






**MANUAL ADMINISTRATIVO DE APLICACIÓN
GENERAL EN LAS MATERIAS DE
TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES Y DE SEGURIDAD DE LA
INFORMACIÓN DEL INSTITUTO NACIONAL DE
GERIATRIA**

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 2 de 7
	Departamento de Informática		




Nombre del instrumento:	MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN LAS MATERIAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE GERIATRÍA.
Unidad Administrativa:	INSTITUTO NACIONAL DE GERIATRÍA
Aprobó	
<hr style="width: 30%; margin: auto;"/> Dr. Luis Miguel Gutiérrez Robledo Director General	
Revisó	
<hr style="width: 30%; margin: auto;"/> Lic. Erika Plata Córdoba Subdirectora de Administración	
Elaboró	
<hr style="width: 30%; margin: auto;"/> Lic. Eduardo Ángeles Velázquez Jefe de Departamento de Informática	

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 7
	Departamento de Informática		




CONTENIDO

INDICE




OBJETIVOS.	1
General	
Específicos	
ÁMBITO DE APLICACIÓN.	1
MARCO JURÍDICO.	1
DEFINICIONES.	3
REGLAS GENERALES.	7
PROCESOS EN LAS MATERIAS DE TIC Y DE SEGURIDAD DE LA INFORMACIÓN.	9
I. PROCESOS DE GOBERNANZA.	10
I.A Proceso de Planeación Estratégica (PE).	10
Objetivo General	
Objetivos Específicos	
Reglas del proceso	
Roles del proceso	
Actividades del proceso	
PE 1 Establecer la gobernabilidad de las operaciones de la UTIC.	11
Factores Críticos	
PE 2 Integrar la información de la Cartera Ejecutiva de Proyectos de TIC.	11
Factores Críticos	
PE 3 Validar, aprobar, comunicar y adecuar, de ser necesario, la Cartera Ejecutiva de Proyectos de TIC.	12
Factores Críticos	
PE 4 Dar seguimiento a la planeación estratégica de TIC.	13
Factores Críticos	
Relación de Productos del proceso	
Indicador del proceso	

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 4 de 7
	Departamento de Informática		




I.B Proceso de Administración del Presupuesto y las Contrataciones (APCT). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	13
APCT 1 Participar en el establecimiento de prioridades del presupuesto de TIC. Factores Críticos	15
APCT 2 Establecer el listado de bienes y servicios de TIC a contratar por la UTIC en cada ejercicio fiscal. Factores Críticos	16
APCT 3 Estudios de Factibilidad. Factores Críticos	16
APCT 4 Participar como área técnica, en los procedimientos de contratación de TIC. Factores Críticos Relación de Productos del proceso Indicador del proceso	17
II. PROCESOS DE ORGANIZACIÓN.	18
II.A Proceso de Administración de Servicios (ADS). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	18
ADS 1 Mantener actualizado el catálogo de servicios de TIC. Factores Críticos	20
ADS 2 Diseñar los servicios de TIC. Factores Críticos	21
ADS 3 Administrar la capacidad de la infraestructura de TIC. Factores Críticos	22
ADS 4 Administrar la continuidad de servicios de TIC. Factores Críticos Relación de Productos del proceso Indicador del proceso	23

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 5 de 7
	Departamento de Informática		




II.B Proceso de Administración de la Configuración (ACNF).	24
Objetivo General	
Objetivos Específicos	
Reglas del proceso	
Roles del proceso	
Actividades del proceso	
ACNF 1 Establecer la cobertura y el alcance de la administración de la configuración.	25
Factores Críticos	
ACNF 2 Definir la estructura del repositorio de configuraciones.	25
Factores Críticos	
ACNF 3 Registrar los elementos de configuración en el repositorio de configuraciones	27
Factores Críticos	
Relación de Productos del proceso	
Indicador del proceso	
II.C Proceso de Administración de la Seguridad de la Información (ASI).	27
Objetivo General	
Objetivos Específicos	
Reglas del proceso	
Roles del proceso	
Actividades del proceso	
ASI 1 Establecer un modelo de gobierno de seguridad de la información.	31
Factores Críticos	
ASI 2 Operar y mantener el modelo de gobierno de seguridad de la información.	31
Factores Críticos	
ASI 3 Diseño del SGSI.	32
Factores Críticos	
ASI 4 Identificar las infraestructuras críticas y los activos clave.	34
Factores Críticos	
ASI 5 Elaborar el análisis de riesgos.	36
Factores Críticos	
ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.	39
Factores Críticos	

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 6 de 7
	Departamento de Informática		

ASI 7 Mejorar el SGSI. Factores Críticos Relación de Productos del proceso Indicador del proceso	41
III. PROCESOS DE ENTREGA.	43
III.A Proceso de Administración de Proyectos (ADP). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	43
ADP 1 Establecer directrices para la gobernabilidad y evaluación del portafolio de proyectos de TIC. Factores Críticos	44
ADP 2 Priorizar, equilibrar y autorizar la Cartera Operativa de Proyectos de TIC.	44
ADP 3 Administrar y monitorear la Cartera Operativa de Proyectos de TIC. Factores Críticos	45
ADP 4 Cerrar iniciativas y proyectos de TIC. Factores Críticos Relación de Productos del proceso Indicador del proceso	46
III.B Proceso de Administración de Proveedores (APRO). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	46
APRO 1 Generar lista de verificación de obligaciones. Factores Críticos	47
APRO 2 Monitorear el avance y desempeño del proveedor. Factores Críticos	48
APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos. Factores Críticos Relación de Productos del proceso Indicador del proceso	48

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 7 de 7
	Departamento de Informática		

III.C Proceso de Administración de la Operación (AOP). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	49
AOP 1 Establecer el mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC. Factores Críticos	50
AOP 2 Programar y ejecutar las tareas de la operación de los sistemas, aplicaciones y servicios de TIC. Factores Críticos	51
AOP 3 Monitorear la infraestructura de TIC en operación. Factores Críticos	52
AOP 4 Implementar y verificar que se cumplan los controles de seguridad física en el centro de datos. Factores Críticos Relación de Productos del proceso Indicador del proceso	52
III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC). Objetivo General Objetivos Específicos Reglas del proceso Roles del proceso Actividades del proceso	53
OPEC 1 Designar un responsable de la supervisión de la implementación de los controles de seguridad definidos en el SGSI y en el análisis de riesgos. Factores Críticos	54
OPEC 2 Establecer los elementos de operación del ERISC. Factores Críticos	54
OPEC 3 Operación del ERISC en la atención de incidentes. Factores Críticos Relación de Productos del proceso Indicador del proceso	55

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 1 de 56
	Departamento de Informática		

OBJETIVOS

Objetivo General:

Definir los procesos en las materias de TIC y de seguridad de la información, con los que el Instituto Nacional de Geriátría deberá regular su operación.

Objetivos Específicos:

1. Enfocar el monitoreo y control sobre las actividades vinculadas con las TIC, en un esquema de gobernanza, organización y entrega.
2. Fortalecer el control sobre los recursos de TIC y mantener alineada la planeación estratégica del Instituto, al Programa, a la EDN, las Bases de Colaboración celebradas por el Instituto y a las disposiciones que de estos instrumentos emanen.
3. Mantener indicadores orientados a resultados basados en el ejercicio del presupuesto y en la entrega de servicios de valor.

ÁMBITO DE APLICACIÓN




El presente manual es de aplicación general para el Instituto Nacional de Geriátría.

El lenguaje empleado en el manual no busca generar ninguna clase de discriminación, ni marcar diferencias entre hombres y mujeres, por lo que las referencias o alusiones hechas al género masculino representan siempre a todos o todas, hombres y mujeres, abarcando claramente ambos sexos.



MARCO JURÍDICO

Los ordenamientos jurídicos referidos en este apartado, se citan de manera enunciativa y no limitativa.

1. Constitución Política de los Estados Unidos Mexicanos.
2. Código Penal Federal.
3. Ley Orgánica de la Administración Pública Federal.
4. Ley Orgánica de la Procuraduría General de la República.
5. Ley General de Bienes Nacionales.
6. Ley Federal de las Entidades Paraestatales.
7. Ley Federal de Presupuesto y Responsabilidad Hacendaria.
8. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

9. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
10. Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
11. Ley Federal de Telecomunicaciones.
12. Ley Federal sobre Metrología y Normalización.
13. Ley Federal de Archivos.
14. Ley de Seguridad Nacional.
15. Ley de Firma Electrónica Avanzada.
16. Ley del Sistema de Horario en los Estados Unidos Mexicanos.
17. Reglamento de la Oficina de la Presidencia de la República.
18. Reglamento Interior de la Secretaría de Gobernación.
19. Reglamento Interior de la Secretaría de la Función Pública.
20. Reglamento de Ley Federal de las Entidades Paraestatales.
21. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
22. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
23. Reglamento de la Ley de Firma Electrónica Avanzada.
24. Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional.
25. Plan Nacional de Desarrollo 2013-2018.
26. Programa para un Gobierno Cercano y Moderno 2013-2018.
27. Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
28. Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
29. Lineamientos de Protección de Datos Personales, expedidos por el entonces Instituto Federal de Acceso a la Información Pública.
30. Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales, emitidos por el entonces Instituto Federal de Acceso a la Información Pública.
31. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.
32. Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.
33. Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.
34. Documento Técnico para la Interoperabilidad de los Sistemas Automatizados de Control de Gestión.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

DEFINICIONES

Para efectos de este manual, se entenderá por:

Términos:

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

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para el Instituto, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Activo de soporte: El que apoya o complementa a un activo primario en su función.

Activo primario: El activo de información asociado a las funciones sustantivas del Instituto.




Activos de proceso: Los elementos de información que son parte de un proceso y que reflejan características específicas del mismo.

Activos de TIC: los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (Service Level Agreement, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (Operational Level Agreement por sus siglas en inglés).

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información del Instituto.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Aplicativo de Cómputo: el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos;

Área contratante: A la facultada en el Instituto para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.



Área requirente: A la que, en el Instituto, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquélla que los utilizará.

Área solicitante o usuaria: A la que, en el Instituto, efectúa originalmente la petición a la UTIC para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en el Instituto, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura Empresarial: la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnología de la información y comunicaciones;

Arquitectura Orientada a Servicios: la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC del Instituto.

Bases de Colaboración: los instrumentos consensuales celebrados por el Instituto para establecer acciones que modernicen y mejoren la prestación de los servicios públicos, promuevan la productividad en el desempeño de sus funciones y reduzcan gastos de operación, a fin de incrementar la eficiencia y eficacia y cumplir con los objetivos previstos en el Programa y formalizar los compromisos, así como sus respectivos indicadores de desempeño;

Bitácora de seguridad: El registro continuo de eventos e incidentes de seguridad de la información que ocurren a los activos de información.

Borrado Seguro: el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;

Cambios administrados: La integración controlada, eficiente, segura y oportuna de componentes y/o activos de TIC, aplicativos de cómputo, soluciones tecnológicas o servicio de TIC, que modifican el ambiente operativo de la UTIC; mediante criterios técnicos y mecanismos para la planeación y ejecución de dichos cambios, a fin de que éstos sean efectuados satisfactoriamente sin exponer el ambiente operativo y la operación de los servicios de TIC.

Centro de Datos: el lugar físico en los que se ubiquen los activos de TIC y desde el que se provén servicios de TIC; IX. CNTSE: el Catálogo Nacional de Trámites y Servicios del Estado, al que se alude en el Programa;




Centro: el Centro de Investigación y Seguridad Nacional, órgano desconcentrado de la Secretaría de Gobernación;

Cómputo en la Nube: al modelo de prestación de servicios digitales que permite al Instituto acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;

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

Declaraciones de aplicabilidad: El documento que contiene los controles aplicados mediante el SGSI de el Instituto como resultado del análisis de riesgos.

Decreto: el Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

público, así como para la modernización de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 10 de diciembre de 2012;

Directriz rectora: El documento estratégico en el que se establecen principios tecnológicos de alto nivel.

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;

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

Documento de planeación del proyecto: El documento que contiene la definición de un proyecto, el control de su avance, así como sus documentos de planeación subsidiarios y documentación complementaria.

Documentos de planeación subsidiarios: Los documentos de planeación del proyecto que se deben instrumentar cuando un proyecto es autorizado, entre otros: plan de administración de riesgos, plan de recursos, plan de presupuestos y plan de comunicación, los cuales se incorporan al documento de planeación del proyecto.

Dominio Tecnológico: las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica del Instituto, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;




EDN: la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;

EIDA: el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

ERISC: equipo de respuesta a incidentes de seguridad en TIC en el Instituto;

Esquema de Tiempo y Materiales: los servicios en que el proveedor asigna, durante un periodo, un determinado número de recursos humanos, que cumplirán actividades definidas mediante un contrato;

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

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

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones para el control y minimización de los riesgos que afecten a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información del Instituto.

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

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información del Instituto, incluido el acceso no autorizado o no programado a éstos.

Infraestructura de TIC: el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;

Infraestructuras Críticas de Información: Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia.




Infraestructuras de Información esenciales: Las redes, servicios, equipos e instalaciones asociados o vinculados con activos de información, TIC y TO, cuya afectación, interrupción o destrucción tendría un impacto mayor en la operación del Instituto.

Iniciativas de TIC: la conceptualización o visualización temprana de una oportunidad para ofrecer un aplicativo de cómputo, solución tecnológica o servicio de TIC o una solución tecnológica en beneficio del Instituto, las cuales podrán o no concretarse en uno o más proyectos de TIC;

Instituto: al Instituto Nacional de Geriátría

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso.

Interdependencia: La interconexión estrecha que existe entre las infraestructuras de información esenciales, y que conlleva a que la falla o falta de una de ellas impacte negativamente en otras, presentándose como consecuencia un efecto cascada de fallas en la prestación de servicios.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Interoperabilidad: La capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnologías de la información y comunicaciones.

Lineamientos: los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;

MAAGMAASSP: el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;

MAAGTICSI: Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información del Instituto Nacional de Geriátria

Manual General: el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información, Anexo Único del presente Acuerdo;




Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en el Instituto.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la UTIC.

PETIC: el Plan Estratégico de Tecnologías de la Información y Comunicaciones que elabora el Instituto en los términos señalados en el Manual General;

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Programa de capacidad: El documento de planeación que contiene la información sobre la capacidad de la infraestructura de TIC considerando los escenarios de necesidades futuras y los acuerdos de niveles de servicio establecidos.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Programa de contingencia: El documento de planeación en el que se plantea la estrategia, el recurso humano en la UTIC, los activos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso crítico, en caso de presentarse un desastre o la materialización de un riesgo.

Programa de continuidad: El documento de planeación que contiene los elementos y las acciones necesarios para asegurar que la operación de los servicios y procesos críticos de TIC del Instituto no se interrumpa.

Programa de disponibilidad: El documento de planeación que contiene los elementos y acciones necesarios para que los componentes de la infraestructura de TIC estén operando y sean accesibles.

Programa de proyectos: La integración de uno o más proyectos de TIC que pueden ser administrados en su conjunto para la obtención de beneficios adicionales a los que se lograrían de ser administrados individualmente durante su ejecución.

Programa de tecnología: El documento de planeación en el que se establecen las acciones estratégicas para la conformación de las arquitecturas de cada dominio tecnológico y de todos ellos en su conjunto, considerando los servicios de TIC existentes y proyectados.

Programa: el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;




Proyectos de TIC: el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC;

Recursos de TIC: La infraestructura, los activos, el recurso humano en la UTIC y el presupuesto de TIC.

Recursos humanos en la UTIC: Los servidores públicos adscritos a la UTIC, o inclusive los servidores públicos de otras áreas del Instituto o personal de terceros cuando participen en alguno de los procesos previstos en el manual y que hayan sido acreditados por algún servidor público facultado para llevar a cabo actividades específicas en dichos procesos.

Repositorio: El espacio en medio magnético u óptico en el que se almacena y mantiene la información digital.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras de información esenciales y/o críticas y activos de información del Instituto.

Seguridad de la información: la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Software de código abierto: El software cuya licencia asegura que el código pueda ser modificado y mejorado por cualquier persona o grupo de personas con las habilidades correctas, debido a que el conocimiento es de dominio público.

Tecnologías de Operación (TO): Hardware o software que detecta o genera un cambio a través del control y/o monitoreo de dispositivos físicos, procesos y eventos en las Instituciones.

Tecnologías Verdes: el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;



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.

Unidad administrativa solicitante: La unidad administrativa de el Instituto que solicita un aplicativo de cómputo o servicio de TIC y que es responsable de definir sus requerimientos, funcionalidades y niveles de servicio.




Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 3 de 56
	Departamento de Informática		

Vulnerabilidades: 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 las infraestructuras de información esenciales y/o críticas, así como a los activos de información.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 9 de 56
	Departamento de Informática		

Acrónimos:

CIDGE: La Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

DTISACG: El Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión emitido por la Secretaría de la Función Pública.

ERISC: El equipo de respuesta a incidentes de seguridad en TIC en la Institución.

SFP: La Secretaría de la Función Pública.




SGSI: El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.

UTIC: La unidad administrativa en la Institución responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas.

REGLAS GENERALES

Las reglas generales aplicables a los nueve procesos de este manual son las siguientes:

1. El titular de la UTIC es el responsable de asegurar que se cumplan las presentes reglas generales.
2. El responsable de cada proceso de este manual, debe asegurar que se cumplan las actividades, factores críticos y reglas que lo constituyan.
3. El titular de la UTIC es responsable de asegurar que la totalidad del personal adscrito a esa unidad administrativa conozca la EDN y el Programa, y que oriente a estos ordenamientos, sus actividades, y el ejercicio de sus atribuciones y facultades, de acuerdo a su competencia y la normatividad aplicable.
4. Los servidores públicos de la UTIC y los usuarios involucrados, al operar los procesos de este manual, deberán apegarse estrictamente a las políticas, líneas de acción, criterios y estándares que se establecen en la EDN, o que de ella emanen, al Programa y a las Bases de Colaboración que el Instituto haya celebrado.
5. Los servidores públicos de la UTIC, así como de las otras unidades administrativas del Instituto, serán responsables de las actividades que en los diversos procesos de la UTIC, les sean asignadas.
6. Los responsables de los procesos de este manual, deberán apegarse a lo que establece la Ley Federal sobre Metrología y Normalización, y hacer uso de las metodologías, mejores

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 9 de 56
	Departamento de Informática		

prácticas nacionales e internacionales listadas en la matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC, que se integran en el Apéndice IV.B de este manual.

7. Para determinar las erogaciones que como área requirente se pretendan realizar en cada ejercicio fiscal en materia de contratación de TIC, la UTIC deberá atender lo dispuesto en los numerales 4.1.1.1 a 4.1.1.6 del MAAGMAASSP, incluyendo la verificación de la existencia de contratos marco en materia de TIC.

8. Cuando se requiera llevar a cabo una contratación en materia de TIC, la UTIC, como área requirente, deberá llevar a cabo las actividades previstas en los numerales 4.2.1.1.1 a 4.2.1.1.9, 4.2.1.1.11 y 4.2.1.1.12, así como en su caso, el 4.2.1.1.10 del MAAGMAASSP.

Asimismo, en caso de identificar la existencia de un contrato marco cuyo objeto sea los bienes o servicios que se pretendan contratar, la UTIC lo indicará al área contratante del Instituto, para los efectos procedentes.



9. El titular de la UTIC deberá asegurar que se integre y mantenga actualizado el registro de los activos de información y recursos de TIC en la Herramienta Diagnóstico Inventario que para tal efecto ponga a disposición la Unidad, a través de su portal.

10. El Instituto deberá, con apego a los procesos del Manual, a las líneas de acción de la EDN y a las definiciones técnicas que de éstas emanen, instrumentar los servicios de TIC comunes en el Instituto, relativos a: monitoreo de activos de información y restauración de fallas; operación de la red de datos; telefonía; correo electrónico; autenticación de certificados digitales y de mensajes y validación de documentos con firma electrónica avanzada; procesamiento de la información; operación de aplicativos y mesa de servicios. Estos servicios deberán ser integrados al catálogo de servicios, de acuerdo a lo que establece el Proceso de Administración de Servicios (ADS).

11. El Instituto, a través de la UTIC, con apego a las líneas de acción de la EDN, deberá instrumentar, entre otros, los componentes y servicios transversales de acceso e interoperabilidad para habilitar los trámites y servicios digitalizados en www.gob.mx, así como aplicaciones únicas para la sustitución del uso de papel, y aquéllas para la administración de recursos institucionales.

12. La UTIC como área requirente deberá, previo a la solicitud que formule al área contratante del Instituto para llevar a cabo un procedimiento de contratación, cumplir las disposiciones relacionadas con la modernización de la Administración Pública Federal mediante el uso de TIC, que se establecen en los Lineamientos, atendiendo a las guías, criterios, procedimientos o instructivos que deriven de éste.

13. Los responsables del Proceso de Planeación Estratégica (PE) y del catálogo de servicios de TIC del Instituto, deberán mantener actualizados el inventario de aplicaciones del Instituto y su catálogo de servicios de TIC, poniendo este último a disposición de la Unidad.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 9 de 56
	Departamento de Informática		

14. El Instituto deberá integrar y mantener actualizado su catálogo de servicios de TIC, considerando al menos la información que se menciona en el Proceso Administración de Servicios (ADS) de este manual.

15. Los roles que se señalan en cada uno de los procesos de este manual, con excepción de los mencionados en el Proceso de Administración de la Seguridad de la Información (ASI) y el Proceso de Operación de los Controles de Seguridad de la Información y del ERISC (OPEC), deberán ser asignados por el titular de la UTIC de acuerdo a sus facultades y a la normatividad aplicable. En el caso de los procesos ASI y OPEC, los servidores públicos que tomarán cada rol serán designados por el responsable de la seguridad de la información institucional (RSII).

16. Los servidores públicos de la UTIC, así como los de otras unidades administrativas del Instituto, serán responsables, de acuerdo a los roles que les sean asignados, de las actividades que en los diversos procesos de este manual se señalen para dichos roles.




17. El titular de la UTIC deberá asegurarse de difundir las disposiciones de las Políticas para la EDN que se establecen en el Acuerdo por el que se expide el Manual General, y de que los responsables de cada proceso, así como la totalidad del personal de la UTIC, se apeguen a dichas disposiciones, dejando en todo momento evidencia de ello.

18. Los responsables de cada proceso se asegurarán, cuando utilicen formatos propios, que los productos de los procesos a su cargo, se elaboren, describan y documenten considerando al menos la información que se indica en los formatos del Apéndice IV.A de este manual, o utilizar éstos.

19. La evidencia derivada de la operación de los procesos de este manual, podrá ser presentada impresa o a través de sistemas o medios informáticos, siempre y cuando el responsable de los mismos documente el tipo de entrega de las evidencias.

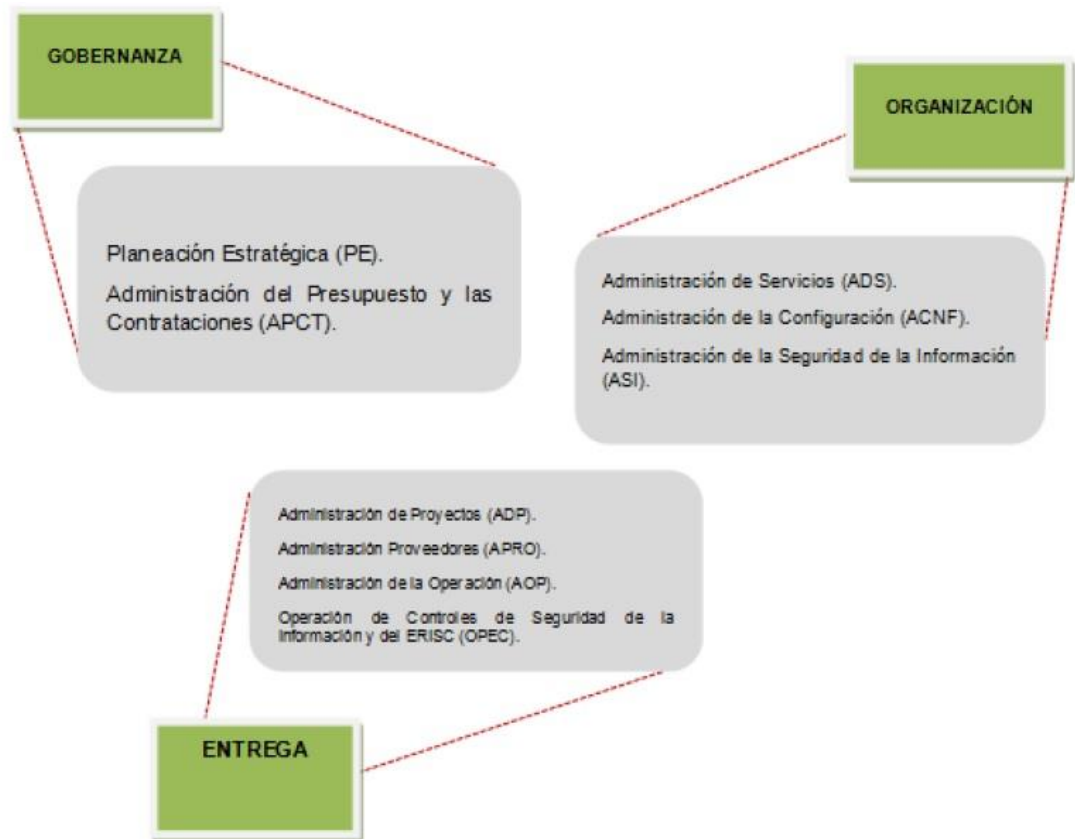
20. El titular de la UTIC deberá asegurarse, conjuntamente con las áreas solicitantes de los aplicativos de cómputo o servicios de TIC, que se incluyan en éstos, cuando así resulte necesario, como campos llave en los esquemas de datos, la Clave Única de Registro de Población (CURP) o la clave del Registro Federal de Contribuyentes (RFC), según corresponda.



21. La operación del presente manual estará sujeta a la disponibilidad de recursos humanos, materiales y financieros aprobados para el Instituto y la UTIC.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALVO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 9 de 56
	Departamento de Informática		

PROCESOS EN LAS MATERIAS DE TIC Y DE SEGURIDAD DE LA INFORMACIÓN

El manual contiene, en tres grupos, los procesos necesarios para propiciar la operación ágil y oportuna de las actividades de TIC del Instituto, conforme a lo siguiente:



	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 10 de 56
	Departamento de Informática		

I. PROCESOS DE GOBERNANZA

I.A. PROCESO DE PLANEACIÓN ESTRATÉGICA (PE)

Objetivo General:

Mantener la operación un modelo de gobierno de TIC en el Instituto, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos y vinculación ordenada con sus usuarios.

Objetivos Específicos:

1. Promover que los mandos medios y los titulares de las unidades administrativas del Instituto, coadyuven con la UTIC en la toma de decisiones para la dirección y control de las TIC, así como para la entrega efectiva y eficiente de los sistemas y servicios de TIC.

2. Prever que el Instituto cuente con una Cartera Ejecutiva de Proyectos TIC, con el objeto de establecer líneas de acción en materia de TIC y su seguimiento, alineadas a los objetivos institucionales, al Plan Nacional de Desarrollo 2013-2018, a los programas sectoriales y especiales que resulten aplicables, así como al Decreto, el Programa, las Bases de colaboración que haya celebrado el Instituto y las líneas de acción de la EDN.

Reglas del proceso:

1. El Titular de la UTIC es el responsable de la Planeación estratégica de TIC del Instituto. El titular de la UTIC podrá designar como corresponsable de la Planeación estratégica de TIC en el Instituto a un colaborador de un nivel inmediato inferior que le reporte directamente.




2. El Titular de la UTIC deberá asegurarse que la Cartera Ejecutiva de Proyectos de TIC del Instituto cumpla con las disposiciones del Acuerdo.

3. El Grupo de trabajo para la dirección de TIC deberá apoyar la implementación, operación y mejora del SGSI, así como las acciones que realice el Grupo estratégico de seguridad de la información.

4. El Responsable de este proceso deberá asegurarse que el PETIC se integre en el sistema que para tales efectos informe la Unidad, habiendo cubierto previamente las autorizaciones correspondientes al interior del Instituto, tal y como lo establece el presente proceso.

Roles del proceso:

1. Titular de la UTIC.
2. Responsable de la Planeación estratégica de la UTIC.
3. Grupo de trabajo para la dirección de TIC.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

Actividades del Proceso.

PE 1 Establecer la gobernabilidad de las operaciones de la UTIC.

Descripción: Establecer el grupo de trabajo para la dirección de TIC, que lleve el gobierno de TIC, tanto en la operación de los procesos de la UTIC y áreas vinculadas, como en la entrega de los servicios de TIC.

Factores Críticos:

El responsable de la planeación estratégica de la UTIC deberá:

1. Solicitar la intervención del titular del Instituto, o el de un inmediato inferior que el titular designe, para establecer el grupo de trabajo para la dirección de TIC, el cual deberá integrarse por personal con capacidad de toma de decisiones sobre los objetivos, metas y proyectos institucionales de TIC, y formalizarse mediante una acta la integración y forma de operación del grupo de trabajo para la dirección de TIC.
2. Definir, implementar y mantener una adecuada organización al interior de la UTIC, mediante la asignación de roles y responsabilidades para la gestión de los procesos de ésta, atendiendo a las necesidades de los procesos y proyectos de la UTIC.
3. Informar al titular del Instituto acerca de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección de TIC.

El grupo de trabajo para la dirección de TIC deberá efectuar, entre otras, las siguientes actividades:




1. Asegurar que el Instituto cuente con una Cartera Ejecutiva de Proyectos de TIC actualizada, conforme al Factor Crítico PE-2
2. Alinear las prioridades de la Cartera Ejecutiva de Proyectos de TIC con las prioridades institucionales, así como con los programas sectoriales y especiales que le competan.
3. Verificar que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución
4. Establecer la coordinación necesaria con el responsable de seguridad de la información en el Instituto para armonizar el gobierno de TIC, la administración de riesgos y el SGSI.

PE-2 Integrar la información de la Cartera Ejecutiva de Proyectos de TIC.

Descripción: Integrar la información de los proyectos que conformarán la Cartera Ejecutiva de Proyectos de TIC institucional, incluyendo su línea base y las fechas de ejecución de las principales actividades para su seguimiento.

Factores críticos:

El responsable de la planeación estratégica de la UTIC deberá:

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

1. Identificar y categorizar el conjunto de proyectos de TIC que integrarán la Cartera Ejecutiva de Proyectos de TIC, de la siguiente forma:
 - a) Proyectos Estratégicos de TIC (PETIC). Identificar un máximo de 7 proyectos de TIC que se consideren estratégicos, para conformar el PETIC, aplicando como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN;
 - b) Proyectos para contratación de bienes y servicios de TIC. Identificar los proyectos de TIC cuyo objetivo sea la contratación de bienes y servicios de TIC.

2. Los proyectos de TIC que no se consideren como estratégicos ni de contratación de bienes y servicios, no formarán parte de la Cartera Ejecutiva de Proyectos de TIC que se reportará a la Unidad, estos proyectos deberán gestionarse a través del proceso de Administración de Proyectos ADP.

3. Integrar, para cada uno de los proyectos de la Cartera Ejecutiva de Proyectos de TIC, la Ficha Técnica Base, que considere la fecha de inicio, fecha de término, presupuesto estimado y fechas estimadas de ejecución de las principales actividades (línea base), según lo establecido por la Herramienta de Gestión de la Política TIC.

4. Los proyectos que conformarán la Cartera Ejecutiva de Proyectos de TIC, deberán categorizarse de acuerdo a la siguiente lista:
 - a) Optimización. En donde por medio de la aplicación de TIC se logra una mejor manera de llevar a cabo actividades.
 - b) Digitalización. Aplicación de TIC para la conversión de contenidos a medios digitales en la generación de trámites y servicios por este medio, así como el acceso a información en este formato.
 - c) Simplificación. Aplicación de TIC para la reducción de tiempos, costos y requisitos en los trámites y servicios, así como en la eliminación o automatización de actividades en los procesos.
 - d) Racionalización. Reducción en el costo de los recursos e insumos obtenidos de mejores prácticas y estrategias en la contratación.




5. Integrar en el PETIC los objetivos institucionales, las metas nacionales, del Programa y de la EDN, así como los elementos de la arquitectura empresarial institucional que lo conformen.

PE-3 Validar, aprobar, comunicar y adecuar, de ser necesario, la Cartera Ejecutiva de Proyectos de TIC.

Descripción: Validar, aprobar, comunicar y adecuar, de ser necesario, la Cartera Ejecutiva de Proyectos de TIC

Factores críticos:

El titular de la UTIC, en la fecha que se determina en el Acuerdo, deberá:

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

1. Revisar y validar la Cartera Ejecutiva de Proyectos de TIC.
2. Presentar la Cartera Ejecutiva de Proyectos de TIC para la autorización del Director General del Instituto, o el de un inmediato inferior que el designe.
3. Registrar y enviar a la Unidad la Cartera Ejecutiva de Proyectos de TIC, una vez cumplido el factor crítico anterior, a través de la Herramienta de Gestión de la Política TIC.

El responsable de la planeación estratégica de la UTIC deberá:

1. Verificar que se obtenga la autorización de la Cartera Ejecutiva de Proyectos de TIC por parte de la Unidad, utilizando para ello el sistema web al que se alude en el factor crítico anterior.
2. Difundir la Cartera Ejecutiva de Proyectos de TIC a todos los involucrados para su cumplimiento en la UTIC y en el Instituto.

PE 4 Dar seguimiento a la planeación estratégica de TIC.

Descripción: Dar seguimiento a los avances de la Cartera Ejecutiva de Proyectos de TIC y reportarlos a la Unidad.

Factores críticos:

El responsable de la planeación estratégica de la UTIC deberá:

1. Dar seguimiento al avance de la Cartera Ejecutiva de Proyectos de TIC, y reportarlo trimestralmente a la Unidad, previa aprobación del titular de la UTIC.
2. Informar trimestralmente al grupo de trabajo para la dirección de TIC sobre el cumplimiento en el avance de los proyectos que conforman la Cartera Ejecutiva de Proyectos de TIC.




Relación de Productos del proceso:

1. "Acta de integración y forma de operación del grupo de trabajo para la dirección de TIC". Formato PE F1.
2. Cartera Ejecutiva de Proyectos de TIC en la Herramienta de Gestión de la Política TIC.

Indicador del proceso:

Nombre: Porcentaje de cumplimiento en la ejecución de los proyectos que integran la Cartera Ejecutiva de Proyectos de TIC.

Objetivo: Medir la eficiencia en la ejecución de los proyectos.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

Descripción: Obtener la eficiencia en la ejecución de los proyectos que integran la Cartera Ejecutiva de Proyectos de TIC, con respecto a la línea base establecida en la planeación de los mismos.

Fórmulas: Por cada uno de los proyectos en la Cartera Ejecutiva de Proyectos de TIC, se deberá realizar el siguiente cálculo:

% Eficiencia en la ejecución del proyecto = (avance real / avance estimado) * 100

Una vez realizado el cálculo de cada uno de los proyectos que integran la Cartera Ejecutiva de Proyectos de TIC, se deberá realizar el siguiente cálculo:

% de eficiencia en la ejecución de los proyectos que integran la Cartera Ejecutiva de Proyectos de TIC = Promedio de la eficiencia de cada proyecto que integra la Cartera Ejecutiva de Proyectos de TIC.

Responsable: El responsable de la Planeación Estratégica de TIC (PE).

Frecuencia de cálculo: Trimestral.




I.B. Proceso de Administración del Presupuesto y las Contrataciones (APCT)

Objetivo General:

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por el Instituto, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones en el Instituto, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.




Objetivos Específicos:

1. Elaborar el listado de bienes y servicios de TIC que la UTIC requiera contratar en cada ejercicio fiscal, considerando las directrices del Instituto, así como las disposiciones que en materia presupuestaria, de adquisiciones, arrendamientos y servicios resulten aplicables.
2. Proporcionar al área contratante, el apoyo y los elementos técnicos necesarios para llevar a cabo los procedimientos de contratación de TIC y participar en los mismos de acuerdo a su ámbito de atribuciones.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

Reglas del proceso:

1. El responsable del seguimiento del presupuesto autorizado, de los procedimientos de contratación de TIC y de los contratos celebrados en materia de TIC, deberá ser designado por el titular de la UTIC, y tener un nivel jerárquico inmediato inferior al de éste.
2. El responsable del proceso deberá asegurarse que éste se ejecute con apego a las disposiciones que en materia presupuestaria resulten aplicables, así como a los procesos de las unidades administrativas facultadas para administrar los recursos financieros y elaborar el anteproyecto anual de presupuesto del Instituto.
3. El responsable de este proceso deberá asegurarse que éste se efectúe con apego a las disposiciones en materia de adquisiciones y arrendamiento de bienes muebles y servicios, al Acuerdo por el que se expide el MAAGMAASSP, al Acuerdo y aquellas en materia presupuestaria, que resulten aplicables.
4. El titular de la UTIC, deberá designar a un representante con los conocimientos técnicos suficientes que permitan dar respuesta clara y precisa a las solicitudes de aclaración de los licitantes en las juntas de aclaraciones de los procedimientos de contratación a los que fuere convocada la UTIC como área técnica.
5. Cuando otras áreas o unidades administrativas del Instituto diversas a la UTIC, tengan asignados recursos financieros para la contratación de bienes o servicios de TIC necesarios para el cumplimiento de sus funciones, deberán contar previo al inicio del procedimiento de contratación de que se trate, con la aprobación por escrito de la UTIC, por medio de un dictamen técnico que será enviado al Órgano Interno de Control y a la Unidad para la aprobación del estudio de factibilidad.
6. En el supuesto a que se refiere la regla anterior, corresponderá al área o unidad administrativa de que se trate, fungir como área técnica, por lo que la UTIC deberá proporcionar el apoyo técnico que le sea requerido por ésta.
7. En aquellos casos en que se integren o adicionen componentes de software a un aplicativo de cómputo o a un servicio de TIC ya existente, el responsable del proceso se deberá asegurar de que se consideren las siguientes pruebas: integrales, de funcionalidad, estrés, volumen, aceptación del usuario y de seguridad, con el propósito de comprobar que la funcionalidad del aplicativo de cómputo o servicio de TIC existente se mantiene inalterada y que la relativa al componente integrado o adicionado es consistente.
8. El responsable de este proceso deberá verificar que cada vez que se suscriba un contrato para la adquisición, arrendamiento o servicios de TIC, éste sea registrado en el sistema electrónico de compras gubernamentales denominado CompraNet, con apego a la

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

normatividad aplicable, así como en la Herramienta de Gestión de la Política TIC, en un plazo no mayor a días 10 hábiles una vez firmado dicho contrato.

9. El titular de la UTIC será el responsable de firmar electrónicamente el Estudio de Factibilidad, dentro de la Herramienta de Gestión de la Política TIC, así como de su trámite ante la Unidad.

10. El titular de la UTIC deberá constatar que se revise el inventario de aplicaciones de la APF para determinar si existe, con el propósito de su reutilización, un aplicativo de cómputo de características similares a los requerimientos que la UTIC reciba o que se generen dentro de la misma. En el caso de que en la revisión se haya determinado la existencia de algún aplicativo de cómputo susceptible de ser reutilizado, deberá dar aviso a la Unidad y gestionar dicha reutilización ante la UTIC del Instituto responsable del aplicativo de cómputo de que se trate.

Roles del proceso:

1. Responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT).
2. Responsable del seguimiento del presupuesto autorizado de TIC.
3. Responsable del listado de bienes y servicios de TIC.

Actividades del Proceso.




APCT 1 Participar en el establecimiento de prioridades del presupuesto de TIC.

Descripción: Participar en la definición de los proyectos a los que se dará prioridad al asignar los recursos financieros destinados a las TIC.

Factores Críticos:

El responsable del seguimiento del presupuesto deberá:

1. Identificar los proyectos y servicios de TIC incluidos en los portafolios de proyectos y servicios de TIC, para los que sea necesaria una asignación presupuestaria.
2. Establecer escenarios para el adecuado ejercicio del presupuesto destinado a las TIC, indicando los gastos indispensables para garantizar la continuidad de la operación, los riesgos operativos y los correspondientes a los proyectos de TIC comprometidos.
3. Estimar los recursos presupuestarios de TIC, de acuerdo con los requerimientos previstos en los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica de la UTIC.
4. Entregar el presupuesto estimado de TIC del ejercicio siguiente, previa autorización del Titular de la UTIC, a la Unidad administrativa facultada y responsable de la integración del anteproyecto anual de presupuesto del Instituto.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

5. Gestionar ante la Subdirección de Administración del Instituto, la suficiencia presupuestal para sustentar la contratación de bienes y servicios de TIC que sean requeridos por la UTIC.

APCT 2 Establecer el listado de bienes y servicios de TIC a contratar por la UTIC en cada ejercicio fiscal.

Descripción: Elaborar la planeación de las contrataciones de bienes y servicios de TIC en cada ejercicio fiscal con base en su presupuesto autorizado y realizar las acciones de apoyo para las contrataciones de TIC.

Factores Críticos:

El responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT), con apoyo del responsable del listado de bienes y servicios de TIC deberán:

1. Elaborar un listado de bienes y servicios de TIC a contratar por la UTIC en el ejercicio fiscal en curso, que incluya el cronograma de las contrataciones de TIC previstas, respecto de la Cartera Ejecutiva de Proyectos de TIC y reportarlo a la Unidad a través de la Herramienta de Gestión de la Política TIC, para que en su caso se emitan sugerencias y comentarios.
2. Verificar, en conjunto con la Unidad, la posibilidad de llevar a cabo contrataciones consolidadas y de utilizar contratos marco u otras estrategias de contratación, a fin de proponerlas al área del Instituto encargada de integrar el programa anual de adquisiciones, arrendamientos y servicios.



APCT 3 Estudios de Factibilidad.

Descripción: Contar con los estudios de factibilidad de las contrataciones en Materia de TIC conforme a la normatividad aplicable.

Factores Críticos:

El responsable del seguimiento del presupuesto, con apoyo de los responsables de los procesos de la UTIC, deberá:

1. Asegurar que, para cada contratación que se prevea, se elabore el Estudio de Factibilidad, y se remita a la Unidad, a través de la Herramienta de Gestión de la Política TIC, según se establece en el Acuerdo, a fin de obtener el dictamen correspondiente.
2. En concordancia con el factor crítico anterior, proponer la estrategia de contratación para los proyectos de TIC autorizados, al área contratante de la Institución.
3. Definir acciones a fin de proveer al área contratante del Instituto con los elementos técnicos necesarios para llevar a cabo los procedimientos de contratación que correspondan.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

4. Verificar que la documentación soporte que deba entregarse al área contratante del Instituto se encuentre debidamente integrada, en términos de lo señalado en el numeral 4.2.1.1.8 del MAAGMAASSP, y particularmente que el anexo técnico que elabore la UTIC contenga las especificaciones y requerimientos técnicos del bien o servicio de TIC que se pretenda contratar, entre otros:




- a) Requerimientos funcionales.
- b) Requerimientos no funcionales, tales como: la disponibilidad del bien o servicio de TIC en función de las necesidades de la unidad administrativa solicitante, así como los controles de seguridad que deberán garantizarse respecto del bien o para la prestación del servicio de TIC de que se trate.
- c) Cuando corresponda, los casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas.
- d) Niveles de servicio.
- e) Términos y condiciones de entrega y de aceptación.
- f) Tiempos de respuesta de soporte y de servicio.
- g) La previsión para que, en su oportunidad, se incluya una cláusula al contrato que se celebre que asegure a la Institución que el proveedor y su personal no harán uso indebido de la documentación, información ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.
- h) La forma en que se llevará a cabo la supervisión del servicio contratado.

5. Integrar los requerimientos técnicos en materia de TIC para que se lleve a cabo la investigación de mercado correspondiente, para lo cual analizará la información enviada por la unidad administrativa solicitante y verificará que ésta contenga los criterios de calidad, de aceptación y los niveles de servicio esperados respecto de los bienes y servicios de TIC que se pretenden contratar.

6. Participar con el área contratante del Instituto, en caso de que no exista un área especializada, en la elaboración de la investigación de mercado, para lo cual podrá realizar entre otras actividades, las siguientes:

- a) Requerir, en su caso, a posibles proveedores, la información sobre los bienes y servicios de TIC que se pretenden contratar.
- b) Analizar las cotizaciones de los proveedores en cuanto a las características técnicas de los bienes o servicios que ofrecen y el monto en relación con el presupuesto autorizado para la contratación.

7. Apoyar al área contratante en la elaboración e integración del proyecto de convocatoria a la licitación pública o del proyecto de invitación a cuando menos tres personas.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALVO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

El responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT) deberá:

8. Mantener informados a los responsables del seguimiento al ejercicio del presupuesto autorizado para las contrataciones de TIC y en su caso, a la unidad administrativa solicitante, sobre los avances y conclusión de los procedimientos de contratación que se hayan llevado a cabo.

APCT 4 Participar como área técnica, en los procedimientos de contratación de TIC.
 Dar acompañamiento técnico, en su carácter de área técnica, en los procedimientos de contratación de TIC, mediante su participación en los actos en que se prevea su intervención.

Factores Críticos:

El servidor público de la UTIC que se designe como representante para el acompañamiento técnico deberá:

1. Participar en la junta o juntas de aclaraciones que se lleven a cabo, apoyando al área contratante a agrupar por temas técnicos las solicitudes de aclaración y resolver las dudas correspondientes, conforme a lo previsto en los numerales 4.2.2.1.9 y 4.2.2.1.10 del MAAGMAASSP.
2. Analizar y evaluar la propuesta técnica de las proposiciones que presenten los licitantes con el apoyo, en su caso, del área contratante.




Relación de Productos del proceso:

1. "Listado de bienes y servicios de TIC que la UTIC requiere se contraten", a través de la Herramienta de Gestión de la Política TIC.
2. "Anexo técnico" (formato de acuerdo a las necesidades del procedimiento de contratación y del bien o servicio que será objeto del procedimiento).
3. "Estudio de Factibilidad", definido en la Herramienta de Gestión de la Política TIC.

Indicador del proceso:

Nombre: Porcentaje de efectividad en la elaboración de Estudios de Factibilidad.

Objetivo: Evaluar la asertividad en la elaboración de los estudios de factibilidad realizados por la UTIC.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

Descripción: Conocer el nivel de efectividad en la elaboración de Estudios de factibilidad a partir de los presentados a la Unidad, con respecto a los resultantes como favorables.

Fórmula: % de eficiencia = (Número de estudios de factibilidad favorables/número de estudios de factibilidad presentados a la Unidad) X 100.

Responsable: Responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT).

Frecuencia de Cálculo: El resultado se mantiene actualizado siempre ya que se automatiza a través de la herramienta de gestión de política TIC.

II. PROCESOS DE ORGANIZACIÓN

II.A. PROCESO DE ADMINISTRACIÓN DE SERVICIOS (ADS).

Objetivo General:




Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento del Instituto, así como identificar iniciativas de servicios de TIC que aporten beneficios importantes en el cumplimiento de los objetivos estratégicos del Instituto, con apego a la EDN y efectuar su instrumentación.

Objetivos Específicos:

1. Diseñar y mantener actualizada la arquitectura empresarial de los servicios de TIC y definir las especificaciones técnicas para satisfacer las necesidades actuales y proyectadas de la Institución, considerando que se deben incluir las definiciones de los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC
2. Identificar y administrar riesgos, desde el diseño de los servicios de TIC, para que puedan ser eliminados, transferidos o mitigados y de ser el caso, aceptados.

Reglas del proceso:

1. El responsable de este proceso deberá ser designado por el titular de la UTIC, y tener un nivel jerárquico inmediato inferior al de éste.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 19 de 56
	Departamento de Informática		

2. El Responsable del proceso Administración de Servicios (ADS) deberá asegurarse que el hardware y el software de recuperación utilizado en la aplicación del programa de continuidad sea funcional, para restablecer, probar y renovar los respaldos al menos semestralmente.




3. El Responsable del proceso Administración de Servicios (ADS) deberá asegurarse que los servicios de TIC y las soluciones tecnológicas que provea la UTIC para oficios electrónicos al interior del Instituto y entre instituciones, cumplan con lo que se establece tanto en los Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, así como en los Documentos Técnicos de Interoperabilidad vigentes y los aplicables que expida la Subcomisión de Interoperabilidad de la CIDGE, derivados del Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.

4. El responsable del diseño de servicios de TIC, conjuntamente con el Responsable de la planeación estratégica de la UTIC, deberán asegurarse que el diseño de nuevas soluciones tecnológicas y servicios de TIC incluya, de ser el caso, aquellos datos que permitan cumplir con la normatividad técnica de domicilios geográficos que para dicho fin emite el **INEGI**.

5. El responsable del diseño de servicios de TIC, conjuntamente con el responsable de la planeación estratégica de la UTIC, deberán asegurarse que se cumpla, para el Cifrado de Datos, como mínimo con estándares tales como 3DES de triple llave, AES-128, AES-192 y AES-256, así como redes con protocolos seguros para su envío.

Roles del proceso:

1. Responsable del proceso Administración de Servicios (ADS) y administrador del catálogo de servicios de TIC.
2. Grupo de trabajo para la dirección de TIC.
3. Responsable del diseño de servicios de TIC.
4. El Responsable de la planeación estratégica de TIC.
5. Responsables de los servicios de TIC en operación.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

Actividades del Proceso.

ADS 1 Mantener actualizado el catálogo de servicios de TIC.




Descripción: Mantener actualizado el catálogo de servicios de TIC, así como el inventario de Arquitectura empresarial, a través de la Herramienta de Gestión de la Política TIC.

Factores Críticos:

El administrador del catálogo de servicios de TIC deberá:

1. Mantener actualizado el catálogo de servicios de TIC, a efecto de que contenga para cada servicio, cuando menos, la información siguiente:

- a) Descripción del servicio, resumida y detallada.
- b) Responsable técnico y en su caso, usuario del servicio (unidad administrativa).
- c) Arquitectura empresarial detallando sus componentes (procesos, aplicaciones e infraestructura tecnológica requerida).
- d) Disponibilidad del servicio (comprometida y real).
- e) Métricas e indicadores.
- f) Costo de operar el servicio.
- g) Garantía de cuando menos los siguientes servicios comunes (en desarrollo y existentes):
 - i. Operación de trámites y servicios a través de la Ventanilla Única Nacional;
 - ii. Mesa de servicios;
 - iii. Reportes estadísticos de la gestión de trámites y servicios;
 - iv. Servicios de apertura de información pública en formato abierto, de acuerdo a las directrices que en esta materia se expidan;
 - v. Servicios con estándares de observancia obligatoria como lo son aquéllos para la integración y publicación de información geoespacial, domicilios geográficos y articulación de padrones, entre otros;
 - vi. Autenticación de certificados digitales;
 - vii. Autenticación de mensajes y validación de documentos con firma digital;
 - viii. Módulo de firmado electrónico de documentos;
 - ix. Aplicaciones únicas de sustitución de uso de papel y generación de oficios electrónicos, de acuerdo con los Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, y el DTISACG;
 - x. Aplicaciones para la gestión sin papel y la automatización de los procesos que se establecen en los Manuales Administrativos de Aplicación General.
- h) Asegurar que los datos que se mantengan en el repositorio de configuraciones del Proceso de Administración de la Configuración (ACNF), se encuentren registrados en la Herramienta de Gestión de la Política TIC.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

i) Mantener informados a los responsables del diseño de los servicios de TIC, y a los responsables de los servicios de TIC en operación, sobre los cambios al catálogo de servicios de TIC.

ADS 2 Diseñar los servicios de TIC.

Descripción: Definir las especificaciones para el diseño de cada servicio de TIC, nuevo o adecuaciones a servicios existentes.

Factores Críticos:

El responsable del proceso, deberá:

1. Asignar un responsable del diseño de servicio de TIC, para cada servicio a desarrollar.

El responsable del diseño de servicios de TIC deberá:




2. Definir, en coordinación con los involucrados, los requerimientos del servicio de TIC.
3. Realizar un análisis de los requerimientos asociados al servicio de TIC, y verificar que se documenten y aprueben por los diversos involucrados. Estos requerimientos serán la base para las actividades de diseño posteriores, por lo que cualquier modificación deberá efectuarse mediante un control de cambios.

El análisis de requerimientos deberá considerar al menos lo siguiente:

- a) Para servicios ya existentes:
 - i) Funcionalidad e infraestructura en términos de arquitectura empresarial.
 - ii) Cambios en los procesos del Instituto, prioridades, importancia e impacto.
 - iii) Cambios en los volúmenes de transacciones del servicio de TIC.
 - iv) Cambios en los niveles de servicio y sus metas.
- b) Para servicios nuevos:
 - i) Funcionalidad e infraestructura en términos de arquitectura empresarial.
 - ii) Administración del servicio.
 - iii) Procesos del Instituto involucrados, prioridades, importancia e impacto y beneficios.
 - iv) Niveles de servicio y sus metas

4. Verificar la infraestructura y capacidad de componentes y servicios de TIC existentes, debiendo especificar la reutilización de elementos que se haya identificado.

5. Efectuar el análisis del impacto al negocio, en el que se contemplen los beneficios y contribución de valor de la solución seleccionada, en cada etapa de su ciclo de vida, así como el cumplimiento con los programas de gobierno y la EDN.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

6. Definir y dar seguimiento al desarrollo y mantenimiento de los servicios, así como la evaluación periódica de estos a través de una hoja de ruta de servicios (roadmap).
7. Evaluar y seleccionar, en coordinación con la unidad administrativa solicitante, la solución más adecuada, así como la capacidad técnica y administrativa requerida por el Instituto para la operación dicha solución.
8. Integrar el expediente del diseño del servicio de TIC de que se trate, con la información obtenida en esta actividad.
9. Actualizar el portafolio de servicios de TIC, con la información del expediente del servicio de TIC diseñado.
10. Se consideren servicios de apertura de información pública en formato abierto, de acuerdo a las directrices que en esta materia se expidan.

ADS 3 Administrar la capacidad de la infraestructura de TIC.

Descripción: Elaborar el programa de capacidad y darle seguimiento, a fin de asegurar la operación de los servicios de TIC conforme a los compromisos y niveles de servicio acordados.




Factores Críticos:

El responsable de este proceso, con apoyo de los responsables de los dominios tecnológicos de la UTIC, deberá:

1. Elaborar el programa de capacidad que le permita a la UTIC cumplir con: los niveles de servicio acordados, el crecimiento previsto de la demanda de infraestructura, la mejora de los niveles de servicio y la incorporación de los nuevos servicios de TIC que, de acuerdo al portafolio de servicios de TIC, se tiene previsto inicien su operación.

Para la elaboración del programa de capacidad, será necesario:

- a) Determinar el balance entre la demanda de los servicios de TIC y la capacidad de la infraestructura de TIC, para conocer la suficiencia de cada uno de sus componentes.
- b) Establecer escenarios para las diversas proyecciones de demanda de los servicios de TIC y considerar, de ser el caso, opciones respecto de los niveles y metas de servicio acordados, señalando invariablemente los riesgos que cada escenario conlleve.
- c) Determinar los componentes de la infraestructura de TIC que son necesarios para cumplir con los requerimientos de desempeño y disponibilidad de los servicios de TIC, tanto de los existentes como de los proyectados.
- d) Identificar los activos de TIC que requieren actualizarse, mejorarse o inclusive, sustituirse, así como las fechas propuestas y los costos estimados en cada caso.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

2. Verificar, al menos trimestralmente, la capacidad y rendimiento de la infraestructura de TIC, para determinar si es suficiente para prestar los servicios de TIC con los niveles de servicio acordados, para lo cual será necesario:

- a) Monitorear el rendimiento actual y la capacidad utilizada.
- b) Obtener información de los incidentes que se han presentado por falta de capacidad.
- c) Evaluar los niveles de la capacidad y rendimiento de la infraestructura con respecto a:
 - i) los niveles de servicio originalmente acordados.
 - ii) los niveles de servicio efectivamente proporcionados.
 - iii) los niveles de servicio que, de acuerdo con el programa de capacidad, se hubieren estimado.

3. Identificar las tendencias de las cargas de trabajo de los componentes de la infraestructura, en condiciones normales y de contingencia, así como determinar sus proyecciones, para que sean incluidas en el programa de capacidad.

4. Definir las acciones a implementar cuando la capacidad y rendimiento de la infraestructura de TIC no estén en el nivel requerido, tales como: ajustar la prioridad de las tareas de los componentes de la infraestructura de TIC, instaurar mecanismos de recuperación en caso de fallas, entre otras.

5. Incluir, en los programas de continuidad, las características de capacidad y rendimiento de cada componente de la infraestructura de TIC, con la finalidad de que éstos se puedan utilizar, en caso necesario, de manera individual.

6. Mantener informados a los responsables de los procesos de la UTIC, así como a los responsables de los dominios tecnológicos de:

- a) Las oportunidades identificadas para mejorar la capacidad de la arquitectura tecnológica en operación y realizar recomendaciones sobre los incidentes por falta de capacidad de la infraestructura de TIC.
- b) Los niveles de servicio alcanzados.




ADS 4 Administrar la continuidad de servicios de TIC.

Descripción: Asegurar al Instituto el mínimo impacto en caso de alguna interrupción en los servicios de TIC.

Factores Críticos:

El responsable del diseño de servicios de TIC deberá:

1. Efectuar el análisis de impacto al negocio, en el que se identifiquen las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona el Instituto que

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias que se generarían.

2. Elaborar el programa de continuidad que articule las diferentes acciones que habrían de realizarse para la continuidad de los servicios de TIC y que permita determinar la resistencia requerida por la infraestructura de TIC.

3. Integrar en el programa de continuidad la siguiente definición:

a) Prioridades en situaciones de recuperación para evitar la recuperación de servicios de menor impacto y asegurarse de que la respuesta y la recuperación se encuentren alineadas con las necesidades prioritarias del Instituto.

4. Efectuar pruebas de recuperación, al menos semestralmente, al programa de continuidad para confirmar que los servicios de TIC puedan ser recuperados de forma efectiva, que las deficiencias serán atendidas y comprobar su vigencia o efectuar actualización.

5. Actualizar el programa de continuidad, con las medidas correctivas que se definan sobre los hallazgos e incidentes que se hayan presentado en las pruebas de recuperación efectuadas, así como con las lecciones aprendidas que apliquen.

6. Llevar a cabo, conjuntamente con los involucrados en el programa de continuidad, al menos cada seis meses, una revisión del contenido del mismo para que cada uno de ellos conozca de manera indubitable cuál será su desempeño en las diversas actividades que habrán de realizarse en caso de requerirse la aplicación del programa.

7. Mantener actualizados y bajo resguardo los respaldos de información considerados por la Institución, siendo éstos aprobados por el Titular de la UTIC.

Relación de Productos del proceso:




1. Catálogo de servicios de TIC y arquitectura empresarial en la Herramienta de Gestión de la Política TIC

2. "Programa de capacidad". Formato ADS F1.

3. "Programa de continuidad". Formato ADS F2.

Indicador del proceso:

Nombre: Mantenimiento actualizado de la información de servicios.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

Objetivo: Medir el cumplimiento en la actualización del catálogo de servicios y arquitectura empresarial.

Descripción: Verificar el mantenimiento de información actualizada a través de la Herramienta de Gestión de la Política TIC.

Fórmula: % de cumplimiento = (número de revisiones efectuadas/número de evaluaciones del periodo que se reporta) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Cuatrimestral.

II.B. PROCESO DE ADMINISTRACIÓN DE LA CONFIGURACIÓN (ACNF).

Objetivo General:




Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.

Objetivos Específicos:

1. Identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.
2. Mantener actualizada la información contenida en el repositorio de configuraciones y disponible para los servidores públicos de la UTIC involucrados en los diversos procesos.

Reglas del proceso:

1. El responsable de este proceso es responsable de la administración del repositorio de configuraciones.
2. El responsable de este proceso deberá mantener una verificación continua del repositorio de configuraciones a fin de constatar que éste se encuentre actualizado en todo momento.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		

Roles del proceso:

1. Responsable del Proceso de Administración de la Configuración (ACNF).

Actividades del Proceso.

ACNF 1 Establecer la cobertura y el alcance de la administración de la configuración.

Descripción: Identificar las soluciones tecnológicas y sus componentes, así como los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, para establecer la cobertura que tendrá el proceso, así como el alcance de la administración sobre los elementos de la configuración y sus componentes.



Factores Críticos:

El responsable de este proceso deberá:

1. Identificar los elementos de configuración para determinar, de acuerdo a las necesidades y recursos con los que cuenta la UTIC, los que serán administrados en este proceso.
2. Elaborar un programa para la integración de los elementos de configuración en el repositorio de configuraciones, el cual, en caso de ser gradual, considerará lo siguiente:
 - a) La criticidad e impacto en caso de falla de los elementos a administrar.
 - b) El tipo de los elementos a administrar.
 - c) Los servicios actuales y los proyectados.
 - d) Las localidades en que se ubican los elementos a administrar.
3. Implementar acciones de control para la administración del repositorio de configuraciones, considerando al menos:
 - a) El mantenimiento al modelo de datos del repositorio de configuraciones.
 - b) La definición y aplicación de criterios técnicos para realizar modificaciones a los estados de los elementos de configuración o componentes.
 - c) Que la incorporación de elementos de configuración o componentes al repositorio de configuraciones se realice mediante cambios administrados.
 - d) Las relativas a la administración de los usuarios del repositorio de configuraciones, incluyendo perfiles y permisos.
 - e) La programación de las revisiones al repositorio de configuraciones y su calendarización.

ACNF 2 Definir la estructura del repositorio de configuraciones.

Descripción: Definir la estructura del repositorio de configuraciones, con base en la identificación de las características de los elementos de configuración y componentes que serán administrados en dicho repositorio, y de la infraestructura de TIC del Instituto.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 26 de 56
	Departamento de Informática		



Factores Críticos:

El responsable de este proceso deberá:

1. Definir la estructura de datos que requerirá el repositorio de configuraciones, considerando al menos:

- a) Los atributos de los elementos de configuración y de sus componentes, como lo son, entre otros: su identificador único, nombre, descripción, ubicación, versión, responsable, interrelación con otros elementos, clase y categoría, así como el estado en que se encuentra el elemento o componente.
- b) Los atributos mínimos para conformar las líneas base de los elementos de configuración; así como de aquellos que no requieran contar con ella
- c) La nomenclatura de los elementos de configuración y de sus componentes, integrada por caracteres que refieran al nombre, versión, clase, grupo y tipo, entre otros.
- d) Identificar la relación funcional y de dependencia entre los elementos de configuración y sus componentes, así como su relación con elementos de otros procesos y sistemas, tales como: líneas base, acuerdos de niveles de servicio, roles, registros de incidentes, problemas, cambios y liberaciones, así como documentación relacionada.
- e) Integrar un catálogo que permita identificar los diferentes estados en que pueden encontrarse los elementos de configuración o sus componentes, considerando entre otros, los siguientes:
 - i) En desarrollo. Aplica a elementos o componentes en proceso de desarrollo, instalación, configuración, personalización, entre otros.
 - ii) Borrador. Aplica a elementos o componentes en proceso de elaboración no concluidos o no aprobados.
 - iii) Aprobado. Aplica a elementos o componentes cuya elaboración o desarrollo se encuentra terminado y aceptado.
 - iv) Activo. Aplica a elementos o componentes en operación.
 - v) Suspendido. Aplica a elementos o componentes que temporalmente se encuentran inactivos, pero que son susceptibles de entrar nuevamente en operación.
 - vi) Retirado. Aplica a elementos o componentes que quedan fuera de operación, pero que son susceptibles de reutilizarse para otros elementos o componentes de configuración.
 - vii) Fuera de uso. Aplica a elementos o componentes que quedan fuera de operación y que no son susceptibles de reutilizarse.
- f) Los criterios técnicos para la modificación de los estados de los elementos de configuración o de alguno de sus componentes.

2. Obtener del titular de la UTIC su autorización al modelo de datos del repositorio de configuraciones, para la implementación del repositorio y comunicar a los responsables de los demás procesos de la UTIC, sobre su disponibilidad.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

ACNF 3 Registrar los elementos de configuración en el repositorio de configuraciones

Descripción: Efectuar el registro en el repositorio de configuraciones, de los datos e información de los elementos de configuración y sus componentes.

Factores Críticos:

El responsable de este proceso deberá:

1. Realizar, de acuerdo con el programa previsto en la actividad ACNF 1, el registro en el repositorio de configuraciones.
2. Incorporar y/o actualizar en el repositorio de configuraciones, la información proveniente de los diversos procesos de la UTIC, a fin de integrar la totalidad de los elementos de la configuración.
3. Asegurar que los datos que se mantengan tanto en el repositorio de configuraciones como en el catálogo de servicios de TIC, y sus correspondientes interrelaciones, sean consistentes con los datos que registre la UTIC en la Herramienta de Gestión de la Política TIC.
4. Registrar los resultados de las revisiones al repositorio de configuraciones, así como determinar las acciones de mejora a ejecutar.

Relación de Productos del proceso:

1. "Repositorio de configuraciones" (Modelo no sujeto a formato, de acuerdo a las necesidades del Instituto).

Indicador del proceso:

Nombre: Mantenimiento actualizado del repositorio de configuraciones.



Objetivo: Medir el cumplimiento en la actualización del repositorio de configuraciones.

Descripción: Verificar el mantenimiento de información actualizada en el Repositorio de configuraciones.

Fórmula: % de eficiencia = (número de revisiones efectuadas al repositorio de configuraciones/número de revisiones programadas al repositorio de configuraciones) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

II.C. PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI).

Objetivo General:




Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información del Instituto, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos del Instituto 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 de información esencial y, en su caso, críticas, así como de activos clave del Instituto, 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 del Instituto, 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 el Instituto.

Reglas del proceso:

1. El responsable de la seguridad de la información en el Instituto está a cargo de este proceso y en su caso, podrá auxiliarse de los servidores públicos que considere necesarios, debiendo para ello notificar por escrito a cada uno para que conozcan los roles que desempeñarán, actividades y responsabilidades.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

2. El responsable de este proceso se deberá asegurar 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 del Instituto que se designe conforme a lo establecido en dicho ordenamiento.

3. 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 de que no se cuente con dichas infraestructuras, que el análisis se oriente a los activos de información clave de la Institución.

4. 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 asegurarse de que éstos conozcan las reglas de operación del mismo y la guía técnica de atención a incidentes.




5. El responsable de la seguridad de la información del Instituto será quien mantendrá comunicación con el Centro 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.

6. El grupo estratégico de seguridad de la información deberá asegurar 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.

7. El grupo 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 del Instituto, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.

8. 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.

9. El grupo 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

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

igual manera, para activos y elementos de configuración de los ambientes de desarrollo, pruebas y preproducción.

10. El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la UTIC, para que se implementen 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.




11. El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la UTIC, para que se implementen 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.

12. El grupo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implemente un control para la elaboración y conservación de bitácoras de seguridad para los sistemas identificados como parte de una infraestructura de información esencial y/o crítica. En estas bitácoras 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.

13. El grupo estratégico de seguridad de la información deberá implementar mecanismos para asegurar que los sistemas y aplicativos para desplegar los servicios de TIC que se desarrollen o adquieran, cumplan con los controles previstos en el Proceso de Administración de la Seguridad de la Información (ASI).

14. El responsable de este proceso deberá coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio SLA y los acuerdos de nivel operacional OLA sean determinados y considerados en función de los programas de continuidad y de contingencia de la UTIC y del proceso.

15. El responsable de este proceso deberá enviar a la Unidad un informe semestral, en los meses de julio del año al que corresponda y en enero del año siguiente. El informe deberá ser elaborado por el responsable del ERISC-OPEC, y contendrá el Proceso ASI con el estado que guarda su cumplimiento y la información relativa a la operación de los controles de seguridad

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

mínimos (establecidos en la actividad ASI 6), así como de aquellos derivados del análisis de riesgos.

16. El responsable de la seguridad de la información del Instituto, podrá considerar a los equipos y/o activos de información, de propósito específico, de control, de monitoreo o industriales, como un dominio tecnológico de TO y de esta manera integrar sus controles de seguridad al SGSI.

17. Los servidores públicos 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 presente manual.

18. El responsable de este proceso deberá efectuar las actualizaciones que deriven de la ejecución de los factores críticos de las actividades del presente proceso.

Roles del proceso:

1. Responsable de la seguridad de la información en el Instituto o RSII.
2. Grupo de estratégico de seguridad de la información o GESI.
3. Equipo de respuesta a incidentes de seguridad o ERISC.

Actividades del Proceso.

ASI 1 Establecer un modelo de gobierno de seguridad de la información.

Descripción: Designar al responsable de la seguridad de la información y establecer el grupo de trabajo encargado de la implementación y adopción del modelo de gobierno de seguridad de la información en el Instituto.




Factores Críticos:

Al Director General del Instituto le corresponderá:

1. Designar al responsable de la seguridad de la información en la Institución, quien deberá tener nivel jerárquico mínimo de director general o equivalente, atendiendo las reglas de este proceso.

El responsable de la seguridad de la información en el Instituto (RSII), deberá:

2. Informar al Centro sobre su designación y de la del enlace responsable de mantener comunicación con los ERISC de otras Instituciones.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 32 de 56
	Departamento de Informática		

3. Establecer el grupo estratégico de seguridad de la información (GESI), que estará integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información, y asegurarse de:

- a) Que el documento contenga, al menos: los objetivos y responsabilidades del grupo de trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo.
- b) Que se comuniquen los roles y responsabilidades de los integrantes del grupo estratégico de seguridad de la información.
- c) Dirigir y coordinar al grupo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas por el mismo.



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

Descripción: Institucionalizar prácticas para asegurar la implementación, seguimiento y control de la seguridad de la información en el Instituto.

Factores Críticos:

El grupo estratégico de seguridad de la información deberá:

1. Coordinar la elaboración y actualización del catálogo de infraestructuras de información esencial y, en su caso, críticas.
2. Establecer, conjuntamente con los responsables de los procesos de la UTIC, así como en su caso con los servidores públicos que corresponda, los mecanismos para garantizar la protección de las infraestructuras de información esenciales y/o críticas que éstos tengan bajo su responsabilidad.
3. Vigilar que los controles de seguridad de la información que se definan e implementen, consideren los mecanismos establecidos en el factor crítico anterior, así como el análisis de riesgos que se indica en la actividad ASI 5.
4. Constatar que se efectúe la implementación del SGSI en el Instituto y que se lleven a cabo revisiones al mismo en periodos no mayores a un año, a fin de verificar su cumplimiento.
5. Dar seguimiento a las acciones de mejora continua derivadas de las revisiones al SGSI.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

ASI 3 Diseño del SGSI.

Descripción: Definir los objetivos y diseñar las directrices para establecer el SGSI en la Institución.

Factores Críticos:

El grupo estratégico de seguridad de la información deberá:

1. Diseñar, en coordinación con las diferentes áreas y unidades administrativas del Instituto, la estrategia de seguridad de la información que será implementada al interior de la misma, así como efectuar su revisión al menos una vez al año. Dicha estrategia será la base para establecer el SGSI, cuyo diseño se efectuará atendiendo a lo siguiente:



- a) Realizar un diagnóstico de los requerimientos de seguridad de la información del Instituto, considerando la participación de las unidades administrativas usuarias de la información para establecer adecuadamente el alcance del SGSI.
- b) Definir el alcance del SGSI, de manera tal que establezca límites de protección desde la perspectiva institucional, para proporcionar la seguridad requerida a los activos de información.
- c) Generar las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos del Instituto.
- d) Desarrollar reglas técnicas para verificar que los controles de seguridad de la información que se definan operen según lo esperado.
- e) Definir métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los activos de información.
- f) Elaborar las reglas técnicas que contengan las acciones para la adecuada operación del SGSI.

2. Integrar, con la información del factor crítico anterior, el documento de definición del SGSI e incluir en éste el programa de implementación del SGSI que se desarrolle.

El responsable de la seguridad de la información del Instituto deberá:

3. Hacer del conocimiento del Director General del Instituto el documento de definición del SGSI, que ya incluya el programa de implementación desarrollado.

4. Asegurarse de que se presente a la unidad administrativa responsable de la capacitación en el Instituto, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, así como la estructura y alcances del SGSI.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

5. Dar a conocer el SGSI, y su programa de implementación, a los servidores públicos del Instituto involucrados con el mismo.

El grupo estratégico de seguridad de la información deberá:

6. Elaborar un programa de evaluaciones del SGSI, integrarlo al documento de definición del SGSI y difundirlo en el Instituto.

7. Elaborar, probar y mantener actualizada una directriz rectora de respuesta a incidentes (establecidos en ASI F3), en coordinación con el ERISC, la cual deberá contener al menos

- a) El rol y el servidor público asignado a éste, quien puede iniciar las tareas de respuesta a incidentes.
- b) El mecanismo de notificación, escalamiento y atención de incidentes en el Instituto.
- c) Los mecanismos de interacción con otras Instituciones u organizaciones externas.
- d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.

8. Ejecutar los programas de implementación para el manejo de riesgos y de implementación del SGSI, de acuerdo a lo que se establece en el documento de definición del SGSI, y con apoyo de los titulares de las unidades administrativas en las cuales se implementarán los controles.

9. Dar seguimiento a la ejecución del programa de implementación del SGSI y actualizar el avance del mismo.




10. Elaborar un informe de resultados de la implementación del SGSI e integrarlo al documento de definición del SGSI.

11. Asegurar que los controles de seguridad se hayan implementado de acuerdo a lo previsto en el documento de definición del SGSI y su programa de implementación del SGSI

12. Elaborar un programa de evaluaciones del SGSI, integrarlo al documento de definición del SGSI y difundirlo en el Instituto.

El Responsable de la seguridad de la información del Instituto deberá:

13. Hacer del conocimiento del órgano interno de control en el Instituto y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI a efecto

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALUDABLE Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

de que se determinen, en su caso, las responsabilidades que procedan en términos de los ordenamientos legales aplicables.

El Responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos deberá:

14. Obtener los datos necesarios para verificar la eficiencia y eficacia de los controles implementados, de acuerdo al programa de evaluaciones del SGSI recibido del grupo estratégico de seguridad de la información.
15. Medir la efectividad de los controles de seguridad implementados.
16. Efectuar, con base en el programa de evaluaciones del SGSI, la evaluación del SGSI.
17. Registrar la información de los intentos de violaciones e incidentes de seguridad, hayan sido exitosos o no, así como efectuar el análisis y evaluación de dicha información.
18. Documentar las acciones de revisión del SGSI que hayan resultado de los factores críticos anteriores, mediante la elaboración de un informe de revisión del SGSI, integrarlo al documento de definición del SGSI y enviarlo al grupo estratégico de seguridad de la información.

ASI 4 Identificar las infraestructuras de información esenciales y, en su caso, críticas, así como los activos clave.

Descripción: Elaborar y mantener actualizado un catálogo de infraestructuras de información esenciales y, en su caso, críticas, a fin de facilitar la definición de los controles que se requieran para protegerlas.



Factores Críticos:

El grupo estratégico de seguridad de la Información deberá:

1. Designar su equipo de trabajo, para conformar el catálogo de infraestructuras de información esenciales y, en su caso, críticas, el responsable del equipo deberá ser funcionario público con conocimientos en seguridad de la información y análisis de riesgos.

El equipo de trabajo para la identificación de infraestructuras de información esencial y/o crítica, así como de activos clave, deberá:

2. Identificar procesos críticos del Instituto, mediante la ejecución de las siguientes acciones:
 - a) Analizar los procesos existentes y determinar cuáles de éstos son críticos y enlistarlos, considerando como tales aquellos de los que depende el Instituto para alcanzar sus

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

objetivos, en los niveles de servicio que tenga establecidos, derivado de sus atribuciones. Dicho análisis se realizará considerando al menos los siguientes elementos:

- i) Proveedores del proceso.
- ii) Insumos del proceso.
- iii) Eventos de inicio que disparan la ejecución del proceso.
- iv) Subprocesos o actividades que lo conforman.
- v) Actores que intervienen en su ejecución.
- vi) Productos o servicios que genera.
- vii) Evento de fin del proceso.
- viii) Clientes o usuarios del proceso.
- ix) Activos de información involucrados en el proceso.

b) Analizar los diagramas de los procesos, a fin de identificar las interdependencias que existan entre éstos así como con otros fuera del Instituto.



3. Identificar las actividades críticas de los procesos críticos ya enlistados, mediante la ejecución de las acciones siguientes:

- a) Enlistar y describir las actividades de cada proceso crítico, así como los factores de éxito para que el proceso se lleve a cabo de manera adecuada.
- b) Identificar y enlistar en esta misma relación, las actividades que resultan críticas para la operación del proceso.

4. Identificar, a partir de los procesos críticos identificados y enlistados en el factor crítico anterior, aquellos que se encuentren vinculados con la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo que señalan los artículos 3 y 5 de la Ley de Seguridad Nacional. En caso de no identificarse este tipo de procesos críticos, no será necesario atender los factores críticos 5 al 14 siguientes, debiendo iniciar la actividad ASI 5.

5. Identificar los activos de información involucrados en los procesos de Seguridad Nacional, mediante la ejecución de las acciones siguientes:

- a) Elaborar una relación de los activos de información que soportan la generación, procesamiento, transmisión y almacenamiento de la información en los procesos, con apoyo de los responsables, según corresponda, de su desarrollo, mantenimiento, operación, uso y seguridad, así como de su administración y resguardo.
- b) Incluir en la relación de los activos de información al responsable de su resguardo.
- c) Clasificar los activos de información como activos primarios o de soporte, de acuerdo a su funcionalidad, alcance o impacto en el proceso.
- d) Definir la nomenclatura para la identificación de los activos de información, a partir de dos campos: en el primero "Id. Activo" se asignará un número consecutivo que, relacionado con

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

el segundo campo “Id. Proceso”, correspondiente al proceso, provea una identificación única para cada activo.

6. Efectuar la valoración de los activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad, para identificar aquellos que deban considerarse como activos de información clave y registrar los resultados de la valoración efectuada, mediante matrices de infraestructuras de información esenciales y/o críticas con respecto de sus activos clave.

7. Utilizar como parámetros para identificar la criticidad de una infraestructura, los tipos de impacto potencial que podrían ocurrir ante la presentación de un incidente. Éstos se deberán representar mediante matrices de impacto.

8. 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.

9. Revisar los resultados obtenidos en los factores críticos anteriores.



El grupo estratégico de seguridad de la información deberá:

10. Verificar los resultados obtenidos en los factores anteriores, por el equipo de trabajo y constatar que las infraestructuras de información esenciales y/o críticas que se hubieren identificado efectivamente tengan ese carácter.

El grupo estratégico de seguridad de la información, con apoyo del equipo de trabajo, deberá:

11. Elaborar el catálogo de infraestructuras de información esencial y/o crítica, con base en la información verificada en el factor crítico anterior, y realizar las siguientes acciones:

- a) Asignar, de acuerdo con la tabla que se contiene en el catálogo de infraestructuras de información esenciales y/o críticas, el sector y subsector que corresponda a cada infraestructura identificada.
- b) Verificar que el catálogo de infraestructuras de información esenciales y/o críticas incorpore los datos de identificación, señalando su descripción, componentes, sector y subsector, Institución y ubicación y las matrices de la infraestructura con respecto de sus activos clave, y los impactos que le fueron determinados.
- c) Incluir en el catálogo de infraestructuras de informaciones esenciales y/o críticas un mapa de localización geográfica, en donde se muestre su ubicación) Incluir en el catálogo de

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

infraestructuras de información esenciales y/o críticas, la información de los miembros y roles del equipo de trabajo a que se refiere el factor crítico 1 de esta actividad.

El responsable de la seguridad de la información del Instituto deberá:

12. Presentar a la aprobación del Director General del Instituto, el catálogo de infraestructuras de información esencial y/o crítica elaborado.

13. Asegurarse de que se observe lo establecido en la Ley de Seguridad Nacional, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, para la clasificación y resguardo de la información generada en esta actividad.

El grupo estratégico de seguridad de la información deberá:

14. Revisar, por lo menos una vez al año, el catálogo de infraestructuras de información esenciales y/o críticas del Instituto e instruir, en su caso, al equipo de trabajo a que se refiere el factor crítico 1 de esta actividad para que se efectúen las acciones para su actualización.

ASI 5 Elaborar el análisis de riesgos.




Descripción: Identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios del Instituto, de manera que se obtengan las matrices de análisis de riesgos.

Factores Críticos:

El grupo estratégico de seguridad de la información deberá:

1. Establecer la directriz de administración de riesgos, efectuando las siguientes acciones:

- a) La definición de estrategias, metodologías y herramientas que se usarán para administrar los riesgos.
- b) La integración del marco normativo que resulte aplicable a los riesgos identificados.
- c) El establecimiento de las reglas para medir la efectividad de los controles en la gestión de los riesgos.
- d) La definición de la forma y periodicidad con las que se informará a los grupos y equipos de trabajo, a las áreas y unidades administrativas del Instituto y externos involucrados, sobre los riesgos a los que se encuentran expuestos los procesos y servicios que utilizan.
- e) La definición de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas del Instituto.
- f) Someter a consideración y aprobación del RSII, las definiciones efectuadas en los incisos anteriores.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

2. Integrar a su equipo de trabajo de análisis de riesgos, el cual deberá:

- a) Tener un responsable, quien deberá ser un funcionario público con conocimientos necesarios de seguridad de la información y análisis de riesgos.
- b) La conformación del equipo se hará con servidores públicos que, preferentemente, deberán tener conocimientos en TIC, seguridad de la información y seguridad física; así como por aquellos que se considere puedan aportar mayor capacidad de análisis y alcance de objetivos.
- c) Que los integrantes del equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan.
- d) Se delimite el objetivo y alcance del análisis de riesgos que se efectuará por el equipo de trabajo.
- e) Se seleccione al líder del equipo y se haga de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados.
- f) Integrar, en caso de ser necesario, más de un equipo de trabajo de análisis de riesgos, para efectuar el adecuado acopio de información e integración que deriva del análisis de riesgos que se efectúa en esta actividad.

El equipo de trabajo de análisis de riesgos, con el apoyo de las diversas áreas o unidades administrativas del Instituto involucradas, deberá:




3. Identificar los procesos críticos, recopilando la información siguiente:

- a) La de aquellos procesos de los el Instituto dependa para alcanzar sus objetivos y niveles de servicio comprometidos, derivada de la identificación realizada conforme al factor crítico 2 de la actividad ASI 4, en los casos en que la Institución no hubiere identificado procesos críticos vinculados con la Seguridad Nacional.
- b) La obtenida como resultado del desarrollo de la actividad ASI 4, por haberse identificado procesos críticos vinculados con la Seguridad Nacional.

4. Identificar los activos de información y consultar a los responsables de éstos, para identificar los elementos que se pretenden proteger ante la posible materialización de amenazas y elaborar una relación detallada con la información obtenida.

5. Identificar las vulnerabilidades, mediante las acciones siguientes:

- a) Integrar, a la relación de activos de información, las características de los mismos que pudieran ser aprovechadas para poner en riesgo la confidencialidad, integridad y

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

disponibilidad de éstos, considerando, asimismo, las características del ambiente y del Instituto en que se ubican.

b) Considerar como vulnerabilidad la ausencia y/o falla de controles.

c) Integrar a los responsables de la administración, operación y, en su caso, resguardo de los activos de información en el proceso de identificación de vulnerabilidades.

6. Identificar las amenazas mediante las acciones siguientes:

a) Registrar las posibles amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información que ya se tiene enlistados.

b) Identificar y registrar los agentes que podrían materializar una amenaza, utilizando la lista de amenazas y agentes que se provee en el formato del producto “Documento de resultados del análisis de riesgos”

7. Efectuar la identificación y evaluación de escenarios de riesgo, evaluando aquellos que se identifiquen y registrando los resultados obtenidos, considerando los datos recopilados en los factores críticos anteriores y efectuando las acciones siguientes:

a) Definir los escenarios de riesgo, para lo cual es necesario efectuar los cálculos para establecer el valor del riesgo para cada escenario, utilizando la fórmula: $R=PI$; en la que “P” es la probabilidad de ocurrencia de la amenaza, e “I” es el impacto ocasionado por la materialización de la misma.



b) Establecer las variables complementarias que se indican en el formato del producto “Documento de resultados del análisis de riesgos”, ya que éstas determinan el valor final del riesgo, utilizando la tabla denominada “Probabilidad de ocurrencia contra impacto”, que se encuentra en el formato de este mismo producto, e integrar en éste el resultado de la identificación y evaluación de los escenarios de riesgo.

c) Definir la estrategia de seguridad para cada riesgo, seleccionando alguna de las establecidas en el citado formato: evitar, mitigar o reducir, financiar o asumir y transferir o compartir, debiendo evaluarse en este mismo orden.

d) Obtener la relación de riesgos que requieren atención, su prioridad y estrategia de seguridad.

8. Elaborar el análisis del costo-beneficio de controles de seguridad, mediante las acciones siguientes:

a) Elaborar la lista de escenarios de riesgo, cuya acción de seguridad implica el uso de controles o la modificación de un proceso para evitar, mitigar o reducir, financiar o asumir y transferir o compartir los riesgos.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

- b) Comparar el costo del control que se proponga contra el impacto que se podría ocasionar por la materialización del riesgo.
- c) Verificar el costo-beneficio de controles de seguridad, debiendo definir los valores indicados en éste, para cada escenario de riesgo, e integrar los datos en el “Documento de resultados del análisis de riesgos”.

9. Elaborar el “Documento de resultados del análisis de riesgos”, mediante las acciones siguientes:

- a) Integrar la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad establecido, indicando además los requerimientos para su implementación.
- b) Incluir, de ser el caso, el nivel de riesgo residual de cada escenario.
- c) Elaborar e integrar las declaraciones de aplicabilidad con los controles necesarios, de acuerdo a los resultados obtenidos de los factores críticos anteriores.
- d) Elaborar e incluir las propuestas para los programas de mitigación de riesgos, considerando los controles establecidos en las declaraciones de aplicabilidad.
- e) Elaborar e incluir en el “Documento de resultados del análisis de riesgos”, un programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERISC.

10. Obtener del grupo estratégico de seguridad de la información, la aprobación del “Documento de resultados del análisis de riesgos” y enviarlo a los responsables de los procesos en las diversas áreas y unidades administrativas del Instituto para su revisión.




Los responsables de los procesos en las diversas áreas y unidades administrativas del Instituto, con el apoyo del equipo de trabajo de análisis de riesgos, deberán:

11. Seleccionar de entre los controles recomendados por el grupo estratégico de seguridad de la información, contenidos en el “Documento de resultados del análisis de riesgos”, aquéllos a implementar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas.

12. Justificar ante el grupo estratégico de seguridad de la información las razones por las cuales existan controles recomendados no seleccionados.

El equipo de trabajo de análisis de riesgos, en coordinación con las áreas y unidades administrativas del Instituto involucradas, deberá:

13. Elaborar, e integrar en el “Documento de resultados del análisis de riesgos”, el programa de implementación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada conforme al factor crítico 11 de esta actividad. Dicho programa deberá incluir la

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

asignación de responsables de la implementación de cada control, integrando éstas al “Documento de resultados del análisis de riesgos” y los datos necesarios para su implementación, así como documentarse conjuntamente con la implementación de las acciones y controles del SGSI.

14. En el programa de implementación para el manejo de riesgos se deberá establecer un responsable de la implementación de cada uno de los riesgos a manejar.

15. Obtener del grupo estratégico de seguridad de la información la aprobación del programa de implementación elaborado y verificar su adecuada integración con las demás actividades de implementación o mejora de los controles de seguridad y las acciones del SGSI.

El grupo estratégico de seguridad de la información deberá:

16. Cuidar que el análisis de riesgos se realice o actualice conforme a los factores críticos de esta actividad, al menos una vez al año, o bien, 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.

17. Asegurar que se ejecuten los factores críticos integralmente y se obtengan los productos de esta actividad debidamente actualizados. Asimismo, se documente la mejora continua que resulte necesaria, derivada del factor crítico anterior.

ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.



Descripción: Definir los controles mínimos de seguridad de la información e integrarlos al SGSI, para su implementación a través de los diversos procesos de la UTIC y de aquellos procesos del Instituto que contengan activos de TIC y TO, activos de información e infraestructuras de información esenciales y, en su caso, críticas.

Factores Críticos:

El grupo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:

1. Definir los controles de seguridad necesarios para salvaguardar los activos de TIC y TO, los activos de información y las infraestructuras de información esenciales de la Institución y, en su caso, las críticas, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:

a) Asegurar que los servidores y estaciones de trabajo, cuenten con software actualizado para detección y protección contra programas para vulnerar la seguridad de los dispositivos de TIC y TO, así como su información y los servicios que proveen. El software debe emitir

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

reportes sobre el estado de actualización de los componentes sobre los que tienen cobertura.

b) La designación de personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información del Instituto, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate.

c) Instalar en los equipos de cómputo de los usuarios, incluyendo los móviles que se conecten a la red de datos, las herramientas antivirus y aquéllas necesarias para prevenir ataques por la vulnerabilidad que el uso de estos equipos conlleva.

d) El ingreso y salida de activos de información.

e) El borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario; y mantener evidencia auditable del proceso.

f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los activos de información.

g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos del Instituto y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.

h) Los criterios de asignación de usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.

i) La configuración de las herramientas de protección implementadas en las redes institucionales.

j) Las conexiones a redes públicas y privadas, así como para los dispositivos electrónicos que contengan información considerada como reservada o sensible para la Institución.

k) La seguridad física y lógica que permita mantener, para los respaldos de información, su confidencialidad, integridad y disponibilidad.

l) El uso del servicio de Internet en el Instituto, el cual debe contar con herramientas de seguridad y de filtrado de contenido.




m) Instalar mecanismos de cifrado de datos en los dispositivos electrónicos móviles que contengan información considerada como reservada o sensible para el Instituto.

n) Que la información clasificada o aquella que tiene valor para el Instituto, sea respaldada y restaurada en el momento en que se requiera.

o) Contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.

p) Implementar mecanismos de TIC Y TO para impedir la conexión a redes inalámbricas externas que se encuentren al alcance de los dispositivos electrónicos institucionales.

q) Definir y establecer las conexiones remotas que den acceso a la red y a los servicios de TIC Y TO institucionales, tanto para usuarios internos como a proveedores, determinando si éstas se establecen a través de canales cifrados de comunicación que aseguren

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

técnicamente la seguridad de los datos. Para estas conexiones se deberá obtener autorización expresa del grupo estratégico de seguridad de la información.

r) Instalar en los componentes de los servicios de correo electrónico, herramientas actualizadas de protección contra correos electrónicos no deseados o no solicitados.

s) Establecer el mecanismo para garantizar la eliminación o modificación de los privilegios de acceso a la información del personal interno y proveedores de servicios, cuando terminen su relación contractual o cuando por algún motivo el nivel de privilegios de accesos asignados cambie.

Los controles de seguridad que se establecen en este factor crítico aplicarán a los activos de TIC y TO, activos de información e infraestructuras de información esenciales y/o críticas que técnica y/o normativamente les corresponda, y de ser el caso, se deberá justificar la no aplicabilidad de los mismos. En aquellos que se haya definido la no aplicabilidad de los controles de este factor crítico, deberán definirse e implementarse los controles que deriven de la ejecución de la actividad ASI 5.

2. Documentar los controles determinados conforme al factor crítico anterior, incluyendo su definición detallada e integrarlos al documento de definición del SGSI y elaborar conjuntamente con los responsables de los procesos institucionales involucrados, el programa de implementación del SGSI e integrarlo al mismo documento. El programa de implementación deberá incluir el nombre del responsable de la implementación de cada uno de los controles de seguridad del SGSI que se hayan establecido.

ASI 7 Mejorar el SGSI.



Descripción: Mejorar la seguridad de la información, a través de la aplicación de acciones preventivas y correctivas derivadas de las revisiones que se efectúen al SGSI.

Factores Críticos:

El grupo estratégico de seguridad de la información deberá:

1. Constatar, en coordinación con las áreas y unidades administrativas involucradas, que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica del Instituto se apliquen, a fin de hacer del conocimiento del titular de la misma el cumplimiento de los controles de seguridad establecidos.

2. Obtener, de la 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 de definición del SGSI.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

3. Elaborar el documento de implementación de la mejora al SGSI e integrarlo al documento de definición del SGSI. El documento de implementación debe utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.

4. Comunicar las mejoras que deberán aplicarse al SGSI al responsable del grupo de trabajo para la implementación de la seguridad de la información, previsto en la actividad OPEC 1, por medio del documento de definición del SGSI, en lo relativo a los resultados de la evaluación del SGSI y la implementación al SGSI.

5. Vigilar y registrar las observaciones necesarias respecto a la implementación de las mejoras mediante un informe de seguimiento a las acciones de mejora al SGSI que deberá integrarse al documento de definición del SGSI.

6. Aplicar las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el grupo estratégico de seguridad de la información.

7. 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.

8. Actualizar el informe de seguimiento a las acciones de mejora al SGSI e integrarlo en el documento de definición del SGSI.

9. Verificar el contenido del informe de seguimiento a las acciones de mejora al SGSI; actualizar el programa de evaluaciones del SGSI, integrarlo en el documento de definición del SGSI y enviar éste al grupo estratégico de seguridad de la información para su revisión.




Relación de Productos del proceso:

1. "Documento de integración y operación del grupo estratégico de seguridad de la información". Formato ASI F1.

2. "Catálogo de infraestructuras de información esenciales y/o críticas". Formato ASI F2.

3. "Documento de resultados del análisis de riesgos". Formato ASI F3.

4. "Documento de definición del SGSI". Formato ASI F4.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

Indicador del proceso:

Nombre: Cumplimiento del Proceso de Administración de la Seguridad de la Información (ASI).

Objetivo: Obtener la eficiencia del proceso en base a su cumplimiento.

Descripción: Medir el cumplimiento en la implementación de los controles establecidos durante el proceso.

Fórmula: % de eficiencia = (controles implementados / controles programados para su implementación) X 100

Responsable: El responsable del Proceso de Administración de la Seguridad de la Información (ASI).

Frecuencia de cálculo: Anual.

III. PROCESOS DE ENTREGA (ASI).

III.A. PROCESO DE ADMINISTRACIÓN DE PROYECTOS (ADP).

Objetivo General:




Administrar la Cartera Operativa de proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios el Instituto.

Objetivos Específicos:

1. Establecer la gobernabilidad de la Cartera Operativa de Proyectos de TIC.
2. Establecer las directrices y visión para administrar la cartera operativa de proyectos TIC.

Reglas del proceso:

1. El responsable de este proceso es el administrador de la Cartera Operativa de Proyectos de TIC.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

2. El administrador de la Cartera Operativa de Proyectos de TIC designará, para cada proyecto que se autorice, al administrador de proyecto o responsable, solicitando para ello autorización al titular de la UTIC.

3. Los administradores del proyecto deberán asegurarse de que todos los proyectos que administren cuenten al menos con su documento de planeación del proyecto, así como los documentos de planeación subsidiarios, desde su inicio hasta su cierre, y de que éste se actualice en tiempo y forma de acuerdo a los avances de los proyectos hasta su cierre.

4. Los administradores de proyecto deben asegurarse que cualquier cambio a un proyecto que administren se realice mediante una solicitud de cambio autorizada por los involucrados.

5. Los responsables de proyecto deberán asegurarse que las metodologías y/o mejores prácticas que se adopten para los diversos tipos de proyectos, se documenten para cada uno de los proyectos que desarrollen en la UTIC.

Roles del proceso:




1. Grupo de trabajo para la dirección de TIC.
2. Responsable del proceso y administrador de la Cartera Operativa de Proyectos de TIC.
3. Responsable de la administración de la Cartera Operativa de Proyectos de TIC.
4. Administradores de proyecto de TIC.

Actividades del Proceso.
ADP 1 Establecer directrices para la gobernabilidad y evaluación del portafolio de proyectos de TIC.
Descripción: Definir las directrices para la asignación y uso de los recursos en proyectos de TIC.

Factores Críticos:

El grupo de trabajo para la dirección de TIC deberá:

1. Tomar acuerdos respecto a la gobernabilidad del portafolio de proyectos de TIC que le presente el titular de la UTIC:
 - a) Autorizar la fijación de prioridades de la Cartera Operativa de Proyectos de TIC.
 - b) Confirmar la asignación de presupuesto estimado para cada uno de los proyectos que integran la Cartera.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

- c) Verificar la alineación de las inversiones en proyectos de TIC con las necesidades, objetivos del Instituto y elementos de Arquitectura Empresarial que apliquen.
- d) Autorizar la suspensión, cambios, cierre o cancelación de proyectos de TIC o la reasignación de recursos entre proyectos pertenecientes a la Cartera Operativa de Proyectos de TIC.

El administrador de la Cartera Operativa de Proyectos de TIC, con apoyo del responsable de cada uno de los Proyectos de TIC, deberá:

2. Integrar la Cartera Operativa de Proyectos de TIC, definiendo los proyectos de TIC que contendrán e identificar los proyectos que se administrarán individualmente.
3. Priorizar y equilibrar la Cartera Operativa de Proyectos de TIC, a efecto de optimizar el uso de los recursos.
4. Dar seguimiento a la Cartera Operativa de Proyectos de TIC y difundirla, a fin de prever riesgos y desviaciones.

El titular de la UTIC deberá:

5. Presentar la Cartera Operativa de Proyectos de TIC al grupo de trabajo para la dirección de TIC, para su aprobación y autorizaciones procedentes.



ADP 2 Priorizar, equilibrar y autorizar la Cartera Operativa de Proyectos de TIC.

Descripción: Priorizar los proyectos e iniciativas pertenecientes a la Cartera Operativa de Proyectos de TIC que estén seleccionadas para su aprobación.

Factores Críticos:

El administrador de la Cartera Operativa de Proyectos de TIC deberá:

1. Evaluar los proyectos e iniciativas pertenecientes a la Cartera Operativa de Proyectos de TIC que serán propuestas al grupo de trabajo para la dirección de TIC para su priorización y, en su caso, autorización. Para llevar a cabo la evaluación deberá considerar, cuando menos, los análisis relativos a:
 - a) Las funciones sustantivas que sustentan la iniciativa o proyecto de TIC.
 - b) La capacidad de recursos humanos.
 - c) La capacidad financiera y/o presupuestaria.
 - d) La capacidad de activos e infraestructura de TIC.
2. Establecer y mantener actualizado la Cartera Operativa de Proyectos de TIC.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

3. Mantener el equilibrio de los recursos, mediante la revisión a los informes de rendimiento de las Cartera Operativa de Proyectos de TIC y de ser el caso, sugerir al grupo de trabajo para la dirección de TIC, un cambio de prioridad o la continuación, suspensión o cancelación de iniciativas, o de proyectos de TIC.
4. Someter a la autorización del grupo de trabajo para la dirección de TIC, los ajustes la Cartera Operativa de Proyectos de TIC y preparar las justificaciones de cada ajuste.
5. Designar responsables para cada iniciativa, o proyecto operativo de TIC, autorizado.
6. Generar con la información recopilada de las actividades de este proceso el documento de planeación y acta de constitución del proyecto para su registro.
7. Actualizar el tablero de control de proyectos de TIC y difundirlo.




ADP 3 Administrar y monitorear la Cartera Operativa de Proyectos de TIC.

Descripción: Administrar la Cartera Operativa de Proyectos de TIC orientando las acciones a una coordinación optimizada de las actividades de administración de los mismos.

Factores Críticos:

El responsable de la administración la Cartera de Operativa de Proyectos de TIC deberá:

1. Determinar los proyectos que integrarán la Cartera de Operativa de Proyectos de TIC y elaborar su justificación.
2. Elaborar un cronograma ejecutivo para la Cartera de TIC, que muestre la duración y las fechas de inicio y fin de cada proyecto, e incluya hitos de control y riesgos potenciales.
3. Asegurarse de que se cuente con las asignaciones y autorizaciones necesarias para el inicio de un programa de proyectos de TIC y sus proyectos.
4. Dar seguimiento a la Cartera de Operativa de Proyectos de TIC, desde su inicio y hasta su conclusión, cambios controlados, incidentes o riesgos que se materialicen.
5. Elaborar el análisis comparativo entre el avance real y el planeado.
6. Actualizar el tablero de control de proyectos, de manera que permita identificar niveles críticos y apoyar la definición de acciones correctivas a la estrategia del programa de proyectos.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

7. Verificar y evaluar de manera continua el estado que guarda cada uno de los proyectos de TIC, de acuerdo a sus hitos y puntos de control, para determinar su contribución al Portafolio de proyectos de TIC y actualizar el tablero de control de proyectos.

8. Mantener permanentemente informado al grupo de trabajo para la dirección de TIC, por medio del tablero de control de proyectos de TIC, el cual deberá contener, al menos, la información sintetizada del avance de la Cartera Operativa de Proyectos de TIC, el resultado de los indicadores del desempeño de la Cartera Operativa de Proyectos y, en su caso, de las eventualidades o riesgos que se hayan presentado.

ADP 4 Cerrar iniciativas y proyectos de TIC.

Descripción: Concluir las iniciativas y proyectos de TIC, mediante la elaboración y presentación de un informe final que contenga la evaluación de los resultados y los beneficios obtenidos.

Factores Críticos:

El administrador de la Cartera Operativa de proyectos de TIC deberá:



1. Revisar los resultados y la documentación de los programas de proyectos y de los proyectos de TIC asociados a la iniciativa de TIC que se pretenda cerrar.
2. Preservar y mantener disponible la información del desarrollo de cada proyecto perteneciente a la Cartera Operativa de proyectos de TIC.

Relación de Productos del proceso:

1. "Tablero de control de proyectos de TIC" (formato de acuerdo a la plataforma tecnológica y recursos de aplicativos de cómputo de la UTIC).
2. "Acta de constitución del proyecto". Formato ADP F1.
3. "Acta de aceptación de entregables". Formato ADP F2.
4. "Acta de cierre de proyecto". Formato ADP F3.

Indicador del proceso:

Nombre: Porcentaje de cumplimiento en la ejecución que integra la Cartera Operativa de Proyectos de TIC.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

Objetivo: Conocer la eficiencia de proyectos pertenecientes a la Cartera Operativa de Proyectos de TIC.

Descripción: Medir la eficiencia del proceso por los beneficios alcanzados.

Fórmula: % de eficiencia= (Número de proyectos pertenecientes a la Cartera Operativa de Proyectos de TIC - número de proyectos cancelados o modificados en alcance / número total proyectos pertenecientes a la Cartera Operativa de proyectos de TIC) X 100.

Responsable: El responsable del portafolio de proyectos de TIC.

Frecuencia de cálculo: Semestral.

III.B. PROCESO DE ADMINISTRACIÓN DE PROVEEDORES (APRO).

Objetivo General:



Establecer un mecanismo que permita verificar el cumplimiento de las obligaciones derivadas de los contratos celebrados para la adquisición, arrendamiento o servicios de TIC.

Objetivos Específicos:

1. Identificar hallazgos, desviaciones y riesgos en el cumplimiento de los contratos en materia de TIC.
2. Proponer acciones preventivas y correctivas que propicien el adecuado cumplimiento del proveedor a sus obligaciones contractuales.

Reglas del proceso:

1. El responsable de este proceso estará a cargo de la operación del centro de cómputo y comunicaciones, o bien, del enlace con los responsables de los servicios de cómputo y comunicaciones que se encuentren contratados.
2. El responsable de este proceso deberá revisar y en su caso, aprobar los cambios a los elementos o componentes del ambiente operativo.
3. El responsable de este proceso, en coordinación con cada responsable de dominio tecnológico, se asegurará de que los servidores de cómputo de la red institucional, así como los componentes del ambiente operativo que manejen fecha y hora en sus sistemas operativos, se encuentren sincronizados a la hora oficial para los Estados Unidos Mexicanos generada por

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

el Centro Nacional de Metrología, en los husos horarios establecidos en la Ley del Sistema de Horario en los Estados Unidos Mexicanos, para lo cual hará uso del servicio que dicho centro proporciona de manera gratuita.

4. El responsable de este proceso se deberá asegurar que se realicen oportunamente las evaluaciones, para determinar la efectividad de los controles de seguridad implementados.

5. El responsable de este proceso deberá verificar que se siguen en todo momento los controles de seguridad establecidos en el SGSI.

6. El titular de la UTIC deberá asignar al Responsable del mantenimiento de la infraestructura.

Roles del proceso:

1. Responsable del Proceso de Administración de la Operación (AOP).
2. Responsable del mantenimiento de la infraestructura.

Actividades del Proceso.
<p>APRO 1 Generar lista de verificación de obligaciones. Descripción: Elaborar una lista de verificación, conforme al contrato celebrado, que sirva como base para dar seguimiento al desarrollo de las obligaciones pactadas.</p>




Factores Críticos:

El responsable de este proceso deberá:

1. Apoyar técnicamente a los administradores de contratos de bienes y servicios de TIC en el seguimiento a las obligaciones adquiridas mediante los contratos celebrados por la UTIC.

El responsable del proceso, para cada contrato suscrito, con apoyo de los administradores de contrato, deberá:

2. Elaborar, de conformidad con el contrato de que se trate, una lista de apoyo para la verificación y seguimiento de las obligaciones contractuales, la cual deberá contener al menos, lo siguiente:
 - a) La totalidad de las obligaciones asumidas por el proveedor y el Instituto.
 - b) Los supuestos en que se aplicarán penalizaciones al proveedor.
 - c) Las fechas de entrega de los bienes o de prestación de los servicios contratados y en su caso, el calendario de entrega de los productos o entregables.
 - d) Los datos del enlace o de los enlaces o responsables, designados por el proveedor.

 	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

3. En los casos en que participen diversos proveedores en un contrato, será necesario identificar qué obligaciones corresponden a cada uno.

APRO 2 Monitorear el avance y desempeño del proveedor.

Descripción: Verificar que el avance de los compromisos y actividades del proveedor se realicen como se especifica en el contrato.

Factores Críticos:

El responsable de este proceso deberá:

1. Solicitar a cada uno de los administradores de contrato, la información relativa a los aspectos siguientes:
 - a) Cumplimiento de las obligaciones asumidas por el proveedor en el contrato.
 - b) Los avances del proveedor y el desempeño al que éste se encuentre obligado.
 - c) La identificación de los incumplimientos del proveedor y las penas convencionales o deductivas que se hubieren aplicado o que deban aplicarse.

El responsable del proceso, con la información obtenida de los administradores del contrato, coadyuvará para:



2. Establecer la coordinación necesaria con el enlace, enlaces o responsables designados por el proveedor, para el cumplimiento de sus obligaciones.
3. Elaborar un reporte de avance sobre el cumplimiento de obligaciones, con el fin de:
 - a) Identificar, analizar y registrar hallazgos, desviaciones y riesgos, y proponer al administrador del proyecto, así como a la unidad administrativa solicitante o a los responsables de los procesos involucrados, las acciones preventivas y/o correctivas correspondientes.
 - b) Dar seguimiento a las acciones preventivas y/o correctivas que se determinen hasta su cierre.

APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos.

Descripción: Coadyuvar, con el área requirente, el área técnica y/o el administrador del contrato, para corroborar que el proveedor de cada contrato, cumpla con las obligaciones estipuladas en el mismo.

Factores Críticos:

El responsable de este proceso deberá realizar las siguientes actividades:

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

1. Apoyar en la revisión del cumplimiento de las obligaciones contractuales del proveedor, principalmente para la aceptación de los bienes o servicios objeto de la contratación.
2. Confirmar, cuando proceda, que los accesos a los activos o servicios de TIC proporcionados al proveedor, para el cumplimiento del contrato, han sido retirados al darse por finiquitado el mismo.
3. Actualizar el reporte de avance sobre el cumplimiento de obligaciones con la información final, y comunicar cualquier incidente o desviación que se detecte al administrador de proyecto y, en su caso, a la unidad administrativa solicitante o a los responsables de los procesos involucrados, así como a la unidad administrativa facultada en el Instituto para efecto de dar por concluidas las obligaciones contractuales, en términos de las disposiciones aplicables.

Relación de Productos del proceso:

1. "Reporte de avance sobre el cumplimiento de obligaciones". Formato APRO F1.

Indicador del proceso:

Nombre: Cumplimiento del proceso.

Objetivo: Conocer el grado de cumplimiento del proceso.

Descripción: Medir el cumplimiento del proceso por medio de la actividad de revisión sobre contratos.

Fórmula: % de eficiencia= (número de revisiones de avance y conclusión ejecutadas / número de revisiones de avance y conclusión programadas) X 100.



Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

III.C. PROCESO DE ADMINISTRACIÓN DE LA OPERACIÓN (AOP).

Objetivo General:

Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 50 de 56
	Departamento de Informática		

Objetivos Específicos:




1. Operar la infraestructura y servicios de TIC, de manera que puedan resistir fallas, ataques deliberados o desastres y, se recuperen los servicios de TIC de manera ágil y segura.
2. Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.

Reglas del proceso:

1. El responsable de este proceso estará a cargo de la operación del centro de cómputo y comunicaciones, o bien, del enlace con los responsables de los servicios de cómputo y comunicaciones que se encuentren contratados.
2. El responsable de este proceso deberá revisar y en su caso, aprobar los cambios a los elementos o componentes del ambiente operativo.
3. El responsable de este proceso, en coordinación con cada responsable de dominio tecnológico, se asegurará de que los servidores de cómputo de la red institucional, así como los componentes del ambiente operativo que manejen fecha y hora en sus sistemas operativos, se encuentren sincronizados a la hora oficial para los Estados Unidos Mexicanos generada por el Centro Nacional de Metrología, en los husos horarios establecidos en la Ley del Sistema de Horario en los Estados Unidos Mexicanos, para lo cual hará uso del servicio que dicho centro proporciona de manera gratuita.
4. El responsable de este proceso se deberá asegurar que se realicen oportunamente las evaluaciones, para determinar la efectividad de los controles de seguridad implementados.
5. El responsable de este proceso deberá verificar que se siguen en todo momento los controles de seguridad establecidos en el SGSI.
6. El titular de la UTIC deberá asignar al Responsable del mantenimiento de la infraestructura.

Roles del proceso:

1. Responsable del Proceso de Administración de la Operación (AOP).
2. Responsable del mantenimiento de la infraestructura.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

Actividades del Proceso.

AOP 1 Establecer el mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC.

Descripción: Establecer las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC, así como el mantenimiento a los componentes de infraestructura.

Factores Críticos:

El responsable de este proceso deberá:

1. Mantener un mecanismo de operación de TIC para los sistemas, aplicaciones y servicios de TIC, que contemple las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación, mantenimiento y respaldo formalizándolas a través del Mecanismo de operación y mantenimiento de TIC.

El responsable de este proceso, con apoyo del titular de la UTIC, deberá:

2. Definir e implementar, en la medida de lo posible y conforme a las necesidades y recursos de la UTIC, herramientas tecnológicas para notificar y rectificar fallas críticas en las tareas de la operación, así como para monitorear el estado y operación de los dispositivos dentro de los límites aceptables, con la finalidad de prevenir fallas en la operación.



El responsable del mantenimiento de la infraestructura deberá:

3. Integrar en el documento Mecanismo de operación y mantenimiento de TIC las acciones de carácter preventivo para evitar fallas a los componentes de dicha infraestructura, y difundirlo a los responsables de los procesos de la UTIC que estén involucrados.

4. Aplicar los controles de mitigación de riesgos establecidos en el Proceso de Administración de la Seguridad de la Información (ASI), relativos a componentes de infraestructura.

5. Implementar, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI, que consideren cuando menos:

- a. La protección de los componentes que serán instalados o que recibirán mantenimiento.
- b. Efectuar el respaldo y protección de los datos almacenados en la infraestructura tecnológica, así como del software que se encuentre instalado.
- c. Verificar que el ambiente de desarrollo y pruebas sea el adecuado para efectuar las tareas de instalación o de mantenimiento a la infraestructura tecnológica.
- d. Verificar que el ambiente de desarrollo y pruebas a que se refiere el inciso anterior esté separado del ambiente productivo.

	MAAGTICSI		Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

- e. Modificar, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.
6. Evaluar la efectividad de los controles de seguridad aplicados en la instalación de los componentes y en las tareas de mantenimiento.
7. Registrar y dar seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica.
8. Informar de los incidentes de mantenimiento a los responsables de los dominios tecnológico involucrados.
9. Registrar el resultado de las pruebas realizadas y mantenerlas disponibles como información de conocimiento.




AOP 2 Programar y ejecutar las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

Descripción: Efectuar la programación de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC, con base en el mecanismo de operación de TIC.

Factores Críticos:

El responsable de este proceso deberá:

1. Mantener un control en la ejecución de tareas para la operación de TIC, que incluya de manera detallada la calendarización, tareas y responsables de estas, así como los elementos de la configuración que se verán afectados.
2. Dar seguimiento a las tareas de mantenimiento calendarizadas.
3. Constatar que el personal a su cargo:
 - a) Ejecute las tareas contenidas en el programa de ejecución de tareas para la operación de TIC que les corresponda desarrollar y documentarlas en una bitácora de operación.
 - b) Registre y dé trámite a las solicitudes de cambio que deriven de la ejecución de las tareas de operación y efectuar tales cambios de manera administrada, estableciendo controles de seguridad en cada caso.
 - c) Registre y dé el trámite que corresponda a cualquier solicitud de servicio con motivo de incidentes de operación que deriven de la ejecución de las tareas de operación, y efectuar el seguimiento de la solicitud de manera administrada, estableciendo controles de seguridad en cada caso.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

4. Revisar las bitácoras de operación, para constatar que las tareas ejecutadas coinciden con las tareas programadas.

AOP 3 Monitorear la infraestructura de TIC en operación.

Descripción: Monitorear en los diferentes dispositivos de la infraestructura y de los servicios de TIC, la ejecución de las tareas de la operación, con el propósito de identificar eventos para prevenir o solucionar fallas e incidentes.

Factores Críticos:

El responsable de este proceso deberá:




1. Revisar que se registre cualquier tarea ejecutada como parte de la operación, a efecto de contar con registros que permitan identificar la causa raíz de incidentes, así como confirmar la ejecución satisfactoria de las tareas de la operación.
2. Identificar los eventos que se presenten en la operación de la infraestructura y de los servicios de TIC, considerando al menos los eventos siguientes:
 - a) Alertas relacionadas con niveles máximos y mínimos de operación.
 - b) Alertas derivadas de alguna excepción en la secuencia de las tareas de operación.
 - c) Alertas por operación o comportamiento inusual.
3. Dar seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes, así como la mejora de las tareas de operación en el Instituto y estar en posibilidad de transmitir las a otras Instituciones.

AOP 4 Implementar y verificar que se cumplan los controles de seguridad física en el centro de datos.

Descripción: Implementar, de acuerdo con el SGSI, los controles de seguridad física en el centro de datos, así como para el acceso al propio centro y a los componentes o elementos del ambiente operativo, ubicados en el mismo.

Factores Críticos:

1. Mantener y actualizar sistema de seguridad física en el centro de datos, en el que se incorporen, de acuerdo con el SGSI, los controles de seguridad para:
 - a) Los riesgos de seguridad física identificados en el Proceso de Administración de la Seguridad de la Información (ASI).
 - b) Limitar el acceso a la información sensible del centro de datos.
 - c) Efectuar el retiro, transporte y almacenamiento de activos de TIC, de forma segura.
 - d) El borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, que sean retirados del ambiente operativo, por daño o reemplazo.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SALDO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

e) El registro de incidentes sobre la seguridad del ambiente físico, mediante la solicitud de servicio respectiva.

2. Integrar al sistema de seguridad física en el centro de datos a que se refiere el factor crítico anterior, los controles de seguridad que de acuerdo con el SGSI se requieran para el acceso físico a las áreas reservadas de la UTIC.

3. Integrar al sistema de seguridad física en el centro de datos, a que se refiere el factor crítico 1 anterior, los controles de seguridad que de acuerdo con el SGSI sean necesarios para hacer frente a los riesgos ambientales.

4. Difundir al interior de la UTIC los controles de seguridad implementados y verificar su cumplimiento.

5. Registrar los incidentes del ambiente físico que se presenten y administrarlos hasta su solución.

Relación de Productos del proceso:

1

. "Mecanismo de operación y mantenimiento de TIC" (formato de acuerdo a las necesidades de la UTIC).

Indicador del proceso:

Nombre: Incidentes en el ambiente operativo.




Objetivo: Medir la eficiencia en el proceso.

Descripción: Obtener el número de Incidentes en la operación resueltos mediante la aplicación del mecanismo de operación de TIC.

Fórmula: % de eficiencia = (incidentes en la operación resueltos / incidentes que se presentaron en el ambiente operativo) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

III.D. PROCESO DE OPERACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y DEL ERISC (OPEC).

Objetivo General:

Implementar y operar los controles de seguridad de la información de acuerdo al programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

Objetivos Específicos:

1. Implementar las mejoras recibidas del Proceso de Administración de la Seguridad de la Información (ASI), para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la información en operación.

Reglas del proceso:

1. El responsable de este proceso estará a cargo de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos.

Roles del proceso:

1. Responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos.
2. Responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos.
3. ERISC.

Actividades del Proceso.




OPEC 1 Designar un responsable de la supervisión de la implementación de los controles de seguridad definidos en el SGSI y en el análisis de riesgos.

Descripción: Designar a un servidor público como responsable de la supervisión de la adecuada implementación de los controles de seguridad de la información definidos en el SGSI y de aquellos resultantes del análisis de riesgos.

Factores Críticos:

El responsable de la seguridad de la información en el Instituto deberá:

1. Asignar a un servidor público que será responsable de supervisar que los responsables de implementar controles de seguridad del SGSI y controles para el manejo de riesgos, lleven a cabo su tarea en tiempo y forma, con apego a la definición del control de seguridad correspondiente.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

2. Comunicar la asignación a todos los involucrados.

El responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

3. Mantener actualizada la información del “Documento de resultados del análisis de riesgos y el programa de implementación del SGSI, incluyendo su avance.

OPEC 2 Establecer los elementos de operación del ERISC.

Descripción: Establecer la operación del ERISC, así como la guía técnica de atención a incidentes.

Factores Críticos:

El responsable de la seguridad de la información en el Instituto deberá:

1. Establecer las reglas de operación del ERISC, en las que se preverán los mecanismos de coordinación del ERISC al interior del Instituto o con otros ERISC u organizaciones externas, en concordancia con la directriz rectora de respuesta a incidentes, incluyendo al menos, los relativos a:

- a) Los canales de comunicación, que deberán ser seguros.
- b) Los relativos a la diseminación de datos de los incidentes.




El ERISC deberá:

2. Elaborar, de acuerdo a lo establecido en 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 en su elaboración al menos los siguientes apartados:

- a) Detección y registro de los incidentes.
- b) Priorización de los incidentes.
- c) Investigación técnica de los incidentes.
- d) Criterios técnicos de contención de los incidentes, de acuerdo a la criticidad de los activos de TIC.
- e) Obtención, preservación y destino de los indicios de los incidentes.
- f) Erradicación de los incidentes.
- g) Recuperación de la operación.
- h) Documentación de las lecciones aprendidas.

3. Establecer el mecanismo de registro de los incidentes de seguridad de la información, que incluya un repositorio para contener los datos de éstos y crear una base de conocimiento.

4. Reportar al responsable de la seguridad de la información, los incidentes de seguridad de la información que se presenten.

 	MAAGTICSI	 INSTITUTO NACIONAL DE GERIATRÍA <small>POR UN ENVEJECIMIENTO SANO Y ACTIVO</small>	Rev. 0
	Subdirección de Administración		Hoja: 56 de 56
	Departamento de Informática		

OPEC 3 Operación del ERISC en la atención de incidentes.

Descripción: Ejecutar las acciones necesarias para atender un incidente de seguridad de la información de acuerdo a la guía técnica elaborada.

Factores Críticos:

El ERISC, en coordinación con el responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

1. Definir las acciones de atención a los incidentes con apoyo de la guía técnica de atención de incidentes, respecto del incidente que se haya presentado.
2. Asegurarse que los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, ejecuten las acciones siguientes:
 - a) Apliquen la solución necesaria.
 - b) Registren los datos del incidente y su solución.
 - c) Comuniquen el incidente y su solución al grupo estratégico de seguridad de la información y a los responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados.
3. Integre los datos del incidente y su solución a los repositorios con los que cuente la UTIC y en su caso, a los repositorios de la Institución que determine el grupo estratégico de seguridad de la información.

Relación de Productos del proceso:

Este proceso utiliza para su operación, consulta y actualización los productos del Proceso de Administración de la Seguridad de la Información (ASI).

Indicador del proceso:

Nombre: Cumplimiento de la administración de riesgos.

Objetivo: Medir la eficiencia de la gestión del proceso.

Descripción: Medir el cumplimiento en la implementación de los controles para la mitigación de riesgos establecidos durante el proceso.

Fórmula: % de eficiencia = (controles implementados en operación de acuerdo a su definición / controles implementados) X 100.

Responsable: El responsable del proceso.

Frecuencia de cálculo: Anual.