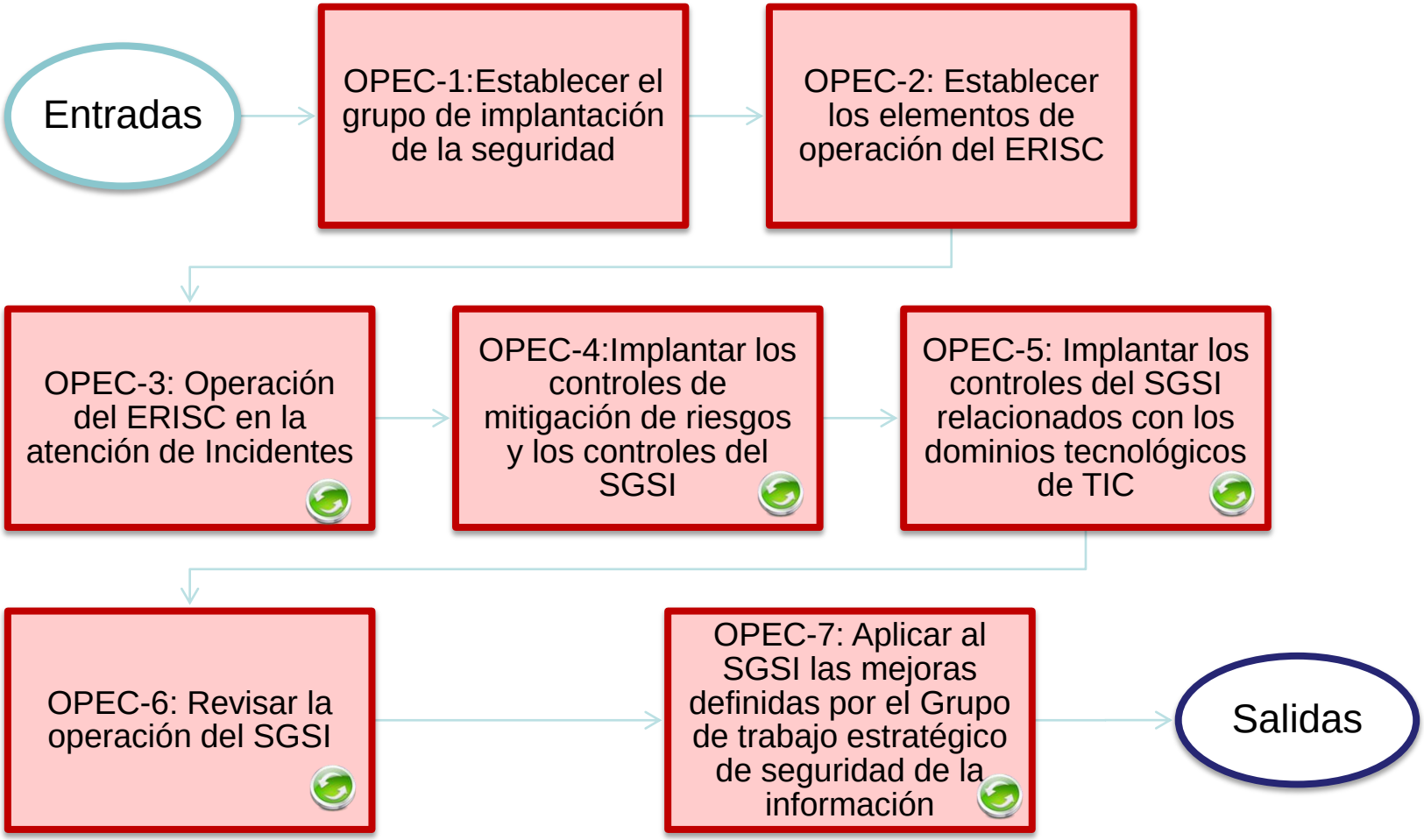
- **Activo de información clave:** El Activo de información que resulta esencial o estratégico para la operación y/o el control de una Infraestructura crítica o incluso de una que no tenga este carácter, pero cuya destrucción, perdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.

- **Infraestructuras críticas:** Las instalaciones, redes, servicios y equipos asociados o vinculados con Activos de TIC o Activos de Información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Actividades del proceso

Gobierno

Dirección y control de la SI



Proceso OPEC

Factores críticos

Gobierno

Dirección y control de la SI

OPEC-1: Establecer el grupo de implantación de la seguridad

Responsable del grupo de trabajo para la implantación de la seguridad de la información

Responsable de la seguridad de la información

- Establecer el Grupo de trabajo para la implantación de la seguridad de la información, mediante el Documento de integración del mismo
- Asegurarse de que se comunique a los involucrados, el establecimiento del grupo de trabajo
- Mantener actualizada la información del Repositorio de riesgos, con la siguiente información: la Directriz rectora para la administración de riesgos y el Programa de implantación para el manejo de riesgos y el Programa de implantación del SGSI, así como su avance

OPEC-2: Establecer los elementos de operación del ERISC

Responsable de la seguridad de la información

ERISC

- Establecer las Reglas de operación del ERISC, previendo los mecanismos de coordinación del ERISC al interior de la Institución o con otros ERISC o entidades externas, en concordancia con la Directriz rectora de respuesta a incidentes
- El ERISC deberá elaborar, de acuerdo a la Directriz rectora de respuesta a incidentes, la Guía técnica de atención a incidentes, de acuerdo a la criticidad de los Activos de TIC afectados, considerando; la detección, priorización, investigación técnica, erradicación, etc., de los incidentes
- Establecer el mecanismo de registro de los Incidentes de seguridad de la información, que incluya un repositorio
- Reportar al Responsable de la seguridad de la información, los Incidentes de seguridad de la información que se presenten

OPEC-3: Operación del ERISC en la atención de Incidentes

Responsable del grupo de trabajo para la implantación de la seguridad de la información

ERISC

- Definir las acciones de atención a los incidentes con apoyo de la Guía técnica, respecto del Incidente que se haya presentado
- Ejecutar la solución necesaria
- Registrar los datos del Incidente y su solución
- Asegurar que se comunique el Incidente y su solución, al Grupo de trabajo estratégico de seguridad de la información y a los Responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados
- Integrar los datos del Incidente y su solución a los repositorios de la UTIC y, en su caso, a los repositorios de la Institución que determine el Grupo de trabajo estratégico de seguridad de la información

Proceso OPEC

SFP SECRETARÍA DE LA FUNCIÓN PÚBLICA

Factores críticos

Responsable del grupo de trabajo para la implantación de la seguridad de la información

Grupo de trabajo para la implantación de la seguridad de la información

Responsable del proceso ADT

Responsable del grupo de trabajo para la implantación de la seguridad de la información

Gobierno

Dirección y control de la SI

OPEC-4: Implantar los controles de mitigación de riesgos y los controles del SGSI

- Ejecutar y actualizar (en su caso) el Programa de implantación para el manejo de riesgos y el Programa de implantación del SGSI, con apoyo de los titulares de las unidades administrativas en las cuales se implantarán los controles
- Elaborar el Informe de resultados de la implantación del SGSI
- Asegurar que los controles de seguridad se hayan implantado de acuerdo a lo previsto en el Documento de definición del SGSI y el Programa de implantación del SGSI
- Elaborar los informes de las desviaciones en la implantación y/o en la operación de los controles de seguridad

OPEC-5: Implantar los controles del SGSI relacionados con los dominios tecnológicos de TIC

- Asegurar que los controles de seguridad para los dominios tecnológicos de TIC se definan y aprueben por el Grupo de trabajo estratégico de seguridad de la información para su integración al SGSI, se efectúe su implantación y se operen de acuerdo a su definición
- Mantener los componentes de los dominios tecnológicos con el SW de seguridad y de administración y monitoreo, actualizado y en operación; incluyendo SW para evitar vulneraciones y accesos no autorizados
- Obtener de Titular de la UTIC, la aprobación de los controles definidos conforme a los factores críticos de esta actividad

OPEC-6: Revisar la operación del SGSI

- Verificar la eficiencia y eficacia de los controles implementados, de acuerdo al Programa de evaluaciones del SGSI
- Medir la efectividad de los controles de seguridad implantados
- Efectuar, con base en el Programa de evaluaciones del SGSI, la evaluación del SGSI
- Registrar la información de los intentos, exitosos y no exitosos, de violaciones e incidentes de seguridad, y efectuar el análisis y evaluación de dicha información
- Documentar las acciones de revisión del SGSI mediante el Informe de revisión del SGSI y enviarlo al Grupo de trabajo estratégico de SI

Factores críticos

Gobierno

Dirección y control de la SI

Grupo de trabajo para la implantación de la seguridad de la información

OPEC-7: Aplicar al SGSI las mejoras definidas por el Grupo de trabajo estratégico de seguridad de la información

Responsable del grupo de trabajo para la implantación de la seguridad de la información

- Aplicar las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el Grupo de trabajo estratégico de seguridad de la información
- Documentar el resultado de la aplicación de la mejora, para cada uno de los controles de seguridad de la información que resultaron impactados, incluyendo las mejoras del SGSI aplicadas
- Actualizar el Informe de seguimiento a las acciones de mejora al SGSI
- Verificar el contenido del Informe de seguimiento a las acciones de mejora al SGSI; actualizar el Programa de evaluaciones del SGSI y enviarlos al Grupo estratégico de seguridad de la información para su revisión

Productos

Gobierno

Dirección y control de la SI

- "Documento de integración del Grupo de trabajo para la implantación de la seguridad de la información"
- "Programa de implantación para el manejo de riesgos"
- "Documento de definición del SGSI"
- "Programa de implantación del SGSI"
- "Programa de evaluaciones del SGSI"
- "Directriz rectora de respuesta a incidentes"

Productos

Gobierno

Dirección y control de la SI

- “Informe de revisión del SGSI”
- “Informe de seguimiento a las acciones de mejora al SGSI”
- “Documento de implantación de la mejora al SGSI”
- “Repositorio de riesgos de TIC”

Indicadores

Gobierno

Dirección y control de la SI

Indicador	Fórmula	Periodicidad
Cumplimiento de la administración de riesgos	% de eficiencia= (Controles implantados / Controles programados para su implantación) X 100	Anual
Resultados del proceso OPEC− Operación de los controles de seguridad de la información y del ERISC	% de eficiencia = Número de Acciones de mejora a los controles implantados implantadas/ Número de acciones de mejora definidas) X 100	Anual

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Responsable del grupo de trabajo para la implantación de la seguridad de la información es el Responsable de este proceso.
- Los servidores de la UTIC y los Usuarios están obligados a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a lo previsto en el MAAGTICSI.
- El Responsable de este proceso se deberá asegurar de que las acciones y los productos obtenidos de la ejecución del presente proceso sean consecuentes con lo previsto en el Acuerdo por el que se emiten *las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno, en lo relativo a la Administración de Riesgos y la Seguridad de la Información*, y de que los mismos se comuniquen al Coordinador de Control Interno de la Institución que se designe conforme a lo establecido en dicho ordenamiento.

Reglas del proceso

Gobierno

Dirección y control de la SI

- El Responsable de este proceso, con apoyo de la totalidad de los Responsables de los procesos de la UTIC, deberá verificar que se implanten los controles que se definan en el SGSI, en los proyectos, procesos y servicios de TIC y de la UTIC a fin de garantizar la seguridad de la información de la Institución.
- Asimismo, deberá constatar que se conserve la evidencia de la implantación de dichos controles.

Agradecemos su atención

Secretaría de Marina
Centro de Estudios Superiores Navales

Ciudad de México,
abril - mayo de 2012